The Challenge

Section 404 of the Sarbanes-Oxley Act (SOX) requires that chief executives attest to the effectiveness and maintenance of internal controls encompassing all IT systems (including hardware, software and networks) involved in financial reporting. IT departments must first identify these controls and then prove to auditors that each has been properly implemented, maintained and monitored to ensure the availability, confidentiality and integrity of financial reporting data. Implementing and enforcing the ongoing operational effectiveness of controls and policies for IT systems is a significant undertaking.

The Solution

Elemental understands the challenges associated with security compliance and has developed a unique framework along with innovative technologies to reduce the overall time and effort involved in demonstrating compliance with SOX IT controls. The Elemental Compliance System helps enterprises easily identify SOX IT systems and provides preventive and detective controls to mitigate risks associated with host misconfigurations and unauthorized network access.

Host Discovery and Inventory

Automatic Host Discovery - New computers connecting to the network present a significant security management challenge. These new computers may be authorized company-owned computing assets—non-malicious computers belonging to partners and contractors—or they may be rogue devices with malicious intent. The Elemental Compliance System discovers and profiles all new machines connecting to the network, thereby providing security administrators with broad visibility.

SOX Host Inventory - SOX requires that enterprises identify and maintain an inventory of all hosts that are directly involved in financial reporting. Enterprise networks are constantly changing, making it difficult to maintain such a list. The Elemental Compliance System continuously detects which hosts are involved in financial reporting and generates SOX host inventory reports so that enterprises can quickly identify their SOX inventory at any point in time.

Host Configuration Controls

System Settings Management - A significant number of intrusions result from exploitation of system configuration errors. This problem is even more acute in heterogeneous computing environments, which are increasingly common. The Elemental Compliance System provides extensive cross-platform computer integrity policy rules based on industry best practices such as those from the National Security Agency (NSA), the Center for Internet Security (CIS) and the SANS (SysAdmin, Audit, Network, Security) Institute.

The Elemental Compliance System makes it easy to demonstrate and maintain compliance with IT security controls for Sarbanes-Oxley. Elemental gives enterprises the general IT controls to detect and prevent issues, reduce risk and reduce the overall time involved in ongoing monitoring and compliance with these controls.
OS Patch and Anti-Virus-Level Profiling - Computers that do not have up-to-date patches or anti-virus .dat files are vulnerable to attack. The Elemental solution identifies these deficient machines and enables automatic quarantine to prevent SOX computers from being harmed or from causing harm to other critical assets on the network.

Network Access Controls
Network Access Restriction - Enterprises need to restrict access to critical SOX hosts from computers that fail to maintain compliance with key security policies (e.g., out-of-date anti-virus .dat files, misconfigured application software and unauthorized hardware or software,) whether or not they are authorized. The policy-based packet filtering capability of the Elemental agent enables the implementation of controls that limit communication between various groups of hosts and users on the network.

Rogue Device Containment - Since the number of computers with a legitimate business need to connect to enterprise networks is increasing dramatically, enterprises must implement controls to assure that only authorized machines gain access.

The Elemental Compliance System quarantines rogue devices to ensure only authorized machines have access to critical SOX hosts and the network.

SOX Baseline Policy
The Elemental Compliance System provides a SOX security policy to help enterprises comply with general IT control requirements. Elemental recommends that this policy be applied to all hosts included in SOX audits. The SOX policy enables enterprises to easily manage and monitor host and network configuration rules that are consistent with industry best practices for cross-platform operating environments.

The Elemental SOX policy includes a rich collection of rules to control the configuration and network behavior of hosts. These rules address host access and authentication, filesystem access and permissions, system logging, kernel and registry settings and configuration of hardware devices. Unlike other products, the Elemental SOX policy also integrates rules to configure the security parameters of applications along with rules to control the network behavior of hosts.

Elemental reduces the administration burden involved in managing regulatory compliance with packaged SOX IT security policies.

The Bottom Line

Saving Time and Effort for the IT Organization
Elemental reduces the administration burden involved in managing SOX compliance with general IT controls. Instead of using disparate and manual processes to create and monitor multi-platform policies, Elemental enables administrators to quickly and intuitively express cross-platform security policies. In addition, Elemental enables automatic policy provisioning so that the right policies are dynamically and automatically deployed to the right set of hosts. Elemental also provides comprehensive and flexible metrics and reports. Instead of manually collating reports from various IT groups, Elemental provides unified rolled-up reports that consolidate compliance measurements and results.