SOLUTION BRIEF

Mapping of Sarbanes-Oxley Act (SOX) to Essential Network Security Controls

The Sarbanes-Oxley Act makes corporate executives explicitly responsible for establishing, evaluating, and monitoring the effectiveness of internal control over financial reporting. For most organizations, the role of IT is crucial to achieving this objective. This situation creates a unique challenge: many IT professionals are held accountable for the quality and integrity of information generated but are not well versed in the intricacies of financial reporting. Moreover, IT and Security must settle on an appropriate framework(s), like COBIT, to address the IT risks of their financial reporting because SOX does not specify which controls to use.

Essential network controls are often steeped in process and interpretation, making them difficult to budget and implement. Isolating these controls enables IT and Security to have common ground to ensure their network policy meets compliance standards.

This mapping shows how FireMon's solutions deliver your essential network controls and how they map to several SOX/COBIT requirements.

Essential Network Security Controls	COBIT Requirements for SOX 404
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 SOX. FireMon helps you find more by: – Eliminating 100% of your blind spots and monitoring changes and modifications to the environment – Discovering, mapping, and alerting on topology changes across the entire hybrid enterprise, including multi-cloud environments	APO13: Manage Security DSS05: Manage Security Services
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	APO13: Manage Security DSS05: Manage Security Services BAI10: Manage Configuration
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 SOX standards – Automatically identifying rules that require immediate analysis based on real-world events – Documenting rule recertification and justification to aid in compliance audits	APO13: Manage Security DSS05: Manage Security Services

Essential Network Security Controls	COBIT Requirements for SOX 404
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 identify those that need to be decommissioned	APO13: Manage Security DSS05: Manage Security Services DSS02: Manage Service Requests and Incidents
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	APO13: Manage Security DSS05: Manage Security Services
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	APO13: Manage Security DSS05: Manage Security Services BAI10: Manage Configuration

FIREMON

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.

SB0082-EN-20240222-02