

Continuous Network Monitoring for the New IT Landscape

March 16, 2015

(Revision 4)

Table of Contents

- Introduction** 3
- The New IT Landscape** 3
- Gaps in the Modern IT Landscape** 5
- Tenable’s Five Critical Cyber Controls** 7
- Tenable’s Continuous Network Monitoring Solution** 8
 - Unique Sensors and Analytics..... 8
 - Deep Integration with Existing Security Systems..... 9
 - Scalability for Tomorrow’s Network 9
 - More Supported Technologies than Any Other Vendor 10
 - Peace of Mind 10
- Conclusion** 11
- About Tenable Network Security**..... 11

Introduction

Recent breaches have targeted a fatal flaw in the way organizations have approached security over the last two decades. While the focus has been on investing in multiple preventive security technologies—centralized authentication, desktop virus prevention, automated patching, next generation firewalls, sandboxes for zero-day malware, and security event management—adversaries have taken advantage of blind spots that have widened as the IT landscape has evolved. The recent breaches occurred not because of unknown weaknesses in the defensive technologies. They occurred because of gaps in coverage, due to the fact that the defensive technologies were not aligned with any security policy or business practices.

For example:

- In 2011, when the term “APT” was first used in the media, most organizations who were victimized didn’t have 100% deployment of anti-virus agents on their desktops.
- The Target data breach, resulting from inappropriate network connections between the corporation’s air conditioning systems and its credit card systems, went unnoticed even after years of compliance with Payment Card Industry Data Security Standards.
- Organizations struggled to effectively patch the Heartbleed and Shellshock vulnerabilities because their vulnerability management programs were focused on applying operating system patches and not taking an application view that included infrastructure vulnerabilities.
- In 2014, Code Spaces lost control of their entire Amazon Web Services infrastructure to hostile attackers.

In each of these cases, defensive technologies were in place, but they were not aligned with the core functions of the network they were protecting. Buying defensive security products alone does not make you secure. Security comes from deploying these products as part of a comprehensive security strategy, designed to minimize your risk.

Fortunately, the concept of continuous network monitoring—defined by NIST as “maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions” — provides this alignment. A continuous network monitoring program leverages automation to ensure your entire security program is working together as designed. This includes performing an assessment of all real-time security defenses, such as anti-virus and intrusion detection systems, as well as slower activities, such as patch management.

Tenable Network Security[®] recognized many years ago that continuous automated testing of a network’s defenses against a security policy is the best method to monitor the health and assurance of your network. We wrote our first paper on this topic, “Real-Time Compliance Monitoring,” in 2004. We also recognized that performing this type of monitoring at scale, including mobile users and cloud based applications, requires new forms of technologies.

Over the past decade, Tenable has invested in and created new types of sensors that allow for the automatic discovery and security assessment of networks that span traditional IT systems, mobile users, virtual networks, and cloud-based applications. We’ve also pioneered how to take this data and leverage big data analytics to automatically report your network’s compliance to a security policy.

The New IT Landscape

Before we discuss the specifics of a continuous network monitoring program, it’s important to acknowledge that the concept of a “network” has changed significantly over the past decade. The traditional definition of a network generally centered on physical machines, but the modern IT network has extended to include much more. Virtual systems, mobile users, and cloud-based applications are now major components of the IT infrastructure along with data center components (such as servers, databases, file systems, Active Directory, and middleware) and the perimeter (including next generation firewalls, IDS/IPS, and mobile). When we talk about “the network” in this paper, we are referring to *all* your systems, not just servers and desktops.

Modern network security strategy has evolved into placing data into various “silos” and then limiting access to the silos to specific users who need it. A silo is dominated by a single application or service. For example, a Human Resources department places their data in applications run locally such as Oracle’s PeopleSoft or online at services such as ADP.

Silos of data can exist on traditional on-premises equipment, or are deployed on someone else’s infrastructure such as Amazon AWS or Rackspace, or are offered entirely as a cloud based application, such as Salesforce.

Microsoft Exchange is a typical example of this type of service. You can run Exchange locally on your network, you can run it on someone else’s infrastructure, and you can also buy Exchange email as a service directly through Microsoft’s Office 365 suite.

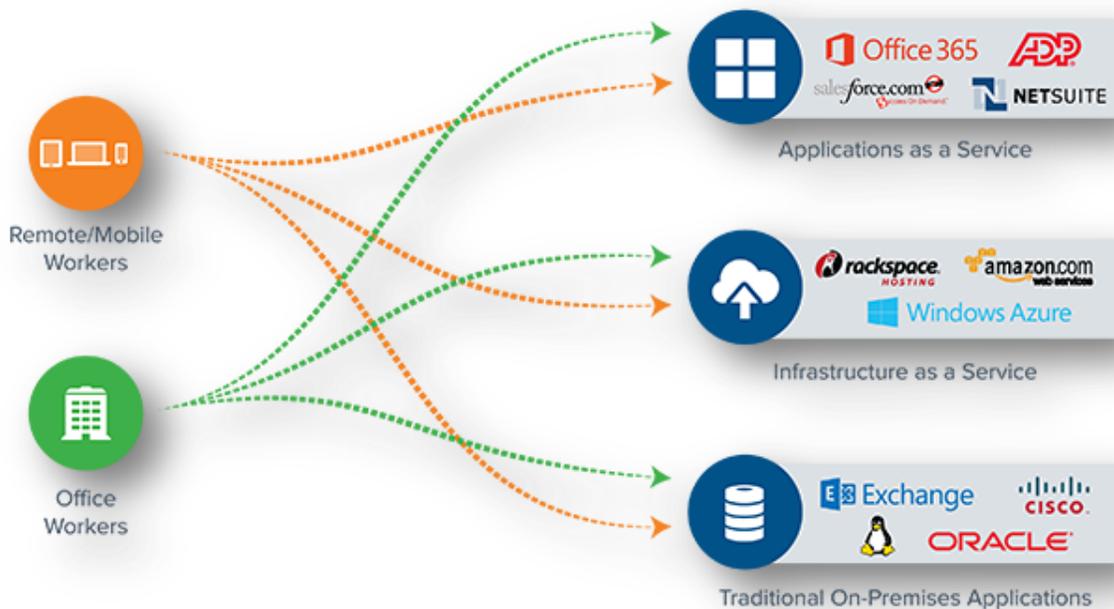
Three different tiers of data silos should be considered for continuous network monitoring:

- Application as a Service (AaaS) – Salesforce, ADP, Office 365
- Infrastructure as a Service (IaaS) – Amazon, Rackspace
- On-Premises Applications – Applications on bare metal or virtualized

Network users fall into two categories: on-premises inside your traditional network or outside of your network.

Tenable recognizes that users may leverage traditional laptops and mobile devices. We also recognize that many organizations allow their users to access personal applications such as Dropbox, Facebook, and LinkedIn. Each user’s access to an organization’s various silos of data must be monitored, audited, and secured continuously, regardless of the technology that is in use.

The following diagram shows how these various types of users and silos relate to each other.



This model addresses the weaknesses or gaps in your security program. And it’s working. Organizations that have implemented continuous network monitoring are more than twice as likely to be satisfied with their vulnerability management approach compared to those who use periodic scanning, according to a 2014 [study by Forrester Research commissioned by Tenable](#).

Tenable has worked with many organizations who have wanted to expand their periodic vulnerability assessment programs to continuous network monitoring. A review of this model demonstrated to these organizations that there were vast portions of their network they hadn't considered monitoring since they did not realize their actual network data flow. It also demonstrated that the audit function was overly focused on finding vulnerabilities rather than on the mitigating controls such as patch management, SIEM deployment, network activity monitoring or malware defenses.

This model is also useful to prioritize users based on which applications they use. For example, with a recent Internet Explorer zero-day vulnerability, organizations had no idea which users used different silos or which users connected to Internet applications on a regular basis and therefore could not prioritize which systems to patch first.

Gaps in the Modern IT Landscape

As companies adopt the modern IT landscape, they are able to realize efficiencies of a dynamic and agile organization. However they also introduce visibility and security gaps that leave the organization open to vulnerabilities, exploits, and breaches. We can enumerate the specific weaknesses by analyzing the model pictured above.

Home and mobile users interacting with corporate resources pose various risks to the organization, whether they are using corporate on-premises applications and data, resources deployed on third party IaaS frameworks, or cloud applications that are developed and deployed by third parties in their entirety. Similarly, office workers who are present at corporate offices utilize on-premises resources in addition to applications developed in-house but deployed on IaaS platforms, as well as cloud applications. While there are specific differences in the security gaps for each of these scenarios, the overarching problem is one of lack of security coverage, and hence, lack of visibility.

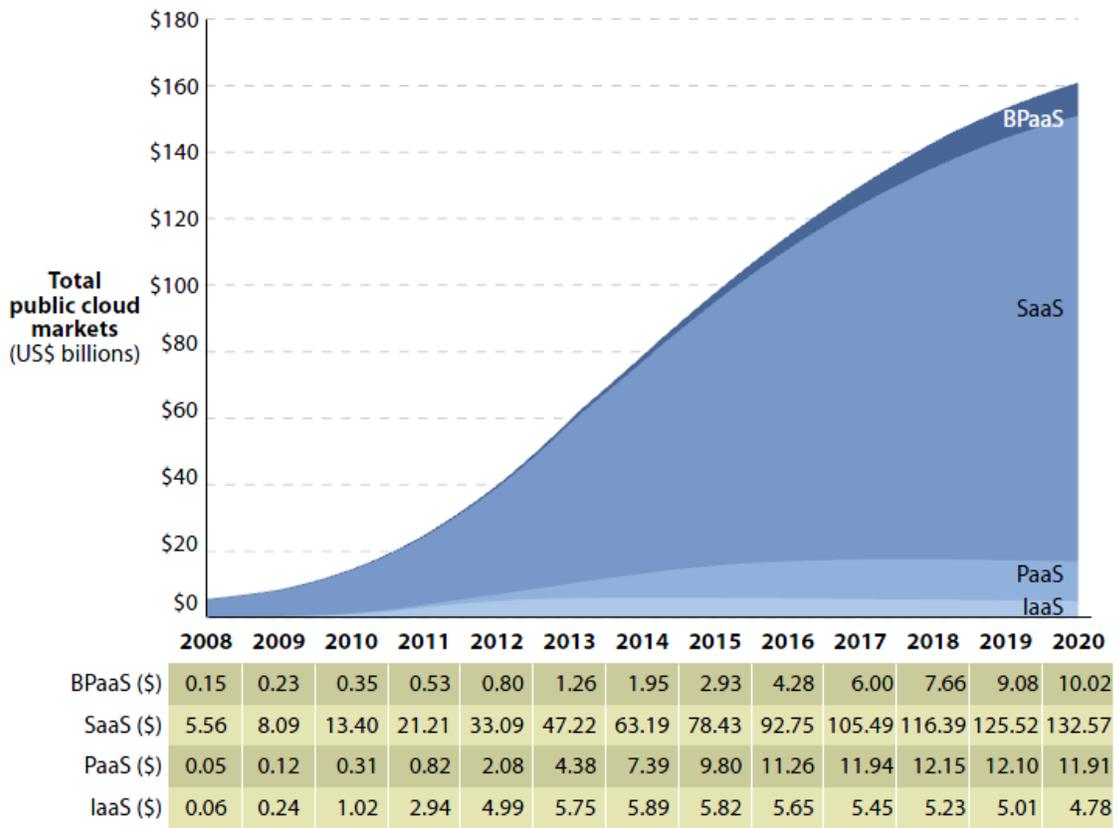
Office workers accessing on-premises applications are faced with the problems of phishing emails, botnets, malware already present on devices, privilege abuse, and out of date AV, patch, and software versions. These gaps are created because of the silos mentioned earlier. However in this simplest scenario, no one is monitoring or assessing the individual security software products deployed in the enterprise. Mobile users accessing on-premises resources and applications are also at risk, but in addition to the threats mentioned they must also be monitored for secure end-to-end authentication and communication while accessing the corporate resources. Home and mobile users also face WiFi hacks, man-in-the-middle attacks, and mobile malware.

Office, home, and mobile users may also have to utilize packaged and custom applications that are deployed in IaaS environments. MS Exchange or the organization's own custom application, for example, can be run in a hosted environment like Rackspace or AWS, etc. This scenario not only exposes these users to the gaps mentioned earlier for on-premises applications, but also introduces additional risk based on the hosted environment. IaaS providers typically enable the platform to deploy the enterprise's application, but give little information or access to monitor the underlying infrastructure. The organization is also at risk if "neighboring" environments in the IaaS provider's datacenter are infected and end up crossing over to the enterprise's applications and users. In this case the assessment and monitoring capabilities must extend to cover the known applications and users as well as typically unknown neighboring environments and network communications.

Cloud applications are becoming increasingly prevalent in enterprise environments. In fact the adoption of cloud infrastructures and SaaS applications has been exponential already, and as can be seen in the following graph, will continue to see explosive growth over the next several years.

Figure 3 Forecast: Global Public Cloud Market Size, 2011 To 2020

The spreadsheet detailing this forecast is available online.



58161

Source: Forrester Research, Inc.

These applications introduce the greatest lack of visibility for home, mobile, and office users. A cloud application is not only hosted entirely on third party servers, but is also built as a completely “black box” environment – an application that does not interact or report to the customer-corporation’s IT or security resources. Many times the cloud application is actually instrumented for performance and security monitoring, but only the most basic information like uptime and other SLA-related metrics are shared with customers. In this scenario the customer’s security and IT staff can only gain visibility and monitoring by accessing tightly embedded APIs or other data access/integration mechanisms that the cloud application provider chooses to allow.

As enterprises try to operate with more agility and efficiency, giving remote workers access to resources that were traditionally only deployed on-premises and only accessible from the office, they must ensure that the new IT paradigms they adopt do not compromise the security posture of the organization.

Tenable's Five Critical Cyber Controls

With an ever changing dynamic IT landscape, where do you start when developing a security policy? How can you know if you are taking the right steps and if you are doing enough to protect your assets, data, and business?

Many organizations look outside their walls to formulate a policy against which to measure their information security practices. Certainly, there is no shortage of good security standards for organizations to adopt:

- The 20 [Critical Security Controls](#) from the SANS Institute and the Council on CyberSecurity
- The [NIST Cybersecurity Framework](#)
- The [National Campaign for Cyber Hygiene](#) from the Center for Internet Security and the Council on CyberSecurity
- The [PCI Data Security Standard \(PCI DSS\)](#)
- The Australian Government Department of Defence, [Strategies to Mitigate Targeting Cyber Intrusions](#)

All of these standards are well thought out and provide a solid foundation for your security policy. However, reading and understanding the standards can often be overwhelming. Which standard should you choose, which guidelines should you follow, and how should you implement the principles?

These standards all share common elements and themes; adopting any standard will help ensure secure and compliant systems. To help you formulate an effective security policy, our Tenable security experts have examined these and other standards and have distilled the recommendations from all these standards into 5 core controls which can mitigate up to 80% of IT security risks in your organization or agency. The **Tenable Critical Cyber Controls** are the best-in-class cyber controls required to running a secure and compliant security program:

- **Track your authorized inventory of hardware and software:** Discovery of all assets is a critical first step, including identification of all authorized or unauthorized hardware and software, transient devices and applications, unknown endpoints, BYOD devices, network devices, platforms, operating systems, virtual systems, cloud applications, and services.
- **Continuously remove vulnerabilities and misconfigurations:** To remove all vulnerabilities, you must implement a regular scanning program, preferably continuous network monitoring. Your scanning technology should include sensors to detect publicly identified vulnerabilities, missing patches for operating systems and applications, and misconfigured applications. Once all vulnerabilities and misconfigurations are identified, you should have a repeatable process to remediate/patch/remove the weaknesses.
- **Deploy a secure network:** Network security should be a daily practice. Segment the network, manage ports and protocols, install firewalls, limit Internet access, monitor network traffic, and secure remote access.
- **Give users access to only what they need:** Limit and control administrative privileges to employees with a business need, avoid using default accounts, enforce strong password creation, and log all accesses.
- **Search for malware and intruders:** You must actively monitor your systems for anomaly detection and exploitation. It is frankly unrealistic to expect your systems to be 100% incident free. Attackers acquire new technologies every day; you have to stay one step ahead of them by proactively managing your systems with real-time continuous scanning for viruses, malware, attackers, and inside threats.

Are you doing all this now? If you see gaps in your information security program and policies, adopting a truly continuous network monitoring solution is the best way to implement these 5 critical cyber controls, to improve organizational effectiveness, mitigate business risk, and to reduce costs without compromising enterprise security.

A continuous network monitoring program allows organizations to leverage automation to easily detect if they are performing these basic security controls. The ability to measure the effectiveness of your IT controls and defense posture is

paramount to maintaining a known, good state. For example, a poor asset management program will lead to non-compliance with PCI, FISMA, and other standards. If your organization standardizes on a more advanced set of security requirements, continuous network monitoring can also be used to instrument those specific requirements.

Tenable's Continuous Network Monitoring Solution

Continuous network monitoring is the process an organization uses to automate the measurement of risk with their entire network. The process continually discovers, assesses, and then reports every component of the network against a security policy.

Tenable provides continuous network monitoring to identify vulnerabilities, reduce risk, and ensure compliance. Our family of products includes SecurityCenter Continuous View™ and Nessus®. SecurityCenter Continuous View (CV) allows for the most comprehensive and integrated view of network health. Nessus is the global standard in detecting and assessing network data.

SecurityCenter CV™ is a category-defining continuous network monitoring platform. It can monitor activity and identify risk in all aspects of the modern IT landscape, including devices that you may not know about, mobile devices, virtual systems, and cloud applications. It can also track the dependencies between them so you can identify who your users are and which silos of data and applications are in use.

Unique Sensors and Analytics

Tenable provides a unique combination of detection, reporting, and pattern recognition utilizing industry recognized algorithms and models. Tenable sensors include vulnerability scanners, system agents, network sniffers, and log analyzers.

Our sensors discover 100% of your infrastructure, regardless of whether it includes AaaS, IaaS, or traditional on-premises hardware or virtualized applications. These sensors discover all of your users, regardless of whether they are on-premises or remote workers.

SecurityCenter CV sensors also perform assessments of the components of your network and your user and application activity. These include traditional vulnerability assessments, configuration analysis, malware detection, and anomaly detection. They also include the detection of malware and malicious insider activity through a wide variety of indicators and algorithms. Tenable has also gone the extra step of embedding a variety of leading edge indicators of compromise into all our telemetry for proactive anti-virus and anti-malware defenses.

Big data analytics are leveraged by SecurityCenter CV to analyze and report the telemetry gathered by our sensors in near-real time. The telemetry of user activity, system health, network activity, application activity, and threat detection provides critical data to any incident response process.

SecurityCenter CV can be used for comprehensive and automatic reporting of your network's compliance with complex standards such as PCI and the NIST Cybersecurity Framework, as well as newer continuous network monitoring standards such as the 20 Critical Controls from the Council on CyberSecurity.

SecurityCenter CV analytics can also report gaps in security coverage, such as web servers running without web application firewalls, or desktops surfing the Internet without proper antivirus and malware defenses.

SecurityCenter CV can also leverage the telemetry from the various sensors to automatically profile and compute which of your local and remote users accesses each of your data silos, including direct access to the Internet. This means that local and mobile users can be classified based on which data silos they've been observed interacting with. Knowing which silos a user accesses also enables you to prioritize defenses for users that leverage multiple or more risky applications.

Deep Integration with Existing Security Systems

SecurityCenter CV has tight integration and API extensibility with SIEMs, malware defenses, patch management tools, mobile security solutions, firewalls, and virtualization systems.

Each of Tenable's sensors has extensive abilities to perform automatic discovery of the device and then assess the device for vulnerabilities, malware, and configuration issues.

SecurityCenter CV also has more integration with existing security infrastructure than any other solution, including:

- **Patch Management:** The ability to assess the effectiveness of existing patch management tools, such as IBM Endpoint Manager, by identifying systems that are not currently managed, or that have not been fully remediated.
- **Mobile Devices:** The ability to combine mobile user and device security information from MDMs, such as MobileIron, with vulnerabilities from the rest of your network to provide a comprehensive view of all user devices.
- **Desktop Malware Defenses:** The ability to assess the effectiveness of all leading antivirus solutions, including reporting on numbers of agents deployed, how current their signatures are, and independently detecting malicious software and zero-day malware with Tenable's sophisticated set of compromise indicators and behaviors.
- **Network Malware Defenses and Indicators of Compromise:** The ability to audit the deployments of modern next generation sandboxes such as FireEye, firewalls such as Palo Alto, and indicator sharing services such as ThreatConnect.
- **SIEM and Log Analysis:** The ability to mine SIEM and log data to demonstrate effective security. For example, if the network policy is to collect NetFlow data on all internal systems, SecurityCenter CV can report known systems without NetFlow records. Similar assessments for authentication, firewall, network access control, and other policies are supported.
- **Cloud Services:** Automatic discovery of IaaS and AaaS through network and system analysis. SecurityCenter CV sensors identify users accessing cloud based services such as Salesforce and also Internet-based user applications such as Dropbox.

Tenable's world-renowned research team is constantly adding new integration with security products and solutions. SecurityCenter CV also has APIs to add data and export data as well as a wide variety of integration points to offer customized log parsing, network traffic parsing, and customer configuration tests of systems, network devices, and cloud based applications.

Scalability for Tomorrow's Network

SecurityCenter CV scales to meet future demands to monitor virtualized systems, cloud services, and the proliferation of devices.

Tenable's sensors are ideal to detect compliance gaps and threats for virtualized applications. They audit the underlying hypervisors, virtual infrastructure, and virtualized applications. They can also identify unknown virtualized infrastructure as well as unknown virtualized applications otherwise known as "virtual sprawl".

Tenable was the first vendor to assess instances of Amazon Web Services (AWS). Our AWS auditing technology detects security issues that typically aren't even checked by traditional IT security systems since they aren't on the local network. These types of exploits were used to attack a company named [Code Spaces](#) who lost complete control over its AWS infrastructure.

SecurityCenter CV sensors can also identify all cloud-based applications in use on a network. This includes basic checks that identify devices that do or do not communicate with the Internet and very discreet checks to identify devices and users that communicate with Facebook, Salesforce, NetSuite, ADP, and hundreds of other business critical, file sharing, and social networking sites.

Finally, as the explosive growth in the number of networked devices continues, Tenable's research team is at the forefront of this industry in our ability to classify and detect these new devices. SecurityCenter CV sensors can detect a wide variety of industrial control systems, mobile devices, and systems using the IPv6 protocol.

SecurityCenter CV can perform this sort of monitoring across very large networks. Our largest customers measure their device counts in millions of units. As your network grows, SecurityCenter CV can grow with it.

SecurityCenter CV helps you implement Tenable's 5 Critical Cyber Controls to reach a desired security state and to maintain it over time.

More Supported Technologies than Any Other Vendor

SecurityCenter CV discovers, assesses, and monitors more technologies than any other vendor including, but not limited to, operating systems, network devices, hypervisors, databases, tablets, phones, web servers, and critical infrastructure.

SecurityCenter CV performs system level patch, configuration, log analysis, application monitoring, and malware auditing for all major operating systems including all versions of Windows, all flavors of Apple OS X, Red Hat Linux, eleven other Linux variants, Solaris, FreeBSD, AIX, IBM iSeries, and HP-UX.

Network assessments are supported on Cisco, Juniper, Palo Alto, ADTRAN, Check Point, Extreme, Huawei, Dell, SonicWall, Brocade, FireEye, Fortinet, and HP ProCurve. Network assessments can be performed with the device's configuration file in an offline mode or with direct access to the device.

Network telemetry is supported by Tenable's network sensors and through support for NetFlow collection.

Hypervisor audits are supported for VMware, Amazon, and Citrix Xen.

Database assessments support includes Oracle, MySQL, Microsoft SQL, MongoDB, DB2, PostgreSQL, Informix, MariaDB, and Sybase. Database activity monitoring is also supported through network protocol analysis and audit logs.

SecurityCenter CV detects a wide variety of mobile phone and devices including all forms of Apple iOS, Android, Windows, and BlackBerry mobile phones.

SecurityCenter CV discovers all web server protocols, including SSL, and the vulnerabilities associated with web servers and web application testing as well as specific configuration audits for Apache and IIS web servers.

SecurityCenter CV performs log normalization from hundreds of unique data sources. Regardless of whether you are sending logs from your SIEM or log data store, or sending them directly to SecurityCenter CV, they will be recognized and mined for vulnerabilities, user identification, and asset discovery.

Finally, SecurityCenter CV automatically discovers all nodes on the network that communicate or perform critical management of power, air conditioning, physical security, and other "industrial" controls.

Many of our assessments include vulnerability checks, the ability to support custom configuration audits and pre-made and certified audits for compliance standards and vendor best practices.

Peace of Mind

More organizations use Tenable to monitor their network than any other vendor. Because of this deployment, we see security issues and new compliance standards well before our competitors. We routinely deliver detections for the latest zero-day vulnerabilities and analytics to track compliance with the latest standards every day.

SecurityCenter CV's proactive continuous network monitoring identifies your biggest risk across the entire enterprise. Tenable's unique sensors and analytics enable you to assess how well your security program is doing across your local and remote users, as well as your local and cloud applications. In today's environment, your biggest unknown risk is the one that can get your company compromised and have your executive management at the center of media attention.

SecurityCenter CV allows you to respond to advanced threats, zero-day vulnerabilities, and new forms of regulatory compliance.

Tenable recognizes that every organization is under attack from advanced threats. Our continuous network monitoring approach, with malware and insider threat detection, ensures your defenses are properly deployed to cover network data flows that you may not realize are in place. And if there is a breach, SecurityCenter CV enables your organization to respond based on the most accurate and comprehensive set of security data for your network available.

SecurityCenter's unique sensors identify vulnerabilities at scale across your entire infrastructure. Not only does this help identify the vulnerabilities being reported in the media, such as Heartbleed or Shellshock, it also enables you to test the effectiveness of your entire patch management program.

Tenable provides the ability to automate reporting against more types of compliance standards than any other vendor. With your network deployed with our unique sensors, testing for a new compliance standard is just a matter of choosing new analytics that are automatically uploaded into SecurityCenter CV every day by our team of data scientists.

Conclusion

Tenable wants to help you stay secure and we believe that the best way to do this is to follow Tenable's 5 Critical Cyber Controls and to monitor your entire set of network defenses continuously to look for gaps that can be exploited.

Our team of experts can have SecurityCenter CV and its sensors deployed on your network in less time than it takes to deploy a typical SIEM or network security solution. More importantly, upon deployment, you will immediately be able to find business critical security issues with full transparency and visibility into your entire network.

To evaluate SecurityCenter CV or to get more information, please contact us at sales@tenable.com.

About Tenable Network Security

Tenable Network Security provides continuous network monitoring to identify vulnerabilities, reduce risk and ensure compliance. Our family of products includes SecurityCenter Continuous View™, which provides the most comprehensive and integrated view of network health, and Nessus®, the global standard in detecting and assessing network data. Tenable is relied upon by many of the world's largest corporations, not-for-profit organizations and public sector agencies, including the entire U.S. Department of Defense. For more information, visit tenable.com.