SOLUTION BRIEF

Mapping of PCI to Essential Network Security Controls

Maintaining consistent compliance for regulatory standards such as PCI-DSS can be challenging, especially if your security policies aren't consistent between your on-premises and hybrid cloud infrastructures. Unfortunately, many more have found the PCI standard lacking in specifics for network security controls often needing clarification. This is especially true for security professionals trying to provision policies required to meet both business and PCI demands.

Essential network controls are often steeped in process and interpterion making them difficult to budget and implement. Isolating the controls relating to network security policy management enables IT and Security to have common ground to ensure their network policy meets compliance standards.

This mapping shows how FireMon's solutions meet the needs of essential network controls and how they map to your PCI requirements.

Essential Network Security Controls	PCI DSS 3.2 Requirements
➔ **Inventory of Authorized and Unauthorized Devices** Knowing what you have in your environment is a cornerstone of your network security strategy, and ultimately, successful compliance with PCI. FireMon helps you find more by: – Eliminating 100% of your blind spots and monitor changes and modifications to the environment – Discovering, mapping, and alerting on topology changes across the entire hybrid enterprise, including multi-cloud environments	2.4 - Maintain an inventory of system components that are in scope
➔ **Continuous Vulnerability Assessment and Remediation** The best way to combat unwarranted access is to preemptively identify areas of vulnerability. FireMon helps manage risk by: – Scoring attack simulations and policy updates for risk and impact and then re-scoring once you've made improvements – Integrating with your vulnerability management solutions (i.e., Qualys, Rapid7, and Tenable) to measure risk and identify potential attacks – Detecting in real-time to uncover vulnerable systems, scope proposed changes before implementation, and to streamline the approval process	6.1 - Establish a process to identify security vulnerabilities 6.2 - Ensure that all system vulnerabilities are patched 11.2 - Run internal and external network vulnerability scans at least quarterly and after any significant change in the network
➔ **Maintenance, Monitoring, and Analysis of Audit Logs** Continuous compliance requires the monitoring and analysis of logs and updates to network devices. FireMon helps you monitor by: – Providing out-of-the-box and customizable assessments to help you ensure compliance with PCI standards – Automatically identifying rules that require immediate analysis based on real-world events – Documenting rule recertification and justification to aid in compliance audits	10.1 - 10.9 - Track and monitor all access to network resources and cardholder data

Essential Network Security Controls	PCI DSS 3.2 Requirements
➔ **Secure Configurations for Network Devices** Secure configuration for network devices starts with firewall policy and the specific management tools deployed. **FireMon helps you with security assessments and hygiene by:** – Eliminating duplicate or shadowed rules that adversely impact device performance – Performing real-time analysis and providing an extensive history for rule and object usage in a policy to help you easily identify unused rules – Showing unique traffic patterns that exist in a rule and report on what data is flowing across a broadly defined address range – Applying event-driven review and verification to help you keep and recertify the rules that are still needed and those that need to be decommissioned	Establish and implement firewall and router configuration standards Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment 2.2 - Develop configuration standards for all system components 6.2 - Ensure that all system vulnerabilities are patched
➔ **Boundary Defense** Network security used to be about maintaining healthy boundaries at the perimeter, but mobile computing, cloud platforms, and digital transformation mean these boundaries are more porous and less defined. **FireMon helps you by:** – Connecting to all on-premises network devices and private public cloud instances to capture security policies, normalize data, and to display through a single pane of glass – Providing insight into any requests that duplicate access or any rules that allow similar access to a new request – Performing a pre-change impact analysis that simulates a potential rule change and analyzes its impact on compliance and security – Integrating with your existing ticketing systems to automate policy approval	1.1 - 1.3 - Install and maintain a firewall configuration to protect cardholder data 8.3 - Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication 10.9 - Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties 11.4 - Use intrusion-detection and intrusion-prevention techniques to detect and/or prevent intrusions into the network
➔ **Incident Response and Management** Preempt breaches through continuous adaptive enforcement. Complete policy lifecycle automation helps reduce the impact of breaches and proactively strengthens your security posture. **FireMon helps you proactively by:** – Eliminating 100% of your blind spots and monitor changes and modifications to the environment – Discovering, mapping, and alerting on topology changes across the entire hybrid enterprise, including multi-cloud environments – Automatically identifying rules that require immediate analysis based on real-world events, like a breach – Showing unique traffic patterns that exist in a rule and report on what data is flowing across a broadly defined address range	12.10 - Be prepared to respond immediately to a system breach

FireMon's mission is to improve security operations that will in turn lead to better security outcomes. FireMon delivers industry-leading security policy management, cloud security operations, and asset management solutions. Our platform is the only real-time solution that reduces firewall and cloud security policy-related risks, manages policy changes, and enforces compliance. FireMon's Cloud Defense solution (formerly DisruptOps) is the only distributed cloud security operations offering that detects and responds to issues in the fast-paced public cloud environments. Our cloud-based Asset Management solution (formerly Lumeta) scans entire infrastructures to identify everything in the environment and provide valuable insights into how it's all connected.