



MAZU NETWORKS SYMANTEC SECURITY INFORMATION MANAGER

Enterprises have a number of security systems and devices in place, including firewalls, intrusion detection and prevention systems, anti-virus solutions, etc. Each of these addresses a specific range of security concerns. While Symantec Security Information Manager (SSIM) provides for the central analysis and storage of events and logs, companies still struggle to protect their assets and applications. **So what's missing?**

Behavior Analysis, Continuous Global Visibility, Integration with Existing Security Products

Behavior Analysis

Behavior analysis enables you to understand what's happening on the network and how a threat or event is affecting your system and users. Without behavior analysis, it can be difficult to take action with confidence.

Continuous Global Visibility

Continuous global visibility is critical in today's complex network environment. There are so many places to watch for so many types of threats. The more visibility you have, the more confident you can be in the protection of your network.

Integration with Existing Security Products

Your ability to address and recover from an event is only as good as your response capabilities. In order to ensure maximum response with minimum damage and disruption, you need integration with the security products already deployed in your environment.

Mazu and Symantec Security Information Manager

Symantec and Mazu Networks have teamed up to address this problem. Mazu's Network Behavior Analysis (NBA) system and Symantec's Security Information Manager have been integrated to increase the behavior analysis, continuous global visibility, and integration with existing security products for enterprise network security in two ways:

- 1) SSIM can correctly receive and correlate Mazu alerts
- 2) SSIM users can easily link to Mazu for a network behavior perspective on any event

SSIM 9500 Series enables IT administrators to proactively identify, prioritize, and respond to security threats that can have an impact on mission-critical business applications. SSIM 9500 Series integrates dynamic correlation with Symantec's sophisticated Global Intelligence Network, delivering proactive threat management to help ensure the integrity and availability of business information assets.

Mazu provides continuous global visibility into how users, applications, hosts, and devices are behaving on a network, and detects if there are meaningful changes from their typical behavior that indicate a network performance issue, a security threat, or an application problem. Through Mazu, enterprises understand usage patterns, consumption rates and dependencies between users, applications and network infrastructure.

The power of using these two solutions in concert is due to their analysis of the same environment from completely different and independent perspectives. Mazu uses the behavioral analysis of network traffic flows, while SSIM correlates host and security device log files. Mazu and SSIM integrate to provide a powerful combination that addresses behavior analysis, continuous global visibility, and integration with existing security products challenge.

Mazu's behavior analysis, providing improved response effectiveness network activity information, can be accessed via the Security Information Manager's user interface. This information on how an event is affecting the network and the services running on it enables enterprises to better understand the impact of event response actions

MAZU NETWORKS SYMANTEC SECURITY INFORMATION MANAGER

Typical Integrated Workflow

There are two typical workflows for an integrated solution in a Security Operations Center (SOC).

In the first workflow, the initial alert is generated by SSIM's analysis of non-Mazu alerts. For example, through the analysis of firewall and Windows logs, SSIM determines there are a dozen potentially compromised systems. As the SOC operator views the alert for each system, his or her first step is to generate a Mazu traffic report for that system directly from the SSIM interface. The Mazu traffic report provides a comparison of the traffic before and after the potential incident to what is typical for that host. A deviation from typical traffic provides substantial corroboration of a compromised host. Mazu can then be used to remove that host from the network.

The second workflow is driven directly by an event generated from Mazu. Mazu will identify zero-day attacks and malicious behavior by credentialed users that often slip through other security solutions. When the Mazu alert appears on the SSIM display, the SOC operator can, with a single mouse click, drill back down to Mazu for a complete view of the potential problem including information such as user identity, switch ports involved, ports, protocols, applications, and traffic volume. A mitigation plan for addressing the issue is presented along with an analysis of the collateral damage to typical traffic if the mitigation plan is implemented.

Continuous Global Visibility

Routers and switches are ubiquitous across the network. Because Mazu monitors flows from the routers and switches, integrating Mazu with SSIM doesn't just add one more security device, it effectively adds every router and switch to the arsenal of data sources.

Easy, Intelligent Integration with Existing Security Products

Mazu delivers mitigation options making it easy to respond to an event via the network infrastructure. Impact analysis capabilities ensure that critical business processes are not needlessly disrupted by response actions.

About Us

Mazu Networks

Mazu Networks provides continuous global visibility into how users, applications, hosts and devices are behaving on a network, and detects if there are meaningful changes from their typical behavior that indicate a network performance issue, a security threat, or an application problem. Through Mazu, enterprises understand usage patterns, consumption rates and dependencies between users, applications and network infrastructure. Only Mazu offers continuous global visibility, automatic and custom behavioral analysis benefits for network operations and security, and superior integration with network and security products. Mazu Networks' customers optimize their network operations, secure their internal networks and maximize application availability.

Symantec Corporation

Symantec is the world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information. Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com.



Mazu Networks

125 CambridgePark Drive
Cambridge, MA 02140
Tel (617) 354-9292
Fax (617) 354-9272
www.mazunetworks.com

Symantec Corporation

2330 Stevens Creek Boulevard
Cupertino, CA 95014
Tel (408) 517-8000
Tel (800) 721-3934
www.symantec.com