



...Wall Street banks on.

intel.

Securities Industry News

Search our site

[Home](#)

[Breaking News](#)

[Current Issue](#)

[Original Sources](#)

[Press Release Ticker](#)

[Supplements](#)

## The Elements of IT Compliance

By Michael Cohn, Correspondent

June 6, 2005 - As financial services firms begin to internalize the data security requirements of the Sarbanes-Oxley and Gramm-Leach-Bliley acts--and as they try to head off legislation on protecting confidential client financial information with preemptive self-regulation--they are busy designing new security processes and architectures.

San Mateo, Calif.-based start-up Elemental Security says it is uniquely qualified to help companies manage data security compliance with a suite of software agents that can monitor information technology systems from the perspective of many different regulatory schemes and quality-assurance standards.

The Elemental Compliance System has two elements: a best-practice approach to systems management, and what the company says is an innovative interface language, called Fuel, that effectively translates the plain-English wording of policies into the detailed actions to be carried out by the software agents out on the network.

Elemental is a policy-based software agent that gets installed on network servers and individual machines, monitoring, analyzing and logging activity. Its security policies are based on state-of-the-art best practices from organizations such as the National Security Agency (NSA), the Center for Internet Security (CIS), and the SysAdmin, Audit, Network & Security Institute (Sans).

For example, organizations can measure their controls for IT risk against the rigorous Control Objectives for Information and Related Technology (Cobit) standard from the IT Governance Institute (ITGI).

On the financial compliance front, Sarbanes-Oxley requires controls on financial and business processes that typically rely on computer systems that contain sensitive data that needs to be protected from unauthorized access and manipulation. Both servers and desktop machines need to be configured so that only authorized users have access, which requires password-choice policies that are routinely enforced. Section 404 of Sarbanes-Oxley requires CEOs to attest to the effectiveness and maintenance of the internal controls on all the IT systems involved in financial reporting. IT departments have to identify the controls and prove to auditors that they have properly maintained, implemented and monitored the systems to ensure the availability, confidentiality and integrity of the financial data.

### Policy Templates

Elemental provides a template for Sarbanes-Oxley that addresses these types of issues

- [Return to issue](#)
- [Return to issue](#)
- [E-Mail this Article](#)
- [Printer-Friendly](#)
- [Related Articles](#)



of host access control, making it easier for system administrators and compliance officers to show that they have a process in place. As part of the template, the software agents are able to identify which machines do work related to the financial statements and ensure that they are properly inventoried and monitored. The system lacks a specific template for Gramm-Leach-Bliley, however.

Financial companies already have written policies and documents in place for protecting this type of information. The problem is that there is often a gap between what is written and what is implemented, which Mike Monzon, product marketing manager at Elemental, calls the "compliance gap." With so many heterogeneous networks running Windows, Linux, and other operating systems, implementing security compliance processes often requires manual steps that can be difficult to follow consistently over time. Elemental aims to automate these processes.

For example, if a written policy dictates that each machine should have a seven-character alphanumeric password, Elemental can detect when compliant passwords are not set. The system also watches back doors that could expose sensitive financial information to outsiders.

The system manages security policies from a central location, using agents to monitor the activity of all devices on the network, including laptop and desktop PCs and servers. The latest version includes agents that work on Windows 2000 desktops, Windows 2000 and 2003 servers, and Red Hat Enterprise Linux 3.0. The central system pushes policies down to each of the software agents running on the network, which can monitor a variety of configuration aspects, including operating system settings, registry settings, file permissions, authorization requirements, hardware and software inventory, and application settings. Each agent reports back to a management console where all the information is correlated.

The system can also note when a machine does not have up-to-date anti-virus protection or when a remote computer is not running a firewall. It can then prevent that machine from accessing the network until it can prove it poses no threat to other network computers. The software also detects and locks out rogue devices trying to communicate wirelessly with the network, essentially quarantining devices that don't have the proper permissions.

Working from the Fuel-based console, network administrators and compliance officers can drill down into the data collected by the agents. The system also generates standard reports that can be run whenever the organization is audited.

### Beta Report

The chief security officer of a prominent financial services organization that wished not to be identified has been testing the Elemental Compliance System for about six months. The firm has been involved with Elemental Security for two years--the company's start-up phase--and helped drive some of the requirements for the product.

"The way we see this working is having far more real-time assessment compliance," says the executive. "A lot of other solutions were in reactive mode to assess whether you were in compliance. If our CEO were to ask me if we're in compliance, I could go to the portal and say that we're doing pretty well."

The firm itself sets high-level preferences on how it wants its Windows and Unix servers configured. "As new boxes roll out, this agent gets put on the box and we run a compliance check to see how well the system administrator builds the box," explains the security officer. If the firm is running a third-party product on a particular machine,



**Wall Street  
banks on.**

**intel.**



for example, Elemental agents can document any exceptions to general compliance policies that the application generates, sparing the staff from having to follow up the same issue every day.

To implement policies in the system, Elemental developed Fuel, a customized policy definition language. Using Fuel, an organization can express its policies in the terms used by written security policies. The language acts as a translation layer to create detailed configurations appropriate for a given platform.

The software also automatically creates dynamic host groupings based on the detected attributes of different machines. As individual machines change their configuration or behavior, the dynamic grouping mechanism automatically assigns them to new groups based on their new attributes or behavior, then assigns them the policies applicable to the new group. This prevents unauthorized or noncompliant computers from communicating with a particular computer, groups of computers, or the entire network.

### **Skeptical Analyst**

Andrew Braunberg, senior analyst for information security at the research firm Current Analysis, has been briefed by Elemental and sees value in the company's system. He has a few reservations, however, mostly having to do with policy sourcing. "I'm pretty positive on them, but one of my concerns is that they took a broad-brush approach rather than specifically targeting individual regulatory regimes," Braunberg says. "You can do a lot with the Fuel policy language. They've got the technology to apply it where you want, but as a first-generation offering, they have to go back and verticalize it more."

Braunberg believes the market for most security policy product vendors like Elemental is in its early days, but notes that this is true of its potential competition--firms like IBM, NetIQ, Symantec, Computer Associates and Pedestal Software, which was recently acquired by Altiris. Elemental says it is working on other functions it hopes will make it stand out from the crowd, including network access control and configuration management.

"It's a pretty broad range of potential competitors," says Braunberg. "It depends on how they bundle it and how effective they are at positioning it. But from a policy point of view for the general corporate sector, those products should be applicable to mapping regulatory requirements into those traditional products."

Elemental also recently joined the Network Admission Control (NAC) program, an initiative spearheaded by Cisco Systems for preventing attacks on networks by using the network infrastructure itself to enforce security policy compliance on the devices trying to access the network. This alliance may give the company an entree into other markets than financial services.

As Elemental advances its product, adding new templates for specific sets of regulatory requirements, it seems to have a decent chance of establishing itself as an innovative process manager and acquiring positive references from early adopters.

[Related Articles](#)

[About Us](#)

[Contact Us](#)

[Media Kit](#)

[Subscriber Services](#)

[Reprints](#)

[Privacy Policy](#)



(c) 2005 *Securities Industry News* and SourceMedia, Inc. All rights reserved.  
Use, duplication, or sale of this service, or data contained herein, is strictly prohibited.