NOVAM Whitepaper

Protection | Visibility | Compliance

NOVAM monitors and automatically mitigates threats to IoT devices and provides auditing & compliance investigation for enterprise.

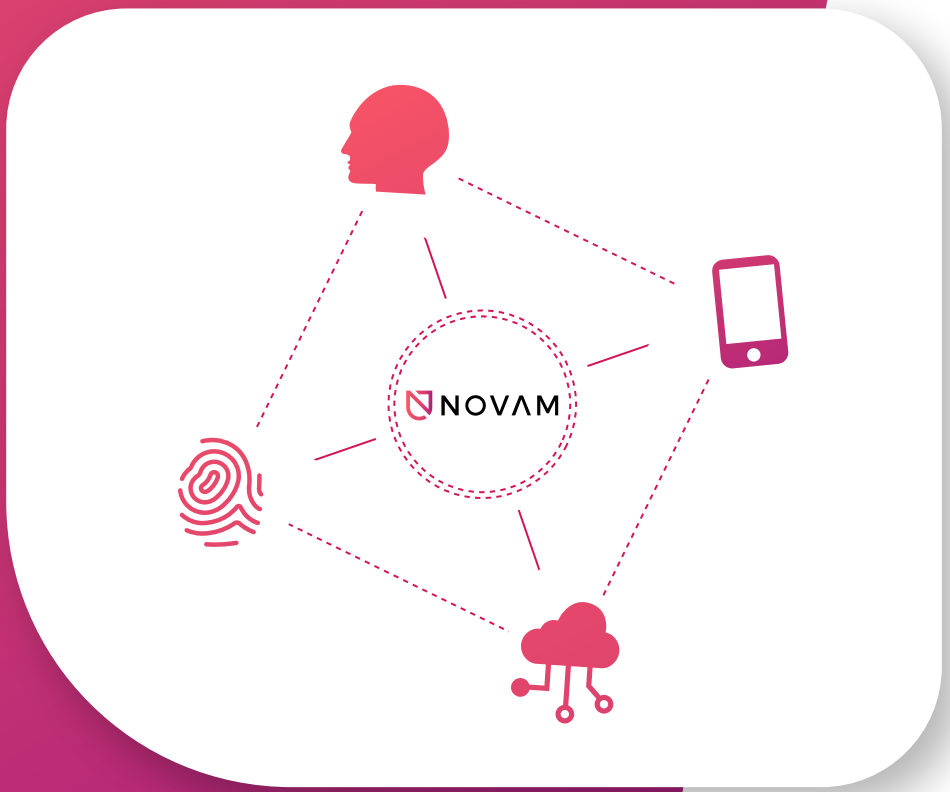


TABLE OF CONTENT

INTRODUCTION

44 PERCENT OF ALL SECURITY INCIDENTS OCCURRED THROUGH THE EXPLOITATION OF MOBILE DEVICES

Followed by Phishing at 42 percent, which further suggest susceptibility to threats due to human error or negligence. Notable compromises also include Employee Error at 37 percent, Social Media and Engineering at 31 percent and Consumer Technology Exploitation (e.g., webcam, home automation, etc.) at 27 percent. [1]

Monitoring of IoT devices: NOVAM secures IoT devices and keeps individuals safe by using Distributed Ledger Technology to help monitor endpoint device threats that target consumers and enterprise.

38 PERCENT OF ALL CYBERSECURITY INCIDENTS IN 2018 WERE DUE TO HUMAN ERROR – UP 13 PERCENT FROM 2017 NUMBERS

According to The Global State of Information Security® Survey 2018, a worldwide study by PwC, CIO and CSO Insights, 38 percent of the more than 9,500 CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT as well as security practices from more than 122 countries sited human error and/or current employees as their most likely source of cybersecurity incidents. [1]

Mitigation of IoT devices: NOVAM mitigates sophisticated cyber attacks aimed at enterprise networks and connected devices, as well as unintentional incidents, by leveraging Distributed Ledger technology to offer businesses and organizations an automated approach to protection.

3 OF THE 5 LARGEST BREACHES EVER IDENTIFIED HAPPENED JUST LAST YEAR

1) DU Caller, China: 2.0 billion exposed records, 2017.
2) River City Media, United States: 1.3 billion exposed records, 2017.
3) NetEase Inc. (dba 163.com), China: 1.2 billion exposed records, 2017. [2]

Auditing and Compliance: NOVAM's Forensic Security Investigation includes proactively identifying and instantly investigating incidents that have the potential to become malicious attacks and/or threats – whether intentional or unintentional.

[1] Base: Singapore - 62 Source: The Global State of Information Security® Survey 2018

[2] 24/7 Wallstreet. https://247wallst.com/technology-3/2018/05/08/worlds-10-largest-10-breaches-in-2018-q1/

PROTECT YOUR ENTIRE BODY OF WORK WITH TECHNOLOGY THAT BEHAVES LIKE AN IMMUNE SYSTEM

Because people and organizations can't continue to go unprotected against cyberattacks – and living in a bubble is not an option, NOVAM draws its inspiration from the innate resilience and purging that the human immune system uses to eliminate threats and ensure health.

NOVAM monitors entire networks, infrastructures and end points to establish full seamless views of global communications and threats. Unless NOVAM was implemented from inception, we assume users, devices and networks have already been compromised – and initiate tailored action plans immediately. Whether you're a blue chip, a startup on the rise or somewhere in between, NOVAM is the immune system no business should live without.

NOVAM IS ALWAYS IN ACTION

NOVAM protects endpoints and networks by monitoring and mitigating threats automatically on global Internet of Things (IoT) devices. We also offer security teams and corporate risk management departments a forensic security investigation platform for auditing and compliance via Distributed Ledger Technology (DLT).

NOVAM operates at the bootloader level connecting IoT devices to the blockchain to insure through the hash that the operating system and hardware is uncompromised.

NOVAM's machine learning, probabilistic mathematics, patent-pending tactics and methods can enable action without prior knowledge of the threat. Proactively, NOVAM is designed to identify, monitor, alert and in some cases initiate an immune system response that automatically mitigates, removes, replaces or quarantines the threat.

NOVAM's focus: Hardware vendors, software vendors and cybersecurity products.
The NOVAM Token is a utility software license that provides access to our network and platform for services that include monitoring and mitigating threats, auditing and regulatory compliance.

NOVAM technology allows for system health checks for user, device and network authentication and verification purposes.

WHEN YOU THINK NOVAM, THINK BIOMIMICRY

Many of man's limitations have been overcome by imitating the models, systems and elements of nature to solve complex human problems – or biomimicry.

NOVAM leverages biomimicry concepts by marrying artificial intelligence and distributed ledger technology to mimic the human immune system.

Why? Because much like the human body, businesses, organizations and people are constantly under attack, whether they know it or not.

Fortunately, just as the human immune system acts as the body's own army, shield and counterattack against a constant stream of possible infections and toxins, NOVAM fights to protect clients against cybercrime and breaches.

Immunity in tech-terms. Let's talk autonomous threat migration. A baseline of the system is taken. Anything that the system deems out of this baseline is flagged for investigation. Abnormalities and threats are then recorded on a DLT system to ensure each threat is investigated. Once on the DLT the organization has an immutable hash incident record for audits, regulatory compliance and forensics.

MITIGATING EXTERNAL THREATS IS NOT ENOUGH

Clearswift Insider Threat Index[1], acknowledges that 74% of security incidents come from the extended enterprise, not hacking groups. Insider threats are creating new challenges to enterprise, and often blindsiding security departments as they fight to protect intellectual property, R&D, HR records, financials and other sensitive data.

NOVAM'S 2018 WHITEPAPER COVERS:

- NOVAM's approach to monitoring threats through device health check systems.
- NOVAM's process to mitigate threats through its Immune System and autonomous threat mitigation.
- How NOVAM provides audit and regulatory compliance with DLT.

[1] Clearswift Insider Threat Index (CITI) http://pages.clearswift.com/rs/591-QHZ-135/images/Clearswift_Insider_Threat_Index_2015_US.pdf

COMPANY BACKGROUND

Inteligus Solutions built a successful business by providing identity and access management solutions in the digital security and surveillance industry. IS also specializes in custom-fit security solutions, identity management, and access control systems for original equipment manufacturers (OEM). Ian Perschke, Adam Perschke and Brooks McMillin are the founders of Inteligus Solutions.

The above founders recognized an opportunity to merge distributed cybersecurity, artificial intelligence and distributed ledger technology to create a company whose mission is to secure and protect entire networks, infrastructures and all endpoints with an automated technology modeled after the human immune system.

Seasoned security experts, our team has extensive experience with physical location and data security, big data aggregation, global networking, enterprise software development and government system architecture in the digital security and surveillance industry.

Deep relationships with industry experts include a leading Hewlett Packard Enterprise (HPE) OEM[2] and Dell EMC OEM[3] partner in enterprise-level storage, networking and video surveillance. Installed worldwide, our associates have over 50,000 purpose-built video surveillance systems[4] and storage networks in 52 countries. Organizations include multi-government embassies, hospitals, correctional facilities, airports, stadiums, cruise lines, universities and retail chains.

A compelling opportunity has presented itself. Over the past few years, building custom applications, software and identity management solutions has given us a rare view and coveted opportunity to analyze the digital security and surveillance space, IoT, blockchain, enterprise systems and other emerging technologies.

Our conclusion is that though there are many emerging technologies, innovative trusted hardware and standards, no one has created an enterprise-ready solution designed to assist identity management, verification, cyber controls and self-healing systems that automatically counteracts cyber threats, while assisting security teams. We see an exceptional opportunity in our distributed cybersecurity, and distributed ledger technology hybrid.

[2] HPE OEM. https://www.hpe.com/h22228/video-gallery/us/en/sss/solutions/solutions-general/1C2C522C-1979-4273-920B-9E5140E8AE8C/bcdvideoandhpeoempartneringforvideosurveillancesolutions/video/

[3] Dell EMC OEM. https://www.securitysales.com/surveillance/bcdvideo-inks-oem-agreement-with-dell-emc/

[4] Underdog NYC. https://underdog.nyc/jeff-burgess

ANALYSIS

The truth doesn't have to hurt. As technology continues to be all-encompassing, threats and anomalies are more ubiquitous than ever. Malicious attacks can come from anywhere, at any time from people and/or machines. The chances of someone or something discovering vulnerabilities, stealing private data and doing damage to organizations and individuals are higher than ever. Exploiting known vulnerabilities, social engineering, and using data to cause damage to reputations, finances and operations has become an industry of its own rife with methodical experts.

The International Data Corporation (IDC) forecasts our global datasphere will encompass 163 Zettabytes by 2025[5]. And that's only the beginning as projections for scale, profit and innovation across most industries are based on an increasingly connected and data-driven world.

The best most authorities can do is watch the news briefs with the rest of us as millions of sensitive records containing personal identifiable information continue to be stolen.

By compromising a vulnerable point of entry into a company or third-party vendor, a malicious attack is over and done – often before discovered. Domestic or global, security trends indicate that threats and attacks are getting harder to detect, especially as enterprise networks and organizations scale.

The increased complexity of connectivity and communication global offices bring, cloud and virtual networks inherit, and the policies physical data centers and bring-your-own-device (BYOD) have baked-in all have amplified the exposure to threats organizations face twenty-four-seven.

The legacy approach utilizes security layers for cyber products, which doesn't allow for communication, seamless updates and limits the views needed to assess the threat landscape.

Internal and external threats are capable of adapting and growing with the digital landscape as new technologies develop. As companies and networks evolve, so must the tasks and responsibilities of IT teams. Many IT professionals are charged with finding and mitigating attacks and anomalies manually. Unfortunately, with more human interaction comes a higher chance of human error.

Plus, as attacks become more intelligent, our network security must match the wit of malware. Without automation it could take thousands of man hours, countless IT professionals, and millions of dollars – and still fail to protect companies from a state of paralysis.

[5] Seagate, Data Age 2025. https://www.seagate.com/files/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf

VISION

COUNTLESS COMPROMISED. BILLIONS BREACHED. ONE SOLUTION.

NOVAM is the first Artificial Intelligence driven cybersecurity program utilizing DLT to increase the accuracy of its health check. Using machine learning and probabilistic mathematics, we plan to offer a security system that is ever-alert, always present and device agnostic.

An immune system designed to protect endpoints and networks by monitoring and mitigating threats automatically on global Internet of Things (IoT) devices, NOVAM not only finds anomalies but also fixes them to boost your tech-immunity system.

As the digital evolution forces us to rethink what we know about cyber security, and shifts in digital landscape continue to expose us to new threats, NOVAM protects businesses, organizations and people with a self-healing platform that's designed to increase tolerance as needed.

NOVAM uses distributed ledger technology and AI to automatically monitor and mitigate IoT threats from the secure boot chain, operating system, mobile application and network.

NOVAM also provides auditing & regulatory compliance integration to threat monitoring and detection services to ensure system events are included on an immutable distributed ledger. NOVAM wants to become the standard distributed ledger for cybersecurity threat detection, device mitigation and compliance.

Our focus is on threat detection and analytics for companies that have customers and want the assurance of an immutable record for auditing, compliance, and investigation needs.

A NOVAM Token is used as an individual software license to access the distributed ledger capabilities, including but not limited to services of monitoring, mitigation, auditing and compliance.

NOVAM intends to target major industries by creating partnerships with security vendors for immutable compliance and investigation. NOVAM will also target hardware and software vendors to integrate the distributed ledger within IoT devices and enterprise networks for monitoring and mitigation services through our patent-pending system health check.

Our market focus breaks down into three distinct categories:

- Monitoring IoT devices and systems
- Threat mitigation of IoT devices and systems
- Auditing and compliance for threat monitoring platforms

TARGET MARKET FOCUS

Due to the nature of our solutions, we can focus on markets in all industries using IoT devices now and in the future. Below is a list of general market focus with layers of integration from fortune 500 organizations to OEMs and cybersecurity firms.

- **Hardware Manufacturers** - Root of Trust, TEEChip, OEMs
- **Software Firms** - Operating Systems, Firmware, Applications
- **Cybersecurity** - Enterprise & consumer protection, endpoint protection & response, Threat intelligence platforms
- **Fortune 500** - Direct integration into security operations center
- **eCommerce / Digital Payments** - Web/Mobile/Retail payment methods

REVENUE STREAMS

We will approach the market in a collaborative and agnostic way to integrate in each category by:

- **White Label / OEM** - Companies pay NOVAM to license and rebrand NOVAM's IP. This includes paying for custom functionality within a system.
- **Channel Partner** - NOVAM receives % of transaction fee for being a channel partner.

NOVAM'S PLATFORM AND TECHNICAL OVERVIEW

PROBABILISTIC MATHEMATICS

Most traditional information security approaches are inflexible, generic and often presented as pre-defined rules based on best practices. Rule-based systems serve as fixed instructions a computer may follow for "if-then" action statements.

NOVAM takes a progressive approach based on probabilistic mathematics. This increases the understanding of nuanced data and interactions.

While a simple "yes or no", or "true or false" alone is not the best way to generate accurate results, probabilistic mathematics indicates degrees of accuracy and understanding in a diverse enterprise environment with large scale data and system interactions.

NOVAM leverages the probabilistic mathematics approach to understand environments, information flow and the ability to detect subtle changes – all without being told what to look for.

SUPERVISED MACHINE LEARNING

Supervised machine learning is an approach that maps an input to an output based on example input-output pairs. Traditionally, it allows sanitized training data to be fed into a system to determine an outcome. In the context of information security, an antivirus can recognize 'known' malicious threats that have been previously-seen, properly labeled, and uploaded to a database for future cross-reference.

The disadvantages of supervised machine learning in information security:

- Malicious behavior that changes shape may become unrecognizable by signature and can compromise a system
- Improperly labeled data prevents a system from accurately classifying malicious behavior, seriously compromising a system and increasing exposure to undetected threats
- Labeling the training data manually increases time and costs

UNSUPERVISED MACHINE LEARNING

Unsupervised machine learning is unique since it draws inferences from unlabeled data and determines previously undefined or unrecognized patterns and relationships. The advantage of unsupervised learning is the discovery of unknown behaviors, without prior knowledge, which aids human security investigators in their hunt for threats.

NOVAM strives to develop and deploy a precise unsupervised machine learning suite, to analyze global network data and endpoints at scale, embrace the unknown and protect.

Without the familiarity of past threats, NOVAM empowers autonomous classifications of system normality to recognize current cyber-attacks. New behaviors that fluctuate may indicate threats, compromise, identification needs, investigation or isolation.

The impact of NOVAM's unsupervised learning on cyber security is imperative:

- Insider threats, which would otherwise go undetected, can be identified, investigated and thwarted.
- Total network visibility and superior detection levels ensure networks have internal defense mechanisms capable of combat against new-age threats.
- Autonomous responses enable faster cyber-threat protection and human analysis.

RANKING THREAT

NOVAM's probabilistic unsupervised learning approach to network security is influenced by Bayesian framework. This approach facilitates the understanding of important information within a noisy network, combines weak indicators of potential abnormal behavior on the network and produces a clear ranking of malicious or non-malicious activities. A "trust but verify" philosophy, subsequent actions are then taken.

All data is not created equal, which can create an uncertain understanding of data. Manual efforts increase unreliability. NOVAM's mathematical approach establishes network normality, identifies subtleties in data, and distinguishes degrees of potential compromise. From start to finish, the appropriate action is taken autonomously. Our method enables ranking of various characteristic measurements allowing for maximized network visibility and threat analysis, without requiring a rule-based approach.

Measurements include, but may not be limited to:

- Credential user
- Data volumes
- DNS requests
- Server access
- Time of events

Each measure of network behavior is then monitored in real time to detect abnormalities.

As we scale and more businesses and organizations are on-boarded, the data feed into the NOVAM Network will allow others to benefit from NOVAM's proactive approach to global security.

CLUSTERING

Modeling devices is important to build a 'normalized' view of behaviors throughout the network. Clustering with unsupervised learning enables an algorithmic relationship grouping that identifies similar devices and interactions happening on the network. Numerous clustering techniques can be employed to inform the modeling and measurements. Each cluster technique defines specific methods of measurements and weights.

NETWORK TOPOGRAPHY

Networks are complex interconnected virtual webs of devices that can be challenging to monitor, maintain and protect. Network topography is expanding rapidly with new devices, users and geographic regions coming online every day. Recognizing the nuances in communication and interactions can become daunting.

To address the increased difficulty in identifying malicious and benign actions, NOVAM employs various mathematical techniques designed to model an all-inclusive understanding of a network's topography. This tactic enables us to detect and prevent threats from causing extensive harm.

OFFLINE FUNCTIONALITY

Note that if a NOVAM node (or subset of NOVAM nodes) gets disconnected from the main NOVAM Network, transactions can still be created and submitted. If there is no full node that can help check and mitigate their risks, the transactions will still exist in an offline DAG until they can be connected to the main NOVAM Network.

However, if there is a full node that is trusted to take care of the security issues being presented, the whole NOVAM process can still take place and these transactions will be added to the main DAG when any node is re-connected to the NOVAM Network.

BOOTLOADER AND CLIENT FUNCTIONS

Every node on the NOVAM Network must have a version of the NOVAM client installed. This client, even without the network connection, offers increased security to the device.

Software is written into the bootloaders of client devices to enable a connection to the NOVAM network before the OS loads. This process involves checking the internal hashes to confirm that device hardware and software has not been compromised.

Major features are below:

Health Check: The NOVAM client comes with the ability to run a health check built into the core functionality. By default, this feature automatically checks the security settings of the NOVAM node before saving the results to a file. This file can be uploaded to a custom CDN right away, or in the case of not being connected to the network, can be queued to be uploaded in the future.

Automatic Remediation: Some of the vulnerabilities caught by a health check can be fixed automatically. These corrections will be carried out as soon as the vulnerability is found, as long as the node has a license token to cover the security fix and a network connection to post the transaction.

An update stating which automatic fixes were deployed will be posted to the NOVAM Network once available. This allows vendors and other analysts to note any issues that may compromise their network.

NOVAM's automatic remediation function will leverage firmware and software provided by clients, businesses and organizations to insure complete and correct updates.

TOKEN USE SOFTWARE LICENSE

A token utilized within the distributed ledger network can contain all or one of the following licenses, including:

- Accessing the network
- Taking advantage of the transaction types
- Client functions
- Security
- Additional technology assistance through whitepapers

Coupling our software license with the NOVAM token provides additional benefits for democratizing the purchase of a software license. In addition, it reduces costs associated with negotiating bulk prices, paying for licenses, and company time to initiate.

SECURITY

Every message sent through NOVAM is digitally signed with the private key of the NOVAM node. All internode traffic is encrypted with TLS. This ensures that eavesdroppers cannot intercept the message – plus, guarantees that every message is from the address that claims to have sent it.

NOVAM nodes are identified with an IP address and port number. This mitigates DNS attacks.

PRIVACY

Using the NOVAM protocol to update system security, where vulnerabilities are published to the NOVAM Network can be a malicious user's paradise.

For greater safety and security information can be sent through private, encrypted channels. The security provider can then use the NOVAM protocol to update the vulnerable node's security.

With NOVAM, every time a transaction is sent from an address, part of the private key is shared. If addresses are reused to send multiple transactions, there could be a security risk. Note: Receiving multiple transactions to the same address has no security risk.

To mitigate risk, and to increase the difficulty for malicious actors looking to learn critical information about a specific system, each transaction has a client's unique ID included in the transaction.

This approach enables vendors and trusted security providers to know which machine is being talked to serviced or addressed, while other observers are unable to identify which machine is vulnerable.

NOVAM'S APPROACH: THE NEW ERA IN AUTOMATION

Cybercrime is anything but new. And as it's an increasingly fertile industry, today's cybercriminals have become as seasoned, savvy and as professional as the businesses and organizations they attack – if not more so.

This advanced level of cybercrime calls for a fresh perspective with greater interest in the multifaceted nature of security breaches, malicious cyber threats and attacks. Now more than ever, an out-of-the-box product, service or solution is needed.

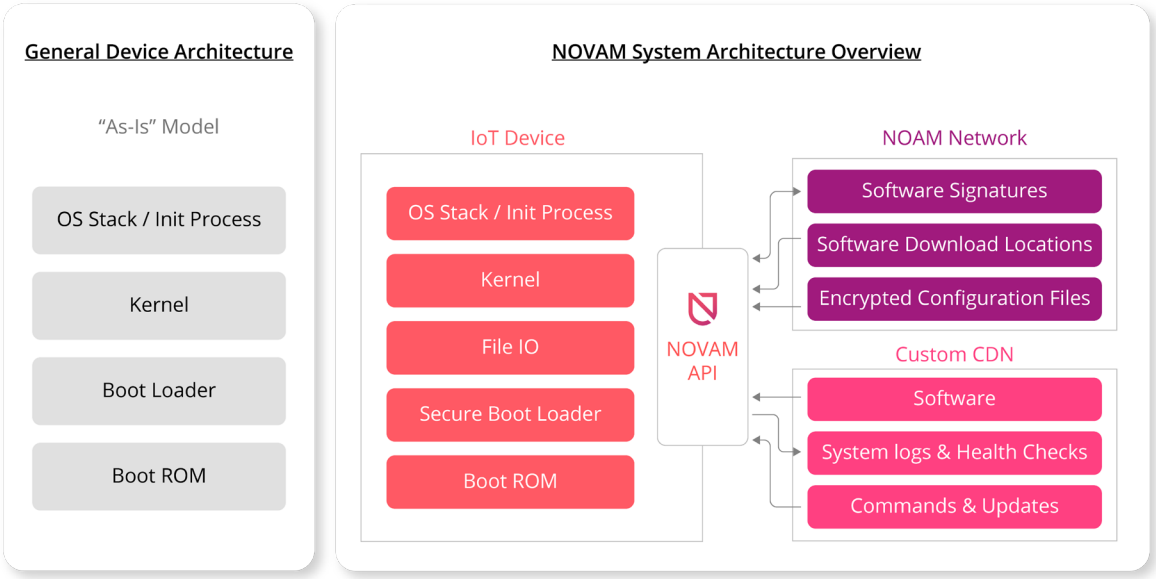
FUTURE FORWARD MEANS BACK TO BIOMIMICRY

Based on NOVAM's premise that many of man's limitations have been overcome by imitating the models, systems and elements of nature to solve complex human problems – or biomimicry, NOVAM combines distributed cybersecurity, artificial intelligence and distributed ledger technology for a system that's designed to be proactive, behaving like the human body's immune system.

NOVAM's complex protection mechanism – or approach provides resistance and removal of threats without prior knowledge of the existing danger. This by nature makes NOVAM an emerging, disruptive technology that's optimized by its innate ability to automatically initiate an immune system-like response that mitigates, removes, replaces or quarantines threats.

SYSTEM HEALTH CHECK

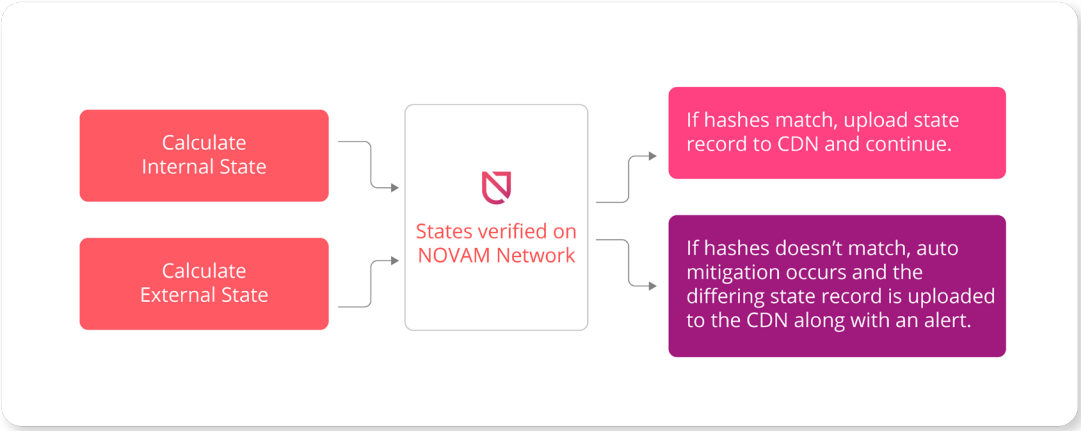
NOVAM's health checks enable users, devices and applications to verify that software packages and hardware components are uncompromised and unmodified by malware or other cyberthreats, across the entire secure boot chain on a device. The current "as-is" model represents general IoT device architecture which can be easily compromised due to a lack of a secure boot process. NOVAM's system architecture will enable an IoT device to boot up and run securely.



If any software associated to boot chain is discovered to be compromised, the health check system can autonomously activate a full or bundled secure software update to mitigate attacks without interaction from an individual or organization.

The health check system ensures connected devices are protected and auto-mitigate themselves against known and unknown threats, allowing both personal and corporate information to remain safe and uncompromised.

The health check system will then calculate internal and external states of a device then compare it to the NOVAM Network. Once the state(s) have been verified, NOVAM will continue to run processes or autonomously mitigate a compromised device.



THE IMMUNE SYSTEM

Rapid cyber-threat detection and attestation in an enterprise is critical to the health of the network and protection of sensitive data. Instead of pre-defining what a bad actor and malicious behavior looks like, we aim to build an embryonic, self-adaptive, model of "normal" activity and behaviors to detect and prevent against abnormalities.

Many existing security vendors have clouds where information about threats is fed in. Although optional, if all the individual systems are learning independently on the customer network, an AI should take advantage of information from other AI systems in the marketplace.

The immune system builds thorough network "vital sign" models of every user, device and network communication, ensuring total network immersion and understanding of "self".

Using machine learning, the immune system is modeled after "self or state" of a device to establish normalized actions and pair signature-less static prevention with behavior detection. Endpoint and network activity is monitored to detect malicious behavior perpetrated by any type of threat, from advanced malware, to exploits and insider threats.

IMMUNE SYSTEM CAPABILITIES

THREAT DETECTION & CLASSIFICATION

NOVAM's approach to network and endpoint information security is powered by advanced machine learning algorithms, unsupervised learning and autonomous, self-learning defense mechanisms.

The understanding of an organization's rapidly evolving network activity and individual device behavior is critical to assist enterprise security analysts in detecting, investigating and mitigating threats in a noisy network environment.

Our algorithmic approach aims to filter out false-positive threat indicators, identify and alert security analysts and executives of critical perceived threat.

Key features include:

- Robust: Evolves with your organization and systems environment
- Self-learning: Understands normal user, device and network behavior
- Probabilistic: Ranks probability of intrusion and threat
- Real-time: Extracts emerging threats
- Data agnostic: Identifies, analyzes and extracts all data
- Relationship Correlation: Models user, device and network behavior
- Attestation: Executes threat analysis, mitigation, remediation and forensics

The mathematical algorithmic approach aims to filter out false-positive threat indicators, identify and alert security analysts and executives of critical perceived threat. Threats are automatically classified according to risk measurements and security teams will have the ability to assess threats based on the organization's incident response plan, corporate policies and regulatory compliance.

AUTONOMOUS RESPONSE

As the human body's immune system intuitively recognizes and defends itself against threats, NOVAM's Immune System Defense aims to detect, filter, investigate and respond to threats in real-time, providing vital resource assistance to security investigators.

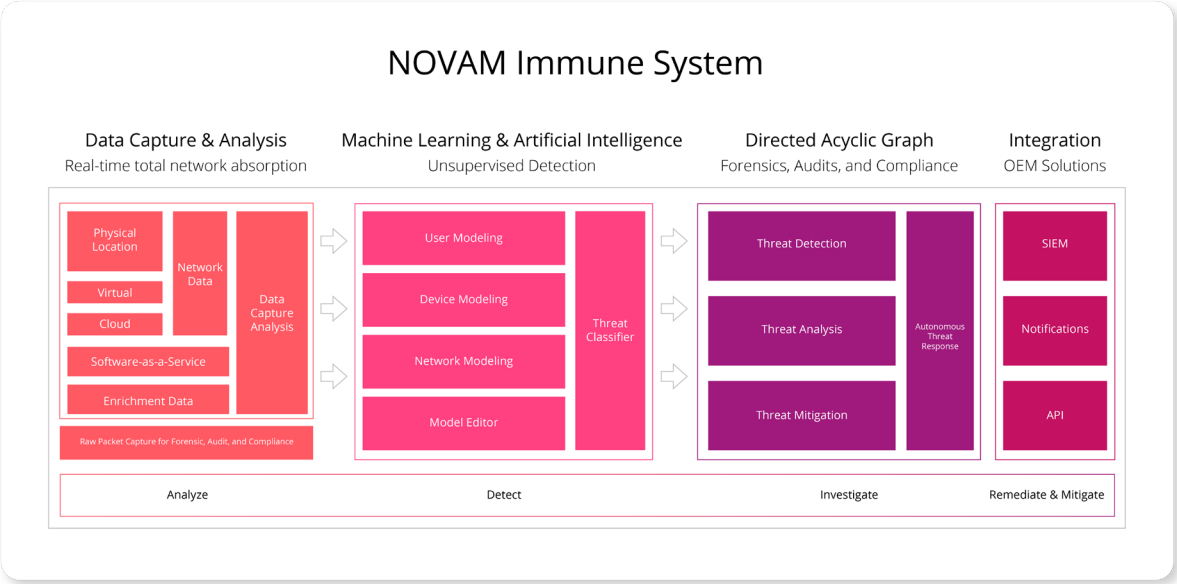
Our algorithmic response allows us to automatically detect and filter cyber-threats. This enables us to determine threat importance by weights and scale, providing analytical foresight.

It can only take several minutes for malicious malware or ransomware to cause crisis in a global network, infecting thousands of devices, compromising credential holders, encrypting data, shutting out administrators or causing harm and disruption to systems outside of the network.

NOVAM's Immune System Defense applies unsupervised learning, mathematical approaches and autonomous reaction aims to respond quickly to different cyber-attacks. NOVAM immobilizes, removes and/or slows down threats to prevent network-wide disarray. Security teams will have more time to investigate dangerous cyber-threats as they emerge. This results in user, device and network uptime, and a decline of financial, operational and reputational damage.

The Immune System Defense can provide the following:

- Immunizes specific perceived threats
- Quarantines or semi-quarantine users, devices and system files
- Identifies content for additional investigation, tracking and forensics
- Rolls back files that have been manipulated



NOVAM can defend all network endpoints against every type of attack, at every stage in the threat lifecycle:

- Complete visibility into all endpoint activity with minimal impact on performance
- Dynamic behavior analysis to detect threats across all major vectors
- Autonomous threat mitigation and remediation

NOVAM'S 5 STEP PROCESS DEVICE HEALTH CHECKS IS AS FOLLOWS:

1. Initiate a health check for a device. This can occur both in the boot process and during runtime, and include the entire Chain of Trust or an individual statistic like firmware, operating system or applications.
2. The state of a device is recorded on an enterprise specific CDN. This can be used as an external element for future device health checks.
3. Subsequent health checks compare the internal and external state of a device with NOVAM stored internal and external states, signed by the vendor, to determine if the device is healthy or compromised.
4. When a device is considered healthy and unmodified no mitigation occurs.
5. If the device is considered unhealthy and compromised, based on the system health check, autonomous mitigation will occur.

Should future authorized updates be required for devices to be fully up-to-date with critical patches or functionalities, NOVAM's team will work directly with manufacturers and developers to ensure the update is recorded and updated automatically and accurately on all devices. Also, API access will enable manufacturers and developers to manage their products and services to ensure compliance, audit, and investigation.

SYSTEM SECURITY

System security is designed to protect both software and hardware, which enables all devices and codes to act in unison across every core component while participating in the network. This includes boot-up process, software updates on various levels and Secure Enclave hardware. This architecture is central to mitigating threats and securing sensitive data in the digital age.

The purpose-built integration of hardware, software, and services ensure that each component of the system is trusted and that the system can be validated as a whole. From initial boot-up to software updates to applications, each stage is analyzed securely to ensure that hardware and software are protected.

The NOVAM Network includes a secure boot chain, chain of trust, a root of trust verification and user and device authentication health checks to ensure devices are enforced properly.

SECURE BOOT CHAIN

Each step of the initiation process of a device during a secure boot chain contains components that are cryptographically signed by an authority to ensure integrity verification. This can include bootloaders, kernel, kernel extensions, and firmware. The secure boot chain helps ensure that even the lowest levels of software aren't tampered with.

When a device is turned on, it's application processor immediately executes code from read-only memory, or the "Boot ROM". This is known as the hardware root of trust in some devices.

A Certificate Authority (CA) public key is generated and verified with the private key from the trusted authority. This is the first step of the chain of trust where each step ensures the next is signed and verified by the authority. The chain of trust continues with each system and subsystem, verifying each process.

The chain of trust is essential for digital verification of a device. A secure boot chain can include digital signatures of Boot ROM, low level boot loaders, firmware, kernel, operating system, hardware, and applications. This ensures all software running on a device, from boot, is valid and secure.

A chain of trust can be used for authentication of mobile payments, private keys, crypto node validators, access control systems and cryptocurrency wallets.

Cyber assaults often come in the form of attack vectors to a typical chain of trust, like forged signatures and certificates, via side channel attacks and other methods.

Using the NOVAM Network allows each element of the chain of trust and secure boot chain to be recorded with a healthy hash upon manufacturing, activation or power-on of a device.

The NOVAM Network will provide a system health check to verify the chain of trust has not been tampered with from its previous healthy hash on record. If a device has been recorded as modified, the NOVAM Network can assist authorities in the reinstallation of full or bundled software packages to mitigate threat.

SYSTEM SOFTWARE AUTHORIZATION

Device manufacturers release software updates to address emerging security concerns, while providing new functionality. Software is typically delivered wirelessly with an Over The Air (OTA) update to single or multiple devices simultaneously.

During system updates connected devices from different manufacturers use a process called System Software Authorization to prevent devices from being downgraded to an older version. If devices are capable of downgrading software, previous vulnerabilities can be introduced and exploited.

A Secure Enclave can utilize a System Software Authorization to ensure the integrity of its software and prevent downgrade installations (Refer to Secure Enclave for more information). OTA software updates can be downloaded in a full copy or the minimal individual components required to mitigate threat.

During an OTA software update a device will connect to an authority installation authorization server (IAS) and digital signatures and key pairs can be measured for each part of the installation bundle. For example: The operating system, kernel, bootloader, application, a random anti-replay value (nonce), and specific device information.

The authorization server checks the list of measurements against the device to determine installation instructions, policies and versions. The server passes signed encrypted data to the device for an update. The chain of trust verifies that the signature came from a trusted authority and measurements are validated, and a software update commences.

Use of the NOVAM Network ensures immutable data integrity throughout the entire chain of trust, installation server communication and component measurements, which allows for true authenticated trust with autonomous mitigation.

SECURE ENCLAVE

Trusted Execution Environments (TEE) and Secure Enclaves are isolated hardware chips executing separate firmware from the core operating system of a device ensuring data, policies and procedures are secure and uncompromising to personal information. Secure Enclaves guarantee code and data loaded inside it are protected with respect to confidentiality and integrity.

There are multiple ways in which Secure Enclaves can execute secure isolated protection including, but not limited to:

- Storing private keys
- Secure messaging on a device
- Monetary transactions
- Software updates
- Device policies
- Device procedures
- Biometrics
- Multi-factor authentication of ‘self’
- System health verification in a secure environment

Biometrics are playing a greater role in the secure identity marketplace. Enterprise access control systems and consumer devices, including unlocking devices, files and authenticating individuals have secured a space for this technology.

HARDWARE SECURITY MODULE

Hardware Security Modules (HSM) are specialized tamper-resistant hardware chips.

HSM are employed to safeguard and manage digital keys, key exchange and encryption for strong authentication. Cryptographic processing is also provided. CloudHSM is used for cloud-based key management which can include software or web-based certifications.

The use of HSM combined with the NOVAM Network and security system enables protection against using insecure private keys, seeds and certificates. This approach enforces data security governance, comprehensive control over encryption keys, integration of applications and storage services. This is done through APIs and management of a key lifecycle from creation to destruction.

NOVAM ensures that blockchain nodes, private keys and authority certificates can be protected against threats, regardless of when they are taking place in the threat landscape.

ENCRYPTION & DATA PROTECTION

Encryption and data protection architecture and design serves to protect user data if an unauthorized party attempts to use or modify a device. The secure boot chain, code signing and runtime process security all help to ensure that only trusted code, apps and transactions can execute on a device.

Additional encryption, use of a trusted hardware environment and data protection features help safeguard user data, even in cases where other parts of the security infrastructure have been compromised – for example, a device with unauthorized modifications. This provides important benefits for both users and IT administrators charged with protecting personal and corporate information.

TWO-FACTOR AUTHENTICATION

Two-factor authentication (2FA) is an extra layer of security for mobile, desktop and application access. True to its name, 2FA uses two pieces of information for verification purposes.

This design ensures that only the account's owner can access the account, even if someone else knows the password. With 2FA, a user's account can be accessed only on trusted devices. Most 2FA is verified on a non-secure operating system, whether phone or computer, and provides ample access to online accounts, applications, and critical systems by malware-infected devices.

Because a password alone is no longer enough to secure a user's account, two-factor authentication improves the security of the user's account and all the personal information they store with the service or device.

Examples of 2FA scenarios include:

- Using Google Authenticator for online and office account access
- SMS messages or emails sent to a user's trusted device with a one-time code to access an account, system or verify suspicious activity
- Mobile and ecommerce payment authorization

Another variation of 2FA is universal two-factor authentication (U2F). U2F is a new universal standard for creating physical authentication tokens.
These tokens can use USB, NFC, or Bluetooth to provide two-factor authentication across a variety of services, while over encrypted communication channels and can also incorporate multi-factor authentication with biometrics.

MULTI-FACTOR AUTHENTICATION

Multi-factor authentication is one of the most secure methods of ensuring unauthorized access to devices, networks and buildings. Couple MFA with trusted hardware in an isolated environment of a device and your security increases exponentially.

Multi-factor authentication works by verifying a user's claimed identity in which a user is granted access only after successfully presenting two or more pieces of evidence or factors to an authentication mechanism:

- Knowledge or something they and only they know
- Possession or something they and only they have
- Inherence or something they and only they are

Examples of MFA scenarios include:

- Swiping a card and entering a PIN
- Logging into a website and being requested to enter an additional one-time password (OTP) that the website's authentication server sends to the requester's phone or email address
- Downloading a VPN client with a valid digital certificate and logging into the VPN before being granted access to a network
- Swiping a card, scanning a fingerprint and answering a security question
- Attaching a USB hardware token to a desktop that generates a one-time passcode and using the one-time passcode to log into a VPN client

APPLICATION SECURITY

Apps are among the most critical components of the present mobile and enterprise security architecture. While applications provide amazing productivity benefits for users, they also have the potential to negatively impact system security, stability, and user data if they're not handled properly.

NOVAM provides layers of protection to ensure that apps are signed and verified using our novel health check solution with trusted hardware. These elements provide a stable, secure platform for apps, protecting user data, application verification and malware-protection.

If capable malware infects an application, a health check will verify the malware, record the infection to the NOVAM Network, and can automatically reinstall a previous device state of the application to an uncompromised, unmodified version.

APP CODE SIGNING

Mobile phone operating systems (OS), like Apple's iOS and Google's Android, provide basic levels of code signing in attempt to ensure that apps come from a known and approved source and haven't been tampered with. Jailbreaking an iPhone or using the more open Android OS has been known to allow malware-infected mobile apps onto phones, compromising credentials and exposing sensitive information.

IT departments and employees have similar circumstances – installing open-source or other applications to critical company infrastructure and unintentionally installing malware software made to look like an approved app.

Sometimes, organizations also write in-house apps for use within their organization, employees and third-party partners. This exposes internal systems to greater security risk.

The NOVAM Network ensures that applications can be verified on any system, for application developer's benefit and corporate security policies and procedures.

By utilizing embedded frameworks, APIs and developer tools, applications can be protected by unaltered verifiable proof of hash and health checks. At runtime, code signature checks of all executable memory are applied to ensure that an app hasn't been modified since it was installed or last updated.

DATA PROTECTION IN APPS

To be developed and available for integrations in the future, NOVAM's Software Development Kit (SDK) will offer a suite of APIs designed to make it easier for third-party and in-house developers to adopt data protection – plus, ensure the highest level of protection in their apps.

Data protection will be available for health checks on installed apps, ecommerce payments, 2FA, MFA and U2F verification and can enable autonomous mitigation of infected apps, operating systems or the boot process.

Client Approaches and Transaction Types:
There are multiple types of transactions that can be sent on the NOVAM Network. Although they have different functionalities, all transactions share a similar format.

Every transaction has five basic elements:

- The recipient address: What node the transaction is being sent to
- The digital signature: Verifies the nodes identity
- The value: Number of tokens being sent
- The transaction type
- The message

TRANSFERRING NOVAM TOKENS

The basic transaction is sending NOVAM Tokens from one address to another address. This process is basic transfer of currency.

Health Check Update

Whenever a client node runs a health check, the results can be uploaded to the CDN. These health checks allow vendors or trusted security providers to identify the security of the devices they are responsible for. Device security is then confirmed, or actions to fix or update the device are enabled.

Some devices may have more security concerns. And some vulnerabilities may be less than ideal for posting publicly. These issues and concerns are addressed by posting vulnerabilities so that they are private communications between the client and vendor, or trusted security provider. With these communications, updates can be posted, and the security status of the client can be publicly confirmed.

Health Check Response

When a vendor or trusted security provider is notified that a device health check doesn't match the previous health check, they can work on restore the client to its previous, secure state.

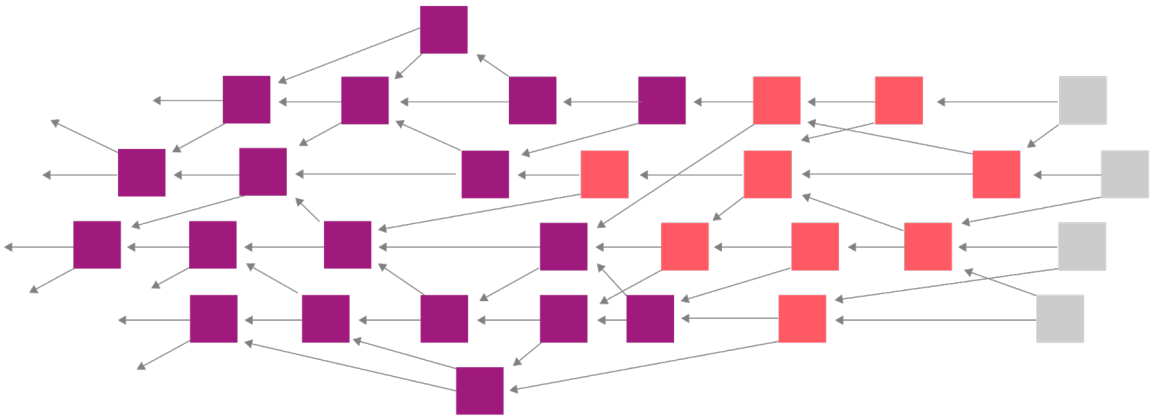
Firmware Update

When a vendor or trusted security provider needs to update the firmware on one or more devices, a Firmware Update command can be sent. This action takes the firmware that has been already verified from a health check on another NOVAM client and initiates the process to transfer the firmware update to all the devices that are not up to date or have been compromised.

NOVAM'S APPROACH: DIRECTED ACYCLIC GRAPH (DAG) ARCHITECTURE

DAG INTRO

A Directed Acyclic Graph (DAG) is a data structure that is topologically sorted in chronological order. Although a distributed ledger, like blockchain technology, DAGs do not incorporate blocks or blockchains. Instead of a global blockchain, DAG transactions are linked from one to another. This works by requiring nodes that wish to submit new transactions to verify multiple existing transactions before they can publish one of their own to the network. This process increases efficiency, lowers latency, and enables greater scale for the solution.



DAG VS BLOCKCHAIN

On blockchain networks, such as Bitcoin and Ethereum, transactions are mined into blocks which point to the previous block, creating a chain of blocks. This maintains order. It's common for two miners to create a new block at the same time. In such a scenario one block will have to be orphaned, meaning the power (both processing and electrical) used to validate those transactions goes to waste.

DAGs replace a standard block with a single transaction. This makes it so that every transaction is directly involved in maintaining the sequence.
Multiple transactions can be created simultaneously which contributes to the stability of the network, rather than being discarded. This also eliminates the need for mining, making the overall network more efficient.

SOME OF THE MAJOR BENEFITS OF USING DAG OVER BLOCKCHAIN ARE AS FOLLOWS:

Unlimited Scalability

If there are too many transactions waiting to be processed, blockchains can fail due to branching faster than the branches can be pruned.

With DAGs this problem is bypassed by having each transaction behave as a self-containing entity that can be created at any time. In combination with low latency and a feeless structure, DAGs can handle thousands of transactions per second.

This makes DAGs optimal for IoT networks where there could be thousands of devices all needing to communicate several times per minute.

Low Latency

Due to the blockless nature of DAGs, transactions can be run directly instead of having to wait for a block to fill up and be processed.

Instead of the 10 minute block time of Bitcoin, or the 15 - 30 second block time of Ethereum, the only limit on transaction speed in a DAG is bandwidth. This makes the network much faster than traditional Proof of Work or Proof of Stake networks.

Feeless

While being feeless is not a default property of DAGs, DAGs offer the opportunity for transactions to directly confirm other transactions, cutting out the need for a fee-paid middleman.

NOVAM takes advantage of this attribute to make transactions and informational tasks free. DAGs also lower the cost for distributed ledger hardware as expensive mining rigs are no longer needed to keep the system running.

DEEP DIVE INTO DAG

Consensus Algorithm

NOVAM[6] is started with a genesis address that contains a balance of all the tokens. The genesis transaction sends these tokens to several other founder addresses. All tokens are created in this genesis transaction. No tokens will be created in the future and there is no way to generate new tokens through other processes, such as mining.

NOVAM uses a somewhat traditional, though more efficient, Proof of Work consensus model. Transactions are made easier for lower powered IoT devices to transmit, while still being able to prevent spamming the network.

The validation process for transactions in NOVAM is as follows:

NOVAM nodes must work to approve two other transactions before they can transmit their own.

This approval process ensures that nodes that issue transactions are contributing to the security of the network.

If a node finds that a transaction is in conflict with NOVAM's history, the node will not approve the conflicting transaction.

When a transaction is created:
- Two previous transactions must be approved
- These approvals are represented by directed edges

If a directed edge between transaction A and transaction B doesn't exist, but there are at least two directed paths from A to B, then it is understood that A has indirectly approved B.

Every transaction must approve the genesis transaction through this process – either directly, or indirectly.

There are no strict rules for how a node chooses which transactions to approve. With that said, if a large number of nodes follow the same reference rule, then for any fixed node, consistency is most prudent and therefore preferred.

As a transaction receives additional approvals, it is accepted by the system with a higher level of confidence. This increases the difficulty of trying to make the system accept a double spending transaction.

[6] Novam takes much of its base functionality from IOTA's Tangle. While it doesn't run on the Tangle, many of the details may be similar. [Serguei Popov. IOTA: The Tangle, 2016. http://iotatoken.com/IOTA_Whitepaper.pdf.]

To issue transactions nodes do the following:

- The node chooses two other transactions to approve according to an algorithm (these transactions may coincide)
- The node confirms the two transactions are not conflicting and does not approve conflicting transactions
- For a node to issue a valid transaction, the node must solve a cryptographic puzzle. This is achieved by finding a nonce with a hash that is concatenated with data from the approved transaction with a particular form

It is important to note that NOVAM is asynchronous. It cannot be assumed that all nodes see the same set of transactions.

The NOVAM Network can also contain conflicting transactions. In the case where two conflicting transactions exist there is a method to determine which transaction is orphaned.

NOVAM runs on a gossip protocol to propagate transactions through the network. This gossip protocol is how all state modifications to the ledger are broadcast to other participants and how consensus of the state is agreed upon.

How transactions propagation works is that nodes will randomly send transactions to their neighbors as they hear about them. This enables each node to be more familiar with the network.

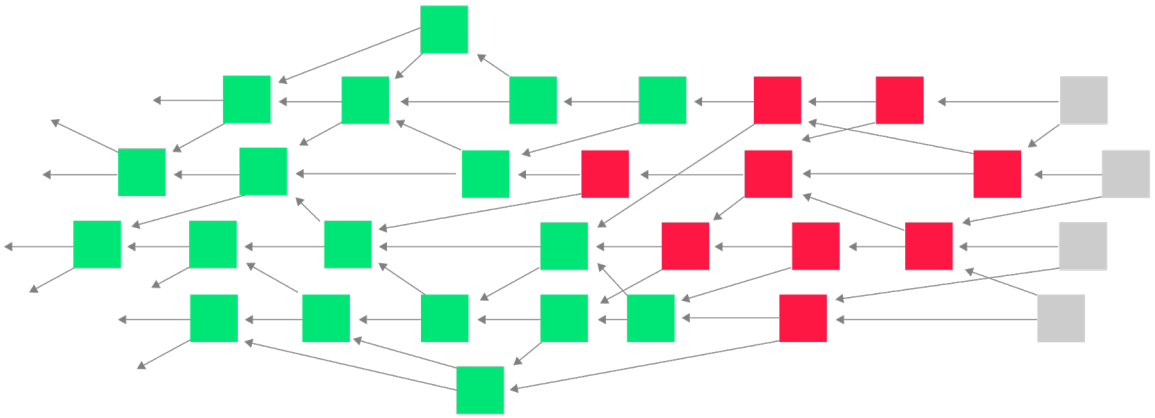
Every new transaction created that has yet to be confirmed is referred to as a tip. NOVAM functions by having each transaction approve two tips.

Tips are chosen by a Random Walk Monte Carlo algorithm which is designed to ensure that only good transaction branches grow.

Note that just because a transaction is referenced by a tip doesn't mean that transaction is considered verified.

Once there is a direct or indirect approval path from every tip, a transaction will be fully verified (as invalidating that transaction would also invalidate all current tips and any future transactions that will approve those tips).

This process is how all NOVAM nodes and their transactions published to the network come to a consensus. Each new transaction further cements these transactions into the permanent NOVAM ledger.



In this diagram, the green squares represent transactions confirmed by every tip. There is a path from every tip to that transaction.

There is no way to submit a NOVAM transaction without further confirming these green transactions.

Although the red transactions have been approved by at least one tip, they have not yet been approved by every tip.

In practice, it may be impractical to wait until every current tip has approved a transaction to consider it verified.

Different vendors and/or systems can set their own specifications: 95 percent of tips, 99 percent of tips, etc.

It's impossible to determine with 100 percent certainty whether young transactions are legitimate or not. If referenced by the majority of the tips returned by the Monte Carlo Random Walk, there is a high probability that older transactions are legitimate.

TRANSACTION WEIGHTS

Having a weight and a cumulative weight on the transaction level is essential to the consensus process. A transaction's weight is determined by a combination of the transactions importance in the hierarchy and the processing power it took to submit the transaction.

Note: Transactions to secure other nodes are ranked higher than information transactions.

The cumulative weight is defined as a transactions individual weight plus the sum of the weights of all the transactions that approve it, either directly or indirectly.
In general, a transaction with a larger weight is more important and reliable than one with a smaller weight.

The weighting algorithm is designed so that no entity should be able to generate an abundance of transactions with acceptable weights in a short period of time. This factor works to greatly decrease the probability of spamming and other attacks in that vein.

SYSTEM STABILITY

Let $L(t)$ be the total number of unapproved transactions, or tips, at time t. It is expected that $L(t)$ should fluctuate around a constant value and not diverge to infinity, as if $L(t)$ went to infinity, there would be many tips that would never be confirmed.

To analyze the stability of $L(t)$, a few assumptions must be made:

The first assumption is that there are a large number of roughly independent entities issuing transactions to the NOVAM Network. This supports the process of incoming transactions to be modeled by a Poisson point process. Let λ be the rate of this Poisson point process.

Assume all devices have roughly the same CPU power and let h be the average time a device needs to perform the PoW calculations needed to submit a transaction.

Assume all nodes need to follow the rule of verifying two transactions at random and then transmitting their transaction.

Nodes don't see the actual state of the NOVAM Network when they submit their transaction. Rather they see the network as it was exactly h time units ago.

This means that a transaction attached to the DAG at time t only becomes visible to other nodes on the network at time $t+h$.

Assume the number of existing tips remains roughly stationary in time and converges at a value $L_0>0$.

Observe that at any given time t we have λh tips that have been attached, but are not yet visible to the other nodes as well as r revealed tips so $L_0=r+\lambda h$.

By stationarity, we can also assume that at time t there are around λh transactions that were tips at time $t-h$, but have been approved since then.

When a new transaction is created, the probability of the node choosing an actual tip (as opposed to a recently approved, no longer tip) is $\frac{L_0-\lambda h}{L_0}=\frac{r}{r+\lambda h}$

This means the average number unapproved transactions chosen is $\frac{2r}{r+\lambda h}$ (due to approving two transactions).

Since this new transaction becomes a tip, the average number of tips approved should be 1 to keep the amount of tips relatively constant. Setting $\frac{2r}{r+\lambda h}=1$, r can be rewritten as $r=\lambda h$ leading to $L_0=2\lambda h$.

Expected Transaction Time

The two extremes that could be occurring must be noted to determine the expected time for a transaction to receive its first approval:

- Low Traffic, a state that occurs when the number of unconfirmed transactions is very small. Under this state the probability of an unconfirmed transaction being approved by multiple new transactions becomes very small
- High Traffic is a state that occurs when there are many unconfirmed transactions. This state makes it very likely that an unconfirmed transaction will be approved by multiple new transactions

In a low traffic state the first approval happens on an average timescale of order λ^{-1} since one of the first incoming transactions will confirm the unconfirmed transactions (as there are so few to choose from).

A high traffic state is one where μ is large. As mentioned above, Poisson flows of approvals to different tips are independent and haven an approximate rate of $2\lambda/\ \mu$. Therefore, the expected time for a transaction to receive its first approval is around $\mu/2\lambda \approx 1.45\mathrm{h}$.

Snapshots

Due to the speed at which NOVAM can grow, as well as the low storage capacity that IoT devices tend to have, there is a necessity for NOVAM nodes to have access to views of the state of the NOVAM Network without having to store every transaction that has ever been made.

The solution for this is to allow the storage of snapshots. Snapshots contain the state of the NOVAM Network at a fixed point in time.

Snapshots can be made by taking the set of all yet to be approved transactions. Any path from a transaction issued after the time the snapshot was made must be verified and approved by a subset of these transactions.

It is important to note that the size of a new set of unapproved transactions in the NOVAM Network occasionally becomes small. One may then use the small set as snapshots for possible DAG pruning and other tasks.

In the future there will be a functionality that enables light nodes to save their transactions. This will be dependent on there being enough full nodes that store all transactions that the light nodes can reference when needed.

Quantum Resistance

It is known that a sufficiently large quantum computer could be very efficient for handling problems that rely on trial and error to find a solution. The process of finding a nonce in order to generate a Bitcoin block is a good example of such a problem.

As of today, one must check an average of 2^{68} nonces to find a suitable hash that allows a new block to be generated. It is known that a quantum computer would need $\Theta(\sqrt{N})$ operations to solve a problem that is analogous to the Bitcoin puzzle stated above. This same problem would need $\Theta(N)$ operations on a classical computer.

Therefore, a quantum computer would be around $\sqrt{2^{68}} = 2^{34} \approx 17$ billion times more efficient at mining the Bitcoin blockchain than a classical computer. Also, it is worth noting that if a blockchain does not increase its difficulty in response to increased hashing power, there would be an increased rate of orphaned blocks.

CLIENT TYPES

Due to the nature of running clients on IoT devices, which may not be as robust a computational platform as traditional Blockchain or DAG nodes, different types of clients are available for different systems.

Light client

The IoT client is a minimalistic version of the NOVAM client. It will snapshot the network more often to conserve space and only store the subset of data that they are interested in.

Light clients can connect to full nodes whenever there's a need to obtain a transaction they may not have. In the future it will be able to run without having to store the transactions from other devices, just its own.

Full Node

The full node is a more traditional Distributed Ledger node. It will have the whole network saved to it initially, though it can still take network snapshots as needed.

Individuals or companies can create full nodes to help interact with their IoT nodes, while creating an optimal security environment.

Every vendor or trusted security provider that wants to monitor and update their subset of devices will need to have at least one full node running.

ARTIFICIAL INTELLIGENCE DAG EXPLORER

The upcoming AI DAG Explorer is an additional piece of software designed to be paired with the Full Node.

The AI DAG Explorer will analyze vulnerabilities and updates identified throughout the network to build a profile for the different types of systems. It will then use this to implement anomaly detection to identify vulnerabilities that are not yet widely known.

The AI DAG Explorer will perform this task by collecting all of a nodes information from known transactions to create a model based on aspects such as transaction patterns.

When suspicious behavior is flagged the AI DAG Explorer can send notifications to users. This information can then be shared with everyone who wants to use it for further security use.

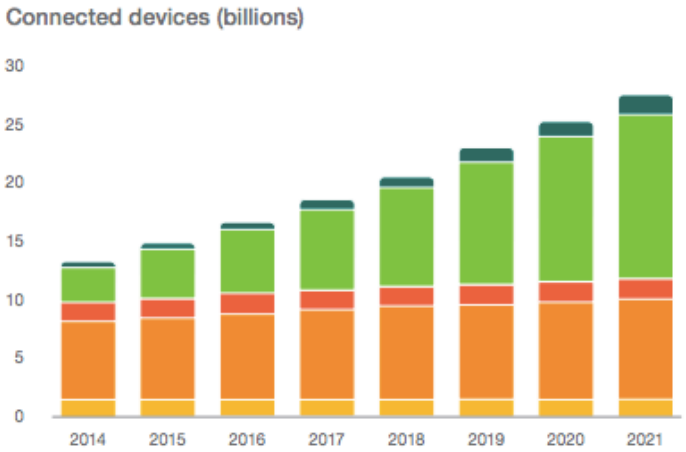
MARKET SIZE

According to Energias Market Research[7], the global Internet of Things (IoT) market is estimated to reach $6.5 trillion by 2024 with an estimated 200 billion IoT devices connected.

The economic value from connected IoT is estimated to be around $1.46 trillion by 2021, according to IDC[8] and $11.1 trillion by 2025 according to McKinsey Global Institute[9].

Internet of Things sensors and devices are expected to exceed mobile phones as the largest category of connected devices in 2018, growing at a 23 percent compound annual growth rate (CAGR) from 2015 to 2021.

Ericsson predicts there will be a total of approximately 28B connected devices worldwide by 2021, with nearly 16B related to IoT[10].



	15 billion	28 billion	CAGR 2015–2021
Cellular IoT	0.4	1.5	27%
Non-cellular IoT	4.2	14.1	22%
PC/laptop/tablet	1.7	1.8	1%
Mobile phones	7.1	8.6	3%
Fixed phones	1.3	1.4	0%
	2015	2021	

Source: Ericsson Mobility Report 2016

[7] Global IoT Market Outlook. https://globenewswire.com/news-release/2018/04/17/1479964/0/en/Global-Internet-of-Things-IoT-Market-to-witness-a-CAGR-of-26-6-during-2018-to-2024-Energias-Market-Research-Pvt-Ltd.html

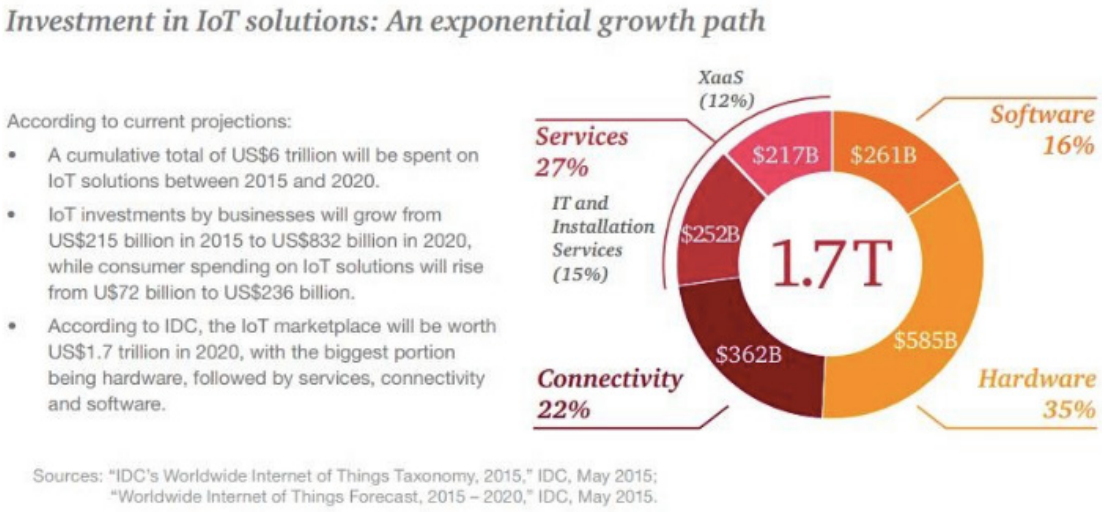
[8] Worldwide Spending IoT Forecast. https://www.idc.com/getdoc.jsp?containerId=prUS42799917

[9] Unlocking the potential of IoT. https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world

[10] Ericcson Mobility Report. https://www.ericsson.com/assets/local/mobility-report/documents/2016/Ericsson-mobility-report-june-2016.pdf

Cybersecurity Ventures[11] predicts global market spending on cybersecurity will exceed $1 trillion from 2017 to 2021.

Ransomware alone has become the number one threat to organizations and is predicted to grow to a $17.36 billion market by 2021, according to ReportLinker[12].



\Worldwide, cyber crime damages are predicted to cost organizations an average of $6 trillion dollars annually by 2021. The demand for cybersecurity professionals will increase to 6 million people globally by 2019, while there will be 3.5 million unfilled cybersecurity jobs by 2021, according to Cybersecurity Ventures[13].

[11] 2018 Cybersecurity Market Report. https://cybersecurityventures.com/cybersecurity-market-report/

[12] Ransomware Market Predictions. https://www.prnewswire.com/news-releases/ransomware-protection-market-expected-to-grow-to-usd-1736-billion-by-2021-300461559.html

[13] Cybersecurity Unemployment Rate. https://cybersecurityventures.com/cybersecurity-unemployment-rate/

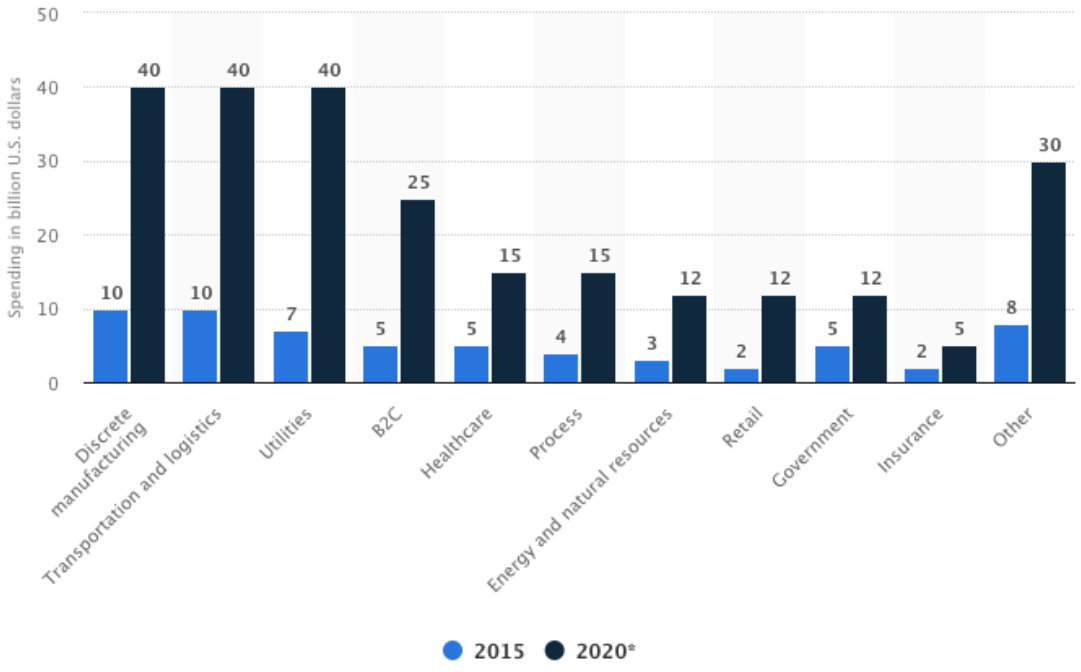
MARKET FOCUS

Due to the nature of NOVAM's computer, mobile phone or IoT device solutions, we can focus on markets across a wide array of industries as the tech landscape grows.

Listed below is our market focus which includes, but is not limited to layers of integration from Fortune 500 organizations to OEMs and cybersecurity firms.

Hardware & Chip Manufacturers	Root of Trust, TEEChip, OEM hardware/chips
Software Firms	Operating Systems, Firmware, Applications
Cybersecurity	Enterprise & consumer protection
Fortune 500	Direct integration into systems
Ecommerce / Digital Payments	Web/Mobile/Retail payment methods

Spending on Internet of Things worldwide by vertical in 2015 and 2020 (in billion U.S. dollars)



Source: Statista, Spending on the Internet of Things worldwide by vertical in 2015 and 2020 (in billions U.S. dollars).

TARGET MARKET BY INDUSTRY

BENEFITS & USE CASES

The benefits, use cases and situational context provided below are to provide an overview of industries, enterprise and consumer impact malware creates.

TELECOMMUNICATIONS

The telecommunications industry plays a critical role in an ever-connected world. To build, operate and manage the complex critical infrastructure used for voice and data transmission, telecom providers share and store vast amounts of sensitive data on a daily basis.

In a quickly-evolving threat landscape, telecommunications organizations are especially vulnerable to cyber-attacks.

Adoption of virtual environments has helped streamline processes throughout remote locations but present new challenges to secure and monitor expanding complex network infrastructure.

Legacy tools struggle to protect the perimeter and insider threats from sophisticated attacks. If telecoms are disabled, the world is without systems.

Telecommunication networks affected by ransomware:

- Telefonica, the largest multinational telecommunication company in Spain, was hit by WannaCry ransomware, compromising 85 percent of internal corporate servers
- Saudi Telecom Company, a Saudi Arabia-based telecommunications company, said 18 percent of their computers were compromised by WannaCry ransomware and affected landline, mobile and internet services for millions
- MegaFon, Russia's telecommunication firm, was infected by WannaCry ransomware, interrupted their national call centers
- Vivo, Brazil's largest telecom operator, had its headquarters infected by WannaCry, interrupting services for the nation
- Vodafone Germany was breached by an insider threat, and two million records were stolen, including PII like names, gender, bank account numbers, bank sort codes and birth dates

Comprehensive visibility into physical and cloud environments and a complex global network enables NOVAM to monitor, detect and respond to threats internally using our Immune System Defense and endpoint health check solution for remote IoT devices.

TRANSPORTATION

Mobility and transportation are a priority to nations, car manufacturers, shared-economy networks, and mobility-as-a-service (MaaS) providers.

New worldwide initiatives have altered travel and logistics by using autonomous, highly connected machines for transportation, electronic ticketing, payment services, bookings, and end-to-end trip planning.

The digital transformation will forge forward with smart cars, unmanned aerial delivery and transportation to connected maritime vessels with IoT transportation and mobility helping to shape and mold the next decade.

With the spoils of innovation and the digital revolution's effect on transportation and mobility comes increased exposure to cyber-threats:

- Kiev Metro, was hit by NotPetya ransomware, disabling bank card payment for use of the city-wide transportation train
- Russian Railways, breached by WannaCry ransomware, infected nationwide IT systems, and halting transportation
- Deutsche Bahn was hit by WannaCry, but only had their railway digital signs compromised. The potential to breach personal identifiable information is a computer length away
- Q-Park, the second largest European parking operator, was infected by WannaCry, which crashed computers and ATMs worldwide

The new wave of smart devices that assist transportation and mobility for citizens and visitors will enhance the world around us by providing convenience and safety.

Unfortunately, larger attack vectors on remote endpoints and global interconnected networks are an undeniable downside.

NOVAM's mission includes securing IoT endpoints of all types using our health check solution and Immune System Defense.

CONSUMER ELECTRONICS

By 2050, the world will see 50 billion connected devices, ranging from phones, computers, wearable devices, smart home appliances, security cameras, smart audio, TVs and more.

The Internet of Things and its widespread use of applications in day to day activities has already changed lives.

According to Market Research Future, by 2023, the global consumer electronics market is predicted to surpass $120 billion.

Personal privacy, unauthorized controlled devices and service interruption are only a few of the concerns that have been newsworthy in recent years.

Notable compromises include Fitbit publicly tracking military personnel in sensitive areas worldwide, to Mirai malware infecting 2.5 million devices and performing distributed denial-of-service attacks on Dyn and other internet infrastructures.

The Internet of Things has hundreds of protocols to address diverse aspects of the IoT ecosystem, including applications and machine-to-machine (M2M) communications.

IoT devices will continue to be targeted, but NOVAM's system health check can verify a device is healthy, without infection and/or automatically install patches to fix infected devices.

SMART BUILDINGS & CITIES

The global smart city market is expected to reach $1.5 trillion dollars in 2020. The rise of IoT innovation offers cities new ways of becoming operationally efficient, reducing costs, improving city management, providing infrastructure resilience, creating environmental sustainability and attracting new organizations.

Smart City IoT include a wide range of solutions:

- Smart Energy: Digital Management of Energy - smart grids, smart meters, intelligent energy storage
- Smart Buildings: Automated Intelligent Buildings; smart HVAC, smart lighting equipment, smart elevator systems
- Smart Technology: Seamless connectivity; 4G & 5G connectivity, super broadband, free city Wi-Fi
- Smart Infrastructure: Digital Management of Infrastructure; sensor networks, digital water and waste management, smart parking, traffic management and public transportation
- Smart Citizen: Civil Digital Natives; use of green mobility options and smart lifestyle choices
- Smart Security: Intelligent Threat Detection; surveillance, biometrics, simulation modelling and crime protection
- Smart Government: Disaster management solutions, alert systems and more

The Internet of Things promises to make great contributions to our society within cities, but IoT's connected infrastructure can also expose us to greater cyber-threats.

The more IoT connectivity, using many competing vendors for specific use-cases, the larger the network web and increased attack vectors to both physical and digital devices.

NOVAM's team has decades of combined experience in city infrastructure, digital surveillance, enterprise servers and big data. Our seasoned experts believe that with our endpoint health check system we can protect connected devices to city networks. And with our Immune System Defense, we can defend against insider threat and anomalies.

GOVERNMENT & DEFENSE

When governments, defense departments and defense contractors get hacked, it opens organizations and citizens to substantial destruction. Vulnerabilities include identity theft, election manipulation, stock market manipulation, and critical national security of our military, officials, war-time defenses and infrastructure.

Advanced Persistent Threat (APT) attacks – well-financed, often state-sponsored, with a specific agenda – are used with the goal of accumulating sensitive data to advance political, economic and military objectives in the future.

Threats, reconnaissance and malware:

- Attempting to manipulate the elections have become pervasive. The U.S. Department of Homeland Security notified 21 states of reconnaissance and hacking attempts of election voter machines. If successful, local, state and federal elections could be manipulated to fit outside nation agendas (2016)
- Philippines Commission on Elections had 55 million registered voters and other sensitive data exposed and is considered the biggest private data leak in Philippine history (2016)
- The U.S. Central Intelligence Agency's most notable insider threat occurred in 2013 when Edward Snowden, who working for Booz Allen Hamilton, revealed details of classified U.S. government surveillance programs and stole intellectual property

The protection of national security data and property is critical for global military operations in countries worldwide.

Access to tools and data enable swift intelligence reporting and the measures required to accomplish operations to the best of an employee's abilities – whether a contractor or government employee.

Vast global networks, virtualized or physical, with millions of user and device access at various privileged levels can make it challenging to monitor, identify and respond to external or insider threats.

NOVAM's technology can assist security investigators in multiple categories from hardware and application verification to network intrusion.

INDUSTRIAL & MANUFACTURING INTERNET-OF-THINGS

The fastest growing Internet of Things market isn't consumer electronics, it's Industrial Internet-of-Things (IIoT).

Estimated to reach $933 billion by 2025, global manufacturers will invest $70 billion in IIoT solutions by 2020. Accenture estimates IIoT could add $14.2 trillion to the global economy by 2030.

Integration with networked sensors and software, additional endpoints, remote monitoring and access, and machine digitization empowers IIoT to assist daily utility.

With the implementation of IIoT devices, multi-cloud architecture, and system interoperability, comes additional vulnerabilities and threats to businesses and organizations.

Malicious cyber-attacks have already compromised manufacturing and industrial systems:

- The Stuxnet worm destroyed uranium enrichment centrifuges in Iran in 2007 by targeting valves, centrifuges and five companies related to the nuclear program
- Hackers destroyed a U.S. Water Utility Company's pump by accessing their SCADA (industrial control) system. Usernames and passwords were stolen, chemicals levels in the treatment plant were altered and 2.5 million customers had personal data stolen
- Puerto Rican Smart Meters were hacked to reduce power bills. Connected meters could have been used to access the main system controlling critical systems and sensitive personal data. Puerto Rico's Utility Industry lost an average of $400 million a year from such attacks (2012)
- In 2015, hackers gained access to German Steel Mill through phishing emails. The attack prevented blast-furnaces from shutting down, resulting in catastrophic damage to the plant, systems and equipment
- Hackers used stolen credentials to gain remote access to the Ukrainian power grid in a systematic attack during 2016. Power was cut for 30 substations and 225,000 customers. The attack involved installation of custom firmware, deletion of files and master boot records, and telephone communications were cut

From manufacturing to critical industrial national infrastructure, securing endpoints, systems, user and device identity is imperative.

Electronics and individual microchips can benefit from automated remediation of firmware, software and applications with tamper-proof authenticity.

NOVAM's Immune System Defense will enable endpoints, network, multi-cloud configurations and user privilege protection with autonomous monitoring, identification, and response to threats.

DIGITAL SECURITY & SURVEILLANCE

According to Markets and Markets digital security surveillance (DSS) is estimated to become a $68 billion industry due to the decreasing price of components, increased demand for surveillance, usability and services.

DSS is utilized worldwide for emergency management, infrastructure protection, public safety, process automation, control access management, traffic flow study and more.

Over the past few years, concerns have grown due to insecure hardware, software and applications. Also, insider threats with privileged credentials can bypass controls intended to monitor external attack threats. A clever spear-phishing attack can allow access to internal servers and controls without alerts.

A simple spear-phishing email can allow malware onto your computer or home network without detection. Undetected, it can then spread to all other devices on the same network and allow full control of your system. This was achieved by a Mirai botnet variant.

NOVAM can help all industries protect and sure their businesses and organizations. For more information and a breakdown on each industry, please refer the below appendix.

DIGITAL LANDSCAPE & PROTECTION LIMITATIONS

DIGITAL TRANSFORMATION

Digital transformation (DX) spending worldwide is predicted to reach $1.7 trillion by 2019, according to International Data Corporation (IDC)[14].

The First Industrial Revolution used water and steam power for production. The Second used electric power to create mass production. The Third used electronics and information to automate production.

The Internet-of-Things (IoT) is the Fourth Industrial Revolution and is positioned to fuse technologies that shape the physical, digital and biological domains. The Fourth Industrial Revolution connects government, enterprise, and individuals, with new ways of collecting, storing and sharing data in a digital world.

A new era of machine-to-machine (M2M) communication, commerce and society is on the rise. As a result, imminent security threats are emerging worldwide. Although the Fourth Industrial Revolution is here today, the security of yesterday, unequipped to handle an ever-changing connected landscape and the threats that come with it is still being used.

DX's expansion within the last decade has increased productivity and connectivity. This has also raised greater cyber threats.

Current cybersecurity controls aren't thorough enough, leaving systems vulnerable to attack and infection of malicious code, which spreads rapidly.

Decentralizing security controls, immutable cryptographic health checks and autonomous system defense can help prevent cybersecurity threats for the digital transformation of the future.

THE SHIFTING THREAT LANDSCAPE

The past decade has been rife with high-profile hacks that have plagued companies and governments in every industry and size.

Executives and leaders must rethink their security strategies and shift more of their resources to protecting sensitive information to stay up to date with company and country legal compliance.

[14] IDC FutureScape: Worldwide Digital Transformation 2018 Predictions. https://www.businesswire.com/news/home/20171101005220/en/IDC-Reveals-Worldwide-Digital-Transformation-Predictions

While the global economy continues to surge, company networks are ever-expanding to keep up with demand. Networks are global. They span different geographies. The digital transformation to cloud and virtualization, and new company practices that include BYOD, remote working, and mobile access have amplified attack vectors for cyber-threats.

When global networks recruit new endpoints to the network, exposure to malicious threats are increased.

Vulnerabilities may include supply chains, contractors, customers, payment processors and an expanding technology stack of open source and patent-pending software. In short, anything that keeps a business operational could be targeted.

Threats continue to compromise users, devices and networks. Traditional security has proven to be vulnerable, inefficient and prone to data loss, including intellectual property, HR & legal records, customer data, and more – but it's not just a question of data loss.

New generations of cyber-attacks target more than just data

Today's most pernicious threats are playing chess, not checkers. They look to disrupt or undermine the very integrity of the data itself.

For example, a healthcare company handling patient data relies on the integrity of that critical information to deliver care and maintain patient confidence. A bank must be able to trust in the fidelity of its customers' bank balances.

What happens if information is not stolen, but simply altered or manipulated? The implications of data being changed without an organization's knowledge are truly concerning and pose an existential threat to businesses and market confidence.

INSIDER THREAT

Due to privileged access and understanding of corporate networks, insider threat is one of the most harmful forms of cyber-threat today.

When organizations think of cyber-threats, they often look at external attacks, with hackers that penetrate structured network borders and device endpoints being the focus.

Whether malicious or not, insider threats can cause major problems, breaches and attacks to global organizations.

Who is an insider? An insider can be any person or credential holder, employee or not, with authorized access to your networks or physical location. This includes employees, contractors, suppliers, customers, maintenance staff and others.

Once inside, credential holders can traverse the network to discover system configurations, take advantage of privileged access and steal or modify data.

Non-malicious insiders can be a liability too. BYOD and remote access practices have become standard in the past decade. Employees can expose organizations to risk while on their own computers or mobile devices.

Spear-phishing campaigns, installed malware and web-based attacks expose sensitive data like source code, corporate files or credentials to internal systems. Implementing industry-standard security practices can help deter attacks, but accidental human error can cripple an organization.

Communication and collaboration are important in today's business atmosphere. Access to tools that ensure employees and contractors can do their jobs to the best of their abilities often entrust privileges to sensitive systems.

Organizations can believe they are well-defended, with highly-vetted staff, industry-leading security policies and best practices and still be vulnerable to insider threat born from communication and collaboration policies. Insider threats of this brand can cause existential financial, reputational and operational damage.

Communication and collaboration thrive on networks that consist of physical, virtual and personal devices with thousands of endpoints. Unfortunately, BYOD policies increase vulnerabilities that are difficult to distinguish, monitor and track.

There's no guarantee that non-malicious employees, who have privileged credentials will be able to accurately prevent against spear-phishing campaigns, avoid clicking unknown links or stay off websites that lead to a web-browser attack.

We can't prevent humans from being curious, even with extensive training. Employees will always be prone to social engineering or taking shortcuts to get the job done, leading to compromised security, regardless of honest intentions.

Disgruntled employees are not to be ignored. It's not uncommon for an employee to become annoyed, irritated or angry at their organization.

This may lead to the release of sensitive information to the public or competitors, causing financial, reputational and operational damage to their company.

LIMITATIONS OF LEGACY SECURITY TOOLS

Legacy security tools can't keep up

As with the way the human body protects against the unknown, there are different legacy protection mechanisms enabled in case of failure, but in a rapidly-evolving threat environment, the legacy approach is limited.

Perimeter Controls

The perimeter defense strategy has been a cornerstone of cybersecurity since the first firewalls hit the market. Yet, as a primary defense, the firewall has not been able to stop the primary method for network penetration – the user.

Web based phishing attacks or malware are the primary tools to gain network access. As the threats have evolved and more functionality has been integrated into the perimeter devices, most network security firms have used this gap as an opportunity to sell additional licenses and functionality – as opposed to solving the underlying issues.

Perimeter control flaws:

- Solely signature-based
- Require code to be installed on every device – even if incompatible
- Extensive ongoing effort required to patch code, for different devices and operating systems
- Not updated on possible unknown attack methods
- Unable to guard against credential holders and insiders
- Resource intensive
- Constantly out of date
- Monitoring global systems is resource intensive for IT departments

Data Loss Prevention

Data loss prevention (DLP) solutions are designed to detect and prevent sensitive and critical information from being shared outside the network as data is being accessed by endpoint devices.

Although organizations try to control which data users can transfer, there are significant limitations with DLP solutions:

- Insider threat – bypassed by credential holders and privileged insiders
- Evasion by new, unknown attack methods
- Ongoing effort to define rule-based permissions
- Improper guidance exposes data
- System improvements are time consuming

Endpoint Security

Endpoint security is typically a rule and policy-based approach to network security that requires endpoint devices to comply with specific criteria before they are granted access to network resources.

Although many organizations implement one form of endpoint security or another, flaws still exist:

- Signature manipulation compromises devices
- Software installation on every device, even if not all devices are not supported
- Relying on prior knowledge of attack methods via threat intelligence networks, so security will be constantly out of date in the face of new or advanced threats
- Circumvention by credential holders and insiders
- Evasion by new or unknown attack methods
- Prevalent effort required to patch code, for different devices and operating systems
- Lack of updates

Sandboxes

A sandbox is a security mechanism in which a separate, restricted environment is created. Certain functions are prohibited and identified, untrusted or harmful threats are placed into a "time out" until cleared.

Sandboxes are often used to detect known threats, but they suffer from the following restrictions:

- Malware can detect sandbox environments and delay the attack until gaining access to the actual network
- Does not address insider threat
- Only checks one point of entry
- Relies on prior knowledge of attack methods
- Regularly defeated by advanced attackers and persistent threats

Threat Intelligence

Threat intelligence is evidence-based knowledge that includes context, mechanisms, indicators, implications and actionable advice about existing threats to assets in a database or information feed.

It is used by security teams to investigate alerts and to determine action. Known, researched, and documented threats are used for future prevention of the same attacks. However, much like other approaches, it is imperfect:

- Backdated method makes it hard to discover, reverse engineer and globally share new intelligence
- Discovered and researched attacks fail to address unknown attacks
- Extensive upkeep is needed to evaluate the quality and applicability of threat intelligence feeds and how threat data should be applied to different defenses

Behavioral Analytics

User and Entity Behavior Analytics (UEBA) are pseudo-mathematical systems that correlate both user activity and other entities such as managed endpoints, applications and networks.

Reliant on threat intelligence, they identify known attacks that are similar to previous attacks. Additionally, behavioral analytic systems look at less informative data than security information and event management (SIEM) systems and monitoring platforms. Limitations include:

- Masked dependence on signatures or threat intelligence of known attacks
- Pseudo-mathematical approaches are only applied to lightweight subsets of security data, as opposed to the entire network view
- Inability to detect new, unknown, and advanced attacks
- Lack of resources required to deploy, manage, and maintain system

Log tools and SIEM

Log analysis tools and SIEM solutions collect logs, monitor the correlation of events in real time, document notifications and are responsible for long-term storage and analysis.

SIEM databases can be useful for investigations, if you know what you're looking for. Although in use for years, organizations have been disappointed by their inherent level of inaccuracy and bloat.

These tools haven't lived up to their potential because they:

- May take years to roll out
- Require significant resources for tuning, updating and filtering corporate policy information
- Typically rely on event signatures, threat intelligence or human queries
- Depend on manual IT resources and time

THE LIMITATIONS OF RULES

Based on past experiences, rule-based approaches are only as good as the knowledge used to create and implement them. New or unknown events are disruptive to rule-based systems and can circumvent or alter what's needed to pass an organization's system requirements.

Binary logic cannot dictate new scenarios beyond the scope of a rule, limiting the system to specific requirements. Depending on the scenario, this can hinder interoperability and collaboration cross-border.

Rule-based approaches can also overload systems, creating substantial false alarms, which ultimately allows for a malicious attack to compromise a network without being detected. Frequent false alarms can desensitize security teams, which leads to treating attacks as less severe than they are.

LIMITATIONS OF IDENTITY VERIFICATION & DEVICE MITIGATION

Identity is defined as who or what a person or thing is. Verification is defined as the process of establishing truth, accuracy, or validity.

In information security identity verification can mean accurately verifying a person or device by identifiable information or characteristics.

The process of identity verification is imperfect when related to a person. If a bad actor gains control of a person's digital identity, they can exploit it. The verification process for hardware can be established with a serial number, software version number, kernel, microkernel or other attribute.

Device verification is limited without the use of instructions, policies and immutable attestation. Current methods for attestation lack a secure, undeniable and cost-efficient way to verify device to prevent against threats automatically.

THREATS & INADEQUATE CYBERSECURITY RESPONSE

MALICIOUS ATTACKS

Over the years, there have been variations of malware and ransomware that have attacked critical systems around the world, hindering services and negatively impacting governments and enterprises.

Instances that could have cut countries off from the world or causes catastrophic impacts to power grids, nuclear power plants and other critical infrastructure to sustain life have occurred.

Our goal is to share variations of malware, ransomware, and different types of attacks that can be accomplished above and beyond disabling the internet, which has become the backbone to our digital society. Technology can initiate life-threatening situations that can impact health and safety worldwide.

DATA BREACHES

Data breaches and their ability to compromise sensitive personal information has caused detrimental privacy concerns.

Targets often include social security numbers, health records, passports and credit card credentials. Enterprise theft, like research and development and intellectual property, is not out of the question.

NOVAM addresses data breaches by monitoring entire networks, infrastructures and end points to establish full seamless views of global communications and threats.

Unless NOVAM was implemented from inception, we assume users, devices and networks have already been compromised – and initiate tailored action plans immediately.

REGULATION COMPLIANCE

In a data-driven world consumer and enterprise data privacy protections have become increasingly important.

Protecting sensitive data while providing easy to use solutions for enterprise and consumers alike is paramount.

NOVAM can assist on both sides. We protect hardware, software and applications from being compromised and provide user data protection for consumers – all while being compliant with data and privacy regulations.

We also help organizations identify compliance issues, become compliant, while providing data protection and authentication for their users, devices and networks.

DATA PROTECTION REGULATION (GDPR)

The EU General Data Protection Regulation (GDPR) was passed in April 2016. Enforcement started on May 25, 2018.

The new policies require businesses to comply with strict consumer protections, or face consequences of up to $20 million, or 4 percent of a company's total net revenue for the year, whichever is greater.

Coupling privacy controls with identity verification, authentication and cyber defense enables organizations to be GDPR compliant, while in turn helping individual users protect their data and prevent personal identification theft.

SECURITY PROFESSIONAL SHORTAGE

Cybersecurity is just as important for global organizations as it is for the future of our connected society.

With the daily volume of cyber-attacks and triggered events increasing rapidly, it's become increasingly challenging for humans to detect, respond and protect the digital landscape, according to Microsoft's Global Incident Response and Recovery Team[15].

According to Cybersecurity Ventures[16], the demand for cybersecurity professionals will increase to approximately 6 million globally by 2019, while 3.5 million global cybersecurity jobs are estimated to be unfilled by 2021.

The rapid demand for global security professionals, the increase in security alerts and breaches and the shortage in talent have shifted innovation toward automation, machine learning and artificial intelligence. A new approach is required to secure connected infrastructure, government, corporate and user data.

NOVAM's machine learning, probabilistic mathematics, patent-pending tactics and methods can enable action without prior knowledge of the threat. Proactively, NOVAM is designed to identify, monitor, alert and in some cases initiate an immune system response that automatically mitigates, removes, replaces or quarantines the threat.

[15] Microsoft Global Incident Response and Recovery Team. https://cloudblogs.microsoft.com/microsoftsecure/2017/08/03/top-5-best-practices-to-automate-security-operations/

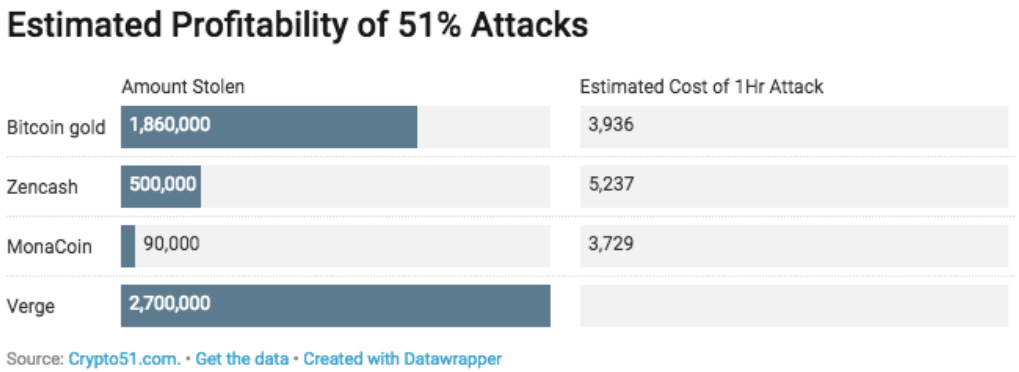
[16] Cybersecurity Jobs Report 2018-2021 https://cybersecurityventures.com/jobs/

POSSIBLE ATTACK SCENARIOS

SYBIL 51% ATTACK

One of the most common attack methods brought to attention by the blockchain community is the 51% attack, which has plagued Bitcoin Gold, ZenCash, Verge, Monacoin and Litecoin Cash[17].

A 51% attack occurs when an attacker is able to gain more than 50% of the voting strength. They can use this power to double spend or make other changes to the network.



The primary defense against this type of attack is voting weight tied to investment in the system. Attempting to flip the ledger would be destructive to the system as a whole, as it would destroy their investment. This attack is also directly proportional to the total market cap.

Malicious actors trying to double spend in NOVAM can never occur accidentally, so nodes can make policy decisions on how to interact with these invalid transactions.

The only time non-attacker accounts are vulnerable to attackers trying to split the network is if they receive a balance from an attacking account. Accounts wanting to be secure from block forks can wait before receiving from an account who generated forks or opt to never receive at all. Receivers could also generate separate accounts for receiving from dubious accounts to protect the rest of their balance.

[17] CoinDesk Article - Alyssa Hertig. https://www.coindesk.com/blockchains-feared-51-attack-now-becoming-regular/

Proof [18]

μ = computing power of the attacker.

$W(n)$ = The time needed to obtain a nonce that gives a double spending transaction a weight of at least n.

This function can be represented as an exponentially distributed random variable with a parameter of μn^{-1}.

λ = rate of transactions issued on the network by honest nodes

w = mean weight of a generic transaction

The cumulative weight grows with linear speed λw.

The total weight of the legitimate branch at the time is $w_1=\lambda w t_0$.

In the NOVAM Network a transaction would be considered "accepted" when its cumulative weight is at least w_0 which happens t_0 time units after the transaction occurs.

To overthrow this legitimate branch, an attacker would need to create a transaction that gets a cumulative weight of n_0, $n_0 > w_1$ in less than t_0 time units. We can express this probability as $P[W(n_0) < t_0]$. In fact, $n_0 \approx w_1$ if w_1 is large.

Using the Cumulative Distribution Function (CDF) this probability expands to be

$$1-\exp(-t_0\mu n_0^{-1}) \approx 1 - \exp(-t_0\mu w_1^{-1}) \approx \frac{t_0\mu}{w_1}$$

This approximation is true in the case where $\frac{t_0\mu}{w_1}$ is small, which is a reasonable assumption.

If this initial attack fails, the attacker can then try to find a nonce that gives a weight $n > n_0$ and hope that when they find it the total legitimate weight is less than n.

The probability of this event occurring is the probability that the attacker's weight is greater than the expected weight after that time. This can be expressed as

$$P[\lambda w W(n) < n] = 1-\exp(-\mu n_0^{-1} \times \frac{n_0}{\lambda w}) = 1-\exp(\frac{-\mu}{\lambda w}) \approx \frac{\mu}{\lambda w}$$

Although $\frac{\mu}{\lambda w}$ should usually be a small number, at every weight n the attack succeeds with a constant probability. Therefore, eventually it will succeed. The expected time until this happens is roughly $\frac{\lambda w}{\mu}$.

Although this number can be quite large, it is not large enough to make the effects of this attack negligible. To counter this attack, we can set a limit on the own weight value.

Consider the scenario where the maximum own weight is capped at 1. Assume that a given transaction gained a cumulative weight w_0 in t_0 time units after it was issued.

This transaction's cumulative weight increases linearly with a speed of λ . If an attacker wants to double-spend the contents of this transaction they would start generating nonsense transactions to approve the double-spending transaction.

If the attackers subtangle outpaces the legitimate subtangle sometime after the merchant accepts the first transaction, the double-spend succeeds. If this does not happen, the double-spending transaction would never be approved due to the conflict and insufficient weight.

For simplicity sake assume transactions propagate instantly.

Let be G_1, G_2, G_3 be Independent and Identically Distributed exponential variables with parameter μ and expected value of $\frac{1}{\mu}$.

Let $V_k=\mu G_k$ so V_1, V_2, V_3 be independent and identically distributed exponential variables with parameter 1.

Say a merchant accepts a transaction with cumulative weight w_0 at time t_0, what is the probability that the attacker successfully double spends? Let $M(\theta)=(1-\theta)^{-1}$ be the moment generating function of the exponential distribution with parameter 1.

Using the Large Deviation Principle $\alpha \in \{0,1\}$ $P[\sum_{k=1}^{n} V_k \leq \alpha n]=\exp(-np(\alpha))$ **(1)**

where $p(\alpha) = -\ln\alpha+\alpha-1$ is the Legendre transformation of $\ln M(\theta)$.

In general $p(\alpha) >0$ for $0 <\alpha < 1$.

Assume that $\frac{\mu t_0}{w_0} < 1$ because otherwise the probability that an attacker can succeed is close to 1.

To outweigh w_0 at time t_0 an attacker needs to be able to issue at least w_0 transactions with maximum own weight m during time t_0 .

There by using **(1)** the probability of the cumulative weight of the double spending transaction being higher than the cumulative weight of the legitimate transaction at time t_0 is represented by

$$P[\sum_{k=1}^{w_0/m} G_k < t_0] = P[\sum_{k=1}^{w_0} V_k < \mu t_0 = P[\sum_{k=1}^{w_0} V_k < w_0 \times \frac{\mu t_0}{w_0}]$$ **(2)**

For this probability to be smal $\frac{w_0}{m}$ needs to be large and $p(\frac{\mu t_0}{w_0})$ can't be very small.
Note that at time $t \geq t_0$ the legitimate weight is roughly $w_0+\lambda(t-t_0)$ because we assume the adaptation period is over, so the cumulative weight grows with a speed λ.

Analogous to **(2)** the probability a double spending transaction has more cumulative weight at time $t \geq t_0$ is roughly $\exp(-(w_0+\lambda(t-t_0))p(\frac{\mu t}{w_0+\lambda(t-t_0)}))$.

Then it must be true that we have $\frac{\mu t_0}{w_0} \geq \frac{\mu}{\lambda}$ since the cumulative weight grows with speed less than λ during the adaptation period. In this scenario the probability is of order $\exp(-w_0 p(\max(\frac{\mu t_0}{w_0}, \frac{\mu}{\lambda})))$ **(3)**.

Example:

Let $\mu=2$ and $\lambda=3$ so that the attacker's power is a little bit less than the rest of the network (the honest nodes). Assume the transaction has a cumulative weight of 32 by time 12 then

$\max(\frac{\mu t_0}{w_0}, \frac{\mu}{\lambda}) = 3/4$, $p(3/4) \approx 0.03768$ and **(3)** gives an upper bound of about 0.2994.

If instead $\mu=1$ then $\max(\frac{\mu t_0}{w_0}, \frac{\mu}{\lambda}) = 3/8$, $p(3/8) \approx 0.3558$ and **(3)** gives us approximately .00001135, a very significant change.

It is important to realize that the inequality $\lambda > 4\mu$ should be true for the system to be secure, or in other words the rate of honest transactions should be large compared to the attacker's computational power, otherwise the estimate in **(3)** would not be valid.

This indicates the need for additional security measures, such as checkpoints, during the early days.

SPLITTING ATTACK

A splitting attack occurs when an attacker tries to split the NOVAM Network into two branches and maintain the balance between them.

This would allow both branches to continue to grow, potentially enabling conflicting transactions. The attacker must place at least two conflicting transactions at the beginning of the split to prevent an honest node from effectively joining the branches by referencing them both simultaneously.

Then, the attacker hopes that roughly half of the network would contribute to each branch so that they would be able to "compensate" for random fluctuations, even with a relatively small amount of personal computing power.

If this technique works, the attacker would be able to spend the same funds on the two branches.

To defend against such an attack, one needs to use a "sharp-threshold" rule that makes it too hard to maintain the balance between the two branches.

An example of such a rule is selecting the longest chain on the Bitcoin network.
Let us translate this concept to the NOVAM Network machine learning, probabilistic mathematics, patent-pending tactics and methods can enable action without prior knowledge of the threat.

Proactively, NOVAM is designed to identify, monitor, alert and in some cases initiate an immune system response that automatically mitigates, removes, replaces or quarantines that threaten the network when it is undergoing a splitting attack.

Assume that the first branch has total weight 537, and the second branch has total weight 528.

If an honest node selects the first branch with probability very close to 1/2, then the attacker would probably be able to maintain the balance between the branches.

However, if an honest node selects the first branch with probability much larger than 1/2, then the attacker would probably be unable to maintain the balance.

The inability to maintain balance between the two branches in the latter case is due to the fact that after an inevitable random fluctuation, the network will quickly choose one of the branches and abandon the other.

In order to make the Monte Carlo Markov Chain (MCMC) algorithm behave this way, one has to choose a very rapidly decaying function f, and initiate the random walk at a node with large depth so that it is highly probable that the walk starts before the branch bifurcation.

In this case, the random walk would choose the “heavier” branch with high probability, even if the difference in cumulative weight between the competing branches is small.

DDOS & TRANSACTION FLOODING

Transaction flooding occurs when an attacker sends as many valid transactions as possible to saturate the network. Usually an attacker will send transactions to other accounts they control so it can be continued indefinitely.

To counter this attack, each transaction has a small amount of work associated with it, around 5 seconds to generate and 1 microsecond to validate.

This work amount causes an attacker to dedicate a large amount to sustain an attack while wasting a small amount of resources by everyone else.

Nodes that are not full historical nodes are able to prune old transactions from their chain, this clamps the storage usage from this type of attack for almost all users.

OUR LEADERSHIP TEAM

The NOVAM Team has decades of experience in security, government system architecture, networking, data centers, IoT, access control systems and corporate innovation.

Adam Perschke
CEO

A serial entrepreneur, Adam Perschke specializes in corporate technology innovation and business development. His technology innovation consultation includes the U.S. Department of Defense National Security Technology Accelerator, Amazon, T-Mobile, Toyota Connected, and the Association for Unmanned Vehicle Systems International.

Brooks McMillin
Security Operations

A cyber security specialist, Brooks McMillin, has developed and secured custom software with the US Naval Research Laboratory and has worked on internal security and penetration testing with the US Department of Health and Human Services.

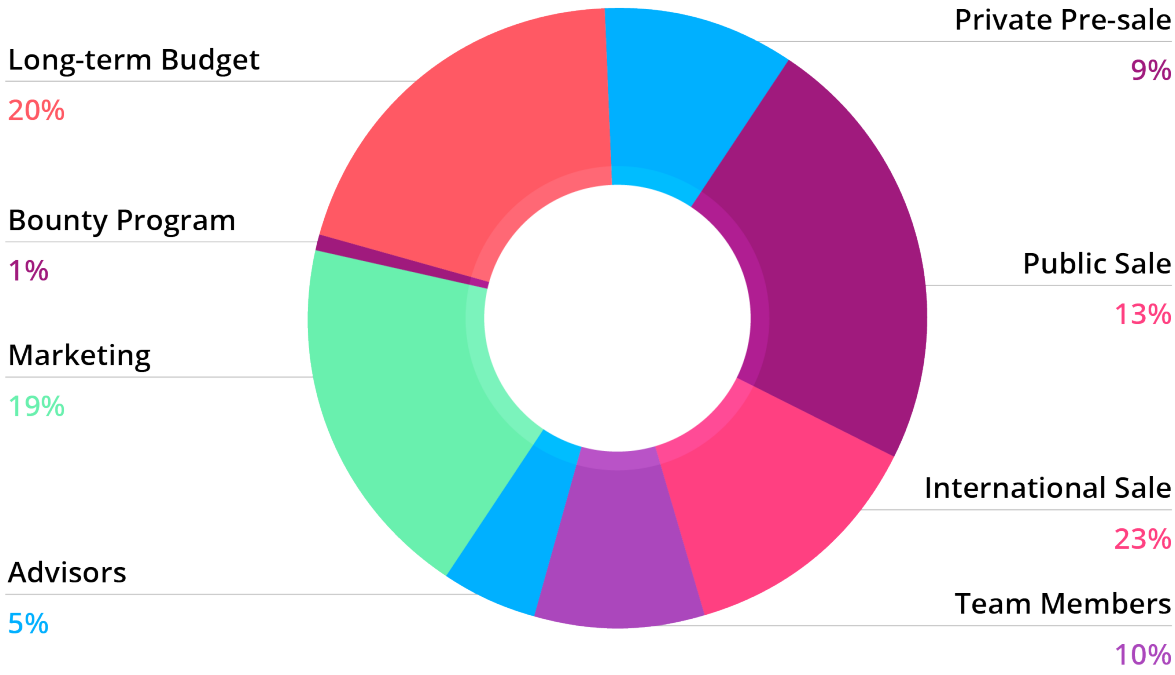
Ian Perschke
Enterprise Architect

A surveillance expert, Ian Perschke ran the digital surveillance system for the city of Chicago, including architecture and oversight of the Chicago Police Department system and other B2G entities. Ian researched, aggregated and streamlined data and video feeds from sister agencies to improve police, fire and emergency response. He was also tapped to become liaison with national law enforcement agencies, including the FBI and Homeland Security for special events around the city.

Ty Bartholomew
Marketing

A communications aficionado, Ty Bartholomew was recruited to build and manage marketing programs, oversee brand management and drive corporate sponsorships. Ty is a seasoned expert at strategic business development and marketing operations.

TOKEN DISTRIBUTION



ROADMAP

2017

Q3 - Ideation & Research

Q4 - Market research with IoT manufacturers

2018

Q1 - Market research, Whitepaper creation

Q2 - R&D, Marketing prep, Advisor consultations, Legal

Q3 - Pre-Sale & Public Token Sale prep, Legal, Marketing campaign

Q4 - Build team, system health check development, bootloader development

2019

Q1 - AI R&D, system health check private testing, additional partnerships, job openings

Q2 - NOVAM TestNet, AI network development, system health check TestNet private partner testing, job openings

Q3 - API build out, Analytics platform build starts

Q4 - Analytics platform and API testing with NOVAM TestNet

2020

Q1 - AI network NOVAM TestNet, beta health check TestNet

Q2 - Rapid expansion to new markets

Q3 - AI Productization, Health Check Productization

Q4 - Marketing increase for new partnerships and clients

APPENDIX

TARGET MARKET BY INDUSTRY

The benefits, use cases, and situational context provided below are to provide an overview of industries, and enterprise and consumer impact malware creates.

Healthcare & Pharmaceuticals

Healthcare and pharma's role in providing preventive, curative, rehabilitative or palliative care service for the global population's health and safety makes the healthcare and pharmaceutical industry high value targets for cyber intrusion.

Market revenues are projected to reach $8.7 trillion by 2020, according to Deloitte. Cyber security costs are expected to reach $65 billion and cybercrime damages will rise to $6 trillion by 2021. The global electronic medical device market alone reached $398 billion in 2017 according to VisionGain.

Even under the strictest compliance and regulation policies, hospitals, health insurers, big pharma, billing credit card processors, and government systems are hacked annually. Millions of personal identifiable information data records are exposed.

Identity theft can slow down the production of life-saving drugs for global distribution. Threats can also divert ambulances, delay emergency care, and prevent doctors from accessing patient records.

Threats to the healthcare and pharmaceutical industries, including personal medical implants and devices, hospital medical machines, drug manufacturing, organization health records and government health records are increasing:

- Wearable medical devices such as pacemakers, defibrillators and insulin pumps have not yet been targeted to cause individual harm. The possibility is plausible, with vulnerabilities detected, which prompted former US Vice President Dick Cheney to have his pacemaker wireless chip disabled. The U.S. FDA recalled half a million pacemakers due to vulnerabilities
- Malware was discovered globally on x-ray, blood gas analyzers, communication devices, cardiac surgery computers, and other medical devices in hospitals, enabling a hacker to cause physical harm, health complications and death
- WannaCry ransomware plagued the world in 2017, infecting and encrypting enterprise servers containing critical information in over 150 countries – plus, the National Health Service in the UK was the hit the hardest with 70,000 devices, including computers, MRI scanners and blood-storage refrigerators affected, crippling health services
- Merck, a pharmaceutical giant, was infected by NotPeyta malware. This led to a shutdown of their factory that produced life-saving cancer, diabetes and hepatitis-C drugs, causing negative global production and distribution for weeks. Estimated loss report rocketed to $310 million due to disruption of worldwide operations, including manufacturing, research and sales. Merck suffered financial, operational and reputational damage

- Anthem, the second largest health insurer in the United States, suffered a breach of 80 million records that included income data, medical IDs, social security numbers, physical addresses, employment information, insurance membership numbers and more

Due to the nature and sensitivity of the information harbored, Cyber-attacks against the healthcare and pharmaceutical industry are relentless.

NOVAM can deploy a health check system for electronics in hospitals, big pharma, healthcare headquarters and other locations to ensure firmware, software and applications are legitimate, and if infected - identify, remove and secure automatically.

NOVAM's Immune System Defense approach on immense networks is designed to protect against threats, external intrusion and insider threat manipulation.

Logistics & Supply Chain

Land, air and sea, logistics and supply chains are critical to our global economy. The global logistics industry is estimated to reach $15.5 trillion by 2023.

Cutting-edge technologies like drones, driverless vehicles and 3D printers will positively impact the logistics industry in the next five years, but it's not without concern.

Weather, internet and satellite connectivity and terminal software updates can cause regular delays, but most concerning is Cyber-threats.

NotPeyta causes billions of dollars in financial, operational and reputation damage across multiple industries.

- FedEx subsidiary, TNT Express, was hit by NotPeyta ransomware, hindering full system activation and land deliveries for three months after the initial attack. Estimated costs peaked at $300 million in financial, operational and reputational damage
- Maersk, the world's largest container shipping business, was infected by NotPeyta and forced to shut down the company and half operations at 76 port APM terminals worldwide, causing upward of $300 million in damage in financial, operational and reputational damage and negatively affecting global shipment volumes for weeks

Logistics companies aren't the only ones affected

Mondelez International, the world's second-largest confectionery company, was infected by NotPeyta and experienced a global IT outage. Investigations, removal and restoration of systems cost $84 million and additional public market reduced revenue, putting the full cost of the incident around $180 million.

The ability to automatically monitor devices to mitigate changes to firmware, OS, and applications can help prevent malware and ransomware from spreading throughout a global network. Immune Defense System can identify new threats in the network that focus on core systems and privileged credentials.

Legal & HR

Cyber-threats consist of more than just attacks to steal personal identifiable information, disrupt operations and cause physical harm.

Intellectual property protection is important for companies innovating with internal research and development and can cause billions of dollars in financial deficit.

Human Resources and legal are the largest custodian of critical personal and corporate data, greatly exposing organizations to attack vectors from phishing emails to browser attacks.

Legal & HR hacks include:

- 2018, nine state-sanctioned Iranian hackers targeted educators, federal and state government agencies, 47 private sector companies in the U.S. and 21 other nations with spear-phishing emails, gaining access to 15 billion pages of intellectual property and stolen data valued at $3.4 billion. The hacker's goal is to obtain, claim ownership and sell for profit
- 2015, the human resource department of the U.S. Office of Personnel Management (OPM) was infiltrated and hackers exfiltrated 21.5 million social security numbers, background checks, names, addresses and birthdays. Further phishing attacks on OPM employees occurred, disguised as identity protection services
- Waymo, an autonomous car company, is suing Uber for stealing 14,000 highly confidential documents and key technology to their self-driving car and systems. An insider threat downloaded the documents, downloaded to an external drive and wiped a company issue computer to hide forensic evidence
- According to the U.S. Commission on Intellectual Property, China is said to be responsible for as much as 80% of all IP theft against US companies

It's important to understand that stolen intellectual property, sensitive data and personal identifiable information can affect companies and governments for decades with addition litigation, investigation resources and future financial projections.

We believe securing IP and HR data starts with self-learning autonomous endpoint and network emersion monitoring and mitigation using Immune System Defense and adding protection for user, device and network authentication and identity on the firmware, operating system and application level.

Energy & Utilities

Energy and utilities uptime are imperative to the success of global economy and critical infrastructure for organizations, governments and daily users.

Interference and sabotage to critical infrastructure, industrial control systems (ICS), and consumer smart meters can cause enormous harm to our economy and to human life.

Ukraine's power grid was infected with TRITON malware in 2015 and 2016, causing city-wide blackouts - preventing commerce, public transportation and critical government systems from remaining online.

2017, Symantec reported in more than 20 incidents. Hackers gained access to US power firms' operational access control and interfaces used to send commands to equipment like circuit breakers. This has the potential to induce blackouts in every major city in America.

Schneider Electric SE's Safety Instrumented System (SIS), used to protect humans, industrial plants and the environment, was infiltrated by TRITON malware. The SIS attack was identified as an insider threat to physical hardware, allowing access to external communication.

The use of sophisticated malware, regardless of physical or remote access, is detrimental to our global ecosystem.

NOVAM can automatically mitigate attacks to hardware, software and applications with our system health checks and provide full network and system security through the Immune System Defense.

Financial Services

The financial services industry has been the most malware-targeted sector for years. This is due to the amount of personal identifiable information (PII) and financial records stored by an organization.

Over a dozen malware variants exist for the financial industry alone, including Gozi (Ursnif), Zeus, Dridex Ramnit, TrickBot, GootKit, Qadars and others. Most are used for institutional cyber-attacks or malware-as-a-service model.

Most malware threats are introduced by simple spear-phishing emails with injection attacks that keep malware hidden. Not all financial services are the result of external threat, but instead insider threat.

Successful major attacks have come in various forms:

- Equifax, a financial and credit reporting company had 145 million U.S consumers and 400 thousand U.K. consumer's personal identifiable information exfiltrated from company servers (2017)
- Korea Credit Bureau, employees copied databases containing 27 million customer details (2014)
- CardSystems Solutions, a third-party payment processor, had 40 million credit card numbers compromised, 14 million issued by MasterCard, by infecting the network with malicious code (2005)
- Heartland Payment Systems, a payment processing firm, responsible at the time for over 275,000 business locations and $80 billion in transactions, exposed more than 130 million credit card numbers to hackers (2008)

Financial services will continue to have adversarial attacks because the information they possess can affect businesses and individuals. The concept of building a wall around the fortress isn't working anymore.

NOVAM understands the need for fortified walls to protect against outsider threats, but with ease, malware from simple spear-fishing, accidental link clicks and other sources has the potential to infect systems and spread rapidly throughout a network.

We want to provide enterprise server protection with our system health checks and our network and endpoint mitigation Immune System Defense.

Media & Entertainment

The media and entertainment industry have experienced increased cyber-threats with intellectual property, including movies, TV shows, video game codes, accounts and more hacked, stolen and then extorted.

With that said, external attacks aren't the only concern. Insider threats, like contractors, are also a liability for publishers.

Notable attacks:

- Sony Pictures was hacked in 2014 exposing confidential information about employees, email conversations and an unreleased movie. Emails and phone systems were paralyzed. All data systems were copied
- WPP, the world's largest advertising agency, was breached by NotPetya ransomware, obstructing global systems and causing financial, operational and reputational damage
- Larson Studios, a post production studio for Netflix and other major TV studios, was compromised. Season 5 of 'Orange Is the New Black' was stolen. Hackers extorted the company. Ultimately, the first 10 seasons were leaked on the Pirate Bay regardless of the payment
- Valve, creator of the Steam Platform, confirmed in 2016 that an average of 77,000 user accounts are hacked every month
- DLH.net was hacked in 2016 with hackers stealing 9.1 million Steam game keys, 3.3 million unique forum credentials, email addresses, date of birth info, names and usernames
- In 2011, the PlayStation Network was hacked. 77 million accounts, including personal identifiable information was compromised. The entire PlayStation network went offline for 23 days, costing Sony $171 million for the outage

The media and entertainment industry use a wide array of internal endpoints, multi-cloud networks and vendors. Add consumer access for TV shows, movies, video games, and mobile applications with individual credentials and an organization's threat index expands on a worldwide level.

The ability to protect user credentials, mitigate unauthorized access, ensure hardware is functioning accurately and enable enterprise systems to protect IP is NOVAM's focus in the media and enterprise industry.

Mining

The global mining industry is enormous with a marketing capitalization of $714 billion and is aimed at exploiting its strategic position in global supply chain.

The use of IoT devices has helped provide mining companies with greater insight on working conditions, safety, autonomous vehicles and predictive maintenance – reducing unplanned and unscheduled downtime.

An example would be a single industrial vehicle used for hauling that may have a 100 wireless sensors.

Cyberthreats have plagued the mining industry from IoT devices, industrial SCACA systems, to corporate networks:

- Goldcorp, one of Canada's largest mining companies, was breached and had 14.8gb of data stolen, including – payroll information, private budget documents, bank account specifics, employee passport scans and more. Data was leaked to public domains for download and viewership
- Detour Gold, a Canadian gold-mining firm, was compromised by hackers. Over 1,300 employee details were exposed, including background checks, social insurance numbers, health card numbers, signatures, addresses and more

According to Trend Micro, the threat landscape in the mining industry will grow as the use of IoT devices increases.

NOVAM intends to service the mining industry with auto-mitigation of endpoint devices globally. Our Immune System Defense will be applied to the entire network and virtualized environments to mitigate attacks attempting to exfiltrate financial or personal information.

Oil & Gas

A report from Siemens & Ponemon Institute indicated that 70% of US oil and gas companies have been hacked. With data compromised and supplies stolen, part of the challenge is how to take adequate action.

Although the oil and gas industry employ 4.2 million people globally and has $2 trillion in revenue, there's an opportunity to increase production, working conditions and reduce costs with the use of IoT.

Recent breaches have exposed confidential information for financial gain and disrupted operational technology (OT). Attacks against industrial control systems have increased.

Thousands of interconnected sensors and controls that run oil and gas facilities allow weak spots and total blind spots – including upstream, midstream and downstream.

The U.S. Coast Guard has reported foreign ships attempting to probe the wireless networks of industrial facilities along U.S. waterways and offshore drilling sites.

Global attacks to date:

- Rosneft, Russia's top oil producer, was hit by a large-scale cyber-attack identified as NotPeyta ransomware, affecting petrol stations and other IT systems
- Saudi Aramco, the Saudi government-owned oil company and world's largest daily oil producer, was breached by NotPetya, affecting 30,000 computers and electronic systems
- PetroChina, state-owned oil giant, was infected by NotPetya. Networks linking internet payments and petrol stations nationwide were compromised for a half day

Ransomware and malware will continue to be a problem for the oil and gas industry in the coming years.

The combination of IoT, pipelines and global networks have enabled the attack vectors to become vast and the security slim.

NOVAM can monitor subtle changes in behavior on the network, measure credential holder's actions and automatically secure intrusions.

Hospitality

As with restaurants and retail, the hospitality industry also uses POS machines to process card transactions for accidental damage holds, food and beverage restaurants, gift shops and services.

These POS systems are vulnerable to malware attacks in the hospitality industry as well.

- InterContinental Hotels Group, owned by parent company IHG, with brands including Crowne Plaza, Holiday Inn, Candlewood Suites and Kimpton Hotels, was infected by POS malware on 1,200 properties worldwide, compromising customer payment card data
- Sabre Hospitality Solutions, a tech company, providing reservation system services for more than 36,000 properties worldwide, was breached, allowing hotel customer payment card data to be compromised. Global hotels affected include Hard Rock Hotels and Casinos, Trump Hotels, Loews Hotels, Kimpton Hotels & Restaurants, RLH Corporation, Club Quarter Hotels, Four Seasons and The Roosevelt Hotel in New York City
- Omni Hotels & Resorts, a Dallas-based hotel company, discovered POS malware at 49 properties, exposing more than 50,000 customer payment card data
- Hyatt Hotels Corporation payment systems were breached again in 2017, exposing payment card data from 41 hotels in 11 countries. China hotels were the most affected
- In 2018, Oracle's MICROS POS system were vulnerable by an insider threat for 300,000 plus payment systems in the hospitality industry. This could lead to organizational compromise, regardless of its size

The hospitality industry utilizes edge devices like POS systems for the front desk, food and beverage, gift shops and more.

Other IoT and mobile devices are becoming standard worldwide for ease of use, reducing costs and optimizing guest experiences, such as traffic flow monitoring, door locks, mobile keyless room entry, smart HVAC and digital surveillance.

NOVAM can protect edge devices with our health check solution, which mitigates malware or unauthorized access, while our Immune System Defense will monitor and secure individual properties and global corporate networks.

Smart Home

IoT devices allow consumers extend their every-day functions manually or automatically by interacting with connected devices.

Connected smart home routers, kitchen appliances, surveillance systems, door locks, thermostats, lighting, vacuums, sprinkler controllers, gas sensors and many more devices make up a home today, but the internet-connected devices may not have malware protection.

Though convenient and cheap, smart home devices come with a caveat; they are vulnerable to a wide array of attacks:

- Mirai botnet, a powerful malware, infected hundreds of thousands of CCTV, DVR and home routers in 164 countries. The botnet Distributed Denial-of-Service (DDoS) attacks took down Dyn DNS provider causing connectivity issues for many companies including, but not limited to, Amazon, Airbnb, CNN, Comcast, DirecTV, Swedish Civil Contingencies Agency, Xbox Live, Swedish Government, Verizon Communications, VISA, Starbucks, PayPal, Heroku and more
- In 2018, VPNFilter, an IoT botnet malware, infected half a million routers and storage devices in at least 54 countries, from router companies Linksys, MikroTik to Netgear and TP-Link. Industrial SCADA systems can be targeted and devices can be disconnected from the internet individually or collectively
- A botnet incorporating over 100,000 devices including routers, multimedia centers, TVs and refrigerator sent 750,000 spam phishing emails to steal credentials, infect machines and cause maximum damage

IoT devices can make our lives easier and help us be more informed about what's happening in and around our home, but without proper protection, we open homes up to cyber-intrusion, potential damage to finances, physical harm and being ensnared in a botnet.

NOVAM intends to protect home IoT devices from malware infections with our health check solution, which in turn protects other aspects of your personal life and businesses in our global economy.

Retail, Restaurants & eCommerce

Technology has enabled stress-free physical and online commerce. Mobile in-app, on web, and wireless in-store payments have enabled zero-friction purchases for every day goods and services.

Due to easily installed malware, point-of-Sale (POS) machines, the hardware used for payment in retail, is the leading cause of card data breaches over the last few years.

POS vendors are bigger targets as well. Malware remotely captures data from each transaction at the register. Retail and restaurants use the same POS machines to accept payments at table-top terminals and free-standing self-service payment kiosks.

Retail and restaurants also use IoT devices for maintenance, monitoring, compliance and security like smart HVAC, refrigerators and digital surveillance.

Beyond POS machines, IoT devices are susceptible to remote and physical intrusion reaching for PII and corporate network access.

Notable intrusions in retail, restaurants, and ecommerce include:

- Target, exposed 145 million personal identifiable information (PII) when a group of hackers infiltrated their HVAC system for access to the network for data exfiltration. The HVAC company was allowed remote access to monitor and maintain systems, which allowed an insider threat scenario. Estimates show Target could face $420 million in damages because of the breach
- Home Depot's Point-of-Sale systems were compromised by malware, exposing 110 million customers' payment card data. The malware, like other POS malware, used RAM-scraping techniques to collect PII from terminals. Home Depot estimated $161 million of pre-tax expenses for the breach
- Cici's Pizza, breached by PoS malware, infected more than 130 locations, and exfiltrated 1.2 million customer payment card data. The malware is said to have been installed by social engineering tricks to allow techs to conduct "support" on POS systems
- Avanti Markets, a self-service payment kiosk vendor, was breached by POS malware exposing 1.6 million customers' payment card data and possibly biometrics, due to a new fingerprint payment method
- eBay was hacked using social engineering and employee credentials to obtain 145 million customer records, Hackers had complete and undetected insider access to the corporate network for 229 days
- Parent company Brinker International, Chili's Bar & Grill restaurants, were hacked by POS malware, exposing an undisclosed amount of payment card data nationwide. Brinker International owns restaurant brands Chili's and Maggiano's and operates in 1,629 locations
- RMH Franchise Holdings, one of the largest Applebee's franchisee, discovered 160 Applebee's restaurants were infected by POS payment and card data stealing malware
- Hudson's Bay, parent company of Saks Fifth Avenue, Saks Off 5th, and Lord & Taylor, reported 5 million customers' payment card data was breach by POS malware and was active for nine months

The list goes on and will continue due to the convenience of online and in-store shopping, restaurant and leisure activities.

Edge devices, like POS systems, HVAC and other smart IoT are standard in the ever-increasing connected marketplace.

An increase in monitoring and maintenance for compliance regulation and innovation in customer experience has expanded cyber-intrusion efforts and attack vectors. As we've expressed in recent past intrusions, it can happen to any organization and in a variety of ways.

NOVAM's edge-device protection health checks can thwart POS malware. We can enable Immune System Defense can protect corporate networks, devices and users from data exfiltration with already existing threats within an organization.

Agriculture & Livestock

According to Markets and Markets, the smart agriculture market is expected to grow to $11.23 billion by 2022. AgTech has become part of our daily food chain.

IoT and connected devices allow farmers and ranchers to monitor and analyze data input and increase production in a sustainable way.

Precise environmental IoT sensors allow for the collection and analysis of data on weather, soil, air quality, water usage and fertilizer amounts. Tractors and other machines are connected to monitor health, autonomous production, and predict maintenance.

Livestock is tracked and monitored for health warnings. Many more innovations will be created for the smart AgTech industry in the future.

The four major cybersecurity threat concerns in smart agriculture are access to services, personal privacy, proprietary information and intellectual property. These cyber-threat concerns are on all the layers of agriculture, from a farmer's property, supply chain, to the data centers and cloud systems storing captured data in silos.

NOVAM's smart system health checks can enable IoT devices to mitigate automated malware and botnet attacks, like Mirai and WannaCry.

The Immune System Defense can protect enterprise against data center, cloud, and unauthorized access from an insider or external threat, covering the AgTech industry from farm to table.

THREATS & INADEQUATE CYBERSECURITY RESPONSE

What ifs are happening now:

- Your mobile phone is compromised by malware, infects an application or operating system (OS) and your personal information (PII) or digital identity, like name, photos, email, passport, credit card among other information is used for fraud or against you
- Your IoT device is infected by malware, permissions get past to your router, home computer or laptop and into other devices attached to your network. This is used to gain access to confidential files and information or to launch an attack on services worldwide in a botnet

- The power grid gets hacked and your country is without power for a week or more hindering economic benefit, crippling enterprise services and can harm or cause loss of life
- Pharmaceutical manufacturers get hacked, you have only a one-week supply left, and your life-saving medicine is weeks away
- You're scheduled for a blood transfusion and the blood refrigerator is hacked. The blood you need goes bad because it's not kept at a steady temperature
- You're driving, your car gets hacked and is instructed to crash into the nearest wall or slam on its breaks to flip the car at high speeds

Mirai Malware

The world witnessed the two of the largest consumer-device Internet-of-Thing (IoT) attacks in recorded history in October 2016. A new strain of malware dubbed Mirai, focused on enslaving household electronic devices from the largest original equipment manufacturers (OEM) of devices such as DVRs, routers and digital closed-circuit cameras was unleashed.

The first attack only infected 24,000 IoT devices but produced a record 620 Gbps DDoS attack against KrebsOnSecurity.com, a prominent security website, taking it offline for days.

Akamai, KrebsOnSecurity DDoS protection provider estimated that the cost of maintaining protection against the attack would have run into the millions if Akamai didn't drop the website from its service.

Akamai couldn't mitigate the attack because it was the largest they'd ever encountered. This attack proved our belief that current mitigation services worldwide aren't ready.

Mirai didn't stop at KrebsOnSecurity.com, which was only a small test. At its peak, Mirai enslaved devices, collectively creating a global botnet controlling more than 600,000 IoT devices.

Larger attacks of higher severity happened only days later. They were focused on Oracle owned Dyn, a large Infrastructure-as-a-Service (IaaS) managed DNS provider.

Mirai successfully attacked and shut down Dyn's infrastructure multiple times with DDos attacks, impacting customers like digital payment processor PayPal, e-commerce giant Amazon, short-term rental marketplace Airbnb, BBC, CNN, Comcast, GitHub, Starbucks, the Swedish Government and many more[19].

[19]Mirai Malware. https://en.wikipedia.org/wiki/2016_Dyn_cyberattack

WannaCry Ransomware

WannaCry, a ransomware was first noticed in May 2017. It infected computers and enterprise servers containing critical information.

It enabled the encryption of all system data running Microsoft Windows Operating System (OS) and demanded ransom payments in Bitcoin cryptocurrency to decrypt data and remove the ransomware.

The ransomware campaign was unprecedented in scale according to Europol, which estimates that more than 200,000 computers were infected across 150 countries.

One of the largest agencies affected by the attack was the National Health Service, a public health service in the United Kingdom. Hospitals infecting around 70,000 devices – including computers, MRI scanners and blood-storage refrigerators.

WannaCry also affected other organizations worldwide such as Boeing Commercial Airplanes, State Governments of India, Hitachi, Honda, Saudi Telecom Company, Russian Railways, PetroChina, Telefonia and many more[20].

NotPetya Malware

Discovered in July 2017, NotPetya is malware that acts like ransomware, but without a payment method and is a variant of Peyta.

Instead of decrypting data once payment is received, NotPetya damages hard drives beyond repair, spreads rapidly and automatically and is intended for massive global destruction of economic systems.

Initially, the attack was caused by a compromise of an accounting software used by 90 percent of Ukraine enterprises and government agencies. Ukraine's[21] Chernobyl nuclear power plant radiation level monitors went offline, subway ticket machines and airport were also affected.

It is said to be the most destructive cyber-attack in history[22]. The total number of companies impacted climbed to 2,000 globally and the total economic and business impact is unknown but estimated to be in the billions.

FedEx subsidiary, TNT Express[23], was infected by NotPeyta, hindering full systems for three months after the initial attack and estimating the ransomware outbreak cost $300 million in lost business and cleanup and repair.

[20] WannaCry Ransomware. https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

[21] NotPetya Ukraine Chernobyl Attack. https://en.wikipedia.org/wiki/2017_cyberattacks_on_Ukraine

[22] Ukraine Cherobyl Attack. https://www.cnet.com/news/uk-said-russia-is-behind-destructive-2017-cyberattack-in-ukraine/

[23] TNT Express. https://www.theregister.co.uk/2017/09/20/fedex_notpetya_damages/

Maersk[24], the world's largest container shipping business, was infected and forced to shut down the company and halt operations at 76 port terminals around the world. This caused more than $300 million in damages. Global business volume was negatively affected for weeks.

TRITON Malware

Triton malware was built to interact with Schneider Triconex Safety Instrumented System (SIS) which is special equipment installed in production lines and other industrial setups and targets Industrial Control Systems (ICS).

SIS reads data from industrial equipment, such as factory values, robots, motors, machinery and other important infrastructure and controllers read data streams to make sure industrial equipment works between certain parameters.

If data deviates from a predetermined safety margin, the Safety Instrumented System controller takes a set of actions, which can include an entire shut down of a factory or production line. If infected, machines can run under approved unsafe parameters or prevent safety mechanisms from executing their intended function, potentially causing harm or loss of life.

Previous ICS malware has been used to target and destroy uranium enrichment centrifuges in Iran and disable Ukraine's electrical power distribution. Simple consumer IoT devices lacking security cause major crashes to important services – worldwide and daily.

NOVAM plans to work with OEMs, IoT manufacturers and Fortune 500 companies to secure the software and hardware of devices with cryptographic health checks. This will help ensure that devices are not infected with malware or ransomware and mitigate in issues in real-time.

DATA BREACHES

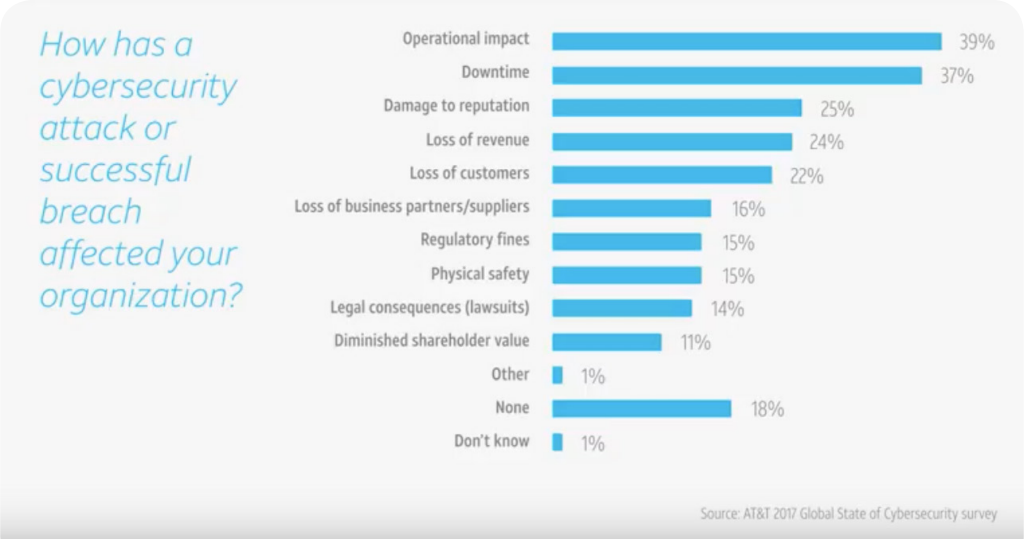
According to Gemalto[25], although in 2017, 2,600,968,280 records were breached globally, only 1,765 breaches were reported. An astounding 400 percent increase of attacker-run vulnerability scans against IoT devices was reported in 2016 by AT&T[26]. This sparked a newfound concern with IoT and endpoint security globally.

A data breach can cause damage to an organization in many ways, with the most prominent being operational impact, downtime, damage to reputation and loss of revenue and customers. Breaches can harm organizations for future financial quarters and years to come.

[24] Maersk NotPetya. https://www.theregister.co.uk/2017/08/16/notpetya_ransomware_attack_cost_us_300m_says_shipping_giant_maersk/

[25] Gemalto Breach Level Index Report 2017. https://breachlevelindex.com/assets/Breach-Level-Index-Report-2017-Gemalto.pdf

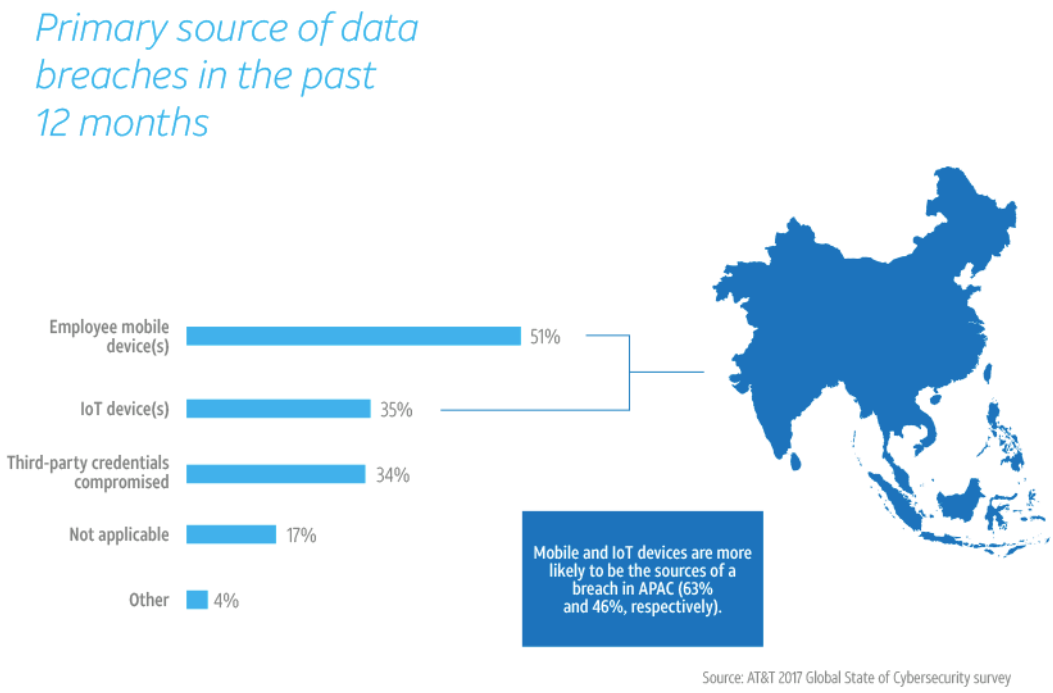
[26] AT&T IoT Vulnerability Scans. http://about.att.com/story/new_research_email_traffic_could_be_malicious.html



BYOD is now common in the workplace, but it creates a challenging landscape to protect against threats.

The primary sources of data breach are employee mobile devices, IoT, and third-party credential compromise, according to AT&T[27].

The increase of employees, third-party contractors, and IoT devices in an organization often comes with an increase threat level.



[27] AT&T 2017 Global State of Cybersecurity. https://www.business.att.com/cybersecurity/archives/v6/

In 2017, global malware infections were the most expensive type of cyber-attack. On average they cost $11.7 million per incident, according to a study by Accenture & Ponemon Institute[28].

Growth of cybercrime costs continue to increase year-over-year due to prevalent attacks on individual users, devices and networks.

Cybercrime is expected to cost global organizations $6 trillion by 2021, according to a Cybersecurity Ventures & Herjavec Group[29].

[28] Accenture & Ponemon Institute: Cost of Cyber Crime Study. https://www.accenture.com/t20171006T095146Z__w__/us-en/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf#zoom=50

[29] 2017 Cybercrime Report. https://1c7fab3im83f5gqiow2qqs2k-wpengine.netdna-ssl.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf


NOVAM