Empowered Government and Public Sector Innovation

Big data, IoT, business process management, and sophisticated monitoring aim to reduce risk and improve security, resource management, and decision making at all levels of government and public transportation.

Introduction

In many ways, a perfect storm has been brewing in the physical security space for quite some time. Owners and administrators of IP security systems face ever-growing resource demands and are experiencing significant management and support challenges daily. Converging threats and burdensome complexity continue to menace organizations that are simply unprepared to face such threats. While IT professionals often focus on data protection and headline-grabbing cyber threats, security professionals must do what they can to protect property and people as well as ensure secure access and maintenance of high-value video.

Meanwhile, the dizzying pace at which organizations adopt emerging technologies continues to generate new challenges. Security professionals are faced with safeguarding overly cumbersome infrastructure with fewer resources. These expanding responsibilities are simply outpacing the ability of resources to respond to and control threats. In addition, technology and resource gaps are allowing preventable security breaches and failures to occur, exposing organizations to both known and unknown threats.

Now, more than ever, it is imperative that security and IT teams collaborate and innovate. A holistic approach must be taken to manage and secure the corporate IT and security networks. Every organization needs a deliberate, organized approach to IT infrastructure that addresses these gaps without adding more people to the payroll.

Top 3 Key Issues Facing Government and Public Sector IT and Security Teams

Scary Fact: Did you know that on average 3%-5% of security devices on unmonitored security networks are offline, misconfigured, or malfunctioning, and NO ONE knows about it?

1. Sensitive Data

Every day across the nation security teams along with local police and fire departments are responsible for the overall safety and transportation of the public. In addition, authorities and public institutions must manage sensitive data of their citizens. All these teams must consistently be ready for action.

Firewalls, virus scanners, and backup systems are the standard building blocks of an integrated security concept. Add to that physical security, and now you need surveillance equipment, access control, and communication devices, along with backup systems. Now, shouldn't you also ensure that all these systems also work reliably?

A comprehensive monitoring solution can and should include all these factors in the monitoring process.

2. Many distributed locations

The best approach to monitoring IT and Security networks is to deploy software designed to continuously collect health and performance data on all IT infrastructure at every location. Then have it send the data in an encrypted form to a central instance that is responsible for the complete evaluation and storage of data. This keeps costs low and expenses for operation and maintenance manageable, while at the same time ensuring IT and Security networks are centrally monitored.

3. Heterogenous IT landscapes

Integration of locations, hardware, and software, are heterogenous. Devices and applications offer their own monitoring tools and insight; however, they contribute little to an overview of the entire IT environment. This calls for a universal solution that can monitor devices and applications independently of manufacturers as well as integrate special solutions into the overall monitoring process. The decisive factors here are, on the one hand, the standardization of the solution in order to keep the costs low and, on the other hand, the flexibility to connect existing special solutions via suitable interfaces.

How monitoring enhances security and technical possibilities

Identify the right monitoring solution

Both internal processes and citizen services highly depend upon a high-availability and high-performance network. In addition, security teams need to have assurance that all of their security systems are online and operational. In order to guarantee this, IT and security teams need the appropriate information. Network monitoring is the information provider. But not every tool meets these special requirements. A thorough evaluation is necessary to determine the safest most appropriate monitoring solution which covers the needs of IT and physical security.

Here's what to consider before introducing an overall monitoring solution.

Independence

Independence is the gold standard for effective monitoring, and in terms of government, this primarily refers to local autonomy (when there are numerous locations of authorities and governmental organizations) and vendor independence. These problems have to be solved with reasonable effort and within a feasible budget; support for common standards is a given.

Reliability and expandability

No aspect of government IT is as important as security or reliability; monitoring critical systems should be error free, protect sensitive data, and help ward off attacks. The extensibility of individual solutions and integration via API rounds up the picture. You should be given the tools that are the most secure for your individual needs.

Long-term data

Historical data not only helps to selectively approach network optimization with regard to relevant problems, but also in the long term, with a defined mission. The possibility of advanced monitoring of a government or public authority network makes it possible to not be distracted by current problems and to not lose sight of the big picture.

Costs and licenses

Let's face it, the public sector has to justify every expenditure. Low-cost models are much more attractive, especially if they don't lack in functionality, reliability, or services. Accordingly, a monitoring solution for government IT should have a licensing model that is low in cost, always transparent, and without high ensuing costs.

Vunetrix Network Monitor

Perfect for monitoring government IT and physical security assets in the public sector.
Includes all features required for monitoring in the field of government.

Many locations. No worries.

Location flexibility must be a top priority in monitoring government and public sector IT, because hardware and software diversity is the name of the game: A wide variety of different products must be dealt with, monitored, and managed. The Vunetrix API and custom sensors allow the solutions and components of individual sites to be easily integrated into the central monitoring solution while at the same time, the solution keeps costs low thanks to a high degree of standardization.

Be alerted when it matters.

The setup and functionality of data transmission, analysis, storage, and publishing in government and public sector IT is somewhat identical to a classic IT network. Vunetrix users can define thresholds to trigger notifications before outages or failures occur. You can decide how to receive notifications: via email, push notification, or SMS, for example. The notification feature is of great value because you can immediately see where the issue is.

Data protection and security

Let's not forget the issue of security in government and public sector IT monitoring: Vunetrix monitors all types of security tools from firewalls to virus scanners to backup systems as well as any IP-based physical security device. It adds a very high level of security by revealing unusual activity that might be an indication of a malware attack. Vunetrix does its job 24/7 without fail and makes sure that all public operations run smoothly, that all security devices are performing properly, and that all data is protected.

Two Deployment Options

Cloud-based Performance Monitoring Software

Vunetrix has a patented, cloud-based app (Vunetrix Network Monitor) which continuously checks networked systems, servers, storage, end points, and power supplies to ensure everything is working at all times. Continuous device health checks and instantaneous notifications lets you know immediately when there’s a problem. This way you can fix small problems before they become BIG problems. You can also proactively identify device issues and fix before failure and before a security event occurs.

On-premises Performance Monitoring Software

Vunetrix, on-premises software is ideal for air-gapped or closed networks. Just like the cloud-based software, Vunetrix continuously checks networked systems, servers, storage, end points, and power

supplies to ensure everything is working at all times. With on-premises software you achieve full software functionality regardless of network design.

Key Operational Benefits

Advanced Diagnostics
Vunetrix advanced diagnostics feature allows you to determine the nature of any device issue quickly. You know in an instant what the problem is, where the problem is and can schedule timely onsite service and repairs with a “First Trip Resolution Promise”.

Inventory Management
Vunetrix drives better business and security infrastructure decisions for your organization’s capacity planning and system performance. With accurate fault and performance trending data available from the performance monitoring software, capital expenses to replace failing equipment or devices which are beginning to act erratically prior to failing can be identified and replacements budgeted with hard data backup.

Operational Cost Reduction
Government agencies enjoy up to 70% operational cost reductions when manual checking of security devices is 100% automated. Vunetrix automates time-consuming tasks and delivers real-time, holistic visibility to your mission-critical devices. With the correct alerts, your security team can expect to use fewer resources to ensure their companies’ security system is operational and functioning with optimal performance.

Reduce Camera Downtime
Continuous health checks mean you know in an instant when there’s a problem with a camera. You can take immediate steps to resolve the problem and assure all cameras are working when a security incident occurs.

Ensure Security System Uptime
Heath monitoring software allows you to maximize your security system uptime. Having all the data on a single dashboard provides you with instant visibility to assess and diagnose operational issues. Vunetrix provides the answers for quick and effective responses.

Video Evidence Quality Guarantee
Vunetrix ensures that surveillance cameras are online and functioning normally. Vunetrix confirms that video streams are sending appropriate levels of data. The software also warns if and when networks are behaving abnormally and could potentially fail or have already failed, assuring quality video evidence is available when needed for investigation.

Strategic Principals for Securing the Internet of Things Department of Homeland Security

(Note: some content in this next section has been inserted using exact language from the DHS White Paper, "Strategic Principals for Securing the Internet of Things, 2016".)
https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

To begin with, there is no easy button. In addition, there is no silver bullet either. Layered security best practices help you to achieve optimal security and mitigate security risks. However, organizations must also take on the responsibility of identifying and enforcing rules and procedures for all individuals using the organization's IT assets and resources.

Incorporate Security at the Design Phase

Security at the design phase, what exactly does this mean?

Design with system and operational disruption in mind. Understanding what consequences could flow from the failure of a device will enable developers, manufacturers, and service providers to make more informed risk-based security decisions. Where feasible, developers should build IoT devices to fail safely and securely, so that the failure does not lead to greater systemic disruption.

Also important is complete separation of the corporate IT network from the security network through the use of Physical or Virtual LANs. It is of utmost importance to establish a clear boundary and partition each business units' network. Placing advanced next generation firewalls between each network also can drastically reduce a cyberattack on the corporate network originating from any IoT device connected to the security network such as a camera or switch. It is also necessary to assure attack vectors are closed which could originate from the corporate IT network into the physical security network.

Advance Security Updates and Vulnerability Management

Botnets operate by continuously scanning for IoT devices that are protected by known factory default usernames and passwords. Since strong security controls such as making the industrial consumer deliberately disable rather than deliberately enable complex passwords have yet to be built, organizations must have specific rules and policies around usernames and passwords for IoT devices and all security systems. Recommended are hard to crack passwords accessed from password vaults like Last Pass, RoboForm, or NordPass. Continuous password rotation is also important and should be considered monthly or at least every quarter.

Multi-factor authentication is another method for protecting unwanted access to any device or system by a nefarious or ill-intentioned individual. These can be generated through email, SMS, authentication apps, and more.

Ensure that software and firmware updates are performed in a timely manner. Never automatically push firmware updates on a camera, system, or any other IoT device. Updates should be checked for bugs and compatibility. And it's always advisable to check camera firmware compatibility with your VMS, lest you cause a complete failure of your surveillance network.

Build on Proven Security Practices

Start with basic software security and cybersecurity practices and apply them to the IoT ecosystem in flexible, adaptive, and innovative ways. Refer to relevant Sector-Specific Guidance, where it exists, as a starting point from which to consider security practices.

Logging system access is a good method for identifying who's in the system/s and for how long. Requiring unique usernames and passwords for each individual who is granted access is one way to achieve this.

Use hardware that incorporates security features to strengthen the protection and integrity of the device. For example, use computer chips that integrate security at the transistor level, embedded in the processor, and provide encryption and anonymity.

Many IoT devices use Linux operating systems, and many may not use the most up-to-date operating system. Using the current operating system ensures that known vulnerabilities will have been mitigated.

Prioritize Security Measures According to Potential Impact

Know a device's intended use and environment, where possible. This awareness helps developers and manufacturers consider the technical characteristics of the IoT device, how the device may operate, and the security measures that may be necessary. Perform a "red-teaming" exercise, where developers actively try to bypass the security measures needed at the application, network, data, or physical layers. The resulting analysis and mitigation planning should help prioritize decisions on where and how to incorporate additional security measures. Identify and authenticate the devices connected to the network, especially for industrial consumers and business networks. Applying authentication measures for known devices and services allows the industrial consumer to control those devices and services that are within their organizational frameworks.

Promote Transparency across IoT

Conduct end-to-end risk assessments that account for both internal and third-party vendor risks, where possible. Developers and manufacturers should include vendors and suppliers in the risk assessment process, which will create transparency and enable them to gain awareness of potential third-party vulnerabilities and promote trust and transparency. Security should be readdressed on an ongoing basis as the component in the supply chain is replaced, removed or upgraded. Consider creating a publicly disclosed mechanism for using vulnerability reports. Bug Bounty programs, for example, rely on crowdsourcing methods to identify vulnerabilities that companies' own internal security teams may not catch. Consider developing and employing a software bill of materials that can be used as a means of building shared trust among vendors and manufacturers. Developers and manufacturers should consider providing a list of known hardware and software components in the device package in a manner which is mindful of the need to protect intellectual property issues. A list can serve as valuable tool for others in the IoT ecosystem to understand and manage their risk and patch any vulnerabilities immediately following any incident.

Connect Carefully and Deliberately

Advise IoT consumers on the intended purpose of any network connections. Direct internet connections may not be needed to operate critical functions of an IoT device, particularly in the industrial setting. Information about the nature and purpose of connections can inform consumer decisions. Make intentional connections. There are instances when it is in the consumer's interest not to connect directly

to the Internet, but instead to a local network that can aggregate and evaluate any critical information. For example, Industrial Control Systems (ICS) should be protected through defense in depth principles as published by https://icscert.us-cert.gov/recommended_practices. Build in controls to allow manufacturers, service providers, and consumers to disable network connections or specific ports when needed or desired to enable selective connectivity. Depending on the purpose of the IoT device, providing the consumers with guidance and control over the end implementation can be a sound practice.

Department of Homeland Security Best Practices. How does Vunetrix measure up?

As with all cybersecurity efforts, IoT risk mitigation is a constantly evolving, shared responsibility between government and the private sector. Below is a summary of Vunetrix efforts to comply with the Department of Homeland Security's Best Practices for IoT devices.

Vunetrix is the ideal monitoring solution for physical security networks and IoT devices while also serving the requirements of the corporate IT network. Considering that Vunetrix has hardening methodologies built into the software and that it is purpose-built for physical security systems, it is the ideal software solution for monitoring government and public sector networks.

Vunetrix Network Monitor is a software application which monitors the health and performance of IT devices. The software features include a SMART Dashboard, Geo-mapping, as well as continuous device health and performance checks. The application uses open IT protocols to collect data from devices and allows for custom API integrations with other security software products.

There are marked vulnerabilities when software and software updates are automatically deployed and installed. A recent breach from a well-known monitoring software manufacturer proves this fact. For these reasons, Vunetrix has always manually distributed software and software updates in all cases, every time.

Vunetrix also allows you to assign different permission levels, i.e., view only vs. administrator, as well as unique usernames and passwords for each system user. In addition, Vunetrix gives you the ability to view only those part of the network which are necessary for your responsibilities while allowing master users to manage and view the entire network through a single-pane-of-glass.

On-premises multi-factor authentication software access can be achieved through email and SMS methodologies. While hosted software multi-factor authentication can be achieved through the use of Azure virtual servers.

Vunetrix takes a security through obscurity approach and only uses one unique and unknown port to send device and system health and performance data through. In addition, further security is achieved by creating an ACL (Access Control List) for the unidentified port and allows it to only send destination traffic to a single source/destination also requiring the port to drop traffic originating from any other outside sources.

The Vunetrix software does not require a change of firmware on any IoT device. In fact, Vunetrix simply collects health, performance, and fault data using read-only protocols. These protocols include SNMP

(v1, v2c, and v3), ICMP, WMI, HTTP/S, SSH, SOAP, NetFlow, jFlow, sFlow, IPFIX, IMAP, POP, SMTP, as well as a RESTful API and API. Health and performance data is encrypted at rest and in transit using US Military Standard AES 256-bit encryption.

Vunetrix software is manually Penetration Tested monthly by ethical "white hat" hackers, techniques, and state-of-the-art-tools in order to assure nefarious individuals cannot breach our systems, data, or network. Every month our partner tests data security defense across the unknown port, networks, applications, and endpoints. Any potential impact or vulnerability is immediately reported and mitigated.

Vunetrix uses highly secure and when required Tier 4 Hosted Data Centers. At a minimum, Vunetrix data centers provide N+1 redundancy or greater across all the major infrastructure systems including Generators, UPSs, Chillers, and Air Handlers, minimizing single points of failure, and maintaining proper floor loading. Most importantly, Vunetrix data centers adhere tightly to internally developed technical change management processes to maintain the uptime of the data centers. Each data center related preventive maintenance is carefully planned, reviewed, and approved prior to work being started. Additionally, strong partnerships with maintenance contractors ensure the quality of their work reflects a commitment to 100% uptime. Our data centers deliver a consistent service level of 99.999% globally.

Conclusion

While the benefits of IoT are undeniable, the reality is that security is not keeping up with the pace of innovation. As we increasingly integrate network connections into our nation's critical infrastructure, important processes that once were performed manually (and thus enjoyed a measure of immunity against malicious cyber activity) are now vulnerable to cyber threats. Our increasing national dependence on network-connected technologies has grown faster than the means to secure it.

The biggest challenge is the IoT ecosystem which introduces risks that include malicious actors manipulating the flow of information to and from network-connected devices or tampering with devices themselves. Each of these concerns can lead to the theft of sensitive data and loss of consumer privacy, interruption of business operations, slowdown of internet functionality through large-scale distributed denial-of-service attacks, and potential disruptions to critical infrastructure.

Since it's not likely for organizations to reverse innovation and go back to analogue devices and systems, it's imperative we do everything we can to protect our networks. The time is now to address the security of IoT devices and at the same time ensure that everything connected to our networks is operating as intended. The only way to achieve this goal, is to deploy monitoring software on the network and to incorporate all the strategic principals for securing the Internet of Things as advised by the Department of Homeland Security into your daily best practices.

For more information regarding the Strategic Principals for Security the Internet of Things, visit the Department of Homeland Security Website at *https://www.dhs.gov*.