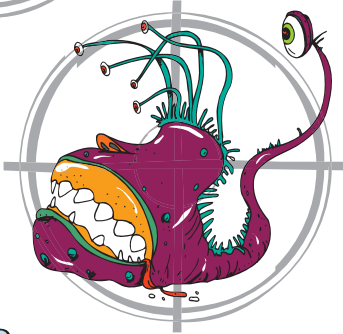
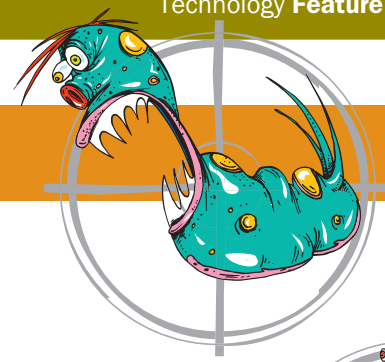


## ADAPTIVE SECURITY

# Staying a Step Ahead of Threats



While on a sales trip, Joe stops off at his company's Hong Kong office. It's Super Bowl time, so he checks his favorite team's Web site and unwittingly infects his laptop with a worm (malicious code). He needs to update sales records and check inventory so next he connects to headquarters in Dallas using the corporate VPN.

In Dallas, an intrusion detection and prevention device (IDP) detects the worm and blocks it, then contacts the VPN device in Hong Kong, informing it that malware has been detected on flow number 47. The VPN platform knows flow 47 belongs to Joe and automatically disconnects him from the network. At the same time, the VPN platform displays a screen on Joe's laptop informing him that malware has been detected on his machine and it will be quarantined until the problem is fixed. The screen directs Joe to a URL for remediation and indicates that his network privileges will be restored once his laptop is clean.

Around the world, VPN and IDP devices on the corporate network have detected the same worm and taken corrective action. In addition, each device has generated 300 to 500 lines in a log file describing what happened. Back in Dallas, a security threat management system has collected and correlated the logs and determined they are different views of the same event. The management system sends an email to an IT manager—who is at home, asleep—notifying him that one event occurred and was resolved.

This type of dynamic, coordinated threat response isn't fiction—it's in use today with adaptive security solutions. Gartner vice president and fellow Neil MacDonald describes an adaptive security infrastructure as a synchronized security system that adapts to threats in real time rather than in the aftermath of an attack. "Security must evolve to an adaptive system of interconnected services that communicate and share information to make better, faster security decisions,"<sup>1</sup> says MacDonald.

In addition to coordinating security and network gear in real time to identify and prevent an attack, adaptive security solutions also provide consolidated logging, event correlation and alerting for troubleshooting and forensic purposes. Gartner's MacDonald and other industry analysts agree that adaptive security represents a significant new approach to combating the increasingly advanced threats that target enterprises. With a little planning and the right systems and tools in place, enterprises can deploy adaptive security solutions that protect them against today's—and tomorrow's—attacks.

1. Source: *A New Spin on Adaptive Security: Gartner's Next-Generation Security Model Has Its Roots in Other Efforts*, June 5, 2008  
By Kelly Jackson Higgins, Senior Editor, *Dark Reading*; [www.darkreading.com/document.asp?doc\\_id=155734](http://www.darkreading.com/document.asp?doc_id=155734)

## The Trouble with Silos

Putting up a unified security front is a challenge. Viruses, worms, denial of service (DoS) and other threats evolve rapidly, and enterprises face ever more sophisticated, blended attacks as well as targeted attacks for which no security signatures exist. Malicious coders and hackers exploit the lack of visibility and coordination among network, host, application, database and content security systems. Attackers also take full advantage of time lags. They create new forms of malware in the gap between when a vulnerability is discovered and when vendors release patches and fixes—and the lag before IT can implement these patches. Finally, attackers exploit high-speed attacks that hit and are gone before the organization knows anything has happened.

Most enterprises have a mix of security and network devices from various vendors. Typically, each device is managed separately and operates independently, tracking events and generating its own voluminous log. As a result, IT must contend with numerous management “silos.” That IT staff often specialize by device type or on a particular vendor’s gear further reinforces this “silo” structure, with costly consequences. Too often, IT staff will monitor only gear they’re familiar with, ignoring alerts and other management data from devices they haven’t been trained on. Or they miss a network breach completely because signs of the attack are identified piecemeal across multiple consoles and there is no realistic way to correlate them.

In addition, management silos make it difficult to identify and counter blended attacks that are built to evade traditional detection mechanisms. The sheer volume of discrete management data makes manual review and correlation impossible; large enterprises and service providers can generate upward of 10,000 events and 400,000 flows per minute. IT’s job is further complicated by the fact that network and security devices are often deployed across geographic locations and time zones. Management silos also complicate IT’s ability to control and audit resource usage, impeding an enterprise’s ability to comply with government and industry regulations.

## Adaptive Security—a Coordinated Response

Adaptive security solutions “tear down these silos,” says Gartner’s MacDonald. By providing network-wide visibility and coordinated threat response across network and security devices, adaptive security solutions enable enterprises to get beyond discrete event analysis to quickly identify and counter threats—and to meet compliance requirements.

When a security breach occurs, time is of the essence. The more quickly a threat can be contained, the less damage it can do. But first it has to be identified and

the root cause determined. The task can feel Herculean when IT has to review logs from multiple management systems and several hundred devices spread over many locations. Having a consolidated view of events is key to identifying and dynamically mitigating complex attacks in real time.

Fortunately, leading vendors have brought to market a new class of management device that delivers this functionality. More than a simple correlation engine, this security information event manager (SIEM) consolidates, analyzes and correlates log and flow data from a wide range of security and network devices, desktops and servers.

A SIEM is a key part of an adaptive security solution. It gives IT network-wide visibility into, and control over, security events, providing real-time and historical views as well as comprehensive reporting. Using correlation rules, IT staff can detect specific or sequential events, enabling them to recognize that a router and firewall are seeing an attack from the same IP address, for example, and take action. Some vendors also leverage the system’s centralized log capabilities to streamline regulatory compliance, providing predefined compliance reports for the Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act (SOX) and other regulations.

The second key element for adaptive security is automated response coordination. This requires security and network platforms to communicate with each other to identify and stop attacks. Routers, switches, firewalls, remote access platforms and gateways, IDPs—all these devices should be able to share what they know about the source of the traffic and nature of the threat and take coordinated actions in response. But remediation shouldn’t be blindly automatic. An adaptive security solution should give IT the flexibility to define the response(s) that security and network devices take when a threat is spotted, or to manually intervene.

## Getting to “Adaptive”

While Gartner’s MacDonald expects adaptive security to evolve, enterprises can take steps today to begin implementing coordinated threat management. As with all security solutions, adaptive security relies on both technology and processes to be effective. With regard to technology, enterprises can begin with the following steps:

### Select standards-based technologies and equipment.

Standards allow for a baseline of interoperability across different vendors’ equipment, which facilitates cross-vendor solutions such as adaptive security. For network access control, for example, look for vendors that support



the Trusted Network Connect open architecture defined by the Trusted Computing Group. This architecture enables interoperability among multi-vendor network endpoints. Another key standard is 802.1X. IT should ensure that all edge switches actively support 802.1X, which may mean upgrading switch code or even swapping out older switches for newer ones. On the management front, the IETF's Netconf network management protocol provides standard mechanisms for device configuration, which simplifies use of centralized policy management systems.

**Deploy a security information event manager.** Given the heterogeneous nature of enterprise networks, a security information event manager must be capable of reading, analyzing and automatically correlating log and flow data from multiple vendors' network and security devices. Unfortunately, there are no industry-wide standard formats for log and flow data, so IT must carefully evaluate a SIEM to ensure it supports their existing network and security infrastructure. Also, look for a system that's scalable. It should accommodate both the current volume of log and flow data and increasing volumes as the deployment grows.

**Look for vendors that support coordinated real-time threat management across devices.** Security and network devices that can communicate and work in concert can identify and mitigate attacks more quickly and reliably than devices operating solo. For example, when a remote access device can communicate and

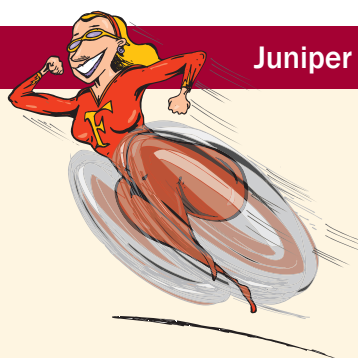
coordinate with an IDP, as in the scenario at the beginning of this article, the IDP can trigger the remote access platform to drop the specific user connection on which malware has been detected.

In terms of processes and policies, the following steps can help an enterprise begin implementing adaptive security.

**Enforce a multitier protection plan.** Many enterprises use a defense-in-depth strategy, deploying layers of security from the core to the perimeter and out to remote sites. This ensures that no one security mechanism is all that stands between critical resources and an attacker—and provides a foundation for cooperative threat management.

**Deploy security technologies best suited for specific purposes and locations.** The data center requires a different security profile than a branch office, which requires different mechanisms than the campus network. Fortunately, enterprises have an array of security products to choose from, including firewalls, IDP/IPS and SSL VPNs. By implementing the best security solution for each specific location, IT can ensure that critical resources are appropriately protected regardless of where or how someone connects to the network.

**Centrally manage all aspects of security.** To the extent possible, reduce the number of management consoles in use. Products such as a SIEM can provide a network-wide view of security information and events and a centralized system from which to analyze threats. Similarly, a central-



## Juniper Networks Security Threat Response Manager

# Identify and Respond to Security Threats in Real Time

Juniper Networks Security Threat Response Manager (STRM) provides network-wide visibility that allows enterprises to identify and respond to security threats in real time. STRM combines, correlates and analyzes log, flow and report data from routers, switches and security appliances onto a single console. So, instead of manually reviewing numerous logs from disparate products, IT staff can see the big picture on the STRM dashboard and can take fast, decisive and informed action against threats.

### A Centralized View of Network Activity

Juniper Networks STRM provides a comprehensive log management and reporting framework that coordinates data from a very broad range of networking and security products—from all major vendors. Scalable and secure log management capabilities are integrated with real-time event correlation, policy monitoring, threat detection and

compliance reporting. Data storage is secured based on industry regulations, and ranges from gigabit to terabit to enable long-term collection, archiving and reporting of events. Users can choose from more than 220 predefined reports or create their own. They can also monitor and investigate events as they happen for faster response.

### Real-time Information

Juniper Networks STRM takes an integrated approach to threat management—bridging the gap between network and security operations to detect complex, IT-based threats. STRM collects data on:

- Network events
- Security logs
- Host and application logs
- Network and application flow logs
- User and asset identity information

“Security must evolve to an adaptive system of interconnected services that communicate and share information to make better, faster security decisions.”

Neil MacDonald, Vice President and Fellow, Gartner

ized network and security policy manager gives IT a single place to provision devices and define policies, ensuring consistent security enforcement across the enterprise.

#### Commit senior staff to adaptive security implementation.

One of the main values of an adaptive security solution is its ability to coordinate threat management across multiple network and security devices. Less seasoned IT staff are often highly trained on a single device or vendor's offerings, and this “silo” perspective can limit their ability to define and implement cross-platform security solutions. Senior staff, with their broader expertise and “big picture” view, bring the right mix of experience and perspective needed for a successful adaptive security deployment.

### Smarter Security with Less Overhead

By providing real-time, network-wide visibility into anomalous traffic and coordinating the actions taken by network and security devices, adaptive security solutions accelerate the identification and mitigation of risks. Enterprises benefit from greater overall corporate security, asset protection and regulatory compliance, as well as a boost in IT's efficiency.

Rather than having to sort through dozens of logs and alerts to identify a single incident, IT sees one consolidated event alert. This expedites troubleshooting and remediation, thus minimizing the impact an attack has on the

enterprise. In addition, adaptive security solutions allow IT to automate threat management, as appropriate. Enabling functions such as user self-remediation and automatic device quarantining ensures problems are nipped in the bud while also reducing calls to IT.

Adaptive security solutions also cut IT overhead by minimizing the number of management systems that staff have to learn, operate and maintain. New employees can get up to speed faster and have everything they need at their fingertips, ensuring nothing is overlooked or ignored. Customers who've adopted adaptive security solutions report being able to reduce their security management teams by a third or more, from five to seven members to three or five.

Adaptive security solutions allow business to stay *in business* by providing the capabilities necessary to meet compliance requirements. For example, customers that handle credit card processing have reported that using adaptive security has helped them avoid fines or being shut down for noncompliance with PCI regulations. By providing out-of-the-box compliance reporting, adaptive security offerings can also significantly cut the number of man-hours needed for regulatory compliance.

With the right products and a little planning, enterprises can put adaptive security solutions to work today, knowing they'll be prepared for whatever tomorrow may bring. **V**

STRM provides hundreds of out-of-the-box correlation rules to detect threats, isolate the unique events that caused an offense, map events to appropriate categories in real time and view prioritized security events to show those with the most impact on the business.

### Regulatory Compliance and Management

Organizations of all sizes in nearly every vertical market face a growing set of IT security regulatory mandates. Because compliance with policies and regulations evolves over time, security solutions must adapt to the changing compliance landscape. Juniper Networks provides the necessary flexibility with STRM based on:

- **Accountability**—who did what and when
- **Transparency**—visibility into the security controls, business applications and assets being protected
- **Measurability**—metrics and reporting around IT risks

Proving compliance is facilitated with hundreds of built-in reports, as well as a report wizard that enables users to combine any network traffic and security event data in a single report.

### Solutions for Various Network Security Needs

With preinstalled software, a hardened operating system and Web-based setup, STRM appliances are easy to deploy. They offer a range of capacities to meet the needs of enterprises of all sizes. The family of products includes an all-in-one security solution that plugs directly into the network and is ideal for small, medium and large enterprises that do not foresee the need to upgrade to higher capacities. There are also solutions for medium-size companies up to large, globally deployed organizations that anticipate the need for additional flow- and event-monitoring capacity in the future.

### STRM Benefits

The Juniper Networks Security Threat Response Manager family of appliances offers:

- Detection of events that would otherwise be missed by point products or operational silos
- Effective management of millions of log files so IT staff can respond to threats in a timely manner
- Implementation of a compliance and policy safety net

The bottom line of the Juniper Networks Security Threat Response Manager is simple deployment, fast implementation and improved security—all at a low total cost of ownership.