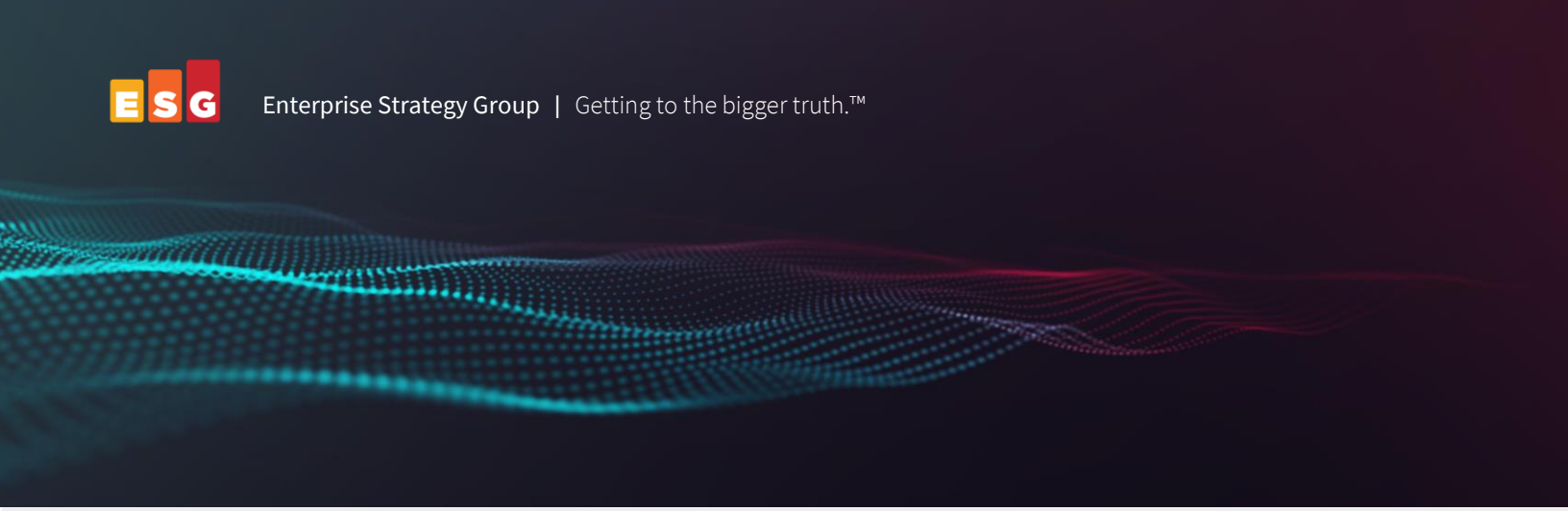

ESG WHITE PAPER

Reimagining Endpoint Security

Endpoint Security Can No Longer Live in Isolation

By Dave Gruber, ESG Senior Analyst

July 2020

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

Contents

Overview 3

Key Trends Driving Endpoint Security Transformation 3

Digital Transformation Initiatives and the Move to the Cloud 4

A Rapidly Expanding Attack Surface 4

Working from Home 4

IoT Initiatives 4

A Diverse and Growing Threat Landscape 5

Reimagining Endpoint Security 5

What's Needed 5

New Endpoint Security Platforms Emerge: Endpoint Security from Cisco 7

The Bigger Truth 7

Overview

Digital transformation initiatives, the move to the cloud, and a rapidly expanding attack surface are driving the need for a new class of endpoint security, capable of defending organizations against a more diverse and sophisticated threat landscape.

Endpoint security continues to be an integral component of the modern security stack. However, the role that it plays is no longer as an isolated control. The scope of what is to be secured in modern endpoint security solutions has grown to include new mobile and IoT devices types, together with hybrid cloud-delivered application workloads used by a diverse and widely distributed group of customers, partners, and supply chain vendors.

Endpoint Security Can No Longer Stand Alone

Endpoint security must include prevention, detection, and response capabilities that are tightly integrated with email, identity, network, and cloud security to provide security teams broad protection and unified visibility into modern, sophisticated attacks.

Together with this rapidly expanding attack surface, the complexity and sophistication of modern threats regularly now extend beyond individual endpoints that involve multiple attack vectors, often leveraging individual endpoints as an initial point of compromise on the way to higher value targets within corporate and cloud infrastructures. Security teams therefore require visibility across multiple security controls, correlating and analyzing telemetry to discovery and understand complex attack campaigns. As organizations reevaluate their endpoint security strategies in the context of this expanded attack surface and threat landscape, most are looking for a broader level of protection that includes, but goes beyond, securing individual endpoints. Endpoint security must include prevention, detection, and response capabilities that are tightly integrated with email, identity, network, and cloud security to provide security teams broad protection and unified visibility into modern, sophisticated attacks. This redefined definition of endpoint protection platforms (EPPs) encompasses all facets of end-user security, protecting organizations from file-based and fileless malware, identity theft, phishing, business email compromise, insider threats, and more.

Beyond securing individual endpoints, modern endpoint security solutions must be architected with the security operations center in mind, delivering the telemetry, visibility, investigation, and remediation capabilities required to support daily security operations. This need is driving new investments in platforms that provide built-in detection and response capabilities as a natural extension of endpoint security and other critical controls. This new approach, known as cross-control detection and response (XDR), simplifies data correlation and enables security teams to see and respond to sophisticated, modern attacks.

Endpoint security is in a state of transformation. A new approach is needed.

Key Trends Driving Endpoint Security Transformation

According to ESG research, this new era of endpoint security is causing 72% of organizations to replace their current endpoint security solutions now or within the next 12-18 months, with 67% desiring a comprehensive endpoint security software suite from a single vendor.[1] There are several factors involved.

[1] Source: ESG Master Survey Results, *Trends in Endpoint Security*, October 2019. All ESG research references in this white paper have been taken from this master survey results set unless otherwise noted.

Digital Transformation Initiatives and the Move to the Cloud

Digital transformation initiatives continue to lead IT investment, driving organizations to adapt business models to capitalize on the digital products and services economy. These same enabling transformative capabilities introduce new opportunities for adversaries to find and exploit vulnerabilities in operational infrastructure, increasing the importance of robust security controls at every level.

Most organizations are moving to the cloud to support the scalability and rapid pace of change required to accelerate these initiatives, yet often do so without a well-formed plan for comprehensive security controls. As employees, partners, and customers interact with these newly deployed cloud applications from a morass of endpoint devices, new risks are introduced, providing adversaries with a path to sensitive and valuable digital assets.

Simple phishing techniques have provided adversaries with a path to steal and utilize credentials to impersonate employee, partner, and customer transactions. Once in, adversaries can navigate to escalate privileges, enabling them to move laterally and locate valuable resources. This simple but frequently used path demonstrates the importance of adding additional security controls, including identity and access control (IAC) and user behavioral analysis (UBA) capabilities, to endpoint security solutions. Without these capabilities, adversaries can gain access to sensitive data and IP stored within cloud applications through simple phishing and credential theft.

A Rapidly Expanding Attack Surface

Endpoint security was once a process of securing individual, corporate-owned devices—typically one per employee—operating both inside the corporate network perimeter and from remote locations during travel. Since that time, most organizations have evolved security programs to support the use of multiple devices on both corporate networks and outside the perimeter through various public and private network access points.

Working from Home

However, no one could have anticipated the overnight need to rapidly accelerate the decentralization of employee, partner, and customer access to business systems. This unprecedented move to a remote workforce across all industries has changed the management and security dynamics of corporate-owned devices to a new model, where multiple personal and corporate-owned devices are utilized from unknown, potentially unsecure home networks.

Forty-two percent of organizations surveyed by ESG research reported that they had policies in place prohibiting the use of "bring-your-own-device" (BYOD) types for business applications. With an average 76% employees now working from home,[2] and 73% of organizations already considering how a zero-trust access model could be applied to endpoint security, this new remote worker environment will likely increase the importance of identity and access control as a means for zero-trust.

Zero-trust and the Remote Worker

While 73% of organizations had already been considering how a zero-trust access model could be applied to endpoint security, this new remote worker environment will likely increase the importance of identity and access control as a means for zero-trust.

IoT Initiatives

Internet of things (IoT) initiatives are further expanding the attack surface with a new level of device complexity. The rapid addition of new device types has left IT and security teams wondering how to implement effective security controls in an

[2] Source: ESG Master Survey Results, *COVID-19 Technology Implications for Knowledge Workers*, May 2020.

environment often deployed and supported outside of IT. With 51% of organizations expecting to use the same endpoint security solution to protect these devices, new challenges exist for endpoint security vendors to support this diverse, specialized environment.

A Diverse and Growing Threat Landscape

The prize for the adversary has never been greater. The adversary has grown in knowledge and sophistication and has ready access to a plethora of attack tools capable of supporting highly targeted and complex attacks. As digital transformation moves more core business transactions, intellectual property, and sensitive information online, adversaries now have a path to stage criminal acts to steal data, ransom assets, and/or impact the digital operations of most modern businesses.

This effort is fueled by a massive, rapidly growing attack economy, enabling thousands of attackers to participate in criminal digital theft. Once requiring technical "hacker" acumen, the modern non-technical adversary can easily purchase attack tools and services from a variety of software firms engaged in the broader criminal attack ecosystem. As defenses evolve, so do attack tools, further requiring layered, well-integrated security strategies to avoid compromise and breach.

Modern attack campaigns are targeted and sophisticated, often involving multiple attack vectors. Endpoints are often involved in one or more parts of the attack chain, but more so, they are being used to gain access to more valuable assets. Modern endpoint security solutions must operate in conjunction with a host of security controls that both protect against and expose adversaries and their attack strategies. No longer can endpoint controls alone stop the modern, more sophisticated adversary. Contextual awareness that can only be seen by looking across security controls is foundational to understanding and responding to the modern threat landscape.

Reimagining Endpoint Security

For the past few years, there has been a tremendous focus on the move to next-gen endpoint security solutions, adding protection from fileless malware attacks and moving to a cloud-delivered endpoint security model. This evolution of endpoint security both addressed the growing threat landscape and sparked a new cloud-delivered endpoint security deployment model, enabling security vendors to leverage big data analytics in the cloud to track and identify new attack patterns. The move to cloud further offered users additional efficiency benefits, with 31% of organizations reporting that they currently utilize cloud-delivered endpoint security solutions, and another 52% planning or interested in moving to a cloud-delivered solution.

As organizations look to continue to improve endpoint security, they desire better threat detection and response capabilities, better threat intelligence, and a built-in platform approach that offers more simplification, automation, and consolidation.

What's Needed

Seamless, Holistic Security Architecture – Defending against the modern adversary requires a new approach to security. No longer is it enough to simply integrate silos of security controls, aggregating and correlating data after the fact. When security controls are architected to work together from the ground up, they can interoperate in detection and response activities in new ways that strengthen security posture while exposing complex attack strategies. Endpoint security can no longer stand alone. Modern endpoint security solutions must be architected to work together with a broad array of security controls to protect against this more sophisticated threat landscape. Endpoint security is not an endgame, but instead an important component of a more comprehensive security architecture, inclusive of network, identity, cloud, and email.

Multifaceted Prevention – Modern endpoint security solutions require multifaceted prevention techniques, combining behavioral analytics, machine learning, and signatures to provide the most robust prevention possible. This prevention architecture must be dynamic in that it must be able to support the addition of new prevention techniques without major re-architecture.

Detection and Response – Threat detection and response is integral to modern endpoint security solutions, and therefore must be both integrated and extensible, providing visibility and correlation across many security controls, including endpoint, network, email, and cloud. Detection and response capabilities need to provide security analysts visibility into precisely what's happening on every endpoint, and equally importantly, provide unified visibility into a macro view across all endpoint, network, cloud, and email telemetry to help analysts understand broad attack strategies.

Combining Device and User Access Controls

As employees, customers, and partners engage with cloud-delivered applications and data from diverse, potentially insecure environments, the use of zero-trust models is becoming more common in security architecture.

User Access – As employees, customers, and partners engage with cloud-delivered applications and data from diverse, potentially insecure environments, the use of zero-trust models is becoming more common in security architecture. Zero-trust requires fine-grained access controls to applications and data, therefore requiring endpoint security solutions to incorporate user access control to verify trust before allowing access to sensitive applications and data.

Threat Intelligence – Threat intelligence underlies prevention and detection, supporting both automated prevention and detection, and extending further to assist security analysts with investigations and threat hunting. While there are many sources of threat intelligence available, the efficacy of endpoint security is highly correlated to the way solutions source and utilize threat intel with core prevention algorithms, machine learning, and cloud analytics to stop new and emerging attacks.

Automation – Automation is core to prevention, detection, and response; however, too much automation can overload security teams with false positives that distract from more important threats. Modern solutions walk a fine line, providing automated detections and preventative measures without getting in the way of valid user actions. Highly configurable solutions must start with conservative defaults, while enabling automation to be added as policies are implemented.

Unified Policy Management – Organizations work hard to refine and align security policies across the security stack. Making policy changes can take time and often results in misalignment across security controls. Modern endpoint security solutions must automate policy management with centralized management tools to both simplify and align controls.

Security Stack Integration – Endpoint security never stands alone in the security stack. While critical to an organization's overall security strategy, endpoint security needs to work together with other core controls, including email, identity and access, network, and cloud. This means not only correlating telemetry for detection and response, but also orchestrating and automating response actions across the many security controls to thwart future attacks.

Integrated Security Controls

Critical to an organization's overall security strategy, endpoint security needs to work together with other core controls, including email, identity and access, network, and cloud.

Cloud and On-prem Deployment – While most organizations are moving toward a cloud-delivered endpoint security deployment model, 35% still want some amount of endpoint security deployed on-premises. To support consistent policy and management, solutions must therefore provide options for both.

Managed Detection and Response – While most organizations have some amount of dedicated security resources who spend their day monitoring, triaging, and responding to threats, most struggle to staff 7x24, and on occasion see spikes in workload that require staff augmentation. Managed detection and response (MDR) service offerings can fill these gaps.

Threat Hunting Services – Beyond staffing, many organizations want to engage in proactive threat hunting initiatives, requiring deep knowledge of emerging threats across the broad threat landscape. Modern security solutions therefore also provide threat hunting services for those organizations that lack the skills or threat landscape knowledge required.

New Endpoint Security Platforms Emerge: Endpoint Security from Cisco

Endpoint Security from Cisco is the industry's first solution to bring together user access and device protection, integrating prevention, detection, response, and access control into a built-in platform, backed by industry-leading threat intelligence from the Cisco Talos threat unit.

- Unified User Access and Device Protection: Unify user and device protection, reducing the attack surface without adding complexity.
- Industry-leading Prevention: Block threats before compromise. Keep the bad guys out with multiple powerful protection capabilities using machine learning, next-generation antivirus, fileless malware and ransomware defenses, internet/DNS-layer security, and more.
- Powerful EDR and XDR Capabilities: Continually detect and respond to threats. Catch any threat that slips through with advanced and extended endpoint detection and response, threat hunting, and attack surface reduction capabilities. Automated playbooks and hundreds of predefined queries come out of the box for threat hunting, incident investigation, vulnerability and compliance, and IT ops—delivering quick time to value from a single, unified endpoint security solution that provides both advanced to extended threat detection and response.
- Unrivaled Threat Intelligence: Unrivaled threat intelligence across web, email, cloud, endpoint, and network from Cisco Talos, the largest non-governmental threat intelligence organization on the planet, to see a threat once, anywhere in the world, and block it everywhere.
- Single Agent: Leverage a single endpoint agent for prevention, detection, and response.
- Integrated and Open Security Platform: As a critical component of Cisco's SecureX platform, Cisco Endpoint Security works together across an organization's entire security infrastructure, including network, cloud, and applications, to generate actionable insights that accelerate threat response. Cisco Endpoint Security enables SecureX to run automated playbooks and perform complex queries across an endpoint fleet for forensics investigation, leading to simplified and accelerated threat hunting, incident investigations, remediation, and vulnerability/compliance assessments.
- Zero-trust: Enforce secure and trusted user access. Let the good guys in with risk-based access control, posture and compliance assessment, multi-factor authentication, and virtual private network controls.

The Bigger Truth

Endpoint security is in transformation. As organizations reevaluate their endpoint security requirements in the context of improving their overall security posture, most are finding that a new, more integrated class of protection is required. Endpoint security is not an endgame, but instead an important, integral component of a broader, unified security strategy.

When endpoint security works in concert with the rest of the security stack, it brings new visibility to modern, complex attack campaigns while increasing the overall efficiency and efficacy of a security program. XDR is a core tenet to achieve these results and to maximize endpoint security investments.

While recent world events have forced organizations to accelerate work-from-home initiatives, adding stress to both IT and security teams, the fundamentals of security in a highly mobile, cloud-enabled business economy remain the same. Organizations need to up their game to become more resilient in the face of the growing threat landscape, expanding attack surface, and digital transformation initiatives.

Effective, modern endpoint security solution platforms must employ multiple prevention techniques, leveraging the best of machine learning, behavioral analytics, and signatures, while depending on industry-leading threat intelligence. They also must be architected to support broad threat detection and response programs that extend beyond the endpoint to include network, cloud, and email.

New endpoint security solution platforms are emerging that are capable of securing highly mobile users together with cloud-delivered applications, data, and collaboration tools. Organizations that are reconsidering endpoint security should consider solutions like Endpoint Security from Cisco to help.

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