SOLUTION BRIEF

CONTINUOUS MONITORING

Many people see a doctor once a year for an annual checkup. That assessment lets you know the general state of your health at that point in time, and identifies potential concerns to address or pay attention to. Although this provides a comprehensive view of your current health in the moment, it does absolutely nothing to detect or prevent any medical issues during the rest of the year.

When it comes to the health and security of your network, the same logic applies. Point-in-time audits are effective for painting a picture of weakness in the moment, but in today's modern landscape, that's simply not enough. The assets on your network and their vulnerabilities are constantly expanding and evolving. With every new platform and approach- IoT, cloud, mobile- your modern attack surface is growing. What's needed is real-time, continuous assessment of your security posture so you can find and fix vulnerabilities faster.

The National Institute of Standards and Technology (NIST) defines continuous monitoring as, "Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions." The simple fact is that in today's threat landscape, effective security requires truly continuous monitoring.

YESTERDAY'S DATA IS STALE DATA

Five or ten years ago it was feasible for a network administrator to have a high degree of confidence with periodic audits. The servers on the network and the endpoints that connected to it comprised a relatively static environment. IT had significantly more control over the hardware and software on the network, so a weekly, or even monthly scan could be sufficient.

That was then, this is now. The digital transformation has opened up a whole new world of opportunities, creating a new attack surface to defend. BYOD policies allow users to introduce random mobile devices, and shadow IT exposes you to risk through unknown and unsanctioned services and applications across different environments. Organizations today exist in a world of cloud services and virtual servers, where DevOps has accelerated the pace of application development and the entire infrastructure can morph at the push of a button.

The pace of change is much more rapid now, which means that the scan you conducted last week has very little relevance to your security posture today. You need to rethink how you monitor a network environment that is both constantly changing, and constantly under attack. You need end-to-end visibility of your security status across your entire infrastructure--including local assets, cloud, mobile, and virtual environments. If a new laptop connects to your network, you need to scan it now, not next week. If one of your systems starts communicating with a known botnet, you need to know instantly. It is also crucial to have context so you can identify the most important security events and effectively prioritize resources--human, technology, and budget--to ensure the right balance and security posture.

CONTINUOUS MONITORING WITH TENABLE.SC

- **Active Scanning** — Periodically examine assets to determine their level of risk to the organization
- **Intelligent Connectors** – Leveraging your other security investments, integrate additional security data to improve context and analysis
- **Agent Scanning** – Instantly audit assets without the need for credentials
- **Continuous Listening** — Monitoring network traffic in real-time provides information on which assets are connected to the network and how they are communicating
- **Host Data** — Actively monitor host activities and events, including who is accessing them and what is changing

CONTINUOUS CHANGE REQUIRES CONTINUOUS MONITORING

Tenable has the deepest and broadest coverage of vulnerability and configuration assessment in the industry, and is the leader in continuous monitoring. With Tenable.sc you can accurately identify, investigate and prioritize vulnerabilities.

Using a diverse array of sensors, Tenable.sc ensures continuous assessment and comprehensive coverage of your network and assets in real-time. You get unified security data from across your organization, using sources such as network traffic, virtual systems, mobile device management, patch management, host activity and monitoring, as well as external sources of threat intelligence to feed our intelligent monitoring system. Tenable.sc thoroughly analyzes asset state with active scanning to identify vulnerabilities, misconfigurations, malware, and other weaknesses. Network traffic and event monitoring identifies new

or never-before-seen devices or applications, and detects suspicious behavior as it happens. Tenable.sc also delivers zero-touch assessment and monitoring across potentially fragile operational technology (OT) like medical devices, building management systems, and industrial control systems, including SCADA devices.

Bringing together information about the state of systems, along with their traffic and activity enables Tenable to provide the critical context needed to prioritize security responses and resources. Examples of this are identifying externally facing, and high traffic hosts to simplify remediation of the most critical issues that you face today. Tenble.sc also maps which systems and users talk to one another so you can trace paths of weakness and take action to limit the scope of potential compromises. By unifying security information, you can take a holistic view of your security posture and increase your team's awareness.

Tenable's research team is dedicated to providing resources so that security teams can hit the ground running with continuous monitoring. Tenable researches and maintains analysis rules, configuration audits, reports, and dashboards so your staff can focus on improving security, not on maintaining tools. Tenable.sc includes hundreds of report templates that you can quickly tailor, if desired, to communicate your security and compliance status to various audiences in your organization, even executives. Remediation guidance, included with every assessment, identifies which changes have the greatest impact to your security posture so you can effectively allocate resources for maximum impact.

COMPREHENSIVE SECURITY WITH CONTINUOUS MONITORING

You can no longer rely solely on point-in-time security measures, or single purpose tools. A resilient security program needs a unified solution to identify, prioritize, and assess the environment and its behavior as a whole, rather than in pieces.

Continuously monitoring the state of networks, as well as the activities of users and hosts is essential for making informed security decisions. Tenable.sc delivers pervasive visibility across your environments, and the critical context to take decisive action to continuously improve your security program. This enables you to continuously adapt your security program to better protect and enable your business.

ABOUT TENABLE

Tenable®, Inc. is the Cyber Exposure company. Over 27,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, more than 25 percent of the Global 2000 and large government agencies. Learn more at www.tenable.com.

For More Information: Please visit **tenable.com**
Contact Us: Please email us at **sales@tenable.com** or visit **tenable.com/contact**