Cisco Cybersecurity
Report Series 2020

cisco Secure

SIMPLIFY TO SECURE

Reduce complexity by integrating your security ecosystem

Contents

Introduction

Managing security is complex as a result of evolving threats, the need to retain talent, and a sprawling vendor landscape. Growing your business securely doesn't just involve adopting new security technologies to counter new threats. Or keeping up with challenges introduced through new business processes. It's more like fighting Hydra of Lerna, the serpentine water monster from Greek and Roman mythology – you cut off one head, and two more will grow back in its place.

Conventional wisdom implies that every new problem requires a new solution. But that new solution can open you up to the herculean task of fighting two new Hydra heads instead of one. Likewise, layering new tech onto every new threat actually makes you less secure as your processes get more complex and your tools more interdependent.

In other words, if you continue to seek the exact technology to solve your newest, most pressing security concern, you may be multiplying security gaps that slow you down instead of simplifying your security environment to accelerate detection and response.

Complexity is the enemy

As a CISO or IT Security Manager, you're constantly battling unrelenting demands to keep your organization secure. You're protecting a workforce that needs to access applications and data on any device, anywhere, at any time. You're fortifying an increasingly digitized business to ensure every part of the ecosystem, from network to cloud, is safe. You're ensuring that workloads are secured wherever they're running, 24/7. You want your organization to make headlines for the right reasons, not the wrong ones.

And there's no question that cyberthreat actors are well funded and constantly innovating. Perennial challenges, like keeping an accurate inventory of users, applications, and devices, never go away. You try to empower teams to move fast, aware of the balancing act between accelerating your success and ensuring the reliability of your security. Between new regulations, board mandates, static budgets, enabling a secure remote workforce, and the revolving door of security talent...the CISO never rests.

To make matters worse, you've been forced to use individual point solutions from an industry that's rife with incompatibility, running your operations across dozens of tools and a plethora of consoles with inconsistent integration. And this, combined with unmet scores of patching and maintenance needs, inevitably leaves vulnerabilities in different point solutions across the security infrastructure.

With disparate solutions and vendors, it seems an insurmountable program to maintain. However, a security platform can transform your infrastructure from a series of disjointed solutions into a fully integrated environment. It can connect the breadth of your security portfolio and your entire security infrastructure to establish coverage across every threat vector and access point and evolve your organization's security to meet the needs of tomorrow.

A platform can unify your security technologies to combine visibility and identify areas for automation, orchestration, and analytics. And in doing so, it can free up and empower your security teams while making decisions based on timely, accurate data to support the overall success of your business.

Digital organizations seeking to reduce complexity and manage risk more efficiently will leverage an integrated security platform for unified visibility and intelligence, operational efficiency, and simplified security.

This approach enables our security team to stop being product integrators, instead focusing on what matters most – securing our solutions to help our customers achieve their goals with confidence.

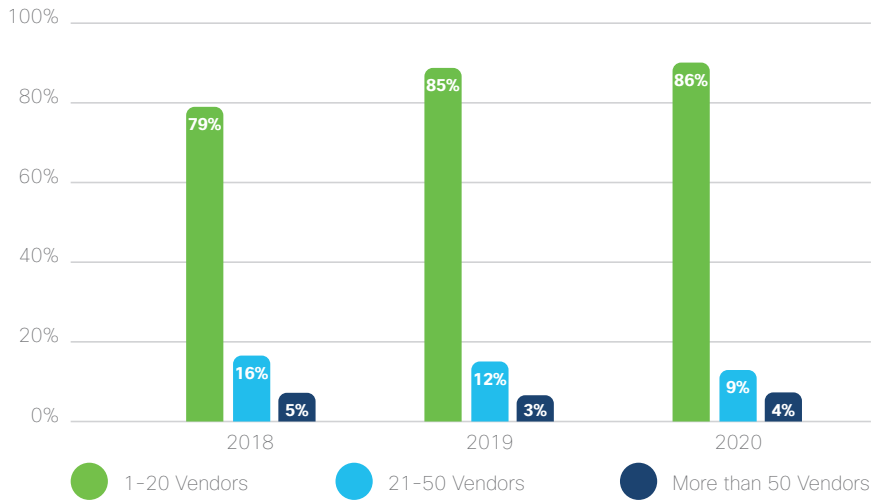
Brad Arkin, Senior Vice President and Chief Security and Trust Officer, Cisco

A closer look at security vendors, products, and their impacts

At every RSA Conference, hundreds of security vendors vie for the security professional's mindshare – with no shortage of vendors offering point solutions that promise quick wins to combat threats. The reality is that most organizations already have an abundance of products designed to address specific challenges – in fact, more than they can manage with so many alerts being generated. But most patched together products lack out-of-the-box integrations to enable a streamlined, mature security practice.

Cisco's 2020 CISO Benchmark Survey of 2,800 security managers revealed that the trend to reduce complexity through vendor consolidation continues, holding steady with 86% of organizations using between 1 and 20 vendors, and only 13% using more than 20 vendors this year (Figure 1).

Figure 1. The number of different security vendors (i.e., brands, manufacturers) used within respondents' security environments over the past three years. N=2800.



Source: Cisco 2020 CISO Benchmark Study. All percentages rounded.

We've seen a consistent rise year over year in the percentage of CISO Benchmark Survey respondents who rate working with multiple security products as somewhat or very challenging – ascending from 74% in 2018 to 80% in 2020.

If you approach your security infrastructure without a platform approach, the product-to-product integrations result in a sprawl of point solutions designed and supported by different vendors. This creates fragmented visibility and manual workflows across your security infrastructure, limiting the value from every solution.

Wouldn't it help if your security infrastructure was greater than the sum of its parts?

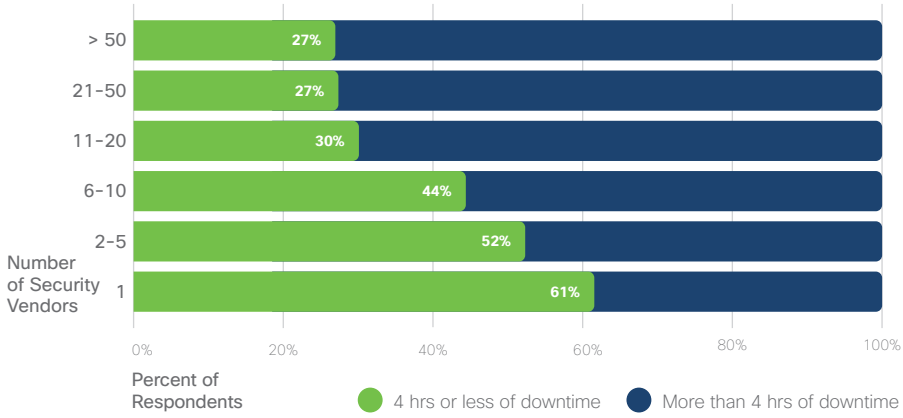
Set up for failure – the data doesn't lie

Reliance on too many consoles reduces operational efficiency, and not surprisingly, adds more risk of human error. Using disjointed tools makes it increasingly difficult to establish broad visibility across the attack surface. This can reduce security effectiveness – often measured in dwell time (the duration of time a threat actor has within a system to move laterally and perform reconnaissance and/or exfiltrate data).

A lack of integration exposes a critical security weakness in an organization's ability to respond to threats rapidly and achieve lower dwell times. Thus, visibility in context becomes much more meaningful.

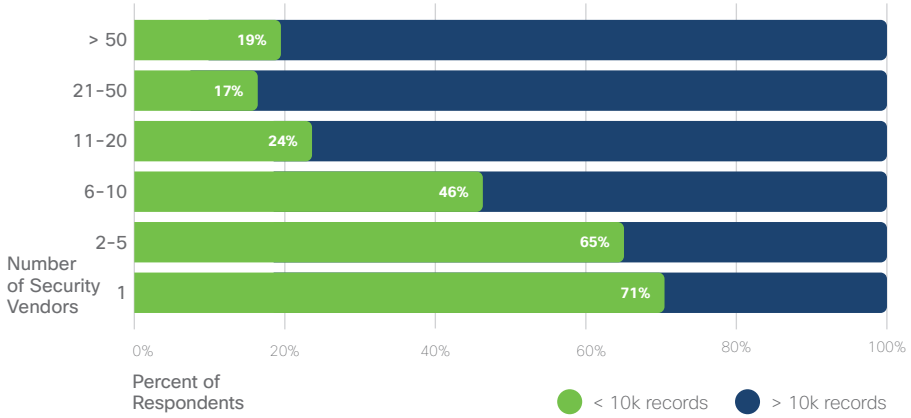
Our 2020 CISO Benchmark Survey also highlighted how vendor and product complexity can significantly degrade an organization's effectiveness in minimizing downtime in response to a cyberattack. We found a correlation between the number of vendors and products in an environment, and the resulting downtime, impacted records, and financial impact of an attack. As Figures 2, 3 and 4 show, those with less vendors tended to experience less impact from an attack.

Figure 2. For the largest breach last year, security respondents reported having **fewer hours of system downtime** when they had fewer vendors in place. N=2490.



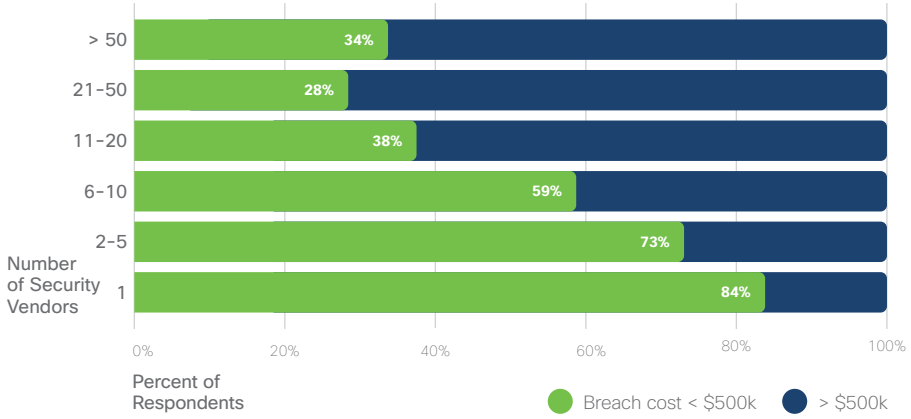
Source: Cisco 2020 CISO Benchmark Study. All percentages rounded.

Figure 3. For the largest breach last year, security respondents reported having **fewer records impacted** when they had fewer vendors in place. N=2490.



Source: Cisco 2020 CISO Benchmark Study. All percentages rounded.

Figure 4. For the largest breach last year, security respondents reported having **less financial impact** when they had fewer vendors in place. N=2490.



Source: Cisco 2020 CISO Benchmark Study. All percentages rounded.

The impact on alert management

Because multiple vendor solutions have multiple point-to-point integrations, if any integrations at all, they don't effectively share context and analytics to identify indicators of compromise. Further, they have limited opportunity to enrich and prioritize alerts and present high-value alerts in concise ways. More problematic, this results in little to no connection between seeing the alert and acting on it.

In our 2020 CISO Benchmark Survey, security professionals reported that they're only able to investigate 51% of their security alerts. Of those investigated alerts, 50% of the legitimate alerts are not remediated.

This multi-vendor approach (instead of an integrated approach) causes the persistent challenge of an overwhelming amount of alerts to continue. In our study, 96% of alert fatigue sufferers said that managing a multi-vendor environment is challenging. While security professionals are attempting to address vendor sprawl and consequences, managing it has not become easier and needs further improvement to optimize resources.

Front-line advice from Cisco Security leadership

Security has evolved in the last decade

The struggle to survive is now on 24/7, and security has evolved in three dimensions. One is **business relevance,** which has proven to be an incredible accelerator for making the case for security. Security is becoming essentially integrated into the fabric of the way businesses operate with increased levels of scrutiny across the organization, from the boardroom to the executive staff, to the various business units' operations.

The second one is **technology,** which is a two-sided coin. The first side of the coin is the evolving **architecture** propelled by the migration to the cloud and proliferation of mobility in applications and devices. The other side is the emergence of **platforms** that allow vendors to exchange threat data in real time, such as threat response platforms and open data exchanges like Cisco pxGrid.

The third is **data**, because nobody sees the whole planet. In the past, the drive toward the right security architecture has been challenged by the lack of a platform that can integrate and harness the power of so much data to meet the evolving attack landscape, infrastructure, and lack of skills.

Advice for CISOs planning on integrating their architecture

Come up with a plan and determine what you're trying to accomplish by building an integrated ecosystem relevant to your business. To me, it's essentially how something is designed, how it will be built, and how it will extend and be able to grow – as well as be validated – to architect in the right way.

First, start with the idea and **develop strategies** for distinctive capabilities that your organization would like to leverage. Secondly, know **what outcomes you're measuring** before you start building something. It's also critical to **partner with vendors** who understand your strategy and can highlight potential blind spots and **integration opportunities** you may have missed.

Metrics you need to track success in your SOC operations

For a long time, the industry has used “Have you gotten breached?” as a metric for success. With my team, I emphasize metrics around **visibility and control.** It’s imperative to define what outcomes you need to achieve, be it fewer breaches, a lower mean-time-to-detection (MTTD) and mean-time-to-remediation (MTTR), a reduction in cost-to-contain, and/or increased efficacy. Metrics that you report to the board should be **tied to these business-level outcomes** that are driven by the underlying security program.

How effective integrations have fueled the Cisco SOC

It’s of course great to get best-in-class, but it’s not always needed to most quickly achieve the desired security outcomes. Besides using our own security products at Cisco, we’ve historically used non-Cisco security products as well. Currently, we’re using the full suite of Cisco products. **And despite having our budget reduced three times in the past three years, we’ve managed to reduce our MTTD to eight hours.**

We made this possible thanks to an integrated platform driven by automation and data intelligence that has allowed my staff to **focus on the most critical incidents and threat hunting,** thereby enhancing resource productivity. Having a consolidated solution with automation capabilities, backed by a platform that works well with your data analytics needs, AND the ability to fill gaps in your existing SecOps workflows, is critical. At Cisco, we built efficiency into the system, which has yielded ROI and brought down our total cost.

Security reimagined

A day in the life...

Let's spend a day in the life of a SOC analyst. If they're covering all their bases, they review increasing numbers of alerts from different solutions. They struggle to keep up with the alert volume, and are doing their best to prioritize and address the most critical of the lot.

They correlate the information from various sources to build a complete picture of each potential threat. They triage and assign priorities, working with their IT and network operations teams. They develop playbooks to help them repeat these activities in a consistent manner.

They perform all these complex tasks with a tremendous sense of urgency. Their goal is to quickly formulate an adequate response strategy based on situational awareness and threat impact, potential scope of compromise, and the potential damage that can ensue.

This manual workflow is often error-prone and time-consuming, requiring a SOC analyst to swivel quickly through multiple consoles. With all the SOC analyst's multi-tasking to size up alerts from numerous point solutions, there's a probability that they'll overlook high-severity threats.

And behold, hiring more experts to manage these alerts doesn't help. Responsiveness is also impacted by the reliance of ITOps and NetOps on SecOps and the bottlenecks these teams create for each other. Organizations need help mitigating the talent shortage by uniting people, processes, and technology into a simpler, more consistent experience. And here, integrations are key.

> Positive shifts in digital transformation have made it evident that security technologies in silos contribute to more complexity. Our teams are losing precious time connecting the dots and integrating all these tools that don't work with one another.
>
> Michael Degroote, Infrastructure Consultant, Mohawk Industries

More focus, less noise

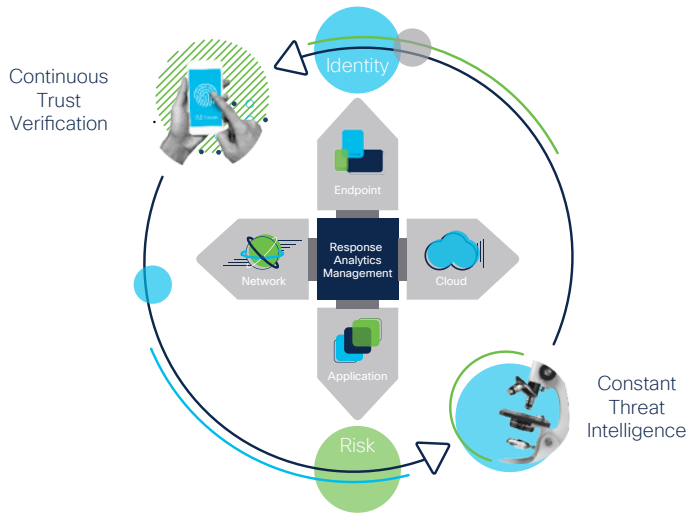
Most CISOs get up every morning to improve efficiencies, optimize their resources, grow maturity, and drive collaboration across their operations. All while managing threats. That's a tall order, and a hard one to achieve with so much noise around cybersecurity. Let's break down the main components of security.

When it comes to managing threats, there are many areas of integration that security platforms can harness, such as:

- **Network security:** Firewalls and zero trust for the workplace
- **User and endpoint protection:** Zero trust for the workforce with endpoint, mobile, and email security
- **Cloud edge:** A broad set of visibility, control, and security functions as a cloud service
- **Application security:** Zero trust for workloads with microsegmentation
- **Threat intelligence:** Malware analysis and feeds
- **Trust verification:** User authentication and device posture assessment
- **Security analytics:** Collection, categorization, and analysis of data in real time to detect anomalies and advanced threats
- **Security services:** Managed detection and response

To achieve security coverage down this long list would require a vast array of security products. But consider – this can be achieved through a platform approach, providing continuous trust verification and constant threat intelligence (Figure 5).

Figure 5. Transform your infrastructure from a series of disjointed solutions into a fully integrated environment with backend integrations translating into better frontend experiences.



This can't all happen overnight. But to move toward this integrated approach, you can begin by listing your priorities, challenges, and workflows.

To start, spend some time answering these foundational questions:

- What are the challenges with my existing security infrastructure?
- Will business changes require me to add to or replace my security investments?
- How can I advance my security maturity with my existing resources?
- What are my priorities to get the most value out of any security investment?
- What context is shared between teams and tools in our workflows?

Thoroughly answering these questions will provide you with a solid grasp of which security challenges need to be solved and in what order. This also serves as a roadmap for identifying what you have, what you need to reach your objectives, why you need it, and what you'll gain from making those changes. The next step is to develop strategies for each capability that your organization needs to have.

Once you've reached a clear understanding of all these aspects, you can then look for solutions that specifically meet those needs – being mindful of exploring solutions **that work together from end-to-end in your security ecosystem and overall infrastructure.**

Merely acquiring best-of-breed tools that operate in isolation without an underlying security platform has become an increasingly less viable option. Any tool with very good functionality – and one that easily integrates with other tools – is probably more valuable and effective than a tool with every bell and whistle imaginable.

Acquiring in this way allows you to start the work of defining cross-tool workflows at a more advanced level. A platform that provides both integration and workflow definition at its core has a measurable impact on your efforts to increase your security maturity.

The point here is this: before you seek out security solutions, know what you are trying to achieve and how it aligns to (or supports) your business goals. Determine how solutions will work together to minimize the noise of too many alerts and reduce the more manual maintenance for which you don't have the resources.

Integration from a security platform

Certainly, no single security solution can keep entire organizations secure. And no single dashboard can fix the security domain's need for greater visibility. Success depends on understanding the relationships between technologies that link systems and using this knowledge to create greater synergy between them. It sounds easier said than done – so how do you translate this vision?

A platform approach to security underscores the importance of openness – the ability to connect your existing security infrastructure to an open, integrated platform with out-of-the-box interoperability. Your business should be free to explore new solutions without having to worry about spending your resources on integrating them later.

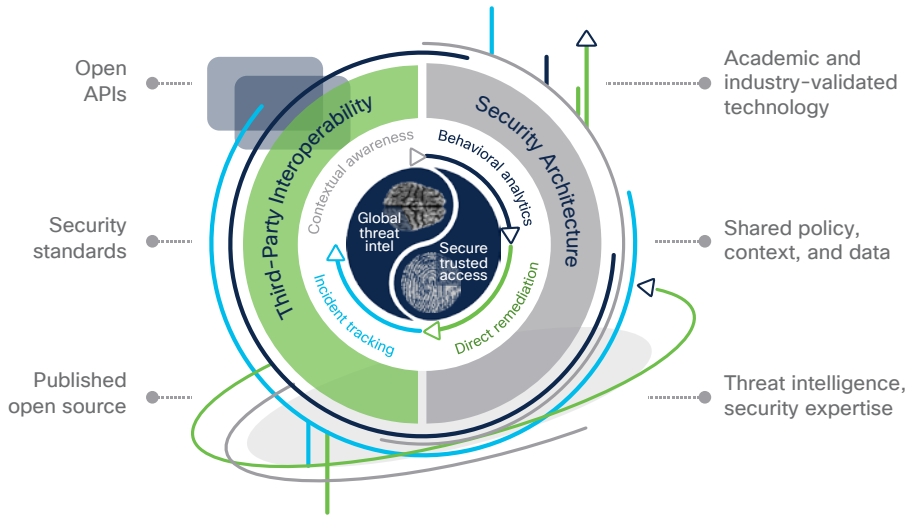
For example, the Cisco Security Technical Alliance facilitates open, multivendor product integrations with more than 170 technology partners to improve security effectiveness through automation and operational simplicity. Our integration through a security platform is designed to give our customers an effective approach to secure access, threat response, and policy management.

While we work on the network side, the security side, the identity side, the access side, and more, we're not closed off. You can bring in technology from any security product – Cisco or otherwise – to create one integrated security environment (Figure 6).

Consider four pillars of enablement in such an environment. You can:

- Know what data is shared to speed time-to-detection
- Run automated policy changes to speed response
- Provide contextual awareness to embed granular controls across your security architecture
- Harmonize your security policies and drive stronger outcomes with SecOps, NetOps, and ITOps collaboration

Figure 6. Create a foundation for your security stack with built-in interoperability that ensures you experience the full potential of your products.



This modular approach to security enables you with access points to harness integration between existing technologies, while ensuring faster access to new technologies without integration tradeoffs. You can create this now with what you have.

Maybe you've already developed the most powerful portfolio of security products and added built-in interoperability. Now, with this approach, you are connecting all of this to a platform that ensures your experience reaches the full potential of your products, with openness and built-in interoperability being the most salient benefits.

The right platform won't just help you improve your security across users, applications, and devices – it will help you measure and prove success. A platform should deliver built-in automation and analytics that aid in policy and device management, detecting unknown threats, and coordinating response and policy change. This new approach is well-positioned to solve the security conundrum and transform security from complex to cohesive.

Quantify the benefits

Adoption of the platform approach creates quantifiable improvements for your business. These improvements include numerous benefits, the most important of which are:

Operational efficiencies: Aggregate threat intelligence, automate enrichment, and improve incident response and policy orchestration to respond more effectively to evolving threats and secure new business endeavors.

- **Cut through alert noise** with contextual awareness and correlations to more deeply understand which alerts need urgent attention. Reduce time-per-alert required for forensic investigation as workflows are integrated and automated through playbooks.
- **Reduce vendor footprint** in your ecosystem by ensuring that strategic security partners can deliver new capabilities as components that can easily integrate.
- **Gain faster access** to those capabilities for the security and IT teams, delivered in a more efficient manner than if they were standalone components.

Innovation: Work with fewer, yet stronger vendor partners who have gained a reputation of bringing more innovative capabilities and services to market that better address evolving architectures and threats. An open platform that allows you to develop workflows that automate your tailored playbooks can drive innovation for your security.

Empower resources through automation: An integrated platform propelled by automation can help tackle the challenges of talent shortage, enabling you to use your limited SOC resources to more strategically orchestrate. This can help improve employee retention and help a Level 1 SOC Analyst perform more complex investigations, so your team has more time to focus on what's most critical.

Reducing complexity: Many security devices and solutions are not capable of integrating into the broader security platform due to a lack of design modularity. Look for cloud-delivered and API-based solutions that can enable rapid response and remediation. Your security platform should enable simplified expansion of security capabilities based on emerging needs.

Rationalizing ROI: The move to an integrated security platform versus going to disparate security vendors can more readily show an impact in KPIs, driving resource productivity and response metrics like MTTD, MTTR, and incident burndown times. This gives you definitive proof points to correlate with breach costs. With disparate tools, it's hard to get at key metrics that really provide measures of performance and efficiency.

Reducing risk: Assess the most critical data and cover the attendant risks on that data across your solution ecosystem by leveraging aggregated threat intelligence, advanced behavioral analytics, orchestration, automation, and continuous threat hunting.

Measuring success: Metrics are an excellent way to understand the disconnect between prevention, detection, and IR operations. The ability to track metrics such as dwell time, protection ratio, incident false positives, ratio of user-identified incidents to SOC-identified incidents, and so on provides a snapshot of vulnerability. Tactical effectiveness of SecOps enables you to mind the gaps and architect a better security program.

Questions to get you started

With so many choices and so many directions in which to go, let's start with 10 critical questions security professionals should consider when looking at vendor products and solutions.

1. **What is the total cost of ownership and ROI benefits I can realize from the consolidation of vendors and integrating my existing portfolio?**
2. **Is our platform unified for threat investigation, security management, and incident response?**
3. **How does this new technology integrate with our existing ecosystem? Will it improve our security efficacy and operational efficiency?**
4. **Does our threat intelligence program enable us to make faster, more definitive decisions?**
5. **How would we rate our solutions' openness to integrate with third parties? How does this work alongside our existing SIEM technologies?**
6. **Does this vendor (or product) enable our team to accelerate key security functions: detection, investigation, and remediation through a unified console?**
7. **Do our existing technologies generate and retain context across the toolset? Do they integrate natively with other tools from that same vendor?**
8. **Does our platform leverage automation to simplify manual workflows? Do these workflows enable us to make NetOps and ITOps an extension of SecOps teams?**
9. **Has our team discussed integration tradeoffs while evaluating products to understand if we need the extra features at the expense of integration?**
10. **Will our current SOC staffing support this? Do we need to hire additional analysts, or can we train the existing team?**

Foundational strategies from our Advisory CISOs

Here are our practical recommendations based on our original research and proven practices consulting with customers.

1. Consider integration to be a key part of your buying decision.

The vendor sprawl in a typical security environment causes unnecessary complexity and inefficient workflows. To make matters worse, chronic talent shortages make it difficult to fully adopt existing solutions, which increases exposure. One tactic to mitigate these challenges is to adopt an open, portfolio-based platform that enables your solutions to work together.

This type of platform approach is unique in two ways. First, it natively integrates the portfolio's back-end solutions with a unified frontend. Second, it enables other vendors' technologies to seamlessly integrate with that frontend.

When the burden of integration is shifted primarily to the vendor, you end up leveraging existing investments, building on what you have, and creating a strong foundation for future needs.

2. Bring NetOps, ITOps, and SecOps into alignment.

Network, IT, and security teams have traditionally worked in siloes, but their reliance on each other to solve problems causes bottlenecks. You can unify your teams with collaborative workflows and shared context to enable ITOps to remediate issues with meaningful alerts and allow NetOps to enforce policies more consistently. This reduces the burden on SecOps and improves the productivity of all three teams.

Achieving this level of collaboration isn't easy, but it's possible with the right approach. An integrated platform can help, so long as it provides a customizable, unified view, allowing each team to see the alerts, metrics, and context that are most meaningful to them without disrupting the others.

3. Guide your decision-making with a security maturity model.

With the pressures of tight budgets, chronic staff shortages, and a constantly changing threat landscape, it is easy to fall into a reactive mode of security. However, in this reactive paradigm, your investments may only help you maintain the status quo rather than free you to mature your security organization.

Pick a security maturity model and be proactive about your trajectory. There are many to choose from, but most models reflect unified visibility across control points, cross-environment automation, and clear security metrics. While it's possible to achieve these outcomes via manual SIEM/SOAR integrations, all of these are native functions of an integrated security platform.

4. Give your people one view to focus on, not twenty.

Your security teams are constantly swiveling between different consoles and interfaces, which slows them down and generates conflicting alerts.

Give them a unified view by integrating your security infrastructure. This streamlines workflows and maximizes the value of your investments. It also enables your teams to act on alerts, harmonize policies, respond to threats, and learn best practices – unlocking value faster with a simpler, more consistent experience.

5. Use automation wherever you can to make your teams more efficient.

Your teams probably lose a lot of time to repetitive, manual processes – this is inefficient and leaves room for human error. With a platform, you can use automation to handle many tasks such as sharing threat and trust context and adapting network or application access for compromised endpoints.

For example, you could use these capabilities together to prevent unhealthy devices from accessing sensitive data. First, use your secure access solution to identify endpoints that are infected or unsecure. Then use automation to change the authentication policy for that device across your entire environment until the threat is remediated.

By blocking access for untrusted devices, you can respond to threats faster and prevent data breaches without getting in the way of business.

Case Study: Istanbul Grand Airport (IGA)

Building a secure, scalable network from the ground up with integration at its core.

Summary

Industry: Transportation

Location: Istanbul, Turkey

Challenge

- Build a secure IT foundation for the world's largest growing airport
- Ensure network flexibility and scalability through three construction phases
- Provide visibility into all parts of the airport's IT infrastructure
- Deliver effective threat hunting and investigation capabilities

Solution

IGA consolidated its security portfolio with objectives to:

- Reduce complexity through vendor consolidation
- Enhance endpoint security
- Increase network visibility and actionable intelligence
- Achieve better threat detection

To fully secure the world's largest growing airport, IGA deployed Cisco's endpoint security solution. With a full Cisco Security integrated platform, IGA now has confidence that customer and business data will be protected and secured.

Results

- Scalability in management with flexible APIs
- Effective security throughout IGA's IT infrastructure from network, web, and email to endpoint
- Integrated platform that allows IGA to see a threat once and block it everywhere in its environment, thus decreasing administrative workload and time-to-remediation
- Enhanced visibility and threat hunting capabilities to prevent attacks from entering IGA's network

Learn more.

We were looking at the integration, visibility, and implementation features of the products, and Cisco was the only vendor that could deliver.

Emrah Bayarcelik, Head of Security, Istanbul Grand Airport

Cisco Security delivers simplicity

Cisco Security continues to build a simplified experience for our customers – security that helps reduce complexity, strengthen operations, and enable teams to spend more time on higher-value initiatives.

At the heart of our security platform, Cisco SecureX, is a simple idea: security solutions should be designed to act as one team. They should learn from each other. They should listen and respond as a coordinated unit. When that happens, security becomes systematic and more effective. With our platform design, we've made it possible to:

- **Confidently secure your business:** Meet your security needs of today and tomorrow with the broadest, most integrated security platform that protects your diverse access points from a variety of threat vectors.
- **Automate security workflows:** Increase the efficiency and precision of your existing resources via automation to advance your security maturity and stay ahead of an ever-changing threat landscape.
- **Collaborate better than ever:** Share context between SecOps, ITOps, and NetOps to harmonize security policies and drive stronger outcomes across workflows that turn security from a blocker to an enabler.
- **Reduce complexity and maximize benefits:** Advance the potential of your Cisco Security investments, try other components of the Cisco portfolio through free trials, and connect to your existing security infrastructure via out-of-the-box interoperability.

Cisco Security gives you a unique opportunity to combine the breadth of our portfolio with your entire security infrastructure for a consistent experience. This unifies visibility, enables automation, and strengthens security across your network, endpoint, cloud, and applications. The environment enables your staff to automate threat detection and response, as well as network policy management, and deploy zero trust access to drive deeper visibility and stronger policy controls. The result is simplified security, built into the solutions you already have.

Imagine eliminating friction points between individual security operations and workflows. Or enabling more rapid development and rollout of new capabilities to help your security teams deploy technologies more quickly and outpace online adversaries. We can deliver.

Each Cisco Security product is backed with industry-leading Talos threat intelligence to block more threats and keep organizations safer. We use trust verification as a foundation to ensure only the right people gain access. Behavioral analytics and machine learning augment all our security efforts, so solutions adapt and become more effective in real time.

All this is supported by automated responses to advanced threats that enable you to streamline operations with integrated threat and security management throughout the portfolio. And lastly, all our products are designed to work with the non-Cisco technologies you have in place for integrated security responses. No more swiveling chairs, conflicting alerts, or inconsistent policy management.

Figure 7. The benefits of the Cisco SecureX platform approach.

Experience simplified | Success accelerated | Future protected

Integration is an essential element to our platform strategy, delivering real automation and visibility across all major threat vectors while reducing your response time to security events.

Find out more at cisco.com/go/secure.

> Having all of Cisco's tools so well integrated really gives us defense-in-depth and layered protection. Having a more holistic security platform has really helped us make more progress toward our end goal in a short amount of time.
>
> Don Bryant, CISO, The University of North Carolina at Pembroke

About our experts

Cisco Security has an Advisory CISO Board comprised of former CISOs holding a wealth of cybersecurity knowledge with backgrounds in a variety of industries. In addition to providing their insight, guidance, and experience to inform the recommendations we offer in the Cybersecurity Report Series, they also support our sellers, partners, and customers on issues from securing digital transformation to compliance, privacy, monitoring and visibility, zero trust and threat intelligence. If you would like to talk with a member of our Advisory CISO team, please contact asktheciso@external.cisco.com.

About the Cisco Cybersecurity Report Series

Throughout the past decade, Cisco has published a wealth of definitive security and threat intelligence information for security professionals interested in the state of global cybersecurity. These comprehensive reports have provided detailed accounts of threat landscapes and their organizational implications, as well as best practices to defend against the adverse impacts of data breaches.

Cisco Security now publishes a series of research-based, data-driven publications under the banner Cisco Cybersecurity Series. We've expanded the number of titles to include different reports for security professionals with different interests. Calling on the depth and breadth of expertise of threat researchers and innovators in the security industry, the reports in each year's series include the Data Privacy Benchmark Study, the Threat Report, and the CISO Benchmark Study, with others published throughout the year.

For more information, and to access all the reports in the Series, visit: www.cisco.com/go/securityreports.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA), Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Published June 2020 RPT_06_2020

cisco Secure