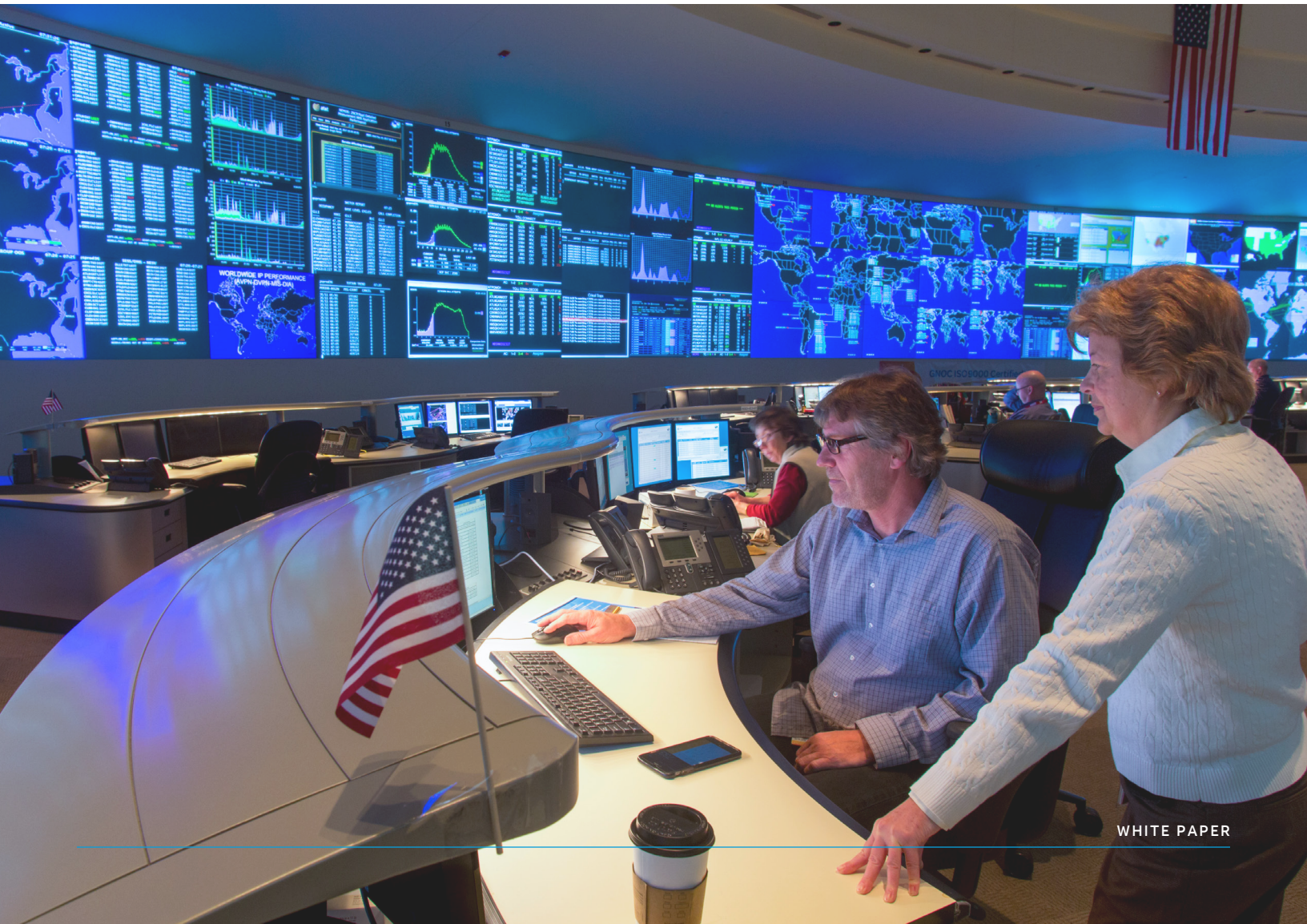
AT&T Business

How to achieve risk-based vulnerability management



WHITE PAPER

Data is the foundation on which digital business is built. But protecting that data is more difficult than ever, as a variety of new devices are added to networks, applications multiply, and 5G networks emerge. Meanwhile, threats are growing in number and sophistication, resulting in information overload that threatens to overwhelm cybersecurity leaders.

The stakes are high. According to a 2020 study by Ponemon Institute, 91% of businesses have suffered at least one business-disrupting cyber event in the past 24 months.[1] And according to Ponemon, it takes 280 days on average to identify and contain a data breach.[2] Taken together, these findings show that organizations face significant risks: Threats are disturbingly widespread, and before they can be mitigated, those threats have plenty of time to do harm.

Cybersecurity professionals have much to do. To start, they must create a risk profile by analyzing the varying risk levels and regulatory compliance requirements of different data types. Then they must communicate that risk profile to their organization's leadership so that both business and technology leaders understand and agree on acceptable levels of risk. Then they must implement a vulnerability management program that aligns with their organization's risk appetite. As a result, when cybersecurity decisions are made, they will align with the organization's risk profile, going beyond compliance requirements to focus on enabling the organization's business mission.

However, the challenges of information overload can overwhelm cybersecurity professionals, causing many to unwisely skip vulnerability mitigation. Consequently, some organizations are operating at unacceptably high levels of risk. To combat information overload, a vulnerability management program needs to prioritize mitigation, which is not always remediation—while mitigation minimizes threats, remediation removes them.

Spotlight on vulnerability management

As on-premises, cloud, remote workers, operational technology (OT), and internet of things (IoT) combine, the attack surface of distributed computing environments is becoming larger and more complex. In this context, vulnerability management is taking on critical importance.

In addition, regulations that mandate the protection of personally identifiable information (PII) add a significant dimension to the risk profile of many organizations. They require organizations to continuously monitor security controls, a process in which vulnerability management plays an essential part.

To strengthen their existing cybersecurity practices and controls, organizations need to hire and retain skilled cybersecurity experts. But qualified cybersecurity pros who have knowledge of changing environments and emerging threats—and how to deal with them—are a rare and expensive breed. According to salary.com, the median annual salary for a Level V Information Security Analyst in the U.S. is $138,283.[3] And according to a 2020 study on behalf of the Information Systems Security Association (ISSA) by the Enterprise Strategy Group, the cybersecurity skills shortage is getting worse. The study found 70% of ISSA members believe their organization has been impacted by the global cybersecurity skills shortage in 2020.[4]

1 "Ponemon Institute Cyber Risk Report: Measuring & Managing the Cyber Risks to Business Operations," Tenable.com, December 2018.
2 "What does a data breach cost in 2020?", Digital Guardian, August 2020.
3 "Information Security Analyst V Salary in the United States," Salary.com.
4 "The Life and Times of Cybersecurity Professionals 2020," Enterprise Strategy Group and ISSA, July 2020.

Experience has shown that known vulnerabilities—even only at medium-level—are often the most dangerous. In 2017, WannaCry hit 230,000 computers in 150 countries causing losses estimated up to billions of dollars. The UK's National Health Service (NHS) alone is estimated to have lost £92 million due to WannaCry.[5]

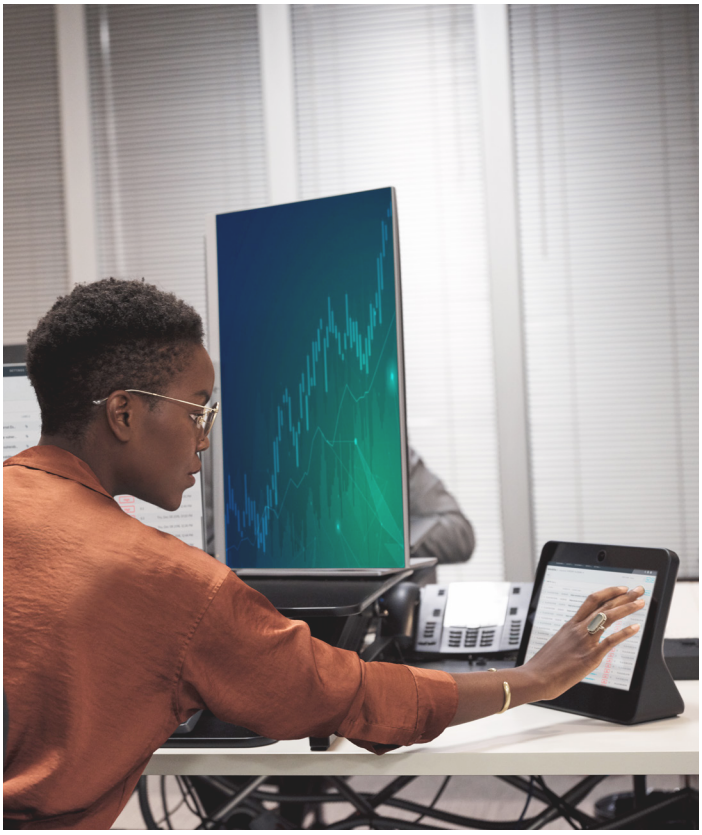
Best practices in vulnerability management include understanding an organization's risk profile as well as prioritizing the mitigation and remediation of vulnerabilities. However, many organizations, utilities and manufacturing companies in particular, can ill afford to shut down business systems in order to perform mitigation or remediation work. Further, configuration drift can take place at organizations of all kinds, allowing vulnerabilities to creep into production environments.

Faced with these challenges, the first step cybersecurity leaders must take is to establish a vulnerability management strategy to gain visibility into their infrastructure so that they can effectively respond to risks that impact operations. Some might choose to implement a standalone vulnerability management system within their IT infrastructure. Yet such implementations have drawbacks: They force organizations to make a capital outlay, and a standalone system can become obsolete if the vendor fails to keep up with threats, or if the vendor should go out of business or be acquired.

An expert team as a trusted advisor

Given the importance of vulnerability management and the reality of the cybersecurity skills gap, IT leaders would do well to call on a team of experts. Such a team will be devoted full time to studying the latest threats and will be familiar with common obstacles to implementation. A team with expertise in vulnerability management can study the particular needs of different client organizations, understanding the different types of risk to which they are exposed and the different levels of risk tolerance that are acceptable.

5 "WannaCry Cost NHS £92 Million," Infosecurity Magazine, October 2018.



A team of security experts with a deep understanding of the threat landscape understands that, given a particular risk profile, some threats must be mitigated immediately, while others might be deferred. An expert team can tailor a solution to fit the specific needs of a given business, implementing the most appropriate technology and help to deliver the best return on investment. In fact, a trusted third party can both increase the level of expertise brought to bear and lower overall cost at the same time, because it will not be necessary for an organization to hire its own experts—if indeed they can be found.

Integration of data from many sources

Because of the proliferation and increasing variety of threats, a third party provider's vulnerability management platform should integrate data from many sources. These include:

- **Threat intelligence** – Knowledge of threats in the wild and how they correlate to an organization's particular vulnerabilities.
- **Vulnerability scanners** – Automated tools that search for weaknesses in networks, systems, and applications.
- **Exploit databases** – Archives of cybersecurity exploits and vulnerable software.
- **Asset management systems** – Software that tracks both software and hardware deployed within an organization.
- **Configuration and remediation management systems** – Software that maintains computer systems and software in a desired state, documenting changes and performing remediation when necessary.

Cloud-based

A vulnerability management platform that is cloud-based has several key advantages. It can be updated continuously, so its database of threats and exploits remain up to date. As an operating expense rather than a capital expense, it is a better business investment. Instead of a single, one-time capital expense that must be amortized over time, a pay-as-you-go approach tracks closely to ongoing revenues and can be readily justified as a budget item. Further, a cloud-based vulnerability management solution is well suited to today's hybrid cloud environments as it can perform its continuous scans across multiple cloud-based and on-premises environments.

Holistic risk management

A vulnerability management platform should take into account the entire spectrum of risks. Thanks to the explosion of IoT and mobile devices, and the disaggregation of networks, risks have increased dramatically. In addition, an organization's complete risk profile now includes compliance with regulations designed to protect personally identifiable information (PII). The most important regulations include:

- **PCI-DSS.** Designed to protect consumer credit card information, PCI-DSS compliance is required of both retail and financial services companies.
- **HIPAA.** With the purpose of protecting personal health information, HIPAA governs patient records maintained by medical practitioners and institutions.
- **GDPR.** The European Union's General Data Protection Regulation gives European citizens control over their PII. Organizations must protect that data and provide it to citizens when requested.
- **CCPA.** The California Consumer Privacy Act gives California residents control over their PII. Upon request, organizations must disclose what PII they have and what they do with it. Other states may follow California's lead.

Violations of these regulations are a serious matter. Organizations may be punished with significant fines and could result in long-lasting reputational damage. Vulnerability management is an essential tool to help prevent data leakage and meet compliance requirements.

Bottom line

The task facing cybersecurity leaders is daunting. They must grapple with the plethora of cybersecurity data, while working within their organizations to communicate the nature of cyber risk. When business and technology leaders understand their organization's overall risk profile, including the varying risk levels of different kinds of data and the burdens of regulatory compliance, they can work together to achieve their organization's business mission.

The AT&T solution

Beginning with a risk-based assessment, AT&T specialists examine an organization holistically, across cloud and on-premises environments. Where appropriate, IoT and OT are included. The assessment encompasses data vulnerabilities as well as compliance requirements, establishing an accurate and comprehensive risk profile. Taking a vendor-agnostic approach, AT&T specialists recommend the best vulnerability management tools to address an organization's specific needs.

AT&T Risk-Based Vulnerability Management

Figure 1

Synergy across managed services addresses the need for mitigation using multiple options, for example: patching, IPS signatures, changes to security policy, configuration changes, and upgrades.

Why organizations turn to Managed Security Service Providers (MSSPs):

- Lack of staff or expertise in vulnerability management.
- Lack of time to deliver on vulnerability management against risk-based requirements of business.
- Reduce capital expense; turn to operational expense.
- Recognition that an external advisor will deliver capabilities more efficiently than is possible internally, including platform deployment and staff hiring and training.

Optimized cybersecurity strategy

A team of experts from AT&T assesses vulnerabilities and risks, recommends mitigation and remediation measures, helps enable compliance, and provides documentation and reporting.

One-stop shop
AT&T works with other third parties to deliver a complete solution.

Cloud-based
Skilled specialists; continuous updates; Opex rather than Capex.

Security experts overcome the skills gap

An AT&T team studies business operations and IT infrastructure in relation to vulnerabilities and participates in regular meetings to fine-tune protection measures. This enables an organization to extend its own security team by adding skill sets that are needed, given the expanded threat landscape and attack points.

Cloud-based

The solution from AT&T delivers all the benefits of a cloud-based implementation, including continuous updates that stay one step ahead of the changing threat landscape. As an operating expense, rather than a capital expense, the AT&T vulnerability management service helps to ease budgeting by eliminating large one-time budget items.

One-stop shop

AT&T works with third parties to deliver a complete solution that goes beyond scanning and vulnerability management to include threat detection and response as well as firewall and security policy management. AT&T experts understand threats, risk and context, to enable intelligent and immediate action when vulnerabilities are identified. The end result, is access to an excellent team that will provide the strategic risk reduction your organization is looking for.

AT&T Cybersecurity

AT&T Cybersecurity helps to reduce the complexity and cost of fighting cybercrime. Together, the power of the AT&T network, our SaaS-based solutions with advanced technologies including virtualization and actionable threat intelligence from AT&T Alien Labs and the Open Threat Exchange™, and our relationship with more than 40 best-of-breed vendors, accelerate your response to cybersecurity threats. Our experienced consultants and SOC analysts help manage your network transformation to reduce cybersecurity risk and overcome the skills gap. Our mission is to be your trusted advisor on your journey to cybersecurity resiliency, making it safer for your business to innovate.

This content was commissioned by AT&T and produced by TechTarget Inc.