SOLUTION SHOWCASE

Check Point Expands Its Integrated Enterprise Security Management

Date: February 2016 **Author:** Jon Oltsik, Senior Principal Analyst

Abstract: Large organizations spend millions of dollars on cybersecurity defenses and budgets continue to rise on an annual basis. Unfortunately, many enterprises continue to be overwhelmed by security alerts, cyber-attacks and data breaches. Why? Some organizations continue to rely on point tools and manual processes for their security needs. However, this strategy doesn't scale and has proven ineffective for the increasingly dangerous threat landscape. Large organizations need a different approach featuring a tightly integrated security management architecture that consolidates policy management/enforcement, supports security management automation and orchestration, and unifies threat management visibility. Check Point Software's recently introduced R80 Platform is designed to deliver this exact type of security management architecture.

Overview

According to ESG research, 79 percent of cybersecurity professionals working at enterprise organizations (i.e., those with more than 1,000 employees) believed that network security had become more difficult from 2012 to 2014 (i.e., network security provisioning, policy management, policy enforcement, network security monitoring, etc.).[1] Similarly, 80 percent of enterprise security professionals believed that endpoint security had become more difficult in the two years leading up to 2015.[2]

Why are these fundamental infosec areas becoming more difficult? While there are numerous reasons for this change, ESG believes that these difficulties are being driven primarily by:

- Increasing Threats. According to multiple threat researchers, the number, sophistication and virulence of cyber-threats continue to grow on an annual basis. Enterprise organizations are experiencing these changes first hand. ESG research indicates that 67 percent of cybersecurity professionals working at U.S.-based critical infrastructure organizations believe that the threat landscape has gotten worse over the past two years (see Figure 1).[3]

[1] Source: ESG Research Report, *Network Security Trends in the Era of Cloud and Mobile Computing*, August 2014.
[2] Source: ESG Research Report, *The Endpoint Security Paradox*, January 2015.
[3] Source: ESG Research Report, *Cyber Supply Chain Security Revisited*, September 2015.

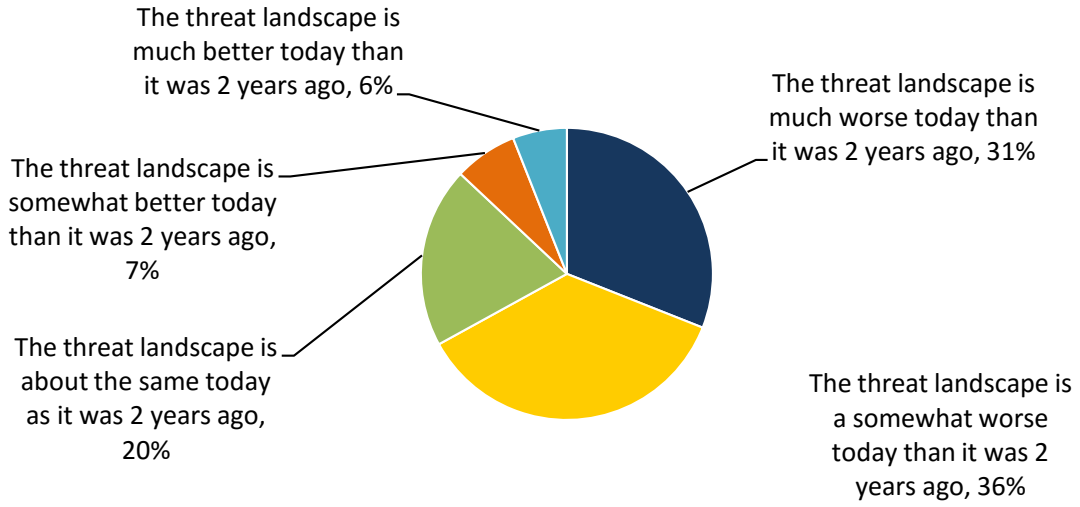
- **A Dependence on Security Point Tools and Manual Processes.** Most organizations build their security defenses organically over time, adding gateways, security agents, and policy enforcement points on an ad-hoc basis. This results in a disconnected morass of point tools, each with its own policy management, configuration management, and reporting engine. This burdens the infosec team to manage security with manual processes, adding tremendous operational overhead—an acute issue given the global cybersecurity skills shortage.

- **A Lack of Real-time Visibility.** The limitations posed by current security technologies also hinder an organization's ability to do continuous monitoring for risk management as well as incident detection and response. Security analysts often find themselves "flying blind" or assessing their security status on a static piecemeal basis.

Overwhelmed CISOs now realize that legacy security tools and processes are no match for today's IT complexity or dangerous threat landscape. Enterprise organizations must make extensive changes to their cybersecurity strategies or face an unacceptable level of cyber-risk moving forward.

FIGURE 1. Cybersecurity Professionals Believe the Threat Landscape is Getting Worse

How would you rate the current threat landscape (i.e., potential security threats such as malicious code attacks, DDoS, targeted attacks, cybercrime, state sponsored industrial espionage, etc.) faced by critical infrastructure industry organizations as compared to the last 2 years? (Percent of



Source: Enterprise Strategy Group, 2016

Enterprise Security Management in Transition

One of the primary concerns with today's cybersecurity infrastructure is directly related to security management. It is too complex and labor-intensive to implement security policies, monitor threats, or respond to issues through a wide assortment of management portals, manual processes, and point tools.

So how can enterprise organizations solve these problems? To address cyber-risks and threats, CISOs must adopt a security management architecture (see Figure 2) designed for:

- **Tight Integration across Security Tools.** The SOC team needs a security management platform that simplifies policy creation and enforcement across security domains like application security, data security, endpoint security, and network security. Given today's distributed and mobile IT infrastructure, security management should also extend for policy enforcement of workloads hosted in private and public cloud environments. The key here is converging security

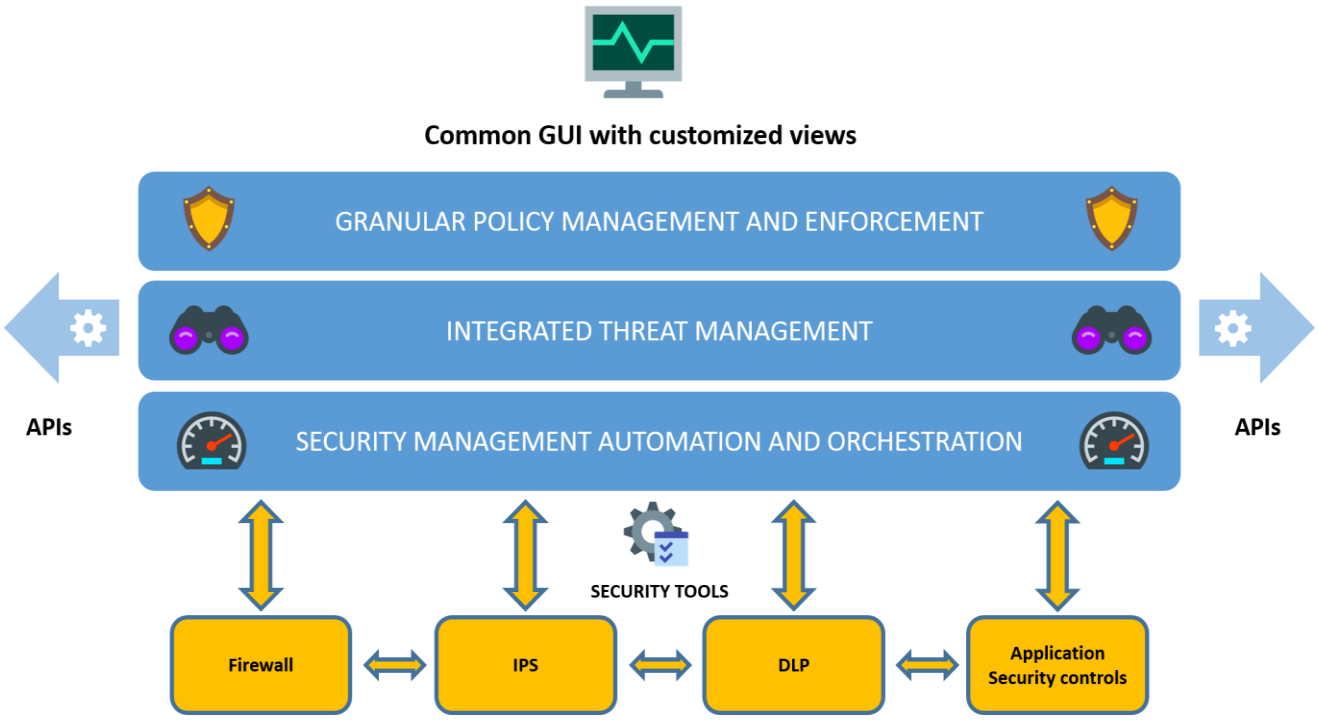
into central "services" that can be accessed, analyzed, and modified by the entire security staff. This type of consolidation can help CISOs gain more effectiveness, efficiency, and productivity out of security people and processes.

- Granular Security Policies That Align With Business Processes. To enable the business, security and IT operations managers need to create and enforce security policies based upon identity attributes like a user's role, location, or the type of device used. A modern security management architecture should also provide a simple interface for policy management, enabling the CISO to support network-based business processes while managing risk. Additionally, granular security policies should apply to new types of micro-segmentation that can be used to decrease the network attack surface.

- End-To-end Visibility for Threat Management. Rather than observe threats on a tool-by-tool basis, security management platforms should aggregate visibility to all logs, events, and alerts into a common user interface. Aside from internal data, security management should also include tight integration with threat intelligence feeds so the CERT team can compare suspicious network behavior with real-time data about what's happening "in the wild." A security management architecture should also include intelligence designed to monitor controls, identify weaknesses, and suggest modifications for further hardening and system protection.

- Process Automation and Orchestration. According to ESG research, 46 percent of organizations claim they have a "problematic shortage" of IT security skills.[4] Given this deficiency, CISOs should look for ways to help them streamline security operations wherever possible. A security management architecture should offer open APIs for software integration for input/output of security data. Security analysts should have further flexibility to customize dashboards, views, and reports based upon their roles, responsibilities, and level of seniority. This is critical for allowing the SOC team to collaborate on policy creation, multi-task, and develop workflows that accelerate incident response responsibilities.

FIGURE 2. Security Management Architecture



[4] Source: ESG Brief, *Cybersecurity Skills Shortage: A State of Emergency,* February 2016.

Check Point Introduces the R80 Security Management Platform

Check Point Software, a well-established leader in cybersecurity, has always been known for its advanced security management. Recently, Check Point introduced a new security management platform (R80) designed to drastically improve security management for its customers.

R80 aligns well with the requirements described above, as it is designed to help CISOs address security management needs across people, process, and technology. Check Point R80 supports:

- Next-generation Security Policies. Check Point's R80 unified policy consolidates policy management—across applications, networks, devices, and cloud-based workloads. Policies can also be easily segmented into more manageable sections for delegation and automation of tasks.
- Integrated Threat Management. R80 is also powerful threat management, giving a single view of risk as it consolidates logs, events, threat intelligence, monitoring, and reporting into a common interface. The CERT team is then able to build customized reports for specialized tasks like forensic investigations, threat "hunting," or monitoring security health and compliance.
- Efficient and Automated Operations. With common policies, R80 helps organizations automate repetitive tasks and improve the productivity of junior and senior cybersecurity staff members. Check Point also instruments R80 with "smart APIs" that can help the SOC team orchestrate workflows and interoperate security management with IT operations tools.

Check Point realizes that enterprise security is often built with heterogeneous technologies, and plans to use its "smart APIs" to create a partner ecosystem as well as help its customers perform their own custom integrations. Check Point also developed an R80 crowdsourcing community so customers can ask questions, share code, and stay up to date. ESG believes this will be especially attractive to large enterprises as well as organizations in particular industries whose cyber-defenses must be tuned for particular industry threats.

The Bigger Truth

Famed physicist Albert Einstein once defined insanity as "doing the same thing over and over again and expecting different results." Unfortunately, this is exactly what many organizations are doing with cybersecurity—continuing to rely on point tools and manual processes while facing a continuous wave of targeted sophisticated threats. This is a proven recipe for failure.

Enterprises must recognize that enterprise security is moving through a period of massive transition. To improve security efficacy and operational efficiency while enabling new business processes, large organizations need to move from point tools to a tightly integrated security management architecture that aggregates policy management/enforcement, supports automation and orchestration, and provides a consolidated view for threat management. CISOs looking for this type of architecture should contact Check Point to see how its recently released R80 aligns with their cybersecurity objectives, requirements, and strategies.