TANIUM.

How Your Organization Can Manage HIPAA Compliance with Tanium

Tanium helps customers maintain HIPAA compliance by dramatically improving visibility into where sensitive data lives and the ability to quickly remediate issues as they arise. Below is a mapping of how Tanium can help organizations achieve HIPAA security standards in the General Rules, Risk Analysis, and Administrative and Technical Safeguards.

HIPAA Security Standards	How Tanium Helps	Relevant Tanium Modules
Security Standards: General Rules		
Confidentiality, integrity, and availability of all PHI data created, received, maintained, or transmitted	• Locate and inventory sensitive PHI data at rest • File integrity monitoring of critical PHI data and system files • Identify and manage variance from secure configuration standards • Identify data leakage on individual assets, even for those services that use encryption	• Tanium Core • Tanium Reveal • Tanium Asset • Tanium Integrity Monitor • Tanium Threat Response
Identify and protect against reasonably anticipated threats to the security of PHI	• Send alerts of malicious activity detected via Tanium Signals, STIX formatted Indicators of Compromise (IOCs), YARA rules, Tanium questions, or reputation to an incident management system with rich detail and context • Isolate machines and collect forensics information off the endpoint	• Tanium Core • Tanium Patch • Tanium Threat Response
Protect against reasonably anticipated, impermissible uses or disclosures of PHI; Ensure compliance of the workforce	• Locate sensitive data at rest • Create an inventory of all assets that contain sensitive data at rest • Automatically populate or update your configuration management database (CMDB) with assets that process or contain PHI. We can enrich the CMDB with accurate hardware, software, and user data.	• Tanium Asset • Tanium Core • Tanium Reveal
Risk Analysis		
Evaluate the likelihood and impact of potential risks to PHI	• Continuously monitor and assess OS and 3rd party patching at scale • Scan for software vulnerabilities based on open standards vulnerability database • Scan for open ports on unmanaged assets over the network	• Tanium Comply • Tanium Deploy • Tanium Patch

HIPAA Security Standards	How Tanium Helps	Relevant Tanium Modules
Implement appropriate security measures to address the risks identified in the risk analysis	• Identify and implement disk encryption on the endpoints • Regularly scan for configuration compliance according to CIS benchmarks • Provide configuration compliance of web browsers and other applications according to CIS benchmarks or Security Technical Implementation Guides (STIGs) • Quickly remediate risks by patching OS and 3rd party applications across the entire enterprise in minutes	• Tanium Comply • Tanium Core • Tanium Patch • Tanium Protect
Maintain continuous, reasonable, and appropriate security protections	• Harness the full power of native OS security tools such as Defender, System Center Endpoint Protection, AppLocker, SRP, Windows Firewall rules and monitoring around EMET anti-exploit configurations with a simplified and intuitive user interface • Send alerts of malicious activity detected on endpoints • Ensure all devices on the network are configured to approved standards; Devices not meeting these standards are quarantines from your network	• Tanium Protect • Tanium Threat Response • Tanium Discover • Tanium Network Quarantine
Administrative Safeguards/ Technical Safeguards		
Access Control	• Identify connections to unencrypted wifi • Report on the use of outdated TLS • Locate and inventory sensitive data at rest	• Tanium Core • Tanium Reveal
Audit Controls	• Ensure information is collected even if system logs have been tampered with or removed • Easily send data from Tanium to a SIEM or many other destinations	• Tanium Threat Response • Tanium Core
Integrity Controls	• File Integrity Monitoring on Windows, Linux, AIX, and Solaris • Provide visibility into backup status for endpoints and backup destinations for risk mitigation • Ensure endpoint agents such as A/V are operating in a healthy state	• Tanium Integrity Monitor • Tanium Core
Transmission Security	• Complete management of the Windows Firewall and IP Tables on non-windows • Track and identify existing IP connections • Detect and prevent communication to known malicious IP addresses	• Tanium Protect • Tanium Core • Tanium Threat Response

TANIUM.

Tanium gives the world’s largest enterprises and government organizations the unique power to secure, control and manage millions of endpoints across the enterprise within seconds. With the unprecedented speed, scale and simplicity of Tanium, security and IT operations teams now have complete and accurate information on the state of endpoints at all times to more effectively protect against modern day threats and realize new levels of cost efficiency in IT operations.

tanium.com   @Tanium   info@tanium.com