tufin

A Healthy Approach to HIPAA with Tufin Continuous Compliance

Solution Brief

Protect Your Electronic Health Records (EHR) from Security Breach

"In healthcare, the frequency of breach events increased by 54 percent and the number of records affected increased by 85 percent from 2012 to 2016," CIO reports.*

The Health Insurance Portability and Accountability Act (HIPAA) security rules define the technical and administrative safeguards required by any enterprise that is responsible for managing or handling electronic protected health information (ePHI). HIPAA enforcement has become a major concern due to severe HIPAA civil and criminal violation penalties. "Heading into 2017, healthcare providers are the bullseye for hackers. Ransomware is plaguing hospitals – and it poses a special challenge for healthcare IT workers," says CSO Steve Morgan.** "Ransomware is plaguing hospitals -- and it poses a special challenge for healthcare IT workers."

As the number of security breaches rapidly grows, IT teams struggle to limit access to vulnerable applications and systems containing or transmitting patient and employee electronic health records (EHR). Coupling increased threats with already lean security teams, IT leaders are facing a challenge to control the regularly rising cost of HIPAA implementation. Despite the prevalence of annual audits, "nearly 90 percent of healthcare organizations have had at least one data breach in the past two years, costing those victims more than $6 billion in total," according to the Poneman Institute, May 2016.

Enterprises that need to institute continuous HIPAA compliance for mitigating ePHI-targeted attacks need to deploy solutions to automate discovery of policy violations, identify and understand the dangers of noncompliant permissions in data access, and reduce network risks to ensure best practices are deployed for EHR protection.

Implementing and Enforcing HIPAA Across Platforms and Vendors

Security managers, internal auditors, and IT staff need to define a centralized network security policy that is aligned with HIPAA security requirements. In an enterprise network that regularly consists of multiple vendors and is susceptible to frequent changes, the ability to enforce a central security policy across vendors and platforms is critical to achieving compliance.

The Tufin Orchestration Suite™ provides the ability to define and enforce a central network security policy to ensure continuous compliance with HIPAA security mandates. Using Tufin, HIPAA-compliant enterprises enforce network segmentation by defining security zones, distinguishing zones with ePHI and EHR, determining network access policies between zones, and maintaining continuous compliance through proactive security risk analysis and change automation. Tufin's native integrations with network and cloud providers enable IT teams to overcome the complexity of increasingly heterogeneous environments and to streamline change requests.

Centralizing Segmentation Policy to Align with HIPAA Safeguards for ePHI

HIPAA requires technical safeguards for defining the connectivity requirements and restrictions between ePHI assets. While many security teams address HIPAA restrictions with administering firewalls and next generation firewalls, complex networks with more than one vendor or a high frequency of firewall changes may find manual network segmentation and firewall rule administration insufficient for monitoring connectivity between zones and maintaining continuous compliance.

Highlights & Benefits

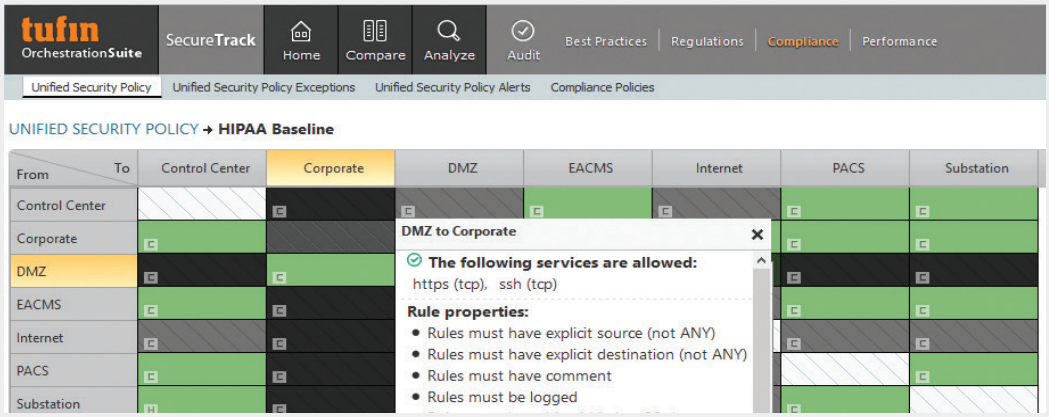
The Tufin Orchestration Suite™ ensures continuous compliance with HIPAA security rules. Benefits include:

- Simplify definition and enforcement of HIPAA technical safeguards with a centralized security policy
- Contain ePHI malicious attacks and security threats with unified network segmentation across platforms and vendors
- Ensure continuous compliance with built-in proactive risk analysis of every connectivity change
- Align with HIPAA administrative safeguards with a streamlined, automated change process
- Reduce compliance complexity across hybrid networks with security management from a single-pane-of-glass
- Reduce audit preparation efforts by up to 70% with automated documentation and reporting

* https://www.cio.com/article/3152861/security/how-cios-prepare-for-tomorrows-healthcare-data-breaches.html
** http://www.csoonline.com/article/3136323/leadership-management/healthcare-industry-is-the-bullseye-for-hackers-in-2017.html

To address the complexity and manage the continuous influx of change requests across a hybrid network, Tufin's Unified Security Policy™ (USP) provides a visual matrix for defining and enforcing a centralized network security configuration. Using the USP, security managers benefit from a centralized console for identifying policy violations that are identified and alerted in real-time across the hybrid network, and review exceptions for approval or rejection with full auditability.

Tufin's centralized network segmentation helps tighten security posture to protect ePHI assets against malicious software. In order to help your security team define the desired network segmentation that aligns with HIPAA technical safeguards ("transmission security") and administrative safeguards ("security management process"), Tufin provides a pre-defined USP baseline. The USP baseline suggests network security zones as well as access restrictions between these zones. Since network architecture is unique to each company, your baseline can be customized with specific definitions for network zones and with additional access restrictions.



Enforcing HIPAA compliance with Tufin's enterprise-wide Unified Security Policy zone matrix

Achieving Continuous HIPAA Compliance via Automation and Proactive Analysis

Even between HIPAA audits, your sensitive ePHI assets must be protected from frequent attempts of cyberattacks. HIPAA specifically requires implementation of technical safeguards to assess the security risks posed to your ePHI, and these safeguards should be maintained throughout continuous network connectivity changes. To achieve continuous compliance. organizations need to proactively review changes to network access in order to identify risks and violations even before they are implemented.

Tufin's policy-based automation ensures continuous HIPAA compliance with a built-in proactive risk analysis of each change against the Unified Security Policy. Instead of a manual change process that is error-prone and inefficient, Tufin's end-to-end automation streamlines network security change approval processes across the team, and applies changes across physical firewalls, and public and hybrid clouds. Using policy-based automation, your network security team increases their agility in responding to business requirements, consistently maintains and enforces their policy control, and ensures accuracy and connectivity during all network access changes.

Automating Audit Preparation to Reduce Effort by up to 70%

HIPAA requires the tracking of all network changes and security controls for proving compliance, and substantiating those changes with visible evidence. Establishing and maintaining HIPAA security rules can be extremely time and resource-intensive, particularly considering the learning curve and continuous effort involved in understanding, documenting, tracking, and maintaining network security procedures across a complex, hybrid network. This time-intensive process can affect other routine business tasks and projects, and lead to an overly bureaucratic process that restricts business agility.

Tufin users can automatically document every change and easily issue audit reports, saving significant staff time while minimizing manual efforts for auditors and security managers. Tufin offers customizable reports to meet HIPAA audit requirements, as well as specific organizational needs unique to your company's security policy compliance mandates. Having a central security management solution makes it easier to keep up with external HIPAA regulatory changes and internal security needs, freeing security and operational teams to focus on addressing core business objectives.

About Tufin

Tufin® is the leader in Network Security Policy Orchestration, serving more than half of the top 50 companies in the Forbes Global 2000. Tufin simplifies management of some of the largest, most complex networks in the world, consisting of thousands of firewall and network devices and emerging hybrid cloud infrastructures. Enterprises select the award-winning Tufin Orchestration Suite™ to increase agility in the face of ever-changing business demands while maintaining a robust security posture. Tufin reduces the attack surface and meets the need for greater visibility into secure and reliable application connectivity. Its network security automation enables enterprises to implement changes in minutes with proactive risk analysis and continuous policy compliance. Tufin serves over 2,000 customers spanning all industries and geographies; its products and technologies are patent-protected in the U.S. and other countries.

tufin
www.tufin.com

SB-09-17