Building an Enterprise Security Architecture

By Jon Oltsik, Senior Principal Analyst

March 2016

This ESG White Paper was commissioned by Forcepoint and is distributed under license from ESG.
Executive Summary

ESG research indicates that 70% of surveyed organizations will increase cybersecurity spending in 2016. While this is welcome news for CISOs, it’s important to note that increased cybersecurity investment is not enough. Rather, large organizations need to adopt a more strategic approach to enterprise security. This white paper concludes:

- **Enterprise security is held back by point tools and manual processes today.** Many large organizations address information security with one-off point tools, each with its own administration, operations, and reporting capabilities. Unfortunately, each tool demands lots of overhead, while stitching together individual tools across the network requires lots of manual processes and leg work. In the meantime, given the global cybersecurity skills shortage, CISOs can’t depend upon people (or point tools) alone to protect the enterprise—especially in light of the constant volume of security alerts they receive on a daily basis.

- **The situation will get even worse.** As if things weren’t bad enough, security professionals face a number of evolving business needs and IT initiatives, making cybersecurity even more difficult. For example, BYOD policies have the potential to add hundreds of devices to the network. In the meantime, application workloads and sensitive data are moving to the public cloud where security controls and monitoring are amorphous at best, making the concept of a network perimeter obsolete. CISOs face a future of more devices, more network traffic, and less control than they have today. At the same time, threats grow increasingly dangerous inside the network and in the wild. This is a recipe for disaster.

- **CISOs need to adopt an enterprise security architecture to improve efficacy and efficiency.** Today’s patchwork security approaches are no longer adequate. So what’s needed? An enterprise security architecture built for integration, central command and control, distributed enforcement, and comprehensive monitoring of all security-related activities.

Overview

According to ESG research, cybersecurity is a top priority. In ESG’s 2016 IT spending intentions research, 43% of organizations identified increasing cybersecurity as a top business initiative driving technology spending (see Figure 1).
While cybersecurity is a high priority moving forward, many organizations remain burdened by their past behavior, with information security practices that are:

- **Built on top of an army of point tools.** Enterprise security infrastructure was built organically over the past 15 years. As new threats emerged, CISOs simply deployed a new software agent or network gateway as a countermeasure on a tool-by-tool basis. As years went by, this approach resulted in an army of independent point tools, each with its own administration, policy management, and reporting. While an individual tool may have its own unique value and cybersecurity professionals have been trained to purchase “best-of-breed” solutions, this type of haphazard security infrastructure makes it difficult if not impossible to get an end-to-end enterprise view of cybersecurity risk or status.

- **Hampered by manual processes.** The morass of security point tools makes operations a real challenge as the security staff trains, administers, operates, and reviews each tool individually. As a result, cybersecurity is often divided into a series of disconnected manual processes dependent upon the dedication and perseverance of the security staff. While security teams deserve admiration, these manual processes depend on key individuals and can suffer when staff members are on PTO or leave the organization. Furthermore, manual processes can’t scale to address increasing cybersecurity workloads. This is especially true as enterprise organizations struggle to process, analyze, prioritize, and respond to a growing avalanche of security alerts.

- **Limited by a global cybersecurity skills shortage.** CISOs also face an external force beyond their control—the global cybersecurity skills shortage. According to ESG research, 46% of organizations say that they have a problematic shortage of cybersecurity skills at present, making cybersecurity skills the most prevalent shortage of any technology area (see Figure 2).² Many have open requisitions to add infosec headcount, but these jobs can remain unfilled for months or years at a time.

---

Taken together, these issues lead to a suboptimal situation where understaffed security teams are:

- **Easy prey for targeted cyber-attacks and malicious insider behavior.** Sophisticated cyber-adversaries capitalize on the lack of security technology integration by exploiting gaps in controls and defenses. The proof? Large organizations like OPM, Sony Pictures, and Target had layered defenses deployed on networks and hosts, but these countermeasures couldn’t help them prevent or detect cyber-attacks that led to damaging data breaches. The same holds true when it comes to insider attacks—even the NSA couldn’t prevent or detect Edward Snowden stealing volumes of sensitive data.

- **Overwhelmed by security alerts and events.** Security tools produce volumes of event data and alerts on a regular basis. Unfortunately, security analysts find it difficult to sort through this data to separate high-priority events from more pedestrian ones. As organizations deploy additional detection tools, security professionals complain that it can actually get more difficult to manage the signal-to-noise ratio.

- **Way behind on incident detection and response.** Based upon industry research, it can take between 100 and 200 days for the average organization to detect and respond to a cybersecurity attack in progress. It is not unusual for cyber-attacks to go completely undetected by the security staff altogether. CISOs often receive bad news from third-parties like law enforcement agencies, security researchers, or industry peers; before hearing from their internal team.

As if things weren’t bad enough, CISOs should anticipate even more work in the days ahead. Why? New IT initiatives like BYOD, cloud computing, and IoT applications will only increase the number of devices on the network and network traffic. At the same time, cloud computing and mobility all but make obsolete the concept of a network perimeter as application workloads, users, and sensitive data regularly move in and out of corporate networks.
Enterprise Security in Transition

Large organizations must face reality: Legacy cybersecurity strategies are no match for today’s sophisticated and targeted cyber-attacks. And while there is a clear need to improve security controls for attack prevention, CISOs must assume that cyber-adversaries and careless or malicious insiders will circumvent security defenses and compromise their networks. This means that enterprises also need to bolster processes and capabilities around incident detection and response. Finally, cybersecurity professionals must be prepared to address risks associated with sophisticated attacks that often employ “low and slow” tactics over weeks or months.

So what should enterprise organizations do? To address cyber-risks and threats, CISOs must adopt an enterprise-class security strategy including (see Figure 3):

- **Central command and control with distributed enforcement.** CISOs need central administration for processes like policy management, configuration management, change management, etc. They also need the ability to do service chaining across distributed enforcement technologies to enable activities for business processes while blocking malicious behaviors. For example, CISOs should have the ability to create policies that span across hosts, networks, and cloud infrastructure so they can apply security controls to specific applications, data, or users regardless of location.

- **Tight integration across security tools.** To enable central command and control and distributed enforcement, infosec teams need a security software architecture that can integrate disparate security point tools into a cohesive cybersecurity system. A security architecture must be built with APIs for data import/export with other security and IT tools when needed.

- **End-to-end visibility for threat management.** Rather than observe threats on a tool-by-tool basis, enterprise security depends upon aggregated visibility of logs, events, alerts, and other internally derived data into a common security analytics platform. Cybersecurity analytics should also include threat intelligence feeds so that security analysts have real-time views of malicious “in-the-wild” activities. Finally, security analytics must include intuitive interfaces so they can be used effectively by all levels of cybersecurity personnel.

- **Process automation and orchestration.** With an acute shortage of cybersecurity talent available, CISOs should look for ways to streamline security operations. Security analysts need the flexibility to customize GUIs and reports based upon their roles, responsibilities, and level of seniority. This can help cybersecurity teams coordinate activities, develop workflows, and accelerate training for junior personnel.
Enter Forcepoint

To address today’s cybersecurity requirements, CISOs should work with technology partners that offer an enterprise-class security architecture by providing the functionality described in Figure 3. Unfortunately, most vendors continue to produce point tools rather than more comprehensive solutions. Forcepoint (i.e., the new company formed through the combination of Raytheon Cyber Products, Websense, and Stonesoft) is an exception, standing out from the cybersecurity vendor crowd.

With a history of strategic acquisitions, Forcepoint has a broad portfolio of security products that the new company is intent on integrating to deliver an enterprise-class platform featuring central command and control and distributed enforcement for safeguarding users, data, and networks. Forcepoint also offers:

- **Comprehensive insider threat and data security.** TRITON AP-DATA can provide sensitive data protection across endpoints, at network ingress/egress points, and when stored in the cloud. This is especially useful for regulatory compliance or for detecting insider threats during the early stages of an attack.

- **Security for helping organizations move their business to the cloud.** Forcepoint enables organizations to use Office 365 and public networks without putting their data at risk. It can also discover shadow IT and the use of risky apps. The solution also enables organizations to protect their own Linux-based cloud app farms against threats that may slip by other defenses.

- **Network security.** Forcepoint’s Stonesoft NGFWs protects enterprise networks with centrally managed security that is easier to set up and maintain, designed for high availability, and defeats the advanced evasion techniques that attackers now use to try to sneak past perimeter defenses.

- **A wide array of services offerings.** Given the global skills shortage, CISOs may need help addressing particular areas of cybersecurity. Forcepoint can help with services in areas like data security, security intelligence, and government certifications.

With its products, services, and aggressive roadmap, Forcepoint is focused on building an integrated cybersecurity architecture that meets the integration, scale, and operations requirements of large organizations. CISOs looking to
narrow their list of security vendors and establish partnerships with enterprise-class cybersecurity vendors should give Forcepoint a call.

**The Bigger Truth**

In order to deliver automobiles to the masses, Henry Ford realized that Ford Motor Company needed to bring down the cost of production. To achieve this goal, Ford used four principles: interchangeable parts, continuous flow, division of labor, and reduced wasted effort. By employing these principles, Ford was able to automate production processes, improve efficiency, and accomplish his goal of lowering production costs.

Similarly, large organizations that want to improve cybersecurity efficiency need integrated tools, customized workflows, specialized skills, and streamlined operations. Unfortunately, they can’t achieve these goals with their current army of point tools and reliance on manual processes.

Large organizations can learn from Henry Ford’s effort by working to improve their organizations in the very same four areas. To get there, they will likely need to work with vendor partners that can support their need for integration, operational efficiency, and enterprise scale. Since this is the exact reason why Raytheon acquired Websense and created Forcepoint, CISOs should find it worthwhile to assess how Forcepoint aligns with current and future cybersecurity needs and objectives.