Next-generation Security Architecture for the Enterprise

By Jon Oltsik, Senior Principal Analyst

October 2014
Contents

Executive Summary .................................................................................................................. 3
Network Security Is Increasingly Difficult – and Increasingly Important .............................. 3
Enterprise Organizations Need a Complete Security Architecture ........................................ 5
Security Architecture Objectives .......................................................................................... 6
Security Architecture in the Enterprise .................................................................................. 7
CISO To-do List ...................................................................................................................... 8
The Bigger Truth .................................................................................................................... 10
Executive Summary

Security architectures largely grew organically over the past ten years as organizations addressed a variety of new threats and tactics. This has resulted in an army of new deployed technologies like firewalls, IDS/IPS, network proxies, gateways, sandboxes, endpoint suites, etc. Over time, this patchwork approach has become more difficult to manage and less effective at blocking legitimate threats.

This situation raises a few obvious questions: Is security getting more difficult to manage? Is the current security strategy and architecture viable? If not, what’s needed? This white paper concludes that:

- **Security is growing more burdensome.** Driven by targeted threats, software vulnerabilities, high volumes of new malware, mobile devices, more users, and an increase in off-network traffic, security professionals acknowledge that network security is more difficult today than it was two years ago.¹

- **Network security presents additional challenges.** Aside from growing more difficult, network security continues to present a number of ongoing challenges. Large organizations claim that there are too many overlapping processes and controls, too many point tools, and too many manual processes. Given all of these new and historical problems, today’s network security is a mismatch for enterprise security requirements.

- **Organizations need a new architectural approach.** Existing problems telegraph what’s needed for security in the future. To be more specific, enterprises need a comprehensive solution that offers scalability, protects against both known and unknown threats, automates manual processes, and replaces point tools with an integrated set of security services. This equates to an integrated security architecture featuring centralized management for distributed visibility and enforcement across all network security services and form factors, regardless of their geographic location. Additionally, a security architecture must be tightly integrated with cloud-based threat intelligence and security analytics to help decrease an organization’s attack surface at all times while vigilantly detecting and preventing anomalous behavior, suspicious traffic, and attacks in progress.

Network Security Is Increasingly Difficult – and Increasingly Important

Since organizations connected internal networks to the Internet in the 1990s, network security has been an enterprise requirement. With all of that history, it would be natural to assume that network security is fairly routine, but just the opposite is true. In fact, recent ESG research indicates that 28% of surveyed security professionals working at enterprise organizations (i.e., more than 1,000 employees) believe that network security (i.e., knowledge, skills, management, operations, etc.) is significantly more difficult today than it was in 2012, while 51% say that network security is somewhat more difficult than it was two years ago.

Why is network security growing more difficult? Security professionals point to a number of factors including (see Figure 1):

- **The insidious threat landscape.** It is clear from the ESG research that security pros believe that the threat landscape is increasingly dangerous and is thus impacting network security efforts. This is attributed to the widespread accessibility of advanced tool kits, and the use of new techniques to avoid detection such as SSL encryption. For example, 38% say that an increase in malware sophistication is making network security more difficult, 32% say an increase in targeted attacks is making network security more difficult, and 25% comment that an increase in malware volume is making network security more difficult.

- **An increasing number of users and devices on the network.** Aside from changes in the malware landscape, security professionals conclude that network security has grown more cumbersome as a result of more network-based devices, users, and mobile devices accessing their networks.

¹ Source: ESG Research Report, *Network Security Trends in the Era of Cloud and Mobile Computing*, August 2014. All ESG research references and charts in this white paper have been taken from this research report unless otherwise noted.
• **More network traffic.** The combination of web-based applications, cloud computing, mobile computing, and technology advancement drives a steady increase in overall network bandwidth and throughput. Nearly one-quarter (23%) believe that this increase in network traffic is making network security more difficult. In addition to a basic increase in traffic volume, communication patterns are also changing. Rather than client-to-server connections, many organizations are seeing traffic spikes between users, mobile devices, and cloud-based applications. Changes like these introduce new dynamic threat vectors, making network security more burdensome.

**Figure 1. Factors Making Network Security More Difficult**

In your opinion, which of the following factors have made network security management and operations more difficult? (Percent of respondents, N=313, three responses accepted)

- An increase in malware sophistication that may lead to malware designed to circumvent traditional network security control: 38%
- An increase in the number of overall devices with access to the network: 36%
- An increase in the number of targeted attacks that may circumvent traditional network security controls: 32%
- An increase in the number of mobile devices accessing the network: 29%
- An increase in the number of users with access to the network: 25%
- An increase in malware volume: 25%
- An increase in network traffic: 23%
- An increase in the use of cloud computing services for corporate use: 21%
- An increase in the “rogue” use of cloud computing services by employees and other users with legitimate access to the network: 17%
- My organization’s IT security department is understaffed: 15%
- My organization lacks the right level of cybersecurity knowledge and skills: 12%


It is important to understand that these challenges aren’t simply minor annoyances. Increasing malware volume, network traffic, and users/devices connected to the network represent a growing cybersecurity vulnerability that increases IT risk on a daily basis. In fact, ESG research indicates that in 2013, 49% of enterprises reported experiencing a successful malware-based security breach over the past two years, and 22% of those large
organizations had more than 25 malware-based security breaches in that timeframe. CISOs have a simple choice: Build a comprehensive security strategy that encompasses the network, cloud, and endpoint to address these challenges, or suffer the consequences.

**Enterprise Organizations Need a Complete Security Architecture**

Network security is at a crossroads. The network is a vital highway for business communications and therefore must remain available and highly secure at all times, but existing tactical network security defenses cannot address nefarious malware threats or execute granular policy enforcement. What’s more, these defenses often present an operations nightmare when it comes to daily care and feeding.

ESG believes that network security requirements are changing rapidly, demanding a new type of approach for network security. To protect business-critical network highways, large enterprises need to think of security as an edge-to-core-to-cloud network and endpoint security architecture offering:

- **Centralized management.** An enterprise security architecture starts with central management for activities like policy management, provisioning, change management, and reporting. Central management can be tiered or federated if need be, but all services, devices, and monitoring should ultimately report up to some type of central console.

- **Support for any form factor in any location.** Network security services should be available in physical, virtual, or cloud-based form factors. In this way, CISOs can implement tailored protection and change form factors over time as needed. This type of flexibility is also needed to align with today’s dynamic IT technologies and business flexibility, particularly within data centers where there is an increasing percentage of east-west traffic. Organizations can unify policies across perimeter-based network security devices at corporate headquarters with cloud-based enforcement used for protecting dozens of smaller remote offices spread throughout the world. This type of coverage is especially important in order to extend security protection to the increasing use of mobile devices and cloud application use.

- **An assortment of network security services.** Network security services will be used to distinguish between productive and malicious packets regardless of application, port, or protocol. To accomplish this, a network security architecture must become super intelligent, perform Layer 2 through 7 tasks, and support ubiquitous packet filtering at the network edge through to the core of the data center. Ubiquitous packet filtering means inspecting for threats such as viruses, worms, DDoS attacks, SPAM, phishing, web threats, content leakage, and application-layer attacks, while also enforcing rules around network access for users, devices, applications, etc. A network security architecture also extends to endpoint devices themselves to coordinate endpoint and network threat prevention, detection, and remediation activities. In this way, a network security architecture can be used to block malware on the one hand and enable secure network access activities on the other.

- **Distributed policy enforcement for granular control.** Security policies for network access control, segmentation, and packet filtering must be executed, coordinated, and audited across a multitude of physical and virtual policy enforcement points across the network. Policy enforcement should be available for any type of network connection based upon the user, application, devices, or even machine-to-machine communications. To fit with modern IT infrastructure, this type of network security architecture should also support the concept of abstraction by integrating into IT and cloud computing orchestration systems. For example, web or database servers may need specific security controls for firewalling, IDS/IPS, and network segmentation to meet corporate governance standards or regulatory compliance. Granular controls should include a host of services across Layer 3 through 7.

- **Blockage for both known and unknown threats on the endpoint.** Endpoints must be protected against all exploit and malware-driven attacks, particularly those involving threats that have never been seen before. This requires a completely different approach on the endpoint, utilizing new technologies that are able to

---


© 2014 by The Enterprise Strategy Group, Inc. All Rights Reserved.
prevent attacks that have never been seen before and often evade detection by network security architectures. This means that CISOs should evaluate new security technologies that focus on attack techniques rather than individual threats.

- **Integration with threat intelligence.** To supplement internal activities, a security architecture should extend both network and endpoint security to cloud-based threat intelligence, detailing malicious darknet activities in the wild. The best threat intelligence will be multifaceted, providing insight on elements like new software vulnerabilities, bad IP addresses, URLs, C&C channels, and malicious files, while reporting on malware tactics as well. This can greatly improve network and endpoint security by using threat intelligence feeds to further strengthen prevention capabilities, and trigger timely remediation actions like creating new firewall rules or IDS/IPS signatures in real time.

- **Comprehensive visibility.** An enterprise security architecture must have the ability to collect real-time data and feed analytics engines so that security analysts can assess risk, modify security controls, or detect/respond to security incidents as soon as possible. Of course, network security visibility must encompass Layer 2 through 7 of the OSI stack—from ARP poisoning to application-layer protection. Finally, network security must include visibility into encrypted SSL/TLS traffic—an increasingly important requirement in light of the growing use of mobile devices and cloud applications.

Each of these capabilities is useful on its own, but large organizations gain the most benefits when all of the components join together to form a tightly integrated security architecture (see Figure 2).

*Figure 2. Enterprise Security Architecture*

![Figure 2. Enterprise Security Architecture](image)

**Security Architecture Objectives**

Aside from its technical components, a security architecture should help CISOs by:

- **Decreasing the attack surface.** Today’s networks block packets, ports, and protocols based upon policy enforcement rules of individual tools. Unfortunately, this type of network security is no longer adequate. To address today’s dynamic combination of users, mobile devices, cloud-based applications, and targeted threats, CISOs need more holistic policies that can be enforced by a tightly integrated network and endpoint security architecture. For example, there is no reason why a user should be able to receive an
executable file via Gmail when using her work PC from the corporate LAN. An architecture should have the ability to block this activity by terminating/inspecting SSL traffic, then applying content inspection rules based upon a particular user, device, and application. Or the architecture should be able to restrict certain behaviors on the endpoint that might increase risk (i.e., prevent the execution of a particular file type directly from removable media). Logical policy enforcement like this could greatly reduce cybersecurity risk.

- **Improving the efficiency of threat detection and prevention.** While a well-planned security architecture can decrease the attack surface, sophisticated exploit and malware-based attacks will inevitably find a path into the network. A security architecture must offer tightly integrated layers of defense designed for full “kill-chain” coverage. When a zero-day exploit or malware file finds its way through a network sandbox, other defenses such as advanced endpoint protection and analytics should be available to detect and prevent attack lifecycle behavior like use of exploit techniques on the endpoint, C&C communications, DNS hijacking, or endpoint registry changes. The combination of integrated layers of defense and comprehensive network and endpoint coverage can help the security team detect a threat and take action at any stage of a cyber-attack.

- **Accelerating remediation processes.** Once a cyber-attack is detected, CISOs must respond quickly to minimize damage. A security architecture can help accelerate remediation by pinpointing malicious activities down to an atomic level such as specific file downloads, network connections, or endpoint configuration changes. Enterprises can use this precise information to actually automate some remediation processes. When a compromised endpoint is detected, it can be quarantined from the network immediately. New darknet threat intelligence can automatically generate firewall rules or IDS/IPS signatures. Automated remediation activities like these can help the security operations team scale to meet the increasing volume and harmfulness of malware attacks.

Meeting these objectives requires more than central management, data exchange, and tight integration. Given the increase in malware, network traffic, users, and devices, a security architecture must be built for extremely high performance and scale in order to inspect, filter, and enforce security policies across billions of packets travelling across corporate and cloud networks. CISOs must remember that any security service causing network latency, endpoint performance degradation, and business disruption won’t be tolerated.

**Security Architecture in the Enterprise**

The security architecture described will come together over the next few years, driven by user requirements and technology innovation. This timing is fortuitous as it aligns perfectly with network and endpoint security strategies at large organizations. When asked to identify the factors that have the most significant impact on shaping their organization’s security strategy, enterprise security professionals pointed to things like preventing/detecting exploit and malware-based threats, support for mobile computing initiatives, and the need for network security to be more flexible to support dynamic business processes (see Figure 3). These requirements are inherent within an enterprise security architecture. Based upon this, it is not surprising that 48% explicitly cited the need to build an integrated security architecture featuring central command-and-control and distributed network security policy enforcement.
CISO To-do List

Large organizations are certainly moving toward a comprehensive security architecture, but there is plenty of work ahead. Many firms remain confused about where to start this process and how to separate industry hype from practical reality. To proceed in an efficient and pragmatic direction, ESG recommends that CISOs:

- **Start at the perimeter and work back into the network.** While an enterprise-wide security architecture offers comprehensive coverage, most organizations have the bulk of their security investment deployed at the perimeter today. Given this, it’s best to start at the perimeter by consolidating incongruent network security technologies into integrated services using physical and virtual controls. For example, an enterprise-class next-generation firewall (NGFW) can help CISOs consolidate firewall, IDS/IPS, web threat management, URL filtering, and sandboxing with advanced malware detection/prevention onto one system, with a single management platform and reporting engine. As organizations implement a network security architecture at the perimeter, they should be poised to extend it with plans for critical internal network intersections, campus Wi-Fi networks, and data centers.

- **Develop granular network access and segmentation policies.** As part of the perimeter phase of a security architecture, enterprises should start to instrument the network with granular network access policy enforcement based upon details like user identity, device type, location, application and data access, etc.
For example, a “contextual” security policy may allow the CFO to access month-end financial data from her iMac on the corporate LAN but block access when she tries to view this data from her iPad on a public network. As the network security architecture project evolves from the network perimeter to the corporate network, security managers should also consider their requirements for fine-grained network segmentation of application flows and machine-to-machine traffic. Network security architecture integration with technologies like software-defined networking (SDN) will enable this type of granularity and flexibility over time.

- **Plan on network and endpoint security alignment.** In the past, network and endpoint security were managed independently for the most part, but this legacy model creates security holes that are easily exploited by sophisticated cyber adversaries and advanced malware. To bridge these gaps, organizations should plan on network and endpoint security integration. For example, advanced malware detection and threat intelligence on the network should collaborate with endpoints to link suspicious traffic to actual endpoint behavior. In this way, security analysts can increase prevention capabilities within both the network and the endpoint, and also utilize the new forensics to quickly pinpoint the timing, impact, and scope of attacks across the network.

- **Create a plan for automated remediation.** Even the most proficient security professionals can no longer keep up with the volume and sophistication of the threat landscape. Given this situation, the security team tends to focus on high-priority investigations and ignore more routine network security hygiene activities that could actually decrease the attack surface across the network. This is understandable but certainly not ideal. CISOs should be addressing this issue with a combination of threat intelligence and network security policy enforcement so they can update security controls on an automated basis. CISOs should also be taking advantage of the automation that exists between sandboxing and next-generation firewalls so new defenses can be immediately applied back to the network without “man-in-the-middle” intervention. In this way, security analysts can focus on the limited number of critical events while technology intelligence and automation manages threat volume to fine-tune network security controls and preventions for the larger majority of attacks.

- **Move to big data security analytics as part of a network security architecture plan.** As the security architecture comes together, it will expose a tremendous amount of data about new threats, users, devices, application sessions, packets, flows, etc. Large organizations should be ready for this eventuality with the right tools to collect, process, store, and analyze growing volumes of data. This will likely require real-time and asymmetric big data security analytics tools based upon streaming processing and big data technologies like Hadoop, Mahout, MapReduce, and Pig. CISOs should assess their security analytics capabilities and fill holes with new technologies and services as required.

- **Cast a wide net for network security technology.** In the past, many organizations fulfilled their network security needs with a series of boxes from assorted vendors or by relying on their networking vendor for routing, security, and switching. While this may have been adequate in the past, it is important to remember that an enterprise security architecture is a new, innovative, and evolving area. Rather than default to the status quo, CISOs should cast a wide net, talk to lots of providers, think outside the proverbial box, and take the time for due diligence before selecting a vendor or vendors to anchor their security architecture moving forward. This is a very important bet, so CISOs must make sure they get it right by applying the appropriate amount of time, resources, research, and open mindedness to their decision making process.
The Bigger Truth

Large organizations must face a number of facts:

1. Network and endpoint security is growing more difficult, driven by an increase in threats, users, devices, and network traffic.
2. As the environment continues to change, enterprises are dealing with existing network and endpoint security challenges across people, processes, and technologies.
3. Large organizations may become even more vulnerable to cyber-attacks because of numerous dynamic IT initiatives like cloud computing, mobile computing, and the big data analytics.

In light of all that is happening, CISOs must realize that status quo security strategies are actually part of the problem. Rather than try to tweak enterprise security with tactical changes, security managers must think more strategically about what they really need in the short and long term.

In an analogous situation from the 1990s, enterprise organizations abandoned departmental business applications in favor of ERP systems. This was a difficult transition, but tightly integrated ERP systems ultimately delivered far-reaching business benefits as departments were able to coordinate workflows, manage finances, and analyze data in a more comprehensive manner. Similarly, an enterprise security architecture involves tearing down old walls and integrating products in pursuit of comparable benefits. Ultimately, an enterprise security architecture should help organizations coordinate defenses, manage operations, and analyze data, leading to more efficient and effective security.