Solution Brief

Managing Secure Access, Mobile Device Usage and Security in Healthcare

Benefits of Cisco, MobileIron and Tenable Joint Solution

Key Challenges

Modern healthcare organizations are undergoing a transformation in which their IT networks are no longer confined within four secure walls. Healthcare staff is demanding access to healthcare resources from any device, at any time, from any location while ensuring protection against security threats and data breaches, and maintaining compliance with industry regulations such as HIPAA.

Typically, IT teams within a healthcare organization deploy and manage individual solutions that address specific aspects of the risk management process (user access, mobile device management and vulnerability and compliance assessment) but these solutions, historically, were not designed to work together. This resulted in operational silos, resource overhead in identifying compliance and security issues, and delays in responding to critical problems.

In such environments, visibility and context about users, devices and data across solutions is essential for building secure access and risk management policies, helping healthcare teams answer questions such as:

- How many different healthcare systems, applications and mobile devices connect to my network? Should these devices be allowed to access the network?
- Which devices are out of compliance, unauthorized or vulnerable? Are any running malware or infecting other hosts? Is there sensitive data stored on or transmitted from them?
- Who are the users associated with the vulnerable healthcare systems and devices? What risks do these systems and devices pose? Which users have access to what systems, from what locations, with what type of access?

This allows organizations to identify which risks require immediate action to prevent out-of-compliance or a security breach.

Solution Overview

Cisco, MobileIron and Tenable™ solutions individually provide essential capabilities that healthcare organizations require:

Components:

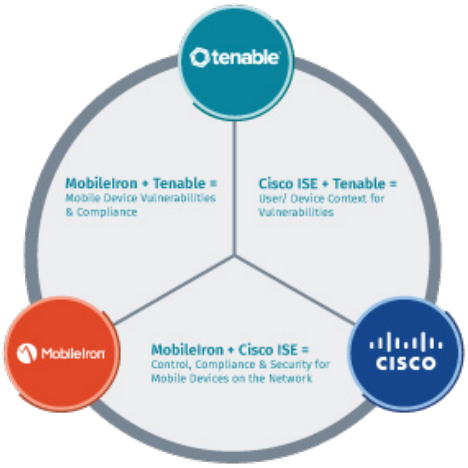
- Tenable Nessus® and SecurityCenter®
- Cisco® Identity Services (ISE) Engine
- MobileIron Enterprise Mobility Management (EMM)

Benefits:

- Increases granularity of risk analysis by joining device detection and user identification with security and compliance assessment
- Facilitates faster response by prioritizing critical issues based on device and user context
- Enables isolation of systems and users that pose risk by initiating quarantine action
- Enables fast, closed loop management of the issue or event
- Centralizes and unifies highly secure access control to provide a consistent network access policy for end users whether they connect through a wired or wireless network or VPN
- Reduces the number of unknown endpoints and potential threats on networks through greater visibility and more accurate device identification with device profiling and device profile feed service
- Accelerates BYOD and enterprise mobility with easy out-of-the-box setup, self-service device onboarding and management, and internal device certificate management
- Protects networks against data loss on mobile devices by leveraging queries for enrollment, PIN-lock, jailbreak and disk encryption

- Cisco Identity Services Engine (ISE) unifies and automates access control to proactively enforce role-based access to enterprise networks and resources, regardless of how a user chooses to connect.
- MobileIron Enterprise Mobility Management (EMM) provides mobile device access control, configuration and application management.
- Tenable's Nessus and SecurityCenter solutions identify risk and compliance violations across servers, hosts and databases.

While these individual solutions are great at performing targeted tasks in their respective areas, they are more powerful when deployed together to provide visibility, access and control over network users. Together, they also centralize, simplify and expedite the detection and remediation of healthcare security and compliance issues.



Device Control: MobileIron captures smartphone and tablet details such as device type, software and OS version. When integrated with Tenable solutions, the MobileIron data is used to identify vulnerabilities and compliance violations from mobile devices. This offers a more complete identification of vulnerabilities on medical systems and mobile devices and identifies security and compliance violations they introduce to the rest of the healthcare environment. Tenable's continuous traffic monitoring solution expands this by detecting unauthorized devices that are not managed by MobileIron. This provides continuous visibility and spotlights healthcare systems that can be brought under MobileIron management and monitoring as they connect to the healthcare networks.

Access Control: Cisco ISE provides endpoint access profiling along with user identity and device context. When integrated with MobileIron, access control can be extended to cover mobile devices so that only authorized devices are granted access. It also allows healthcare security and compliance teams to create access policies for mobile devices with user context. Healthcare IT teams can thus manage and provide access for those users connected to the network. When combined with Tenable solutions, this can be further refined to provide or deny access to systems based on their security or compliance posture – for example, limiting access to systems with critical and exploitable vulnerabilities or those that have malicious processes running on them.

User Control: Cisco ISE captures user identification and device type context in order to provide role-based network access policies. When integrated with Tenable solutions, it allows healthcare organizations to not only identify risk introduced by devices that connect to the network, but also merges context about the users associated with those devices. This enables healthcare teams to make informed decisions about initiating appropriate responses. For example, for critical security and compliance issues, Tenable includes the ability to initiate quarantine action to Cisco ISE for a closed-loop workflow to swiftly mitigate the out-of-compliance or security issue.

Data Control: Tenable solutions can identify not only all devices that are connected, but also detect sensitive data and medical information that are stored or transmitted by these systems. The context from MobileIron provides mobile device information in case sensitive data is transmitted from critical systems to mobile devices. The user identity information from Cisco ISE can further help in identifying users who are associated with transmitting systems - regardless of whether the target destination is a server, mobile device or a cloud destination.

Cisco, MobileIron and Tenable Network Security solutions work together to simplify the management and monitoring of devices and users to assist organizations in improving the security and healthcare compliance workflow.

About Cisco

Cisco (NASDAQ: CSCO) is the worldwide leader in IT that helps companies seize the opportunities of tomorrow. Cisco delivers intelligent cybersecurity for the real world with advanced threat protection solutions across the broadest set of attack vectors. Cisco's threat-centric and operationalized approach to security reduces complexity, provides unmatched visibility, consistent control, and advanced threat protection before, during, and after an attack. For more information visit cisco.com.

About MobileIron

MobileIron provides the foundation for companies around the world to transform into Mobile First organizations that embrace mobility as a primary computing platform. Mobile First organizations focus on building superb mobile user experiences that are available anywhere users need them. For more information visit mobileiron.com.

About Tenable

Tenable™ transforms security technology for the business needs of tomorrow through comprehensive solutions that provide continuous visibility and critical context, enabling decisive actions to protect your organization. Tenable eliminates blind spots, prioritizes threats and reduces exposure and loss. With more than one million users and more than 21,000 customers worldwide, organizations trust Tenable for proven security innovation. Tenable customers range from Fortune Global 500 companies, to the global public sector, to mid-sized enterprises in all sectors, including finance, government, healthcare, higher education, retail and energy. Transform security with Tenable, the creators of Nessus® and leaders in continuous monitoring, by visiting tenable.com.

tenable™

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