White Paper

McAfee's Enterprise-class Cybersecurity Technology Platform

By Jon Oltsik, Senior Principal Analyst and ESG Fellow

April 2019

This ESG White Paper was commissioned by McAfee and is distributed under license from ESG.

Contents

Executive Summary

Enterprise organizations anchor their cybersecurity requirements with an army of disconnected point tools today, but this strategy no longer offers the scale, efficacy, or efficiency needed for preventing, detecting, and responding to cyber-attacks. To address this mismatch, ESG research indicates that many organizations are already consolidating the number of vendors and tools they use for security, replacing point tools with integrated security technology architectures. This portends a new era of security products—cybersecurity technology "platforms." McAfee's cybersecurity technology platform is anchored by ePolicy Orchestrator (ePO) for central administration and context-aware operations with the Data Exchange Layer (DXL) for communication. The McAfee platform model aligns well with ESG's platform definition and high-priority enterprise customer requirements.

Situational Analysis

Many organizations are actively consolidating the number of security vendors they do business with and the number of security point tools they use. Indeed, ESG research indicates that consolidation is widespread and growing—22% of organizations are actively consolidating the number of cybersecurity vendors they do business with on a large scale while 44% are consolidating the number of cybersecurity vendors they do business with on a limited basis.[1] ESG expects this trend to gain momentum over the next 12 to 24 months.

What do organizations hope to achieve through this vendor and security technology consolidation? The research indicates that:

- 41% believe they can gain operational efficiencies across security and IT teams.
- 32% claim they can attain tighter integration between previously disparate security controls.
- 31% want to work with well-resourced vendors that can fund research and development initiatives that yield a greater level of innovation to address the evolving threat landscape.
- 31% want to establish deep relationships in which cybersecurity vendors better understand their business, computing environment, and strategic initiatives.

Toward Cybersecurity Platforms?

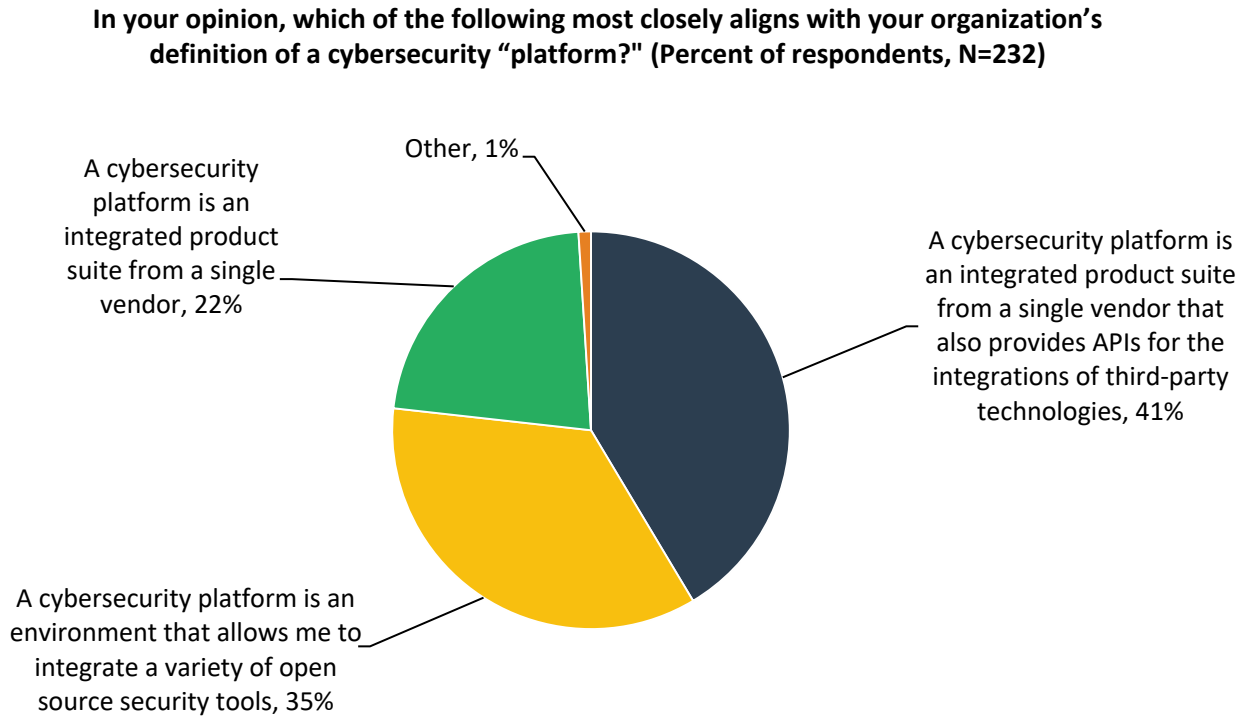
As users actively reduce the number of cybersecurity technologies, vendors are scrambling to integrate their assorted point tools into consolidated cybersecurity "platforms." Unfortunately, industry hyperbole has led to user confusion about what qualifies (and doesn't qualify) as a cybersecurity technology platform. While 36% say that one or more vendor has conveyed a clear definition of a cybersecurity platform, 38% of ESG's survey respondents say that one or more cybersecurity vendors have provided a general definition of a cybersecurity platform, but they would like to hear a more specific definition.[2] Additionally, 12% say that no vendor has provided a clear definition of what a cybersecurity platform is and why they should care.

> Industry hyperbole has led to user confusion about what qualifies as a cybersecurity technology platform.

[1] Source: ESG Brief, *Cybersecurity Landscape: The Evolution of Enterprise-class Vendors*, November 2018.
[2] Source: ESG Master Survey Results, *Cybersecurity Landscape: The Evolution of Enterprise-class Vendors and Platforms*, October 2018. All ESG research references and charts in this white paper have been taken from this set of master survey results unless otherwise noted.

Survey respondents were also given a few definitions and asked to identify the one that most closely matched their own interpretation of a cybersecurity platform. The data supports the notion of "platform" misperceptions. Figure 1 reveals that 41% of security and IT professionals believe that a cybersecurity platform is an integrated product suite from a single vendor that also provides APIs for the integration of third-party technologies (note: this definition most closely aligns with that of ESG). Still, 57% lean toward other definitions, such as an integration hub for open source security tools or an integrated suite from a single vendor (i.e., a proprietary offering, open source messaging fabrics, etc.).

Figure 1. Definitions of a Cybersecurity 'Platform'



Source: Enterprise Strategy Group

Cybersecurity Platforms Defined

Given all this market confusion, ESG has defined the term "cybersecurity platform" (consistent with the 41% above) and describes eight attributes that should be present in all cybersecurity platforms henceforth. A cybersecurity platform should include:

1. **Prevention, detection, and response capabilities**. Cybersecurity platforms should have strong defenses (e.g., rules, heuristics, machine learning models, behavioral algorithms, threat intelligence integration, etc.) used for blocking and detecting threats with close to 100% efficacy. When threats are detected, cybersecurity platforms should have low false positive rates and provide clear and concise forensic evidence to analysts that includes a breadcrumb trail of events that led to an alert. Finally, cybersecurity platforms should include simple mitigation techniques like quarantining a system, halting a process, or terminating a network connection. Users should be able to automate these remediation actions if they choose to do so.

2. **Coverage that spans endpoints, networks, servers, and cloud-based workloads and API-driven services.** Cybersecurity platforms should be able to prevent, detect, and respond to threats across an enterprise IT

infrastructure (i.e., endpoints, networks, servers, or cloud-based workloads and API-driven services). Prevention, detection, and response capabilities should be tightly coupled so that security and IT operations teams can monitor activities and take actions across any security technology controls regardless of location.

3. **Central management and reporting across all products and services.** All security controls should report to a central management plane providing configuration management, policy management, monitoring, and remediation capabilities. Central management must be built for scale, support role-based access control, and offer multiple UIs and functions customized for different security and IT operations profiles.

4. **An "open" design.** Security platforms must be built for integration by supporting common messaging buses and open APIs. Vendors offering best-in-class cybersecurity platforms will also support third-party developers and security vendors with developer support resources, partner ecosystems, technical support services, and go-to-market programs.

5. **Tightly coupled plug-and-play products and managed services.** The transition from point tools to cybersecurity platforms may be an onerous journey that evolves through a phased implementation. Therefore, cybersecurity platforms must act as a force multiplier by providing incremental value with the integration of additional products and services. In other words, each supplementary security product or managed service should increase the security efficacy and operational efficiency of the entire platform.

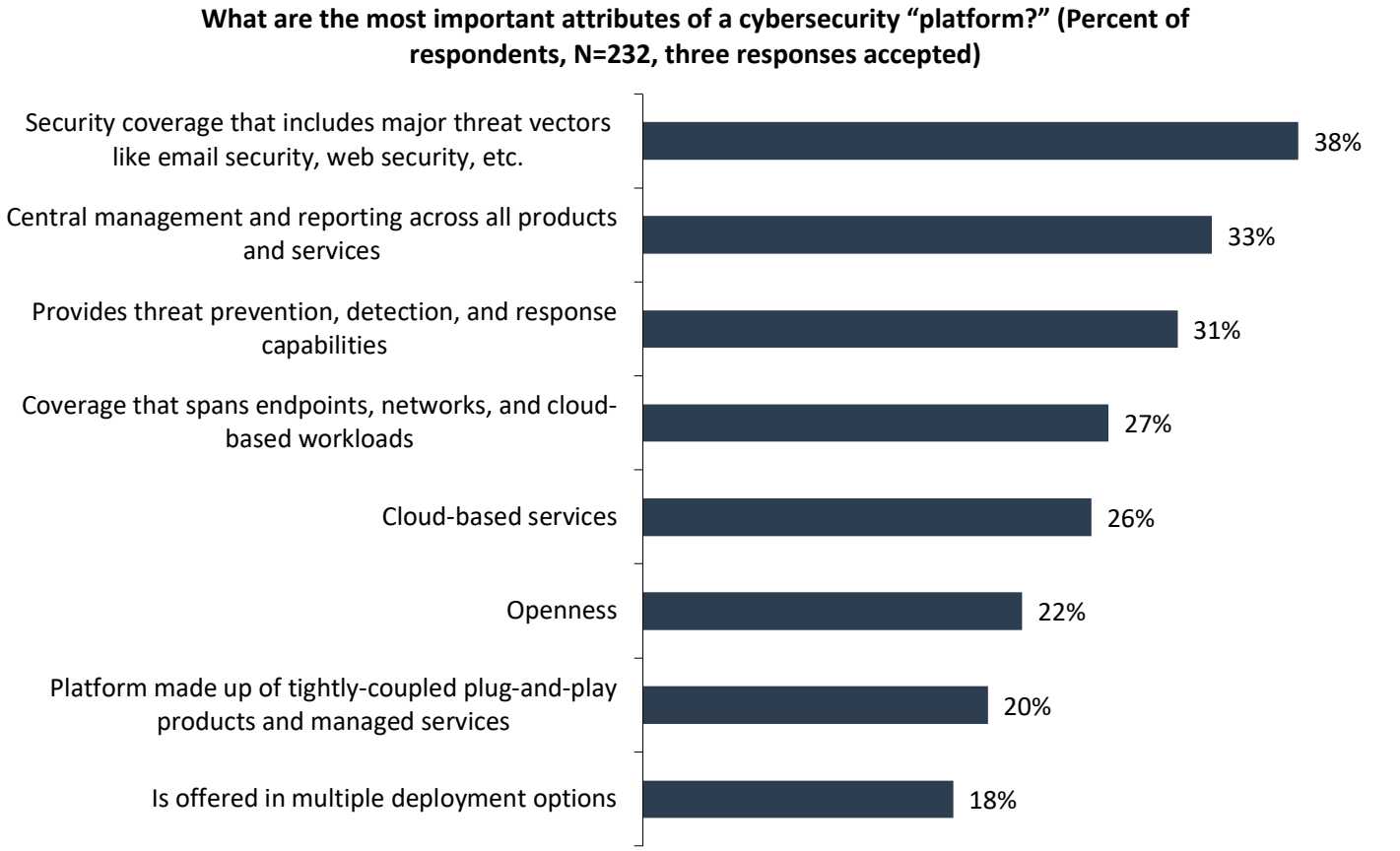
6. **Security coverage that includes major threat vectors like email security, web security, etc.** Despite today's cyber-attack sophistication, most malware attacks emanate through compromised systems using techniques like phishing, malicious attachments/links, and drive-by downloads. Accordingly, cybersecurity platforms must include strong prevention/detection filters that sit inline and service the entire IT infrastructure. These filters can be provided by the platform vendor or through third-party integrations.

7. **Cloud-based services.** Cybersecurity platforms should take advantage of cloud-based resources for activities like file analysis, threat intelligence integration, behavioral analytics, and reputation list maintenance. Cloud-based resources should be applied to all cybersecurity platform users in real time. When a malicious file is detected at one site, all other platform customers should be updated with prevention and detection rules to safeguard them from that threat.

8. **Multiple deployment options and form factors.** The components of cybersecurity platforms should be offered as on-premises software/devices, cloud-based server implementation, SaaS, or some combination including all possibilities. For example, a large global enterprise may deploy on-premises software/devices at corporate headquarters, cloud-based server implementation for large regional offices, and SaaS for remote workers. Once again, all form factor options should be anchored by central configuration management, policy management, and global monitoring.

ESG then asked survey respondents which of these attributes are most important. The data reveals that 38% say one of the most important attributes of a cybersecurity platform is security coverage that includes major threat vectors (like email security, web security, etc.), 33% say these platforms must have central management and reporting across all products and services, and 31% say a cybersecurity platform must provide threat prevention, detection, and response capabilities (see Figure 2).

Figure 2. Most Important Attribute of a Cybersecurity 'Platform'



Source: Enterprise Strategy Group

ESG believes that these attribute preferences should be viewed as point-in-time priorities. Initial cybersecurity platform implementation will tend to focus on improving security efficacy and streamlining security operations, making security vector coverage, central management, and threat lifecycle support top priorities. As cybersecurity platform deployments mature, organizations will want greater coverage and flexibility. Therefore, security professionals will likely look to supplement initial cybersecurity platforms by adding elements like cloud-based services (as opposed to on-premises options) and integrating third-party tools and services.

Given this evolution, CISOs should approach cybersecurity platforms with a long-term strategy and project plan that spans a 24- to 36-month timeframe.

McAfee's ePO-based Cybersecurity Platform

As large organizations abandon their point tools-based cybersecurity infrastructure, they will seek out vendors offering tightly integrated cybersecurity technology platforms with the features and functionality described above. McAfee is one of few vendors that fits this description today.

Unlike other vendors that simply bundle disparate products, McAfee anchors its cybersecurity technology platform around its ePolicy Orchestrator (ePO), a proven central security management engine leveraging the Data Exchange Layer (DXL) for communication. This creates a collaborative framework for visibility and control. McAfee describes its ePO/DXL platform as follows:

With McAfee ePO software, IT administrators can unify security management across endpoints, networks, data, and compliance solutions from McAfee and third-party solutions. McAfee ePO software provides flexible, automated

management capabilities so you identify, manage, and respond to security issues and threats. You define how McAfee ePO software should direct alerts and security responses based on the type and criticality of security events in your environment, as well as create automated workflows between your security and IT operations systems to quickly remediate outstanding issues. The DXL communication fabric is one of the most mature and active fabrics in the security industry—it connects and optimizes security actions across multiple vendor products, as well as internally developed and open source solutions. As a result, you save time and money—with a more effective security program. McAfee ePO software helps drive down the cost and complexity of managing security.

McAfee ePO was first released in 1999 and has since been updated through multiple product revisions. McAfee ePO is used for central security management at some of the world's largest organizations, which have over 100k devices under management. In 2018, McAfee introduced a significant enhancement to ePO with the release of MVISION ePO, a SaaS-based offering that helps organizations remove the setup and maintenance of security management infrastructure, while maintaining the established central security management functionality of ePO for monitoring and controlling endpoints and mobile devices. MVISION ePO is part of the MVISION portfolio of new cloud-based security offerings.

With an ePO and DXL foundation, McAfee can offer its customers a cybersecurity technology platform featuring the critical functionality called out in the ESG research:

1. **Security coverage that includes major threat vectors like email security, web security, etc.** McAfee ePO integrates key security control points such as endpoint security, browser-based security, data loss prevention, and encryption. When combined with DXL, the entire platform can integrate with security devices such as IPS, firewalls, web gateways, email security, and sandbox technologies. This integration allows for the sharing of critical threat data between all these technologies so that every control point can learn from the other and provide superior protection capabilities. McAfee ePO is a true centralized management console that unifies the defenses with data and policy consolidation. It is not just packaging products with a notion of coming from one console (dashboard with a dashboard).

2. **Central management and reporting across all products and services.** This requirement aligns perfectly with ePO's design point: Large organizations have used ePO for central configuration and policy management, reporting, threat prevention, policy enforcement, and remediation for many years. Security analysts can also take advantage of ePO dashboards and reports to assess security posture and drill down for more details for risk management, security investigation, or threat mitigation. In addition, ePO can manage and synchronize updates from native controls like Win10 Defender, making ePO a distinct console uniting security controls.

3. **Prevention, detection, and response capabilities**. Again, these requirements align with the ePO design. For prevention, ePO interoperates with McAfee endpoint protection technologies including signatures (for blocking pedestrian malware) and machine learning (for blocking targeted attacks and reducing false positives). As previously stated, ePO and DXL interoperates with other threat prevention controls for email, web, and network security as well. The ePO platform also integrates with tools like Rapid 7 and others for vulnerability and patch management to minimize the attack surface. For detection, McAfee monitors system, network, and other threat vector behaviors, analyzes this behavior in the cloud, and then generates and distributes threat prevention rules when malicious activity is identified. Finally, ePO's Automatic Response allows for continuous policy enforcement and automated mitigation tactics such as quarantine, scan a system, etc. And because the ePO platform manages multiple security products and their policies, some advanced customers have seen substantial efficacy improvements, including as much as a 95% decrease in incident response times according to McAfee.

4. **Coverage that spans endpoints, networks, servers, and cloud-based workloads and API-driven services.** McAfee ePO supports common security management with visibility and control for all devices and cloud workloads

across McAfee endpoint security (ENS), MVISION endpoint detection and response (EDR), and McAfee cloud workload security (CWS), which has McAfee network intrusion prevention system (IPS) integrated for risk and network flow information. McAfee controls also extend to data security through ePO integration with McAfee total protection for DLP. The company also has an extensive partner ecosystem within security innovation alliance (SIA). Through SIA, ePO can interoperate with third-party products from companies like BeyondTrust, Check Point, Cisco, Forcepoint, Fortinet, IBM, MobileIron, ServiceNow, Swimlane, ThreatQuotient, etc.

5. **Cloud-based services.** While the SaaS offering via MVISION ePO is being enhanced to include additional capability, ePO and DXL are tightly integrated with McAfee's cloud-based security services (e.g., McAfee Real Protect), behavioral machine learning in the cloud, global threat intelligence, open source malware information sharing platforms (MISPs), etc. MVISION ePO also shares data with all other MVISION offerings, feeding cloud-based analytics for threat prevention and detection across the entire MVISION portfolio.

6. **An "open" design.** McAfee deserves credit for its commitment to an open platform. The ePO platform is built on top of the Data Exchange Layer (DXL), an open and extensible messaging bus. DXL was designed to eliminate the use of proprietary APIs with an "integrate once and use many times" methodology. DXL allows rapid sharing of threat information and orchestration, reducing the threat migration cycle and maximizing each security control point. ESG is especially impressed by DXL's market momentum and metrics. For example, according to McAfee, DXL is used as a messaging layer to connect over 10 million clients and has experienced year-over-year growth of 92%, with over 100K downloads of the DXL open client (includes SDK). DXL is also establishing itself with the cybersecurity diaspora with 108 published community-built integrations and 32 SIA-certified integrations. Over 6,000 McAfee customers are using DXL communication for McAfee-to-McAfee integration. DXL makes the McAfee ePO cybersecurity technology platform an "open book" for customer and vendor integration moving forward.

7. **Tightly coupled plug-and-play products and managed services.** Through ePO, MVISION, DXL, and the SIA, McAfee allows products to work together better by sharing data and centralizing management for streamlining security processes. This can help accelerate threat prevention, detection, response, and remediation, resulting in higher efficacy.

8. **Multiple deployment options and form factors.** McAfee ePO is available as traditional on-premises software as well as cloud-based options: IaaS and SaaS. For distributed enterprises with large central facilities and remote branches, ePO can be deployed as a hybrid architecture with on-premises and cloud-based components.

McAfee's ePO cybersecurity technology platform aligns with ESG's eight key cybersecurity technology platform attributes. This can result in several benefits that help CISOs improve security efficacy, enhance security operations efficiency, and enable the business (see Table 1):

Table 1. McAfee ePO Cybersecurity Technology Platform Aligns with User Requirements

Cybersecurity Technology Platform Attribute	Benefits from the McAfee ePO Cybersecurity Technology Platform
Security coverage across major threat vectors	Maximizes threat prevention while coordinating policy management and reporting. Helps organizations block most threats, thus freeing up time and resources for more valuable tasks (e.g., new threat detection, strategic planning, training, etc.).
Central management	Eliminates the need to pivot across security management consoles, promoting better collaboration. Centralized policy management and compliance reporting can help CISOs better align security with business mission, objectives, and processes and assure compliance and audit successes.
Prevention, detection, and response capabilities	Helps coordinate threat management strategies. Provides a dashboard for security policy, investigations, and remediation actions. Can help structure and guide a formal IR program.
Coverage spanning endpoints, networks, servers, and cloud-based workloads	Central policy management, policy enforcement, and reporting can help organizations streamline operations while improving security efficacy. Helps eliminate many tools and manual processes.
Cloud-based services	Eases deployment and infrastructure cost/operations. Takes advantage of cloud scale for collecting, processing, and analyzing massive amounts of customer data and threat intelligence.
Open design	Allows for ease of integration and development. Provides flexibility for McAfee customers to quickly add or develop new functionality.
Tightly coupled plug-and-play products and managed services	Eliminates costly and inefficient point tools, eliminating the operational overhead of deploying, training, and operations of a disconnected security infrastructure.
Multiple deployment options and form factors	Provides for current and future flexibility in organizations with numerous geographically dispersed facilities.

The Bigger Truth

The ESG research paints a clear and alarming picture: Current cybersecurity tactics just aren't effective or efficient. The result? High cost, complex operations, overwhelmed cybersecurity staff, and frequent security incidents.

The research also indicates that CISOs have reached a tipping point where the current cybersecurity technology situation is no longer acceptable. As a result, they are abandoning cybersecurity point tools in favor of more consolidated and integrated cybersecurity technology platforms.

This white paper describes eight key attributes that should be included in all RFIs/RFPs and become part of every cybersecurity technology platform. As they research potential options, CISOs would be well served to explore McAfee's ePO-based cybersecurity technology platform, as it aligns well with current and future cybersecurity requirements for improving security efficacy, increasing operations efficiency, and enabling the business.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides actionable insight and intelligence to the global IT community.


www.esg-global.com


contact@esg-global.com


P: 508.482.0188