ESG SHOWCASE

Integrating the Stack with Cisco SecureX

Date: March 2021 **Author:** Doug Cahill, Senior Analyst

ABSTRACT: Complexity, long an enemy of cybersecurity, has become even more of a factor due to the heterogeneous nature of today's hybrid, multi-cloud environments. As cybersecurity teams begin to address complexity via the use of integrated cybersecurity platforms, third-party controls will still continue to play an important role in the security operations center (SOC). Cisco SecureX serves as a cybersecurity platform, not only to unify Cisco's portfolio of cybersecurity technologies, but also to integrate a variety of third-party controls and threat intelligence sources.

The Challenges of a Disjointed Cybersecurity Tool Set

Point Tools Drives Cost and Complexity

For most enterprises, the modern data center is a distributed cloud comprised of disparate infrastructures, leading 75% of organizations surveyed by ESG to state that IT has gotten more complicated over the last few years.[1] To secure a heterogeneous mix of domains, many organizations have defaulted to using separate cybersecurity controls for separate environments, which contributes to point tool sprawl. Point tools are often also employed to address discreet problems. Just how many cybersecurity controls do organizations typically employ? ESG research indicates that 60% of organizations have 25 or more different cybersecurity products currently in use, all of which require organizations to develop core competencies and manage. Managing an assortment of security products results in a myriad of operational challenges and introduces incremental cost (see Figure 1).[2]

To secure a heterogenous mix of infrastructure domains, many organizations default to using separate controls for separate environments, which contributes to point tool sprawl.

Silos Results in Alert Fatigue, Highlighting the Need for a Unified Approach

Islands of controls provide little integration between one another beyond simple alert propagation. As a result, such alerts are often isolated, and thus out of context, requiring time-intensive measures, including switching between consoles to manually correlate events that may or may not constitute an incident worthy of investigation. That is, while discrete point tools may provide visibility into a specific technology stack or environment, they too often do so out of context of the attack chain. The sheer volume of alerts makes prioritizing and investigating security incidents another top challenge. The ongoing problematic shortage of cybersecurity skills, an issue reported by 48% of organizations, further exacerbates the challenge of triaging an ongoing flood of alerts.[3]

[1] Source: ESG Research Report, *2021 Technology Spending Intentions*, January 2021.
[2] Source: ESG Master Survey Results, *Enterprise-class Cybersecurity Vendor Sentiment*, March 2020.
[3] Source: ESG Research Report, *2021 Technology Spending Intentions*, January 2021.

Figure 1. Challenges Associated with Managing an Assortment of Security Products

Source: Enterprise Strategy Group

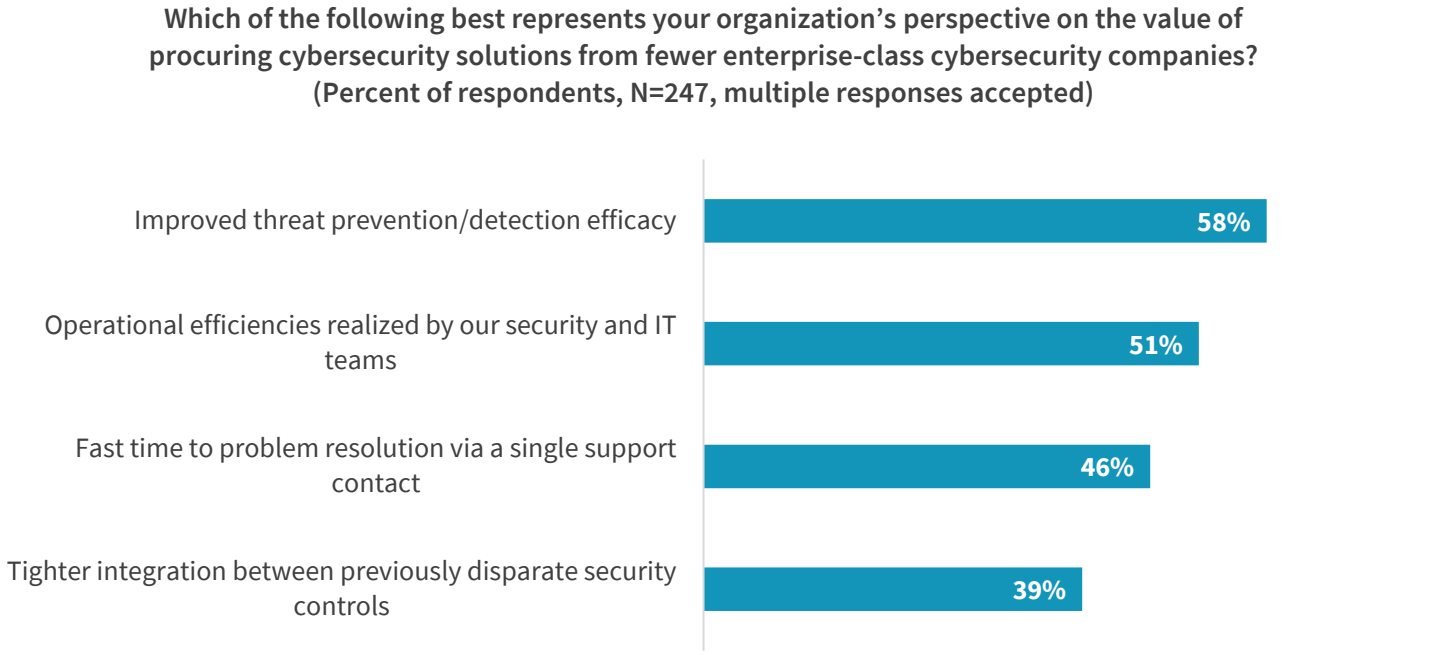
Efficacy and Efficiency Outcomes are Driving Consolidation and Convergence

Best-of-breed is Still Required Amidst Vendor Consolidation

How are cybersecurity teams responding to the challenges associated with a disjointed stack of security controls? According to ESG research, they clearly intend to both consolidate vendors and converge controls in platforms to realize outcomes that have too often been mutually exclusive: improving the efficacy of detecting and preventing threats and doing so in a more operationally efficient manner (see Figure 2).[4]

[4] Source: ESG Master Survey Results, *Enterprise-class Cybersecurity Vendor Sentiment*, March 2020.

Figure 2. Perceived Value of Working with Fewer Cybersecurity Vendors, Top Four Responses



Source: Enterprise Strategy Group

The trend toward consolidation does not, however, obviate the need for nor interest in best-of-breed security technologies. After all, ever-present and motivated cyber adversaries require ongoing innovation from the community at large, inclusive of both established major brand and emerging startups. As such, the need for integration has signaled the emergence of cybersecurity platforms, especially since integration and openness have become critical ingredients for enabling best-of-breed solutions.

The Emergence of Cybersecurity Platforms

As organizations seek out cybersecurity platforms, a clear theme has emerged: integration. In fact, the following attributes cited by research participants as the most important for a cybersecurity platform speak to the need for integration.[5]

- Coverage across attack vectors (e.g., email, endpoint, web, etc.).
- Security analytics.
- Integration with threat intelligence for threat detection and remediation use cases.

An integrated approach enabled by cybersecurity platforms is increasingly becoming viewed as a critical success factor for cybersecurity programs. According to Cisco's Security Outcomes study, well-integrated technology improves the probability of a successful cybersecurity program by 10.5%.[6]

So, just how are organizations beginning to employ cybersecurity platforms? The action most commonly taken by research respondents (42%) in pursuit of implementing a tightly integrated cybersecurity platform is the use of security operations

[5] Ibid.
[6] Source: Cisco, *Cisco 2021 Security Outcomes Study*, December 2020.

process automation tools to integrate the output of security tools into runbooks or workflows,[7] one of the use cases supported by Cisco's SecureX platform.

Third-party Integrations with Cisco SecureX

Based on a cloud-native architecture, SecureX was designed to integrate the Cisco portfolio of cybersecurity controls and threat intelligence, as well as those from a third-party ecosystem. With dozens of such third-party controls now integrated, SecureX offers three types of pre-built integrations to simplify SecOps three key use cases.

Integration Types

Enriched Intelligence Sources

SecureX offers an API via which threat intelligence (TI) from third-party sources can be ingested and normalized. Third-party TI, such as known bad file hash values, domains, and IP addresses, as well as more contextual IOCs, allow for these TI markers to be enrichened by SecureX. That is, discrete pieces of TI are put into a greater context, i.e., that of the attack surface being protected and the attack chain being analyzed. These integrations provide SOC analysts a consolidated view of intelligence from multiple community and vendor sources and the ability to take response/remediation actions from the same view.

Visibility and Protection Subscriptions

As a bi-directional platform, SecureX also provides threat intelligence to third-party controls. Third-party security controls can connect to SecureX to receive TI from Cisco's Talos threat research team and other connected TI sources. This "north-bound" integration allows SOC analysts to leverage additional intelligence in third-party cybersecurity products through SecureX, including network detection and response (NDR) products, threat hunting platforms, and controls that protect externally facing applications such as web application firewalls (WAF).

Operationalizing via SecOps Tools

SOC analysts employ a variety of tools to reactively detect, proactively hunt, orchestrate workflows, and automate actions, representing a clear need for integration. In addition to integrating with security information and event management (SIEM) platforms, SecureX also enables integrated orchestration use cases, such as ticket management, and automates remediation steps, such as removing malware, updating firewall rules, and quarantining infected endpoints.

Core SecureX Use Cases

Detect and Hunt for Threats

Indicator of Compromise (IOC) aggregation not only eliminates the need to view issues in multiple consoles but also provides the context necessary to expedite alert curation, reducing the mean time to detect (MTTD).

In addition to expediting reactive investigations by triangulating alerts with native and third-party intelligence sources, environment-specific context enables proactive threat hunting.

In addition to expediting reactive investigations by triangulating alerts with native and third-party intelligence sources, environment-specific context enables proactive threat hunting.

[7] Source: ESG Master Survey Results, *Enterprise-class Cybersecurity Vendor Sentiment*, March 2020.

Respond to Incidents

A disjointed tool set adversely impacts the ability of SOC teams to quickly respond by identifying affected assets and effectively containing an incident. SecureX provides out-of-the-box third-party integrations to expedite common remediation steps, such as isolating infected endpoints, blocking/banning known bad hashes (i.e., malware on all endpoints), kicking off an analysis of downloadable files associated with a malicious URL, disabling certain ports, and blocking certain protocols that that have been determined to communicate with a command-and-control (CnC) server.

Orchestrate and Automate Response

Manual incident response measures are time-consuming and inefficient, extending dwell time. As such, SOC teams strive to establish repeatable processes, expedite response, and simplify administrative tasks. Maximizing the efficiency of such response measures to lower mean time to remediation (MTTR) requires automation and streamlining of the workflows employed by SOC and incident response (IR) teams. SecureX delivers the ability to orchestrate workflows (e.g., ticket management) across Cisco Secure, as well as third-party security control points, via robust integration with IT service management (ITSM) platforms to provide a coordinated response. The platform also provides automation via the invocation of workflows/runbooks to automate remedial tasks.

The Bigger Truth

The emergence of cybersecurity platforms is a promising trend in the cybersecurity industry, given the need to alleviate the cost and complexity associated with managing a multitude of controls that operate in isolation. Third-party integration is an essential aspect of such platforms, allowing organizations to leverage prior investments and provide best-of-breed optionality moving forward. Cisco SecureX manages to strike this balance by unifying the Cisco Secure portfolio of cybersecurity solutions with an open architecture that integrates a range of third-party controls, bolstering a series of use cases central to protecting the modern enterprise.

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

www.esg-global.com contact@esg-global.com 508.482.0188