White Paper

The Importance of Comprehensive Asset Discovery and Network Insight for Cybersecurity

Sponsored by: Forescout

Pete Finalle Carlos Gonzalez
December 2023

IN THIS WHITE PAPER

The Internet of Things (IoT) and connectivity growth are rapidly increasing. The COVID-19 pandemic shined a light on how digital transformation is essential. Organizations that had established connected infrastructure, cloud services, and data management were able to excel and maintain operations.

Organizations across all verticals, from industrial operations and manufacturing to city infrastructure and agriculture, are investing in IoT networks and connected devices. The influx of data and innovations in the field of artificial intelligence will help drive a new level of productivity and efficiency for operations.

However, with this new rise in connectivity comes the threat of cyberattacks. Organizations are realizing that the lack of visibility across the network and the potential security gaps can disrupt service and create potential harm. Organizations have some combination of information technology (IT), industrial IoT (IIoT), and operational technology (OT). These are fundamental components of the modern, interconnected enterprise attack surface, which must wholistically be secured.

It is challenging to secure what you are unaware of, and while IT environments are well defined, IoT and OT environments can be nebulous. Modernizing and hardening the entire ecosystem is a journey that starts with understanding and unshrouding under-secured environments through enhanced visibility. A clear picture of the number and type of assets connected across the hybrid ecosystem and contextual information to further identify their purpose can help build a device identity, which is essential for segmentation and security enforcement. However, bridges between environments are not limited to technologies alone. While security tools can be used for discovery and management, interdepartmental working relationships must be forged, with security professionals sharing reports and data and engineering professionals sharing operational knowledge.

This study focuses on the importance of asset discovery. As IoT networks introduce new connected devices into a company's ecosystem, new threat vectors are also created. Every connected asset on a network that is not up-to-date, is missing antivirus software, or lacks login credentials is a possible point of entry for a cyberattack. Asset discovery and management can help organizations secure their assets from vulnerability. With asset discovery, so too will a change of culture arise. Companies must develop new protocols and standardized best practices, train employees, and hire new personnel to maintain security for their IoT networks.

December 2023, IDC #US51504123

TODAY'S THREAT LEVEL OF A HYBRID IOT ECOSYSTEM

Growing IoT Infrastructures

The COVID-19 pandemic in 2020 accelerated the adoption of the IoT environment as it became essential for organizations to stay in business. IDC predicts that by 2027, there will be 57 billion connected IoT devices (or "things").

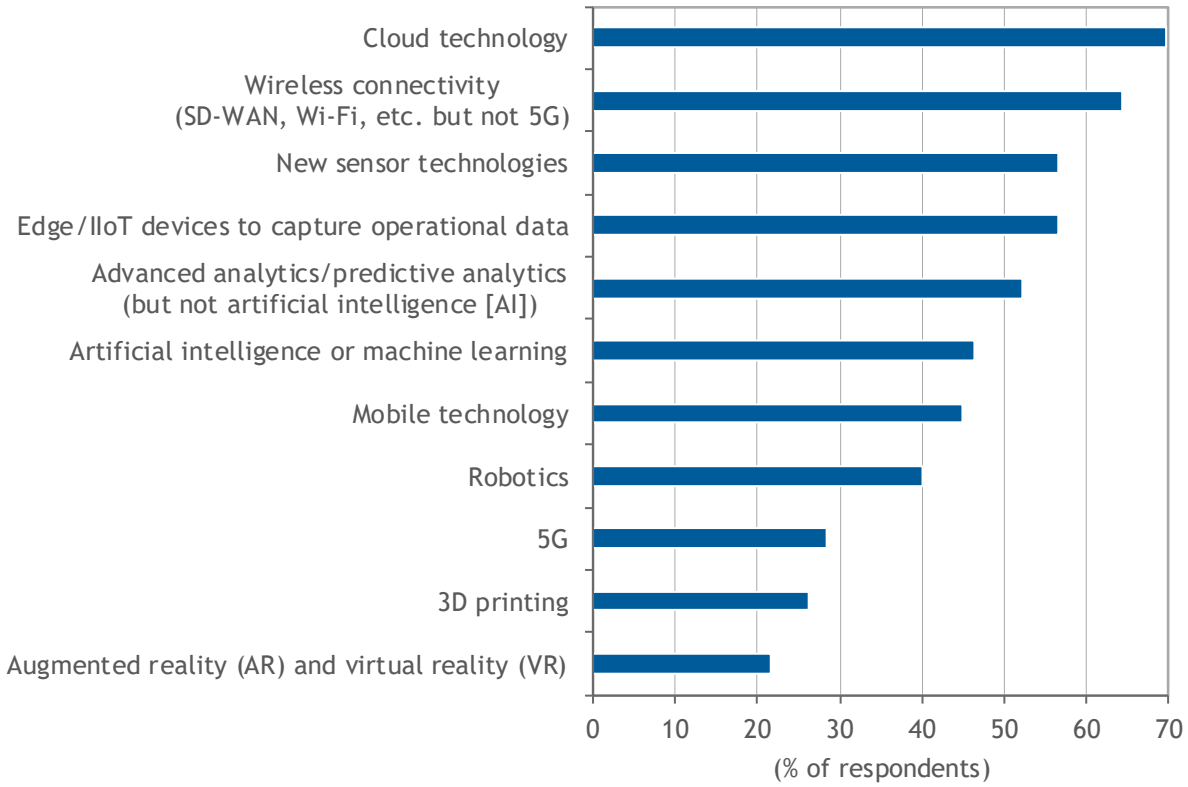
IDC's 2022 *Future of Operations Survey* reported that respondents who embraced digital technology were more likely to improve operations. The survey showed that 49.3% of respondents claimed that digital technology and data have been central to improving operations since 2020.

As a result, investment into a digital IoT environment is ramping up. According to IDC's 2023 *Future of Operations Survey,* 42.5% of respondents have IoT projects in production and have shown a return on investment (ROI). The survey shows that 63% have realized paybacks on their IoT initiatives. The survey also showed that respondents listed cloud technology, wireless connectivity tools, and IoT devices as top investment priorities for their organizations (see Figure 1).

FIGURE 1

Future Investment in IoT Technology Solutions

Q. Over the next three years, in which of these technologies and tools is operations planning to make significant new investments?



n = 750

Source: IDC's *Future of Operations Survey,* 2023

This increased investment into IoT projects has resulted in larger IoT networks with thousands upon thousands of connected devices. According to IDC's 2022 *Security Services View Survey,* 56% of organizations have a multicloud environment with various IoT-connected devices. IDC estimates an organization must deal with, on average, five multihybrid environments, including public cloud and on-premises private cloud environments.

As a result of expanding IoT networks, there has been an increased threat of cyberattacks, which plagues heavy on the minds of C-suite executives. IDC's 2022 *CEO Survey* showed that 52% of CEOs rank cybersecurity threats as the most important among executive board priorities. The survey found that security technologies are the highest priority in digital spending.

Hybrid Ecosystems and Security Complexities

While increasingly interconnected, IT, IoT, and OT networks have combined to create a heterogeneous environment with dissimilar security postures and subsequent levels of risk. IT environments are typically the most secure and have had a head start for at least two decades to develop best practices, software solutions, and infrastructure to protect from attacks. However, IoT and OT environments have not received the same attention over the years, and security professionals are still developing their tools and best practices, creating new vulnerabilities. The majority of issues arise from the need for more visibility across the network.

Depending on the technology and operational area, some of these devices are more than 20 years old or are simple sensing devices that lack the proper security configuration, making them vulnerable to outside attacks. Forescout's report, *The Riskiest Connected Devices in 2023*, listed the following connected devices as the most vulnerable:

- Computers, servers, and routers in IT
- Printers, IP cameras, and VoIP in IoT
- UPS, programmable logic controllers (PLCs), and building automation in OT
- Healthcare workstations, imaging devices, nuclear medicine, and patient monitors for the Internet of Medical Things (IoMT)

The report showed a significant increase in common vulnerabilities and exposures (CVEs) since 2022. According to Forescout's research, 16,556 new vulnerabilities were published, an average of 78 new CVEs per day or 2,365 per month from January to July 2023. That is 2,220 more than in the same period last year, an increase of 15%. Of the 4,000 vulnerabilities found by Forescout that affect devices, 78% affect IT devices, 14% affect IoT, 6% affect OT, and 2% affect IoMT.

These vulnerabilities exist due to devices' software being out of date, and access is unrestricted. Legacy devices that run older versions of the Windows operating system, for example, continue to run and manage several assets on the network. Legacy operating systems lack the antivirus software, firewalls, and security authentication needed for today's networks. Forescout reports that for OT and IoMT environments, 63% and 35% of devices are running Windows legacy versions, respectively.

The Human Factor

One of the consistent issues in dealing with cyberattacks and securing an organization is the need for more skilled and expert cybersecurity professionals. According to IDC's *Security Services View Survey,* 49% of respondents indicated significant skills gaps within their organization. At the top of the list of needed skills by security domains is cloud security at 33%, data management at 23%, and security analytics and intelligence at 22%.

The lack of security skills is only expanded by the need for more communication between IT and other network areas. Security professionals have years of experience developing best practices to secure their networks. However, OT and IoT areas are still developing their protocols on how to secure their devices best. IT security teams focus on data breaches and ensuring data integrity and security. OT/IoT operators must ensure that there is no disruption to services. Their main focus is to continue operations no matter the cost. The stoppage of operations not only means the loss of productivity but also means a potential safety risk to personnel.

The challenge in securing connected assets will only progress with top-down change management strategies and integrated IT/OT organizations that focus on identifying hardware assets comprehensively along the network. Ensuring that the assets are monitored and maintained effectively is the promise brought forth by having an effective asset detection and management system.

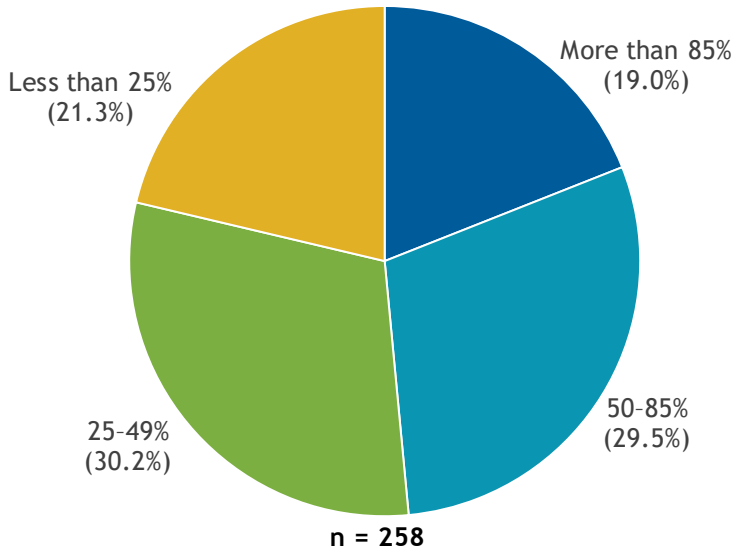
VISIBILITY FOR SECURING DEVICES AND TRAFFIC

The Lack of Network Visibility

Visibility is one of the key concerns for protecting both new and existing devices on the network. Without a complete inventory of existing assets that need to be secured and a firm grasp on new equipment, security infrastructures are faced with the challenge of securing the unknown. According to Forescout, organizations are only aware of 70% of actual devices on the network, and the lack of visibility is only getting worse as remote work increases. IDC's 2023 *Cybersecurity Capabilities Assessment Framework (CCAF) Survey* highlighted that for the professional services industry, 40.5% of respondents said their businesses do not systematically monitor or scan remote endpoints, and 26% of all enterprises have no remote endpoint monitoring or scanning processes. The study concluded that off-premises connected network devices such as laptops, smartphones, and other devices that allow for remote access are likely among the weakest security links in a company's infrastructure (see Figure 2).

FIGURE 2

Data Analytics Drives Increased Security Efficacy



Note: For more details, see *Top Enterprise Cybersecurity Shortcomings, 2023* (IDC #US51295323, October 2023).

Source: IDC's *Cybersecurity Capabilities Assessment Framework (CCAF) Survey,* 2023

The *CCAF Survey* also highlighted that companies that use analytical data methods such as logs and metrics to identify anomalies need to catch up. According to the survey, more than 90% of businesses

surveyed employ data analytics for cybersecurity purposes, 21.3% claim to monitor and analyze fewer than 25% of all available network logs and metrics, and approximately 10% that do no analysis.

Asset Visibility and Security Integrations Can Transform Security Posture

Advanced network visibility capabilities are essential to any modern network security stack and necessary for governing access, segmenting networks, and enabling other security tools. Having detailed visibility, identification, and classification data on assets and their respective traffic gives insights into which devices require connectivity to specific assets, how logically to segment a network, and what anomalous behavior can be observed from devices, as well as information on device status, version, and configuration.

Network access control (NAC) has evolved significantly since its inception, maturing past its roots as a powerful security tool that was hampered by a high degree of difficulty in implementation or use. Modern NAC solutions add versatility and ease of use through a combination of network monitoring and network probing techniques to discover, classify, and assess endpoints without requiring network infrastructure changes or endpoint agents in many cases.

Modern NAC's visibility capabilities can also amplify the effectiveness of the entire security stack by extending meaningful security policy and enforcement to devices that were either previously undiscovered or lacked sufficient contextual information. Additional benefits of NAC's visibility capabilities to security professionals include the following:

- Providing a significantly enhanced view of the attack surface for the entire corporate ecosystem (This also includes an improved understanding of the security posture and potential vulnerabilities.)
- Discovering valuable information that can be used to guide configuration changes, security policy creation, and new product purchases to increase security posture (Knowing what exists, what isn't secured, and what needs to be secured should be the first step for any business looking to modernize or harden its security.)
- Actively monitoring and assessing ecosystem changes and additions that can provide accountability and security for new devices as they enter the ecosystem (Understanding future changes and anticipating security challenges before they are exploited allow for a more proactive approach to securing the unknown.)

In IDC's primary research, customers expressed frustration with a general lack of visibility and understanding of their own network environments and the devices connected to them. Deploying and updating new and existing network security capabilities has a stunted impact if they are essentially thrown into the dark, with the expectation of increasing cybersecurity readiness. After deploying NAC and completing basic asset discovery and visibility tasks, customers were provided with significantly improved clarity and understanding of their ecosystem and security risks. This led not only to configuration changes and tighter firmware control, which immediately and effectively increased security posture, but also to new playbooks and protocols to handle potential threats.

NAC Visibility Capabilities Are Essential for Modern Zero Trust Security Initiatives

Modern businesses are pressured to adopt a number of zero trust–oriented approaches and new technologies, like SASE and ZTNA, to improve their security posture. At the same time, most need an adequate view of what they are attempting to secure. Without adequate visibility into devices and traffic within the corporate ecosystem, concepts like zero trust cannot be truly achieved, leaving significant gaps in protection throughout the corporate environment. Zero trust effectively incorporates three network security approaches, and while ZTNA protects users and micro-segmentation protects workloads, NAC is a necessity for protecting devices.

While hybrid work and multicloud adoption are accelerating the need for network security capabilities outside of the traditional network perimeter, the convergence of IT, OT, and IoT is creating new demand for on-premises security. Businesses are increasingly looking at security for the entire enterprise, from user devices to sensors in the field, a holistic approach that requires tools that can effectively bridge multiple gaps between unique environments. This has business benefits that stem from consolidation and maximizing the efficiency of security personnel and security efficacy benefits, which improve the security posture for the entire business.

Business factors influencing the consolidation of security products across unique environments include the following:

- Most businesses cannot afford to have separate security teams and professionals managing separate IT, OT, and IoT security products and tools. Security professionals are a finite resource and subsequently expensive, necessitating the need to centralize and consolidate as much of the security stack as possible to maximize efficiency.
- Cybersecurity purchases typically come down to the CISO, and consolidated products across network environments carry a better ROI than multiple products to do the same thing. In addition, with fewer tools to learn, security professionals gain a higher level of familiarity and proficiency, which can directly impact security efficacy.
- Modern business ecosystems increasingly require a consistent security posture across all assets and networks, whether in the cloud or a manufacturing facility. A single product that crosses all domains streamlines this security process and increases consistency across all networks and devices.

Security capability factors influencing the need for visibility across unique environments in the enterprise include the following:

- Having consistent visibility capabilities across the enterprise is the only way for businesses to achieve a single source of truth that identifies all devices and traffic over IT, OT, and IoT environments. This is increasingly becoming a vital capability, as securing the unknown is difficult, and complete visibility enables better security efficacy throughout the security stack.
- Unknown, undiscovered, and unmanaged devices are a risk to the greater corporate environment and can often affect known devices that are thought to be secure. Having blind spots within the corporate network, which bad actors can exploit, effectively reduces the security posture for all assets on the network. IT, OT, and IoT are increasingly interconnected, and unknown devices in one environment can serve as a back door to another, effectively compromising existing security measures across networks.

- Advanced visibility capabilities also increase the overall network security stack's ability to detect and react to threats quickly and efficiently. NAC is a key component in quickly detecting anomalous activity, which can be used to alert security professionals, deny access to affected devices, or share threat and visibility information with other cybersecurity tools on the network. NAC can also empower security operations center (SOC) analysts and threat hunting through meaningful integrations with XDR and SOAR.

NAC's Visibility Capabilities Strengthen Security Tools and Control Points

As the name implies, network access control is not simply a visibility tool but a powerful security enforcement tool as well, capable of allowing or denying access to devices on the network based on their security posture and behavior. In a sense, NAC has been implementing zero trust policies since before the term was coined and continues to be an essential element for rigorous security implementation in the most demanding environments, including industrial facilities, regulated industries, and the government.

While, historically, businesses have been hesitant to deploy potentially disruptive security tools in their sensitive OT environments, NAC has evolved from its 802.1x days as a true cross-environment tool that is easier to deploy, configure, and manage. In IDC's primary research, customers expressed a renewed interest in using network access control for policy enforcement, specifically in their sensitive, industrial environments, citing it as one of the few tools capable of addressing the unique needs of their business. While automated enforcement may still be more acceptable in the IT environment, NAC can be deployed in a more manual configuration for sensitive environments, requiring input from security and engineering staff to navigate the remediation of threats.

In addition, while NAC is a powerful security tool with significant merit as a standalone security solution, it greatly benefits from integrating other components in the security ecosystem. NAC is unique in that many foundational security technologies, such as SIEM, firewall, and endpoint, benefit from the visualization and classification data that NAC can provide. This can be used to strengthen most security components and create a significantly stronger security posture than would be possible for these products by themselves. Since nearly all businesses deploy these foundational security technologies across their environments, in IT, OT, and IoT, NAC's presence can be felt universally throughout the enterprise.

DEPLOYING NAC INTO UNIQUE ECOSYSTEMS

Utilizing an asset management system to discover assets on the network will impact several areas of your organization. This includes relations with your vendors and how you train your employees, hire new personnel, and scale pilot programs for a cybersecurity suite.

Developing Partnerships for a Complete Security Suite

Establishing a security suite requires partnerships, especially in the developing OT/IoT sectors. Solutions that integrate several key operating standards have been developed in the IT sector. However, for OT/IoT, an all-encompassing solution does not exist. Many factors contribute to this. First, every operation is unique, with different hardware assets and operating systems. Some hardware assets have a 10–20-year life span. For example, some programmable logic controllers and human-machine interfaces (HMIs) used today have been in use since the early 2000s.

Another example is that IoT sensing equipment typically is piecemeal over time. As industrial organizations develop their IoT networks, they will add sensors, vision systems, and automation on a case-by-case basis, creating a network of miscellaneous assets. As such, partnerships between vendors and service providers will allow end users to create a unique security suite for their organizations and processes.

Product and vendor consolidation is a crucial security trend in enterprises, driving security convergences across IT, OT, and IoT sectors. As networks and their interconnections continue to grow in complexity and the subsequent threat landscape expands, security cannot respond with additional increased complexity.

According to Terry Tusher, vice president of Enterprise Security at Acuity Brands, Forescout has helped his organization identify and manage assets. "We don't have the malware problems like we used to have, and certainly Forescout has helped us to get to that point," Tusher said. "Gaining the visibility of things that could have antivirus on it and don't, and then being able to remediate them and apply antivirus software to those devices has been one of our top goals."

Product and vendor consolidation provides better security outcomes across the business and is the path forward for improved security in under-secured, critical environments. Security cost savings and more reliable defense against potential production-disrupting cyberthreats add to the already strong ROI for network visibility capabilities.

Justifying the Return on Investment

When implementing security solutions, justification of ROI is crucial to expand. Often, end users do not strategize a scalable and economical solution. This happens for a variety of reasons:

- Lack of a road map and missing step-by-step details
- Lack of key personnel to aid in the deployment and rollout
- Lack of partnerships to help guide the process
- Lack of data integration and analysis to demonstrate beneficial results

As organizations deploy an IoT strategy, it is crucial that the process is well documented and thought-out and with achievable markers to ensure that it can be implemented in other areas of the organization.

Industrial operators should start with small-scale deployments to prove the ROI to C-suite management. For example, by beginning a solution with asset discovery, organizations can establish a baseline of devices. Creating an inventory list is the first step to developing an asset management system that can apply antivirus solutions, patch management, software upgrades, and user authentication. Once that has been deployed in one area, the lessons learned and the insights gathered will enable organizations to transfer the process to a new area faster and more efficiently.

Upskilling and Developing Security Personnel

One of the most significant factors in developing a cybersecurity solution is the skill level of an organization's workforce. Several workforce factors are impacting security. The skills gap is a pressing one. IDC's 2022 *Future of Enterprise Resiliency and Spending Survey* found that there was a 40% increase in security risks due to staff shortages. There is a lack of available personnel with technical knowledge of how IoT assets operate within the network and familiarity with cybersecurity best practices.

There has also been an increase in remote work in recent years. The survey found that 42% of organizations have changed remote/hybrid policies to mitigate the departing of employees to retain and attract talent. As discussed, the increase in remote work has introduced more unmonitored remote assets that can be potential threat vectors for attack. According to IDC's 2022 *Future of Work Global Survey,* sensitive information accessed via unmanaged devices was the highest concern for organizations.

There is also a need for more training for existing personnel. Insider threats circumvent network security at the perimeter, increasing the importance of complete visibility and advanced detection within the network. As attacks have become more sophisticated, workers unfamiliar with the latest attack methods may inadvertently click on malicious malware, infecting equipment. With the sudden rise in artificial intelligence, attacks can now be generated to appear more genuine and enticing to interact with. Developing standard practices for asset deployment, for example, has been one of the benefits of using asset discovery tools like the ones developed by Forescout. Matthew Gouveia, senior network engineer at Rockwell Automation, said that using asset management software helped develop best practices for the organization.

"One of the benefits we found from using Forescout was the need to push for standardization within our Layer 2 and 3 environments," Gouveia said. "A predominant concern has been devices that are avoiding or evading policies for updates, from antivirus software to operating systems. We weren't even aware of IoT devices set up by our engineers, such as security cameras, that had default passwords based on manufacturer types."

Organizations must invest time in developing cybersecurity personnel, especially for OT and IoT areas where it has yet to be the primary focus. These areas need more focused personnel and security operations centers. They can better communicate with IT security teams by establishing designated security personnel within OT and IoT areas. IT security teams need to understand how OT and IoT systems function. Interchanging cybersecurity practices with operational needs can help develop enhanced security practices that do not impede operations. For example, a successful zero trust architecture in IoT and OT must implement the concept of least privileged access without creating false positives or triggering a stop to operations. In these environments, security efficacy and disruption from security require a difficult balance and careful implementation/configuration.

Applying a Visibility-First Approach

Complete asset discovery and visibility across the entire corporate environment should be the first step for any company looking to modernize or harden its security posture. A holistic view of the entire environment, spanning IT, OT, and IoT, with contextual information on devices and traffic is foundational. It allows for security policies and enforcement to be more consistently layered across these environments. When unknown devices or gaps in visibility exist on OT or IoT networks, the ability to effectively implement security tools and enforcement suffers greatly, reducing the security posture for the entire company. Additional benefits that visibility brings to security include the following:

- Asset visibility enables closer adherence to zero trust principles. Many customers are starting their zero trust journey, investing in new products and tools, and making architectural changes to their networks. However, without complete visibility across all interconnected networks and devices, the concept of least privileged access is limited to only known devices, which are typically the most secure. Discovering all assets, identifying what they are, and limiting their access are necessary for preventing the lateral movement of threats across IT, OT, and IoT.

- Segmentation is essential for reducing the spread of threats once they successfully enter the corporate network. After identifying devices across the corporate environment, businesses can also isolate critical assets from ingress/egress points of the network. By limiting access to these essential components, operations and uptime can be protected from many security events.
- Asset visibility brings deep contextual information regarding the devices on the network, allowing security professionals to understand their attack surface better. This can lead to changes and updates to the security architecture and provide valuable information on device firmware and version. With this information, security professionals can better deliver firmware and software updates and patch security vulnerabilities that were previously undetected.

Single-purpose IT, OT, or IoT security tools add to the growing problem of security product sprawl, which is costly, adds complexity to deployment and management, and negatively impacts security efficacy. With growing interconnections between these environments, customers benefit from security that reduces complexity, as opposed to adding to it. Thus security tools that span IT, OT, and IoT and can be managed centrally should be deemed necessary for customers with diverse networks and environments, as they can reduce costs and complexity while increasing security efficacy and response time.

CONCLUSION

Consistent security across unique and proprietary devices and traffic over dissimilar network/environment architectures are not only necessity but also complex. IT, OT, and IoT environments are not only fundamentally different but are in varying stages of their own security evolution. However, the interconnectivity between these environments means their security postures are interdependent, and a security vulnerability in one environment can have widespread effects across the entire ecosystem. Thus it creates a scenario where modernizing foundational security in the OT environment can be as beneficial for the overall security posture as adopting the latest/cutting-edge security products in the IT environment.

Visibility is the first step in achieving consistent security across the modern heterogeneous network environment and requires a security product that can bridge the gap between IT, OT, and IoT. Having unknown devices and traffic across the network is no longer acceptable and creates security blind spots, reduces efficacy, makes zero trust adherence impossible, and compromises the digital transformation journey. With the rapid proliferation of unique devices across these ecosystems, it has become increasingly essential that the modern connected enterprise adopts a visibility-first approach to cybersecurity, which in turn empowers the security stack in its entirety to operate more effectively.

NAC can provide this level of visibility, identifying and categorizing unique devices across ecosystems, providing contextual information while detecting anomalous behavior, and sharing telemetry across corporate security control points. Not requiring agents or enforcement enablement but benefiting from both, NAC is flexible across the connected ecosystem, maximizing its potential in the most restricted and accommodating environments. However, most important is NAC's complete view of the holistic network, leaving no stone unturned and no device unnoticed, removing blind spots, and improving security posture and zero trust adherence more than any single environment tool/approach can.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology, IT benchmarking and sourcing, and industry opportunities and trends in over 110 countries. IDC'"s analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives. Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.).

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com