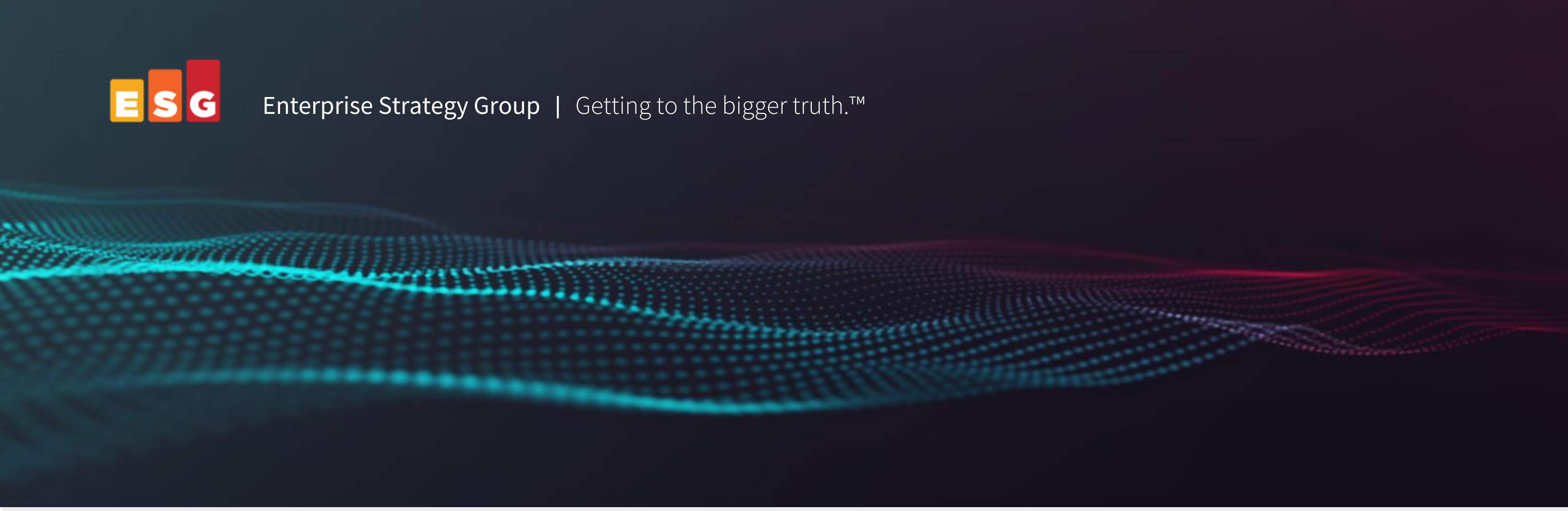


Enterprise Strategy Group | Getting to the bigger truth.™

ESG WHITE PAPER

The Importance of Endpoint Security in the Evolution of Modern Security Architecture

Rearchitecting Security Strategies for Zero Trust, SASE, and XDR

By Dave Gruber, ESG Senior Analyst

February 2021

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

Contents

Modern Security Architectural Strategies – The Imperative for Change

While IT infrastructure is, and has always been, in a constant state of change, the fallout from the pandemic has accelerated the pace of this change to levels not seen before, requiring architects to rethink and rearchitect core infrastructure and controls. As IT and security teams respond to the pandemic-driven remote work environment, accelerated digital transformation projects, and the move to the cloud, new architectural strategies are required to both scale infrastructure and mitigate new areas of risk. And for most, time is of the essence, as digital-born businesses race ahead with cloud-first strategies.

Architects have a daunting task ahead as they re-architect age-old IT and security infrastructure in support of this modern operating environment. While core pillars of cybersecurity remain constant, each pillar must evolve to support new use cases, development and runtime models, modern operational models, and a rapidly growing and complex threat landscape. Architects must reevaluate individual security controls for network, endpoint, virtual and physical server workloads, public and private cloud workloads, data and privacy, identity and access, and SaaS application workloads in the context of a more advanced threat landscape that requires these controls to work together in defense of modern, sophisticated attacks.

This paper outlines the challenges and opportunities for security architects as they race to keep up with this rapidly changing environment, with a special focus on the importance of endpoint security solutions against a backdrop of the three important mega-trends affecting the overall security industry, including zero trust, secure access service edge (SASE), and extended detection and response (XDR).

Securing a New Operating Environment

The COVID-19 pandemic and the associated move to working remotely has had a dramatic impact on both IT and security strategies, redefining the operating and security perimeter. As digital transformation initiatives accelerate, more organizations are moving core operating infrastructure and applications to public cloud delivery mechanisms in support of improved collaboration and customer interaction.

This move to public-cloud delivered applications is forcing security architects to redesign security infrastructure that can operate efficiently and effectively in a cloud-first operating environment.

While infrastructure teams scurry to address these changes, line-of-business teams continue to accelerate key business initiatives to redefine and refine core business offerings. ESG research shows that 72% of organizations now have digital transformation initiatives that are either mature or in process, up 14% over last year,[1] in response to this new work environment.

Digital Transformation Initiatives Up 14% from Last Year

72% of organizations now have digital transformation initiatives that are either mature or in process, up 14% over last year.

[1] Source: ESG Research Report, *2021 Technology Spending Intentions Survey*, January 2021.

72%

of organizations now have digital transformation initiatives that are either mature or in process, up 14% over last year, in response to this new work environment.

Source: Enterprise Strategy Group

A Rapidly Expanding Attack Surface

For most organizations, the modern attack surface includes endpoints, server workloads, public and private cloud workloads, network devices, IoT devices, and SaaS applications operated by third parties. This complex environment is typically distributed across multiple physical locations, including secure private data centers; one or more public cloud-service-providers; edge data centers; branch/regional/field offices and facilities; and, more recently, home networks.

New device and workload types further expand this already-complex attack surface, requiring organizations to add security controls. While organizations strive to reduce complexity, new controls often introduce more operational silos of security and data, which all too often works against integration strategies focused on streamlining and optimizing security operations.

A More Sophisticated Threat Landscape

Further, today's threat landscape involves a new level of advanced threats that have pushed both prevention and detection tools to their limits. When security teams begin to fall behind the adversary, organizations face increased levels of business risk, with more frequent disruption to business-critical systems, impacting the bottom line. Balancing performance, availability, and security in these environments has become exponentially more complicated, requiring security and IT architects to rethink many of the fundamental techniques they use to operate and secure their environments.

Mega-trends in Security Offer New Opportunities

Securing users, data, and workloads in this complex, varied environment requires new approaches to security architecture. Three industry mega-trends have emerged to address the modern operating environment. These mega-trends offer security architects new strategies to address both operating and security challenges.

New Strategies Emerge

Zero trust, secure access service edge, and extended detection and response offer security architects new hope in addressing the modern operating environment.

Zero Trust

As remote workers have moved to a direct-to-cloud model, utilizing public network access to public cloud services, security teams have lost the ability to secure corporate infrastructure using traditional methods. Many are moving to zero-trust architectures that can provide authentication at an atomic level for applications, services, and data. The implementation of a zero-trust architecture is a journey for most, requiring modifications to many of the core security pillars, including network, endpoint, identity and access, server and cloud workloads, and data security. Effective zero-trust security also requires these controls to work together, providing user and access context that can inform and enable individual controls to uphold zero-trust principles.

Secure Access Service Edge

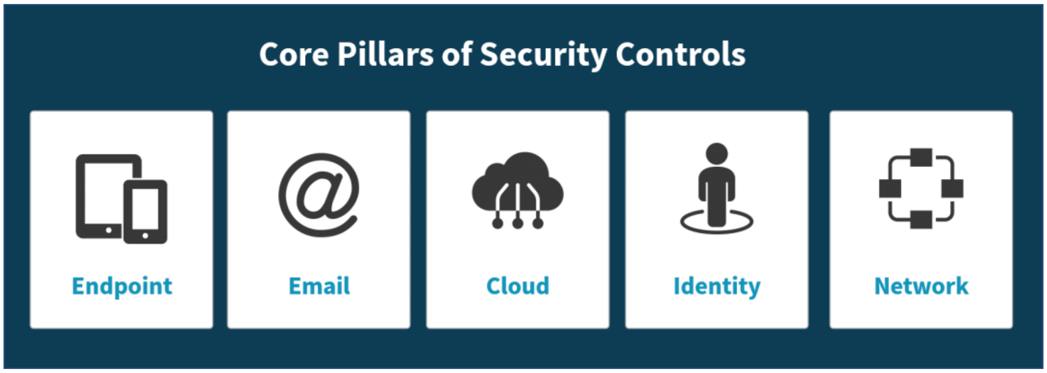
As remote-to-cloud access becomes commonplace, utilizing traditional corporate network security controls requires hairpinning users through corporate controls before allowing them to access cloud applications and data. This inefficient, costly model is being replaced by a more efficient secure access service edge (SASE) approach, converging SD-WAN capability with network security controls. This important advancement provides an efficient, secure approach to the direct-to-cloud access required by modern cloud application deployments.

Extended Detection and Response

As the threat landscape has become more sophisticated, advanced attacks have become more and more challenging for individual security controls to keep up with. To overcome this challenge, security teams have been working to integrate security data across multiple security controls to gain additional visibility into these more sophisticated attacks. This has required security teams to dramatically increase the amount of security data collected, aggregated, correlated, and analyzed, to a level that has overwhelmed many. Extended detection and response (XDR) solutions are emerging to automate this process, offering security analysts turnkey solutions that can expose and allow analysts to respond rapidly to these more advanced threats.

Security Pillars Remain the Same but Require New Levels of Integration

Despite these changes, most pillars of security remain the same. Security teams must still protect endpoints, networks, application workloads, data, communications and collaboration, and user/workload access control. However, because operating models associated with each pillar are evolving so rapidly, security strategies must also change to support these new models.



Source: Enterprise Strategy Group

Meanwhile, the adversary never rests. As attack surfaces change and grow, the adversary continues to strengthen attack techniques, exploiting many of the most basic vulnerabilities, while increasing the sophistication of more complex, *low-and-slow* attacks. These more complex attacks frequently leverage multiple attack vectors involving multiple pillars of security controls in an attempt to evade detection by individual controls.

To combat these attacks, many architects are driving initiatives to further integrate security controls that can lead to increased visibility and efficacy of both prevention and detection. However, despite these initiatives, many report that the sheer number of individual, disparate security tools and the overwhelming amount of data that they generate has created challenges difficult to overcome, despite reporting integration as a high priority investment area.

The Move Toward Platform-Driven Architectures

Modern security architecture requires an intricate selection of interlocking security controls and operations management tools that can prevent, detect, and assist security analysts in the mitigation of threats. With 60% of organizations running 25 or more security tools,[2] modern security architects are forced to continuously prioritize, evaluate, and reevaluate point products together with overall integration architectures as they strive to protect their organizations' rapidly expanding attack surface from an increasingly complex threat landscape.

While many security professionals have long proclaimed a preference toward a best-of-breed strategy, the sheer number of security tools has driven many to reassess and elevate the importance of utilizing security tools designed and architected to work together, with the goal of driving down complexity. ESG research finds that 67% of organizations desire consolidation of suites or platforms of security tools from a single vendor,[3] driving the move to platform-driven architectures.

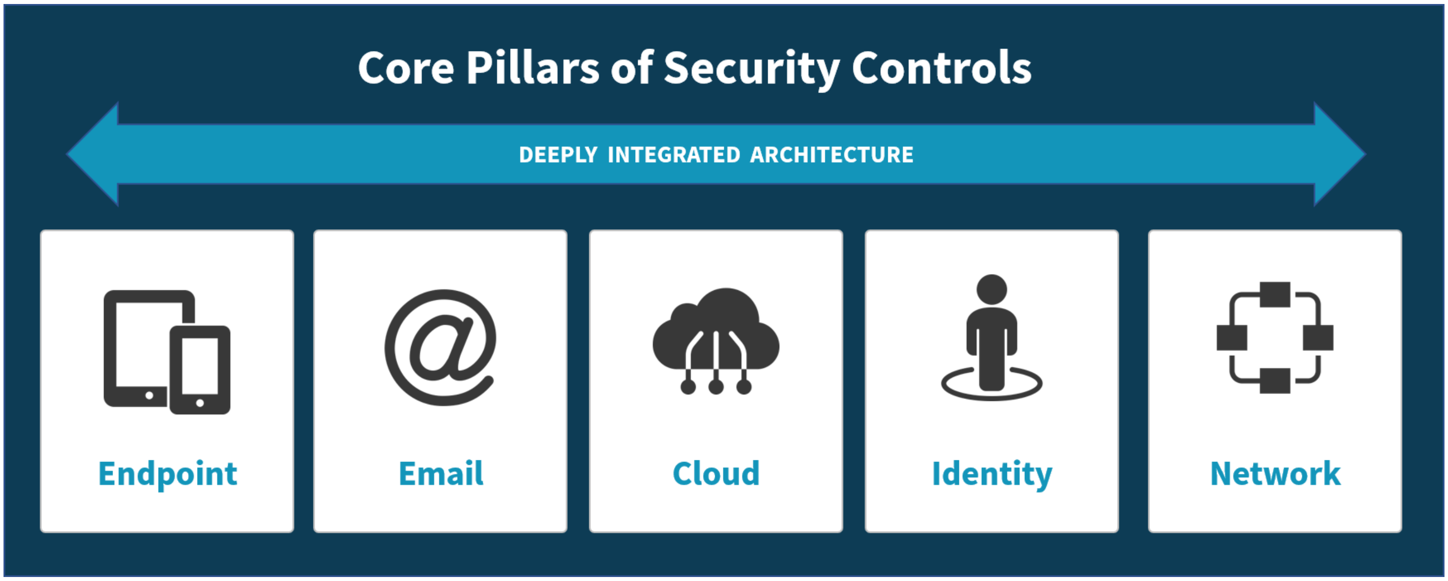
Converging Disparate Tools into 'Mini-platforms'

Security vendors have responded with integrated portfolios of security controls and operations tools, designed to simplify operations while upholding the high levels of efficacy required to keep up with the rapidly changing threat landscape. As tools converge into mini-platforms, new opportunity emerges for these platforms to provide both efficiency and efficacy gains, reducing risk while enabling security teams to recognize significant operational benefits.

For the security architect, this means that, instead of integrating 30+ security tools, they can focus on selecting mini-platforms that align with security and operational objectives, reducing the implementation and integration investments required. This strategy shifts a significant amount of the burden of integration to security vendors, who can architect in native data and workflow integrations.

A New Class of Security Platform Vendor

New classes of large-scale security and IT platform vendors can further offer architects even greater capabilities, as they bring together integrated offerings around many of the core pillars of security.


Core Pillars of Security Controls
DEEPLY INTEGRATED ARCHITECTURE
Endpoint
Email
Cloud
Identity
Network

Source: Enterprise Strategy Group

[2] Source: ESG Master Survey Results, *Enterprise-class Cybersecurity Vendor Sentiment*, March 2020.
[3] Source: ESG Research Report, *Trends in Endpoint Security*, July 2020.

When security vendors can deliver integrated endpoint, network, cloud workload, data protection, email, and identity and access solutions, security teams benefit from pre-built integrations of both data and workflow, further increasing the efficacy and the efficiency of the collective security solutions.

This new integrated environment can enable organizations to leverage new security innovations more rapidly, such as XDR, zero-trust, and secure access service edge (SASE) solutions. When integrated platforms can operationalize integrated security data, they can provide users secure and performant access to both applications and data while providing security analysts with an ability to detect and respond to more advanced threats.

These emerging, integrated security platforms offer security architects relief from a never-ending challenge of prioritizing where to focus the next security project as their attack surface continues to grow. Instead, they can focus on implementing and optimizing new controls, spending less time and money on integration activities.

Choices of Core Security Pillars Matter: The Need for Integrated Endpoint Security

Endpoint security decisions are foundational to enabling advances in security architecture, including zero trust, SASE, and XDR. Because endpoint security solutions have broad visibility into user behaviors, they can provide necessary context to identify advanced attacks when tightly integrated into broader security platforms.

Endpoint Security and Zero Trust

Zero trust (ZT) has gained significant momentum in the past 12 months, heavily driven by a combination of the remote worker and the new level of advanced threats. As organizations strive to provide least-privileged access to applications and data, endpoint security solutions can play a critical role in enabling zero trust.

Because most endpoint security solutions operate in isolation, limited to the visibility that can be obtained on a single, local system, more sophisticated attacks can evade endpoint controls by mimicking local user behavior. Yet when endpoint security can work collectively with other security controls, including identity and access, email security, and data protection, the combination can more easily identify account takeover (ATO) and other impersonation attack techniques.

This integrated approach to security controls provides the necessary context to support zero-trust models.

Endpoint Security and SASE

As SASE solutions combine WAN capabilities with network security functions, they offer needed operational and performance gains in support of direct-to-cloud operating models. By bringing together capabilities offered in secure web gateways, cloud access security brokers, firewall-as-a-service offerings, and zero-trust network access, they can further offer improved efficacy and efficiency of key security controls.

When endpoint security solutions are further integrated into the equation, they can act as a local control point and early warning system for more advanced threats.

Endpoint Security and XDR

As advanced threats leverage multiple attack vectors, individual security controls struggle to keep up. Yet when individual controls can share insights and context, they can recognize and stop attacks in progress, without the need for analyst intervention. XDR solutions are bringing together security telemetry across multiple controls, helping analysts detect and respond faster. When endpoint security telemetry is architected to support XDR, optimizations in detection and response are enabled. Security platform vendors understand this opportunity and are customizing endpoint data to optimize XDR solutions, delivering better efficacy and efficiency gains.

Endpoint Security: A Core Security Pillar

As security architecture and infrastructure continue to evolve, mainstay controls, such as endpoint security, are critical to enabling security architects to keep pace with a rapidly expanding attack surface and IT infrastructure operating models. As endpoints interact with public and private cloud-delivered resources, endpoint security solutions must work seamlessly together with web gateways, DNS, firewalls, and identity and access controls to detect and stop sophisticated, modern attacks.

Cisco Secure Endpoint

Cisco Secure Endpoint is a core pillar and control point within Cisco's SecureX open, cloud-native security platform. Cisco Secure Endpoint is the industry's first endpoint security solution to bring together user access with device protection, integrating prevention, detection, response, and access control into a built-in platform, backed by industry-leading threat intelligence from Cisco Talos.

- 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, behavioral analytics and protection, next-generation antivirus, fileless malware and ransomware defenses, integrated 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 ITOps—delivering quick time to value from a single, unified endpoint security solution that provides both advanced and 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 control point and component of Cisco's SecureX platform, Cisco Secure Endpoint works together across an organization's entire security infrastructure, including network, cloud, and applications, to generate actionable insights that accelerate threat response. With Cisco SecureX built into Cisco Secure Endpoint, you can 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

While security teams rally around modern security initiatives including zero trust, SASE, and XDR, core security pillar choices become key enablers. When endpoint security solutions are architected with these initiatives in mind, they facilitate rapid implementation and adoption with less friction.

Device diversity will continue to accelerate, requiring security teams to depend on endpoint security solutions that are dynamic enough to keep up. Equally important will be the ability to integrate and work together with the rest of the security stack, bringing new levels of visibility and protection for advanced threats as the attack landscape continues to grow.

When considering converged security platforms, ESG recommends paying close attention to endpoint security solutions, as they play an integral role in facilitating the implementation of modern security architecture leading to increases in both efficacy and efficiency.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.

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