Enterprise Strategy Group™ by TechTarget

WHITE PAPER

A Platform Advantage

Building a Modern, Scalable Security Architecture for the Hybrid Multi-cloud Future

By Dave Gruber, Principal Analyst
Enterprise Strategy Group

May 2023

Contents

Introduction 3
Current Strategies Are Failing 3
Transformation Is Underway, but More Is Needed 4
- Zero Trust 4
- SASE and the Role of Security Services Edge 4
- XDR 4
- MDR 4
- MITRE ATT&CK Framework 5
- Tools Consolidation 5

A More Collaborative Approach to Security 5
Integrated Security Solution Advantages 5
- Accelerating Operational Performance Across User Types 7

The Role of Extensibility 7
A Roadmap for Change 8
Introducing Cisco Security Cloud 8
Conclusion 8

Introduction

Technology has seeped into virtually every aspect of our lives, often blurring the boundaries between personal and professional activities. Business transactions and human collaboration have merged into a seamless environment, supporting virtually every aspect of customer and operational interaction.

Where and how we interact and transact with both private and public sector services have never been more diverse, dynamic, and distributed, where people, applications, devices, and data can be accessed from anywhere. Continuous internet connectivity, paired with widely available, cloud-delivered applications are enabling every aspect of our private and professional lives to be facilitated by technology.

Quickly surpassing value-added enablement, our society is becoming deeply dependent on this technology-enabled world, catapulting the importance of continuous availability and risk mitigation strategies. Cybersecurity has never been more important.

Cybersecurity has never been more important

Our society has become deeply dependent on a technology-enabled world, catapulting the importance of both continuous availability and risk mitigation strategies.

Business, IT, and security leaders must work closely together to operate effectively within this technology-enabled world. As IT advancements enable businesses to expand and operate digitally, security leaders must carefully align security program development with IT infrastructure and application investments, including strategies, architecture, and operations. Yet, while well-thought-out strategies and architectural decisions can often endure some level of scale and expansion over time, most will eventually require a more holistic re-architecture as business and operational requirements grow and change.

For many security leaders, this tipping point is now. A fundamental re-architecture is needed to support the future of continued digital growth.

Current Strategies Are Failing

Modern security strategies continue to evolve in support of highly diverse and distributed computing and worker models. As security leaders further expand the scope of their programs in support of cloud-native applications, new and more diverse device types, and a growing number of non-corporate managed devices and network, many are reaching the limits of existing security architecture, enabling bad actors to exploit vulnerable systems and thwart existing security controls using more advanced, complex attack strategies.

As security architects scurry to keep up with the addition of more security controls, many are inadvertently adding complexity as they race to close gaps within their rapidly expanding attack surfaces. The large number of security tools in use is creating an assortment of challenges for most organizations, including difficulty getting a holistic picture of security, increased training requirements, and the need for manual intervention to fill gaps between security products.[1] Security is further adding friction for end users, IT and SecOps teams, developers, and executives, which, collectively, is burdening business growth velocity and the overall cost of operations.

Meanwhile more advanced attacks are leveraging this growing complexity to evade individual security controls, resulting in longer dwell times and higher attack success rates. Criminal activity has no boundaries, leveraging

[1] Source: Enterprise Strategy Group Complete Survey Results, *ESG/ISSA Cybersecurity Process and Technology Survey*, July 2022.

extortion, shaming, denial of service, embezzlement, insider involvement, business and supply chain email compromise, and more, while identity and credential theft also runs rampant.

Transformation Is Underway, but More Is Needed

Significant change in security strategies has taken place over the past three years, influenced by industry mega-trends, including zero trust, secure access service edge (SASE), extended detection and response (XDR), managed detection and response (MDR), and the use of MITRE ATT&CK framework. Yet significant challenges still exist in how and where these important advancements are being applied, leaving many with a long road ahead.

Zero Trust

Core security controls and prevention mechanisms have embraced the notion of zero trust, forcing significant change across an array of network, endpoint, cloud, and identity security controls. The lack of standard implementation practices has, however, challenged many security architects as they face their own zero trust journey, building highly customized plans designed for their own environments, tools, and architecture.

Change Is Underway, but Significant Challenges Persist

Despite investment in widely accepted industry security strategies, most continue to struggle to achieve desired security outcomes.

SASE and the Role of Security Services Edge

While SASE has enabled the convergence network and network security controls, more is needed. Hybrid work is here to stay. Workers now expect the same experience they once had when working in an office. But for most, this is not the case. Today, workers must navigate multiple access mechanisms throughout their day, leveraging VPN for some applications, zero trust network access (ZTNA) for others, while accessing some directly from the Internet. The user is expected to understand and navigate each access path, adding friction, and potentially making them an easier target for attackers. Further adding complexity, many organizations depend on multiple solutions for secure access (VPN, ZTNA, DNS security), creating a suboptimal user experience and an IT policy management challenge.

XDR

Attack surface expansion, together with a more advanced threat landscape, has spawned the XDR movement, driving many to rearchitect the security operations tech stack. Organizations report struggling to detect and investigate advance threats as one of the top challenges driving their interest and investment in XDR solutions.[2] XDR solutions are helping to provide a more holistic, cross-controls perspective, capable of detecting and responding to advanced threats, across multiple threat vectors. XDR strategies are not, however, without challenges, as security architects navigate a plethora of solution offerings to find the right fit and capabilities best aligned to their specific organizational needs.

MDR

As security teams strive to accelerate and strengthen security programs, MDR providers are helping fill skills gaps, while bringing proven security strategies, processes, and technologies into organizations struggling to modernize. A wide variety of managed service providers exist, and many organizations are engaging with at least 2 service

[2] Source: Enterprise Strategy Group Research Report, *SOC Modernization and the Role of XDR*, October 2022.

providers across different use cases. Beyond filling gaps, MDR providers are becoming strategic operating partners for 77% of organizations.[3]

MITRE ATT&CK Framework

Meanwhile, the MITRE ATT&ACK framework, adopted by 89% of organizations and used extensively by almost half,[4] has offered up a model to assess, architect, and operate security programs. This important framework is helping security architects see and understand the importance of how security controls work together to detect and protect against advance threats. As security teams further understand and embrace MITRE ATT&CK, its usage is expanding to multiple use cases across both proactive and reactive security strategies.

Tools Consolidation

As the number of security tools continues to grow, two-thirds of organizations are actively consolidating security operations tools, aimed at reducing cost, complexity, and policy alignment.[5] While many organizations are making progress, some continue to employ more than 15 security tools,[6] each operating with its own, limited view into what else is happening across other parts of the IT environment.

As security industry mega-trends are helping to integrate specific security functions, most are still too siloed, resulting in ongoing efficacy and efficiency challenges. A broader transformation is needed.

A More Collaborative Approach to Security

A more collaborative approach to risk and asset assessment, access, prevention, detection, and response is needed, one where individual security controls can work more holistically together to secure all aspects of digital business operations and infrastructure.

> **Inherent Advantages Come with Integrated Solutions**
>
> When multiple security controls and tools operate in concert, they see more, operate more efficiently, and strengthen protection.

Emerging, integrated, security solutions are addressing these challenges, enabling the multiple security controls and tools to operate in concert, leveraging rich threat intelligence, powerful analytics, and effective detection, investigation, and response mechanisms.

This integrated approach is bringing together security data across multiple threat vectors, leveraging a common data model, analytics engine, and orchestration engine, providing estate-wide visibility and detection of the most advanced threats. These integrated solutions are providing IT and security teams new levels of hope in modernizing security strategies and architecture capable of keeping up with the continued growth and diversity of attack surfaces across an increasingly more complex threat landscape.

Integrated Security Solution Advantages

Integrated, collaborative security solutions offer many advantages over siloed, independent tools. When security solutions share foundational constructs, they are more able to:

- **Share things easily**, such as the following:

[3] Source: Enterprise Strategy Group Research Report, *What Security Teams Want from MDR Providers*, March 2023.
[4] Source: Enterprise Strategy Group Research Report, *SOC Modernization and the Role of XDR*, October 2022.
[5] Source: Enterprise Strategy Group Complete Survey Results, *SOC Modernization and the Role of XDR*, September 2022.
[6] Source: Enterprise Strategy Group Complete Survey Results, *Managing the Endpoint Vulnerability Gap*, April 2023.

- Common services that bring together all the personas so they can work to defend and protect in unison across architectural and organizational boundaries.
- A consistent representation of assets, infrastructure, and data being protected.
- Consistency in risk assessment and risk tolerance measurement.
- Common tenancy.
- Consistent policy management applied to multiple controls.
- Shared trust.
- Threat indicators across multiple controls and analytics functions.

Integrations Improve Outcomes

When security solutions work together, they are able to drive improved outcomes in efficacy, efficiency, and scalability. They can further help people work better together, in a more consistent, collaborative manner.

- **Leverage Cross-domain Telemetry** to enable:
  - Detection of advanced threats operating across multiple threat vectors.
  - More confident automated investigation and response activities, based on higher fidelity detections.
  - Rapid threat hunting.
- **Inherit things from other solutions**, such as the following:
  - User work performed once and applied everywhere.
  - Configurations.
  - Provisioning and identity and access management.
  - Persistent customer preferences.
  - Policies.
  - Security outcomes.
  - Product innovation.
- **Facilitate collaboration**, in order to:
  - More seamlessly and efficiently integrate workflows across users.
  - Eliminate duplicative work efforts.
  - Improve administrative efficiency and consistency.
  - Leverage common inventories and identities for automation.
- **Provide a consistent user experience (UX)**, which includes:
  - Common interaction patterns.
  - New products that are easier to learn how to use.
  - Greater familiarity and trust.
  - An experience that anticipates users' actions and makes them feel seen.
- **Provide integrated, consistent operations that deliver**:
  - A frictionless and enhanced user experience.
  - Seamless, orchestrated response actions.
  - Common data structures support scalable, unified defense execution.

- **Upgrade seamlessly**, enabling:
  - New options that fit together well.
  - Capabilities to continue to work in concert with other parts of the platform when upgraded.
  - A shared set of data models for AI/ML that upgrade all functions together.

Accelerating Operational Performance Across User Types

Security challenges are adding friction across many types of end users for many organizations, slowing business performance and potential outcomes. Emerging and integrated security solutions have the potential to drive significant positive outcomes for end users, IT teams, security professionals, and application developers, among others.

- **End users -** By providing secure access to applications anywhere with minimal friction, end users experience seamless and fast connections, with a continuous and dynamic granting of trust.
- **IT teams –** When IT teams can define, manage, and enforce policy centrally and consistently, security is strengthened with less effort. Centralized, cloud-delivered policy management across multi-cloud and on-premises environments reduces effort and improves consistency.
- **Security analysts -** When security controls and analytics work collaboratively, they stop threats faster, providing better protection, detection, and response with less analyst intervention required. The result is fewer successful attacks, shorter dwell-times, and a reduced risk of disruption and damage.
- **Application developers -** When security policy can be implemented through code, developers can be freed to focus on business logic instead of security functions.

Integrated Security Solutions Drive Value Beyond Basic Security Objectives

Cybersecurity has become commonplace in everyone's life, supporting the access and usage for all aspects of technology. When security adds unnecessary friction, people resist and find ways to avoid it. UX matters to every person involved.

The Role of Extensibility

Defense-in-depth security strategies have long been proven as an effective means of defense against cyber attacks. As security architects strive to converge more mature security mechanisms, new innovations will continue, requiring rapid and effective integration across systems and data. Integrated, collaborative security solutions must, therefore, be architected to support continuous and seamless extensibility, including a model that supports both out-of-the-box integrations and custom bi-directional integrations. This architecture must further enable security architects to extend and integrate their security stack freely, without a dependance on individual solution providers.

Integration engineering complexity can consume inordinate amounts of security investment dollars, highlighting the importance of this core architectural function. This includes data model extensibility, API extensibility, and integrated response extensibility.

Further, the engineering of detection rules can also require specialized skills and high levels of resource investment, highlighting the importance of extensible threat intelligence and detection rules mechanisms within the solution. Out-of-the-box threat intelligence and detection rules are important but must be customizable and extensible to scale over time. 58% reported that they wouldn't use threat detection technology without the ability to create custom detection rules.[7]

[7] Source: Enterprise Strategy Group Complete Survey Results, *SOC Modernization and the Role of XDR*, September 2022.

Supporting these extensibility requirements, integrated solutions with robust ecosystems involving other security tools providers accelerate integration efforts without the need for more advanced skills.

A Roadmap for Change

Moving to a highly integrated, collaborative security solution is a journey that should enable improved outcomes along the way. TechTarget's Enterprise Strategy Group recommends that security leaders consider combining the move to an integrated platform with shorter-term priorities, focusing on filling functional security gaps together with architectural change.

For example, if strengthening cloud security is a priority, then organizations should consider combining the implementation of an integrated solution platform and its cloud security solution to close this gap. The right integrated security solution will enable architects to begin the journey from different places, adding more integrated capabilities over time. This progression will produce stronger benefits over time as more capabilities are added.

Once an integrated solution architecture is in place, the addition of other modules will be easier and should provide a cumulative improvement in operational efficiency and security efficacy. These platforms are also typically capable of providing visibility into these improvements so they can be measured over time.

Introducing Cisco Security Cloud

The Cisco Security Cloud is a unified platform for end-to-end security across hybrid multi-cloud environments that optimizes performance while improving security efficacy at machine scale by leveraging Cisco's cross domain telemetry. It offers the full breadth of capabilities needed for securely connecting people and devices everywhere to applications and data anywhere, plus threat prevention, detection, response, and remediation at scale.

Cisco Security Cloud delivers a comprehensive, integrated set of security services with public cloud economics and no public cloud lock-in, enabling organizations to protect their entire IT ecosystem while simplifying end-user experience. Benefits include:

- Simplify security with a cloud-native platform that securely connects users, devices, and IoT to an organization's systems, apps, and data—across multiple clouds and networks.
- Reduce friction by placing security closer to users, their data, and their applications—and simplify how they interact with all these things.
- Increase efficiency with unified policy, management, UI, and dashboards to help security work seamlessly from end to end.
- Work flexibly at scale, with no vendor lock-in. Take advantage of APIs for integration, and a robust developer ecosystem, so your environment can evolve along with your business.
- Improve visibility and threat protection with actionable insights across networks, clouds, endpoints, and applications to help SecOps teams hunt, investigate, and remediate threats.

Cisco's comprehensive, integrated set of security services take a cloud-first approach that can protect an organization's entire IT ecosystem—in the cloud, on premises, or a combination of both.

Conclusion

The digital economy is predicated on the premise that people and businesses can securely communicate and operate in a trusted, secure environment. Yet legacy security strategies and architecture are hindering critical security program advancement at a time when security is more critical than ever.

As security leaders push to accelerate program development to keep up with IT infrastructure and application investments, they face unprecedented challenges in complexity and diversity, requiring new thinking in their approach. More collaborative, integrated architecture is needed, which can become a foundation for expansion and growth without adding more complexity. Collaboration and extensibility are key characteristics of such a solution, together with the ability easily interoperate with other solutions.

Enterprise Strategy Group strongly recommends that security leaders consider moving to integrated, collaborative solutions and platforms from vendors such as Cisco, as a foundational technology construct in program modernization initiatives.

About Enterprise Strategy Group
Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community. © TechTarget 2023.

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