



WHITE PAPER

The Pressing Need for an Adaptive Threat Management Architecture

By Jon Oltsik

March, 2009

Table of Contents

Table of Contents	i
Executive Summary	1
The Dangerous State of the Network	1
Why is Network Security so Poor?.....	2
What's Needed? An Adaptive Threat Management Architecture (ATMA)	4
The Benefits Associated with ATMA:.....	6
The ATMA Roadmap	7

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of the Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at (508) 482-0188. This ESG White Paper was developed with the assistance and funding of Juniper Networks.

Executive Summary

Many pundits agree that information is the new currency for 21st century business success. Organizations that capture, analyze, share, and react to information quickly will prosper, while those that lag behind will ultimately suffer. If this is accepted as a fundamental fact, then communication networks that move information are also invaluable assets. Networks that offer high performance and availability can help enable business success while problematic networks may become a hindrance.

Of course, no organization would purposefully create a network that can't meet business demands, but this may happen by proxy—as a result of poor and increasingly ineffective network security. Logic dictates then that sub-par network security could be the difference between business prosperity and failure. This paper concludes that:

- **The network has become a dangerous neighborhood.** Complex networks, massive numbers of new devices, application layer attacks, and sophisticated cyber adversaries have led to a growing number of security breaches. Unfortunately, many organizations are falling farther and farther behind.
- **Security point tools are part of the problem.** Past efforts to secure the network led to the implementation of dozens and dozens of tactical security point tools designed to safeguard against a particular type of threat. This has led to a state of “point tools fatigue” where organizations struggle to monitor and manage individual devices. Additionally, this army of point tools has limited integration, so security professionals struggle to get an overall picture of enterprise security, detect/remediate security events, and control capital and operating costs.
- **Large organizations need an Adaptive Threat Management Architecture (ATMA).** What's needed is an integrated set of tools that links networking and security together to prevent, detect, monitor, and react to ever-changing security threats. This is called the adaptive threat management architecture. Over time, the adaptive threat management architecture will be implemented from core-to-edge across the enterprise network in order to enforce user access controls, implement perimeter rules, inspect all packets, address internal threats, and react to security events by enforcing granular security policies. It will be based upon central monitoring, reporting, and command-and-control.
- **CIOs must develop an adaptive threat management architecture plan.** Rather than rip and replace current tools, IT executives must assess business and IT needs, pick a high priority area to begin ATMA implementation, build a 3 year migration plan, and develop metrics to monitor progress along the way. As this project progresses, CIOs should see fewer security emergencies, more flexibility to react to emerging threats, and lower overall costs.

The Dangerous State of the Network

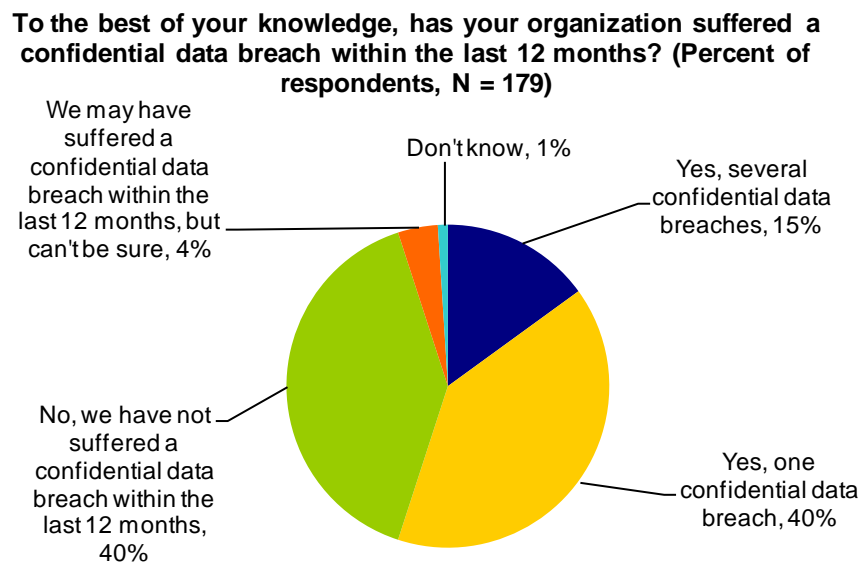
As the first decade of the 21st century draws to an end, IP networks have never been more important—or more threatened. Given global Internet connectivity, large organizations have come to depend upon IP networks to anchor business processes, critical applications, and communications. As networks flourished, however, network security risks increased precipitously, threatening network availability as well as data confidentiality and integrity. Yes, networks have always been exposed to security breaches, but today's network threats are exacerbated because:

- **Users and devices are mobile and plentiful.** Employees, business partners, and customers are all accessing the network using laptop computers, IP phones, managed/unmanaged devices, and smart cell phones. It is difficult for IT to keep up with this growing volume and one infected device can spread malware throughout the network, impact critical network services, and affect business operations.

- **Applications have become the preferred target.** A few years ago, most security attacks were targeted at the network itself, but this is no longer true. With so many “network-based” applications, cyber criminals now prefer to go after business applications themselves. Why? To paraphrase the infamous bank robber Willie Sutton, “because that’s where the money is.” About 70% to 80% of today’s attacks target applications in search of valuable information like credit card numbers, healthcare records, and Intellectual Property (IP).
- **The bad guys are sophisticated and organized.** Hacking is no longer the domain of anti-social teenagers. In 2009, cybercrime is a multi-billion dollar, global, and highly specialized business. For the right price, anyone can buy credit card numbers, hire software developers, or lease a Botnet to launch an attack. This sophistication has led to the growth of targeted attacks based on geographies, industries, or even individual organizations. One network vulnerability could let the bad guys in quickly.

Rising security threats have led to an inevitable increase in security breaches. As of this writing, the Privacy Rights Clearinghouse reports a total of 54 publicly-disclosed data breaches in 2009 (source: www.privacyrights.org), including major breaches at CheckFree Corp. (5,000,000 records), Heartland Payment Systems (up to 100,000,000 records), and the Federal Aviation Administration (43,000 records). These breaches are not unusual. According to ESG research, a frightening 55% of large organizations admit that their organization suffered at least one data breach within the last 12 months (see Figure 1).

FIGURE 1. DATA BREACH FREQUENCY



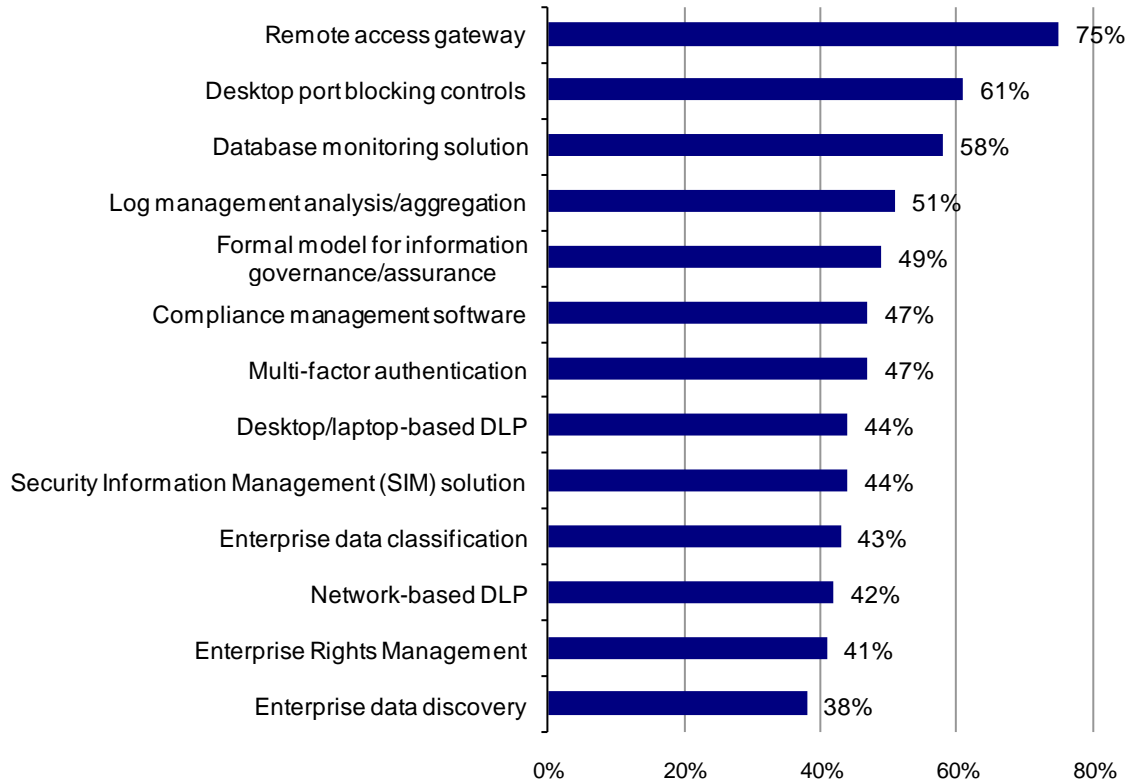
Source: Enterprise Strategy Group, 2008

Why is Network Security so Poor?

Network security is nothing new; large organizations have been investing in a network security for years. If this is the case, why aren't existing network security defenses more effective? Unfortunately, current network security defenses may be part of the problem. Rather than construct an integrated network security architecture, many organizations rely on a series of tactical point tools for security protection. This situation is illustrated by a recent ESG Research study on data security and privacy. When asked which security safeguards they used to protect confidential data, large organizations identified a large number of individual point tools, such as remote access gateways, desktop port blocking controls, database monitoring solutions, and log management monitoring (see Figure 2).

FIGURE 2. NETWORK SECURITY IS BASED UPON AN ASSORTMENT OF POINT TOOLS

**With respect to securing confidential data, please describe your organization's usage of each of the following security measures.
(Percent of respondents, N = 308)**



Source: Enterprise Strategy Group, 2008

Point tools are not inherently bad—in fact, many could be considered “best of breed” security safeguards. Unfortunately, security defenses based upon a collection of point tools makes network security more difficult because (see Figure 3):

- **Security monitoring is scattered throughout the network.** Since point tools are designed for individual threats, they don’t share information with other security systems. When the IDS detects a spike in SQL Server traffic, network and security administrators must rely on manual processes and individual monitoring tools to piece together a comprehensive view of what is happening in the network. This situation makes problem detection, isolation, and remediation far more difficult as security and IT operations specialists must rely on firefighting skills rather than accurate, detailed information.
- **Risk increases.** Piecing together a picture of overall security leaves a lot of room for speculation, omission, and human error. Additionally, point products may not be able to detect sophisticated attacks that “fly under the radar” to purposefully avoid detection. One unknown vulnerability or configuration error could leave the entire network open to attack.
- **Poor security can be costly.** To add insult to injury, a security infrastructure based upon point tools can increase capital costs and operating costs. Why? Each tool requires hardware and software licensing as well as annual maintenance fees. Day-to-day operations depend upon trained specialized administrators dedicated to a few point tools alone who can’t easily cover other devices because their management systems are so distinctive. These dollars can add up quickly.

FIGURE 3. PROBLEMS ASSOCIATED WITH NETWORK SECURITY ASSOCIATED WITH POINT TOOLS

Source: Enterprise Strategy Group, 2008

Unfortunately, the current economic recession may be aggravating this already bad situation. Many CIOs being asked to “do more with less” continue to fill security holes with point tools in spite of their known enterprise weaknesses. This may address vulnerabilities in the short term, but can only result in ultimate failure. IT managers will find that in spite of this sea of tactical tools, network security monitoring is impossible, risks escalate, and costs spiral out of control. When CEOs realize that they are paying for an expensive insecure network, IT heads will roll.

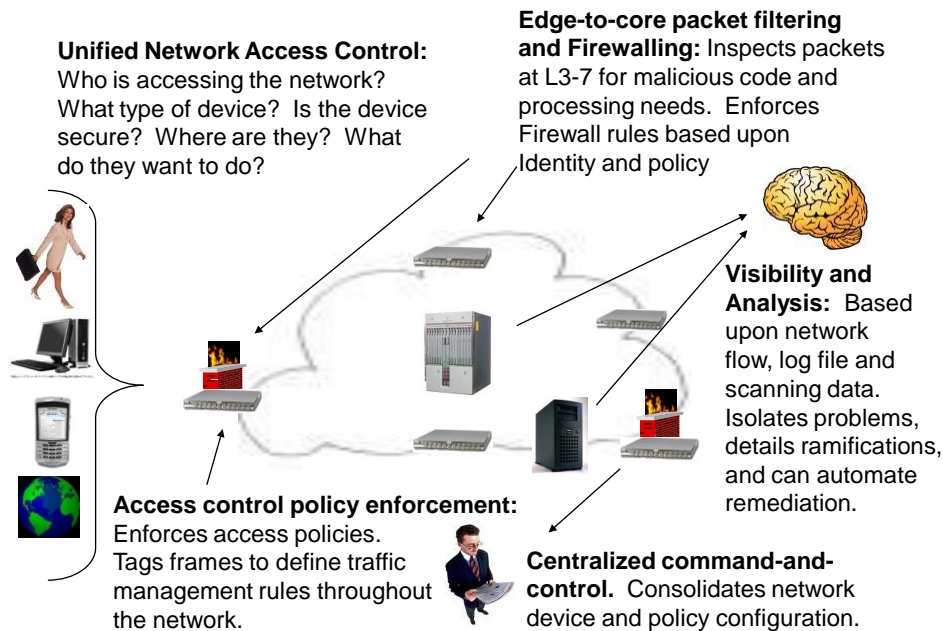
What’s Needed? An Adaptive Threat Management Architecture (ATMA)

Network security is at an important junction. The network is essential for business communications and therefore must remain available at all times, but today’s tactical and perimeter-centric network security defenses cannot provide an adequate level of protection.

To safeguard business-critical networks, large enterprises need to think in terms of network security as an edge-to-core adaptive threat management architecture that is tightly integrated with Layer 2/3 switching and routing. ATMA is built to do exactly this because it can adapt to changes in the threat landscape based upon rules and policies. When ATMA senses an attack in one area of the network, it can adapt by strengthening access policies in another. Additionally, ATMA is an architectural approach from the ground up. Network elements, security policy engines, and enforcement points all coordinate together to monitor, enforce, and audit security policies.

In order to provide this kind of comprehensive protection, ATMA is composed of:

- **Unified network access control.** Most of today's LANs are built around the notion of a dumb edge and intelligent core, but this type of architecture treats edge-based packets similarly and opens the network to malicious code attacks from infected endpoints and targeted attacks. What's needed is an intelligent network edge that enforces access policies and tags Ethernet frames regardless of whether users are located on the LAN, WAN, or remote access VPN. In short, the network edge should be able to act as an entry point which assigns network rules based upon the user, device, location, time-of-day, and type of traffic.
- **Edge-to-core packet filtering and firewalling.** Networking equipment must be able to differentiate between productive and malicious packets, regardless of location or protocol. To accomplish this, network devices must become super intelligent and perform L2-7 tasks that improve network efficiency and security. Ubiquitous packet filtering means inspecting for threats such as viruses, worms, DOS attacks, and application layer attacks throughout the network. Additionally, networks should be configurable so that consistent firewall rules can be pushed down to network access ports while an attack in one network location can trigger security enforcement actions in another.
- **Network-wide visibility and analysis.** Network security depends upon the real time monitoring of all network activity including servers, hosts, security systems, users, applications, and virtual activity—with associated data correlation and behavior analysis. Without total visibility and network intelligence, it would be impossible to properly respond to threats. Historically, this information was based upon IDS event and log-file analysis, but data from disparate systems does not provide a comprehensive picture of real-time network-wide status or historical data. This is beginning to change with the growing deployment of Security Information and Event Management (SIEM) and Network Behavior Anomaly (NBAD) systems. SIEM and NBAD systems provide full automation, including monitoring, analysis, and threat response based on the appropriate business and IT context.
- **Centralized command-and-control.** To simplify network and security management, ATMA should be based upon centralized automation and management for network and security device configuration and provisioning. This will accomplish four things: 1) Improve security by enabling IT Operations to make consistent configuration and policy changes, 2) Increase cost and operational efficiencies by reducing manual, error-prone practices, 3) Enable rapid deployment of new services due to enhanced ability to scale operations, and 4) Reduce the operating expenses associated with learning and administering multiple security management products.

FIGURE 4. ELEMENTS OF AN ADAPTIVE THREAT MANAGEMENT ARCHITECTURE

Source: Enterprise Strategy Group, 2009

Aside from these technologies themselves, ATMA will also have other technology features. ATMA devices must be highly scalable to address increasing traffic volumes of 10, 40, and 100 GbE pipes. ATMA must be tightly integrated with the network itself so it can block unwanted packets and accelerate others that are mission critical. Finally, ATMA must support current and future open standards for ease of integration and enhanced functionality over time.

ATMA may sound like an industry vision that may see the light of day in 3 to 5 years, but early implementations are actually available today. One example is the Adaptive Threat Management Solutions initiative by market leader Juniper Networks. Since its acquisition of NetScreen Technologies in 2004, Juniper has fastidiously introduced high performance devices while integrating networking and security functionality across its entire product line. In 2008, the company announced its Adaptive Threat Management Solutions initiative, which ties together its networking equipment, firewalls, high performance security devices (SRX), Universal Access Control, network and security management, and Security Threat Response Manager (STRM). Each product stands out on its own, but Juniper integrates them so the value of the whole is actually greater than the sum of its parts. Juniper is enhancing its Adaptive Threat Management Solutions with new product announcements in March 2009.

The Benefits Associated with ATMA:

Ultimately, ATMA is meant to overcome all of the weaknesses associated with point tool-based network security architecture. Since ATMA can adapt to threats in a coordinated architectural fashion, it can deliver:

- **Improved threat detection and remediation.** Since ATMA is woven into the entire network fabric, it can detect suspicious activities quickly and can then report to security professionals on threat levels or undertake automated remediation actions based upon overall security policies. This should help IT managers act quickly to limit the impact of isolated issues before they affect the availability and integrity of the network across the enterprise.
- **Respond to new types of threats.** Rapid changes to IT configurations undoubtedly will lead to new types of threats and vulnerabilities, but ATMA is designed to address these as well. New firewall rules

can be centrally configured and then distributed to perimeter and core devices. IDS/IPS rules can follow the same path. A new threat can automatically enforce a new user access policy. The central point is that ATMA allows for rapid and coordinated responses supported by centralized monitoring. The alternative is device-by-device changes, human error, and limited visibility.

- **Central reporting for forensic investigations and compliance audits.** Since ATMA centralizes all log data, it simplifies activities such as controls monitoring for regulatory compliance and corporate governance initiatives. When problems do arise, ATMA makes it possible to quickly assess who did what when.
- **Lower capital and operating costs.** ATMA is based upon a common architecture where individual pieces combine to make a more valuable whole. Multi-function ATMA components can replace numerous tactical appliances to save money on hardware, software, maintenance, and utilities. Additionally, ATMA can be centrally managed, eliminating the need for specialized administrators for individual tools and technologies. ATMA also defines best policy to help IT operations rapidly deploy solutions. Finally, ATMA's ability to detect and remediate network security threats quickly should reduce the costs associated with emergency response processes, service interruption, and network downtime.
- **Policy-based network access controls to enhance business processes with strong security.** With ATMA, users and devices can be controlled with granular access management policies for authentication and authorization. For example, Susan in HR can gain access to the HR portal when working within the corporate campus, but not from an unknown laptop or an un-trusted network. A remote consultant can gain network access, but only to certain IP addresses, ports, and protocols. In all cases, network endpoints can be checked for configuration policy compliance. In this way, ATMA can make it easier—and safer—to open the network, extend applications to remote users, and share critical data with business partners, customers, and suppliers.

In addition to these benefits, ATMA should also help large organizations simplify network configurations. With fewer appliances necessary, networking engineers can eliminate multiple network “choke points” that add latency and complexity to the network. This can add to network performance while reducing configuration and traffic management problems.

The ATMA Roadmap

ATMA is not a one-off concept, rather, it is a clear reflection of where network security must head. In the grip of economic turmoil, cost-conscious CIOs may be tempted to steer clear of strategic initiatives, but this would be a mistake leading to higher risks and costs. ESG recommends that IT executives think of ATMA as a journey rather than an ultimate destination. To proceed in the right direction, savvy CIOs should:

- **Assess business, networking, and security needs to pick a starting point.** Is the organization about to deploy new web-based applications? Do you plan to open network access to numerous non-employees? Is there any plan to consolidate data centers, deploy IP phones, or pilot new mobile applications? Any of these business and IT changes can open the network to new types of threats that demand an appropriate countermeasure. By linking ATMA to new business initiatives, IT managers can enhance protection while beginning an architectural plan for the future.
- **Think strategically, act tactically.** It is important to visualize an end goal and then work backward based upon existing network security technologies, resource constraints, and pressing security needs. Ultimately, network and security managers should create a 3 year migration plan to ATMA. Start with a business initiative or particular pain-point and move forward. To judge your success, create metrics around network downtime, helpdesk call volume, overtime hours for emergency response, and time needed for compliance audits. These should improve as the ATMA initiative progresses.

The Pressing Need for an Adaptive Threat Management Architecture

- **Partner with a leader.** ATMA security and networking integration won't likely come from an army of point tools vendors. Rather, ATMA will be delivered by market leaders with deep understanding of current and future networking requirements and security safeguards. Judge vendors on their product portfolios, network management strategy, roadmaps, completeness of vision, and commitment.

As stated above, CIOs should seek to have a fully functional ATMA as an essential component of their IT infrastructure within the next 3 years. This won't eliminate attacks, but it will lower risks, increase flexibility, and lower costs. These benefits alone should pay for the cost of admission.



20 Asylum Street
Milford, MA 01757
Tel: 508-482-0188
Fax: 508-482-0218

www.enterprisestrategygroup.com