FORTINET

WHITE PAPER

What to Look for in a Cybersecurity Open Ecosystem

Executive Summary

Enterprise IT is growing more complex, with rapid advances in areas ranging from multi-cloud to microservices, from machine learning to containers. One global survey of CIOs reveals that a single mobile or web transaction crosses about 35 different technology systems, up from 22 only five years ago.[1] This growing complexity makes it difficult for security teams to monitor and protect enterprise IT. It doesn't help that, by one analysis, there are 70 categories of security solutions covering everything from application security testing to wireless intrusion detection.[2] Typically, these solutions aren't aware of each other and work independently in silos, and that creates a huge security gap. What's needed is a cybersecurity open ecosystem, one that unifies solutions—enabling them to communicate and work together. But what should the underlying security architecture look like? What security elements are needed to make it work? And what new benefits and use cases could it enable?

Evaluating Architectural Elements

A number of factors are making cybersecurity increasingly challenging:

- The attack surface is rapidly expanding and evolving, with 1 million new Internet-of-Things (IoT) devices being added daily.[3]
- Security solutions proliferate, but operate in silos: enterprises have an average of 75 security products in use.[4]
- Threats are evolving quickly and becoming more sophisticated (e.g., 97% of viruses now employ polymorphism[5]).
- Deploying security solutions can be complex and error-prone: almost 90% of cyberattacks are caused by human error or behavior.[6]
- There is a shortage of security staffing and expertise: 1 million cybersecurity roles are currently unfilled.[7]

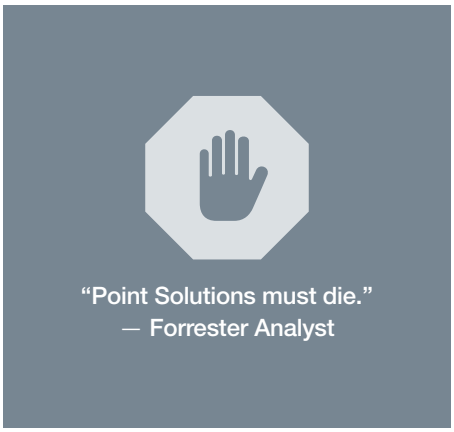
To address these challenges, an open cybersecurity ecosystem is required, one that unifies multivendor solutions. The resulting collection of solutions should be broad, integrated, and automated. Specifically, a security approach needs to:

- **Provide broad visibility** by enabling previously siloed security elements to communicate with each other.
- **Integrate solutions** so they can share threat intelligence against advanced threats, and coordinate an automated response and enforce policies in a consistent manner.
- **Maximize automation** to eliminate routine manual steps and errors, help alleviate the shortage of security expertise, and deliver synchronized and consistent security as a force multiplier.
- **Simplify deployment** by providing a large ecosystem of preintegrated, prevalidated, and unified solutions, speeding time to protection and minimizing systems integration costs.

"Point solutions must die," notes a Forrester analyst, who indicates that when he was a security practitioner, he sought to purchase only best-of-breed, stand-alone point solutions. "One of the problems with this approach is that it results in a bloated security portfolio with little integration between security controls. This bloat adds unneeded friction to the infosec team's operational responsibilities."[8] He proceeds to note that, "Incident response isn't about point solutions; it's about ecosystems."[9]

Open Ecosystem Architecture Should Include Certain Elements

The problem is that most cybersecurity solutions aren't aware of each other, and this lack of integration and resulting complexity slows security teams and provides attackers with opportunities to exploit. An open ecosystem needs to include three architectural elements:



Open Architecture and APIs

An open architecture enables multivendor security solutions to interconnect to each other to share information and perform coordinated actions. Application programming interfaces (APIs) enable different applications and systems to communicate with each other. As these components of the open architecture share threat intelligence, they can deliver broad visibility over the attack surface to enable IT and security teams to understand what is going on in the deployment, and enable a more effective, coordinated response.

Connectors

A connector enables deep integration between security products and other products, platforms, and the open ecosystem. Such purpose-built integration modules facilitate real-time communications and enable automatic updates across the ecosystem, including capabilities such as automatic synchronization with operational changes in the infrastructure, reducing risk and saving the security team from the burden of manual updates.

Connectors leverage the open architecture and interfaces to make it possible to integrate complex solutions with as little as a single click. Capabilities they can deliver include:

- Share policies across multiple clouds and software-defined networks (SDNs)
- Automatically trigger coordinated actions between solutions based on events
- Integrate with IT service management and incident response systems
- Integrate external threat feeds and automate security remediation
- Automatically apply security protection profiles assigned to each user
- Automatically quarantine endpoints when there are indicators of compromise (IOCs)

DevOps Automation Tools and Scripts

Another way to unify solutions is with automation tools and scripts, which are especially relevant for DevOps teams and associated processes. These automate security provisioning, configuration, and response, among other functions. They enhance consistency in policy enforcement and accelerate remediation. They enable short-staffed DevOps teams to quickly and efficiently deploy new security solutions to address their business and security policy needs.

Consider the example of an automation script written to protect workloads in the cloud by linking a threat detection feed from the cloud provider to actions by virtual firewalls in the workload environment. The script enables the information in the threat feed to propagate to the firewalls so they can automatically block traffic from any compromised source identified in the feed. Scripts like this can automate responses and workflows throughout the environment, unifying security.

The community associated with an open ecosystem, including vendors, partners, and customers, develops these tools and scripts, and shares them through code repositories such as GitHub. Having these community-developed resources promotes collaboration and drives security innovation from anyone.

Security Use Cases Enabled by Integrated and Automated Solutions

When today's security solutions are integrated with open APIs, connectors, and automation tools and scripts, their capabilities can be combined in new, innovative ways to address a variety of use cases. For the purposes of this paper, a few of the more prominent and representative ones are highlighted below.

Coordinated Security Policy Management

It is complex to administer security policies in a large enterprise, especially with multivendor products in a heterogeneous deployment. It is not unusual for firewalls to be spread across different types of IP, wireless, and SD-WAN networks, and hosted in private and public clouds from different vendors in different regions. Administrators must access different consoles to manage the firewalls, and it's difficult to see what's going on.

What is needed is an open ecosystem that integrates security products and technologies and enables coordinated management and enforcement of security polices. With an open security architecture, multiple technology vendors can enhance security policy management by plugging their security components into the open security architecture—through APIs, connectors, or automation tools. Security leaders need to look for management capabilities that:

- Provide broad visibility across the networking and security components in the deployment, including policy information configured in each security component.
- Reduce the attack surface by modifying security policies to optimally restrict access and traffic to address security imperatives.
- Streamline network security changes by automating their design and provisioning.
- Check rules against compliance policies to flag risks.
- Identify and fix security policy rules that are misconfigured or unused.
- Provide automated audit trails to comply with regulatory standards such as PCI DSS and SOX.

Connectors ... deliver deep integration with as little as a single click.

Capabilities can be combined in new ways with an open ecosystem approach.

Transforming Endpoint Security

Organizations are seeing their network environments become more complex as they extend their network architecture to the cloud, mobile, and IoT/OT (operational technology) networks. The result is a rapidly expanding attack surface.

To address the expanding attack surface and proliferation in endpoints, security leaders must ensure that security solutions they add fit into a broader, open, integrated security architecture. In addition, endpoint security must transform in this scenario, delivering multilayer, machine learning-driven endpoint prevention, detection, and response. Endpoint security can no longer operate in a silo, isolated from the broader network. Rather, it must seamlessly integrate firewall, sandbox, client, mail, network access control (NAC), and security information and event management (SIEM) protection. Capabilities include the ability to:

- Detect zero-day and sophisticated malware attacks.
- Share threat intelligence to block advanced threats inside and outside the perimeter.
- Block a device when an active threat is detected on that endpoint, stopping attackers from using the hijacked device.
- Synchronize remediation in real time across endpoint security, network security, and other security components at any point in the threat life cycle.

Securing the Cloud

Cloud environments reduce costs and increase agility. As a result, one-third of enterprise applications are now cloud-based—an average of 61 per enterprise.[10] At the same time, 90% of cybersecurity professionals confirm they are concerned about cloud security, up 11% from the prior year.[11]

Cloud vendors have made it clear that customers share security and compliance responsibilities. End-users have a responsibility to configure their own security for elements such as guest operating systems, databases, and applications.

In this instance, organizations need to be able to extend a unified security posture from their data centers, distributed locations, and branch offices to their cloud environments. A unified security architecture and open ecosystem that integrates security solutions make this possible. The resulting capabilities include the ability to:

- Integrate firewall, intrusion prevention, antivirus, application control, WAN optimization, data loss prevention, web filtering, and antispam filtering functions on cloud platforms and other environments.
- Automatically update all elements with advanced threat intelligence.
- Automatically scale virtual firewall instances in the cloud when cloud workloads scale, maintaining performance during peak demand.

Protecting Operational Technology (OT)

OT includes industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems. These regulate equipment such as valves, switches, and machinery across many industries including energy, electric, water, manufacturing, and even military applications.

Because OT governs critical infrastructure, it's a primary target for attack. Within the past 12 months, 51% of organizations report an OT-related security breach.[12] Part of the problem is that organizations are increasingly connecting these systems to IP networks so they can be centrally managed and updated. However, OT systems are often decades old and lack security features such as basic authentication and encryption, increasing risk and exposing vulnerabilities that cyber criminals will exploit.

Security leaders need to look for an integrated security architecture and associated open ecosystem that deliver on OT security by integrating monitoring, firewall, SSL inspection, and threat detection and remediation capabilities for their OT deployments. This enables them to:

- Gain visibility on their OT networks across hundreds of facilities from a single console.
- Use artificial intelligence (AI) to profile system behavior and detect anomalies in real time.
- Send alerts when an anomaly is detected, and modify firewall policies to block it.
- Segment the network to contain attacks to only one portion and prevent lateral propagation of threats.
- Incorporate a global threat intelligence feed that enables visibility and control for advanced threats and zero-day attacks.

Cybersecurity Must Come Together

There are 2,500 cybersecurity vendors today, almost double the number of a few years ago—and few work together.[13] Look for a cybersecurity open ecosystem that provides broad visibility, integrated threat detection, and automated response and analytics. Some of the core attributes include:

- Open architecture that enables security solutions from multiple vendors to work together and be managed across heterogeneous platforms in multiple regions.
- Integration across security systems via open APIs, connectors, and automation tools and scripts.
- Greater visibility, enhanced compliance, and increased protection against advanced threats.
- Faster time to deployment of security solutions and reduced systems integration costs as a result of prevalidated solutions.
- Security automation critical to countering a global shortage of cybersecurity skills.[14]

This open ecosystem model aligns with recommendations from the U.S. Department of Homeland Security: "We must reach a point where the only barriers to collaboration across devices, people, and organizations are those we choose to impose by policy, not those that are imposed on us by technology."[15]

[1] "CIOs Reveal Rapid Growth in Technology Makes it Hard To Adapt," The Millennium Alliance, March 7, 2019.

[2] Joe Howard, "The 70 Cyber Security Product Categories (and What it Means)," LinkedIn, May 12, 2017.

[3] "25% Of Cyberattacks Will Target IoT In 2020," Retail TouchPoints, accessed September 6, 2018.

[4] Kacy Zurkus, "Defense in depth: Stop spending, start consolidating," CSO Online, March 14, 2016.

[5] Kevin Williams, "Threat Spotlight: Advanced polymorphic malware," SmarterMSP.com, June 13, 2018.

[6] Ross Kelly, "Almost 90% of Cyber Attacks are Caused by Human Error or Behavior," Chief Executive, March 3, 2017.

[7] Steve Morgan, "Cybersecurity Jobs Report 2018-2021," Cybersecurity Ventures, May 31, 2017.

[8] Rick Holland, "Point Solutions Must Die," Forrester, August 19, 2013.

[9] Rick Holland, "Incident Response Isn't About Point Solutions: It's About An Ecosystem," Forrester, September 20, 2012.

[10] "Threat Landscape Report Q3 2017," Fortinet, November 17, 2017.

[11] Tara Seals, "Cloud Security Concerns Surge," Infosecurity, March 27, 2018.

[12] "Securing Converging OT Networks," Fortinet, March 30, 2018.

[13] Liana B. Baker, "Under threat: Cyber security startups fall on harder times," Reuters, January 17, 2018.

[14] Jeannette Jarvis, "Addressing the Cybersecurity Skills Shortage with Automation," Fortinet, May 8, 2018.

[15] "Enabling Distributed Security in Cyberspace," U.S. Department of Homeland Security, March 23, 2011.

May 18, 2019 2:19 AM

184949-A-0-EN

F:\Fortinet\PDF Files\DG\FA\FA - WP - Open Ecosystem Solution