



White paper

THE MOVE TO INTEGRATED NETWORK SECURITY

Prepared by:

Mitchell Ashley
CTO and VP Customer Experience
StillSecure®

June 2006

Table of Contents

Introduction	2
The path to integrated security	2
Integration in action: The anatomy of an attack	3
1. Compromise.	3
2. Policy compliance check, device quarantine	3
3. In-depth vulnerability scanning of selected devices	3
4. Shield the at-risk device from further impact	3
5. Remediation and verification	3
6. Policy Implementation	3
Beyond security applications:	
Integration within the IT environment	4
The StillSecure suite:	
Taking the lead in integrated layered security	4
Conclusion	4

About the author

Mitchell Ashley Mitchell Ashley serves as Chief Technology Officer (CTO) and VP of Customer Experience at StillSecure. As CTO, Mr. Ashley is responsible for the product strategy and development of the StillSecure suite of network security products. As VP of Customer Experience, Mr. Ashley leads StillSecure in providing a 'best-in-class' experience throughout all customer interactions. The creator of StillSecure's endpoint security and vulnerability management products, Mr. Ashley has more than 20 years of industry experience.

INTRODUCTION

Network security is rapidly evolving. The numerous technologies that fall within the network security domain—such as firewalls, intrusion prevention systems, vulnerability assessment systems, antivirus, and endpoint compliance solutions—are beginning to share data and reporting functions, and security management is being centralized and consolidated. This is an important development. Previously, single-function, vertical security tools and products were only able to do part of the job in a true layered-security environment. Today, integrated, cooperative security technologies that can leverage each other's security information and enforcement capabilities are on the forefront of innovation in the security marketplace.

The move toward integration has evolved in response to a number of factors:

- The continually escalating threat environment
- The enactment and enforcement of data security regulations
- The calamitous costs associated with compromised data and network downtime
- The shortage of security staffing resources.

In an attempt to get an enterprise view of security information, many organizations have turned to Security Information Managers (SIMs) as a way to collect and correlate data from multiple security tools. While helpful, this approach requires even more staff resources to correlate information from disparate security systems. In the end, only limited value is achieved as staff are still required to manually act upon the correlated data.

Organizations are seeking proactive, correlated, comprehensive security management that provides a view into their security posture and automates appropriate responses to identified threats. This integrated approach goes beyond the event log correlation provided by SIMs because it automates the appropriate actions that mitigate the threats.

Integrated network security provides tangible tactical advantages:

- Relevant information is correlated among multiple security systems
- Automated, protective actions are triggered in real time based on correlated data
- Threats are identified, isolated, and acted on quickly, minimizing exposure to risk
- Security is administered with maximum efficiency.

This paper examines the trend toward security integration and illustrates how a real-world threat could be isolated and defended against in an integrated environment.

THE PATH TO INTEGRATED SECURITY

The emergence of the Internet in the early 1990s created the need for a disciplined approach to network security. Connectivity was a boon to the speed and efficiency with which business is transacted, yet it came at the price of exposing private network assets and proprietary data to the world at large. The first wave of security technologies—primarily firewalls and anti-virus (AV)—quickly emerged to lock down the network perimeter and afford some protection to networked endpoints.

While no network would be considered secure without a firewall and AV, today they are insufficient to protect the network by themselves. An analogy would be the business owner located in a high-crime area who only installs locks on his doors. It's a good start, but without an alarm system, camera surveillance, guard dogs, and regularly scheduled police patrols, his investment is inadequately protected.

By 2000, additional security technologies were making inroads into the market. Recognizing that there was no silver bullet to secure the network, organizations began implementing a 'layered' approach, installing additional solutions beyond the firewall and AV. The effective mix of solutions depends on the organization's size, culture, and business flows. Technologies in the layered security mix include virtual private networks (VPN), intrusion detection/prevention systems (IDS/IPS), identity management and authentication, patch management systems, vulnerability assessment tools, endpoint compliance solutions, and others.

While the layered approach represents a dramatic improvement in the level of security, it comes with a number of administrative drawbacks. Security technologies are point solutions, which collectively introduce a number of operational inefficiencies:

- They are typically independent, standalone, vertical technologies that must be individually managed.
- Prioritizing security work activities and allocating resources is difficult as there is no relative weighting of criticality among events generated by differing security systems.
- Relevant information is locked within each product—information that could be acted upon by other systems were it readily available and discernable.

Such drawbacks prohibit the layered security approach from reaching its true potential.

The key that unlocks the potential of a layered security architecture is integration. By bringing network security systems together, the organization immediately realizes considerable synergistic benefits. Integrated security systems can be managed and monitored centrally, yet authority for local actions can be dispersed as needed throughout the enterprise. Responses to security threats can be immediate, not just at the network perimeter but at the desktop device, or even the point of entry into the network. Security issues can be automatically elevated, follow-up tasks can be assigned to the appropriate administrator or technician, and security enforcement systems can take action to limit the exposure posed from an offending device.

INTEGRATION IN ACTION: THE ANATOMY OF AN ATTACK

Tracking the lifecycle of a well-known attack in a network protected by integrated, layered security demonstrates the efficacy of this approach. In the example that follows, we'll examine how integrated security defends against a recent peer-to-peer (P2P) attack. The network in this example includes the following integrated technologies: firewall, AV, intrusion prevention system (IPS), an endpoint policy compliance solution, a vulnerability management system, and a patch manager.

1. Compromise

In this scenario, a corporation's Chief Operations Officer (COO) takes her company-owned laptop home on Friday evening. Over the weekend a family member uses the machine to share music files with others on the Internet using the latest music sharing program.

2. Policy compliance check, device quarantine

Upon returning to work Monday morning, the COO connects to the corporate network, at which point the company's endpoint compliance solution tests the device for compliance against the organization's established security access policies. The access policy dictates that:

- Devices must have the latest IT-approved operating system patches.
- The corporate standard anti-virus protection is running and up-to-date.
- Corporate patch management client software is operational on the device.

Although the endpoint security system could check for other policy requirements, such as restricted programs or other security configurations, these were not part of the applied access policy tests. The COO's laptop meets all the defined requirements and is allowed access into the network.

3. In-depth vulnerability scanning of selected devices

Within the integrated security environment, the endpoint compliance solution is able to inform the vulnerability management system (VMS) that this laptop, which is a corporate asset, has returned to the network after being disconnected for a few days. The VMS launches a full vulnerability scan of the device to ensure no new vulnerabilities are present.

The vulnerability scan detects that unauthorized TCP ports on the device are open and active. Because the laptop is assigned to an officer of the company, it is considered to be a high-importance device. As such, it is given a high repair priority within the vulnerability management system's repair workflow. In this integrated security environment, the VMS coordinates this repair information with the IT trouble-ticketing system, where a high-priority ticket is opened and assigned to the system administrator responsible for desktop maintenance. In parallel, the VMS informs the network intrusion prevention system (IPS) that this laptop device has potential vulnerabilities on the authorized ports identified during the vulnerability scan.

4. Shield the at-risk device from further impact

After connecting her laptop to the network, the COO heads off to a staff meeting. While she is away, the network perimeter intrusion prevention system (IPS) begins to detect a large number of inbound and outbound connections emanating from the IP

address of the COO's machine. These connections are oriented outside the corporate network using file sharing protocols and network ports typically used by peer-to-peer file-sharing programs. The IPS is configured to block any suspicious peer-to-peer traffic and drops all offending data packets to and from the laptop. As part of the attack identification process, the IPS correlates the suspicious traffic with known device vulnerabilities, informs the VMS that attacks of this type are occurring on the device, and flags these attacks for special attention by the security staff. Because there is potential information loss, the IPS also informs the endpoint compliance system, which immediately places the laptop in quarantine.

5. Remediation and verification

The security staff has now been alerted to the situation and determines the best course of action. Through the VMS they instruct the patch management system to deliver a script to the laptop which will uninstall the offending P2P program. To prevent further similar problems on this device, the security team installs a personal firewall on the laptop. As part of the closed-loop vulnerability management process, the VMS then (1) rescans the laptop to verify the identified vulnerabilities have been removed and then (2) instructs the endpoint security system to release the device from quarantine and place it back onto the full network.

6. Policy Implementation

Because of this incident, the security team decides to accelerate the rollout of the personal firewall security program for all traveling laptop users and update the endpoint security policy to restrict the use of unauthorized P2P music and file-sharing programs.

The team begins the process by 'pre-rolling' policies in the endpoint security system to test, but not yet quarantine, devices for the required personal firewall program and any restricted P2P applications. The results from the policy pre-roll testing show that most laptops have the corporate-standard personal firewall installed, but a surprisingly large number of internal desktops and traveling laptops are running unauthorized P2P and instant messaging applications. The team immediately adds a new policy to the endpoint compliance system to require the use of the personal firewall on all corporate laptops.

Additionally, the security team sends an email to all staff members re-enforcing restrictions about unauthorized applications, and then rolls out a script to remove them. Once the unauthorized applications have been removed, the security team adds checks to the endpoint security system to quarantine any non-compliant devices.

BEYOND SECURITY APPLICATIONS: INTEGRATION WITHIN THE IT ENVIRONMENT

Integration is not only occurring among security applications; it is also occurring between security applications and other systems in the IT environment. In the example above, the integration between the vulnerability management system and the trouble-ticketing system is one example of this wider integration. Other potentially integratable systems are shown in Table 1. Wider integration further enhances the key benefits of improved security, improved reporting and control, and improved administrative efficiencies.

Advantages of integration within the IT environment include:

- Centralized management of security data
- Security management across disparate systems

- Leveraged IT investments – increases the value of existing IT systems and processes, streamlines security administration, and reduces training and management costs
- Proactive risk mitigation – Integrated security requires less overhead and provides a repeatable means to continually mitigate the risk of an attack on the network.

Sources of security-related data:

- Asset inventory systems
- Vulnerability scanners
- Passive scanners
- Data from external security audits
- LDAP/AD directories
- Data from third-party security products (IDS/IPS, anti-virus, etc.)

Remediation-related systems and processes:

- Automated repair/patch management systems
- Trouble ticketing systems
- Intrusion detection/prevention for attack correlation
- Change management systems

Management systems:

- Security portals
- Security information managers (SIMs)
- Third-party monitors of monitors (MOMs)

THE STILLSECURE SUITE: TAKING THE LEAD IN INTEGRATED LAYERED SECURITY

StillSecure holds a unique position among network security software vendors—offering products that are both integrated and integratable. The StillSecure suite includes three integrated products:

- StillSecure VAM™ – vulnerability management platform
- StillSecure Safe Access™ – endpoint compliance solution
- StillSecure Strata Guard™ – intrusion detection/prevention system

The suite's key benefits include:

- Layered security from a single provider
- Enhanced security through solution integration/data correlation
- Leveraging of existing security investments through open architecture—enables integration with third-party security systems for centralized command and control
- Simplified administration with suite-wide common functionality, usability, and data management.

By integrating vulnerability management, endpoint policy compliance, and intrusion prevention/detection, StillSecure comprehensively protects organizations from attack. Data is correlated across the solutions to better protect the network and simplify security management. The result is a highly protective, highly automated security environment. The StillSecure suite is integratable with existing IT systems through the StillSecure Integration Framework™. This framework allows external systems to import data to, export data from, and act on data within suite.

For example, through the Integration Framework, StillSecure VAM serves as a network vulnerability command center, consolidating data and processes from other vulnerability-related systems, such as third-party scanning tools and patch managers. This gives you a centralized common view of all vulnerability data, including both VAM-generated data and data from external systems. VAM streamlines the vulnerability remediation process, ensuring that all vulnerability-related activities are executed and managed consistently.

CONCLUSION

Sophisticated threats bombard your network continuously. Protecting your organization from attack, preventing your proprietary data from being compromised, and achieving compliance with applicable data security regulations require more than a firewall and anti-virus. Today, security-conscious organizations are adopting a layered approach to network security to mitigate their risk.

The current trend is building on the layered approach by integrating security technologies. The integrated approach enhances security, streamlines workflow and reporting, and dramatically improves the efficiency with which security is managed. The StillSecure suite is at the forefront of the drive toward security integration.