Whitepaper
Cisco Public

From Complex to Cohesive

How a Platform Approach Can Solve Today's Security Conundrum

Contents

Executive Summary

The demands of securing your organization are significant. You need to protect your:

- Mobile workforce in any location, on any device
- Entire digitized workplace including your infrastructure, network, and cloud
- Workloads, wherever they are running, 24/7

This is a tall order, and to make matters worse, you have to work with an assortment of independent solutions, which has put you on an endless treadmill of stitching up products that don't easily fit together. To top it all off, you also must constantly contend with new regulations, board mandates, budgets, the revolving door of security talent. The grind never stops.

It's time for a new approach that redefines security. An approach that enables security teams, processes, and technologies to work as a coordinated unit and helps SecOps, ITOps, and NetOps work more collaboratively. An approach that strengthens your security across your network, endpoints, cloud, and applications while reducing complexities.

This paper provides an overview and the pros and cons of the three platform approaches in the market: solution-based, technology-based, and portfolio-based, **then explains why an integrated portfolio-based approach tends to deliver the most value**. Read on to learn how the right platform can help you stop the grind, simplify your experience, accelerate your success, and protect your future while breaking down the siloes created by independent solutions.

How 'Best-of-Breed' Thinking Created a Conundrum

On the heels of digital transformation, malicious actors are pursuing innovations of their own and finding novel ways to exploit weaknesses in the sprawling digital landscape. When it comes to securing their digital infrastructure, many organizations are still trying to fight these sophisticated, well-funded, and patient adversaries the same way they did a decade ago – one point solution at a time. Unfortunately, it's no longer working.

Traditionally, businesses have tried to protect themselves against emergent threats by deploying new solutions, but this leaves them managing a massive security infrastructure that generates an overwhelming number of alerts. In our 2020 CISO Benchmark Study, we found that 44% of organizations see more than 10,000 daily alerts and only respond to half of them[1]. Not surprising, 82% of the CISOs acknowledged that orchestrating alerts from multiple vendor products was challenging.

Security becomes a grind

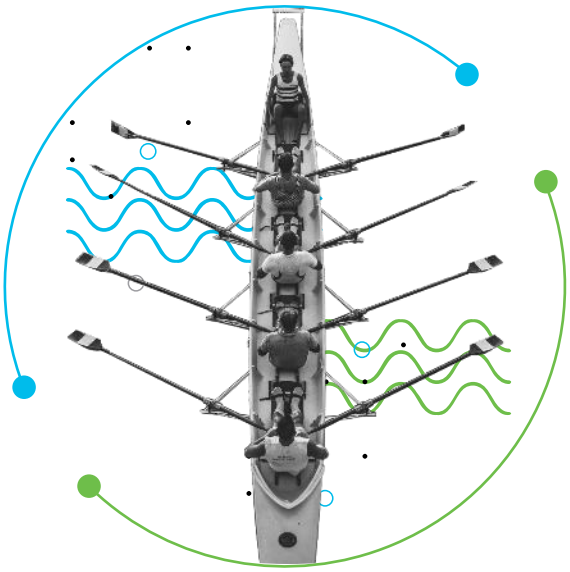
A key reason for this complexity is buying behavior. The current paradigm is "see a problem, buy a solution" with solution efficacy being a primary concern. Though building a solid foundation with "best of breed" solutions feels prudent, decisions based on the efficacy of individual products alone tend to overlook the more strategic question: Will they all integrate into the blended environment, or will they cause disharmony, leading to operational inefficiencies, unnecessary complexities, and time-consuming workflows?

The result is a vicious cycle that has turned security into a grind for cybersecurity professionals – especially as 74% believe that cyber-risk management is more difficult today due to an expanding attack surface; increasing software vulnerabilities; and more sophisticated tactics, techniques, and procedures used by adversaries[2].

Solutions should work as a team

You need more from the security solutions you already have, not additional solutions which will just make your infrastructure more complex. As it is, lack of staff expertise is the top barrier to the full adoption or use of a vendor's existing technology[3]. This leaves holes for attackers to exploit and compounds your security risks. With 3.5 million cybersecurity jobs expected to be unfilled by 2021[4], security teams need to get leaner and more efficient. Unified platforms that simplify security will become a necessity rather than "nice to have."

> One of CISO's hardest jobs is how to fit the security controls into their particular environment. Most vendors assume a level of standardization when they design their products – but that just doesn't exist. This means every tool, no matter how it was intended to function, requires manual adaption that security teams are just not set up to handle.
>
> Wendy Nather, Head of Advisory CISOs, Cisco



A phrase we hear often is that security is a team sport. Think of it like a rowing team. To move fast and keep the boat balanced, the team needs to be in perfect sync, stay highly aware of each other, and react quickly to changes. Today's security processes, however, resemble anything but harmonious strokes of oars. Instead of coordinating and working together as a unit, each security solution and process works independently and pulls in its own direction, weakening the group effort.

The Shift to Security Platforms

Platforms can unify technology, processes, and people

Imagine a rowing boat without its coxswain. Sitting at the stern of the boat, the "cox" steers the boat and instructs the crew, executing the strategy of the race. The coxswain is both the team's "brains" and director who unifies the crew members. Without one, all you have is a group of skilled rowers paddling blind, doing their best to operate their own oars but lacking any idea of where they are going.

> I need visibility to help my team understand what's happening in our environment, whether it's on prem, in the cloud, or wherever it is. If I have to do it through 20 or more vendors, I'm never going to get that visibility across all of it.
>
> Steve Martino, Chief Information Security Officer, Cisco

That is what security is missing today – a "coxswain" that turns disparate technology, processes, and people into a unified, harmonious team whose components build on rather than stifle each other. A platform that connects all the security tools to unify visibility, enable automation, and strengthen security across the network, endpoints, cloud, and applications.

Customers want simplification, integration

As digital transformation reaches a crescendo over the next few years, security, too, must come to an inflection point. Already, 72% of organizations say the complexity of the environment is their top concern[5]. The majority believe they could improve operational efficiency and their security teams' productivity through simplification.

This is where a platform approach comes in. Our CISO surveys from the past few years, as well as analyst research, indicate a growing trend toward vendor consolidation. A platform serves to simplify security while consolidating your vendor landscape, and IDC predicts that 30% of security budgets by 2020 will be spent on vendors who offer integrated platforms[6].

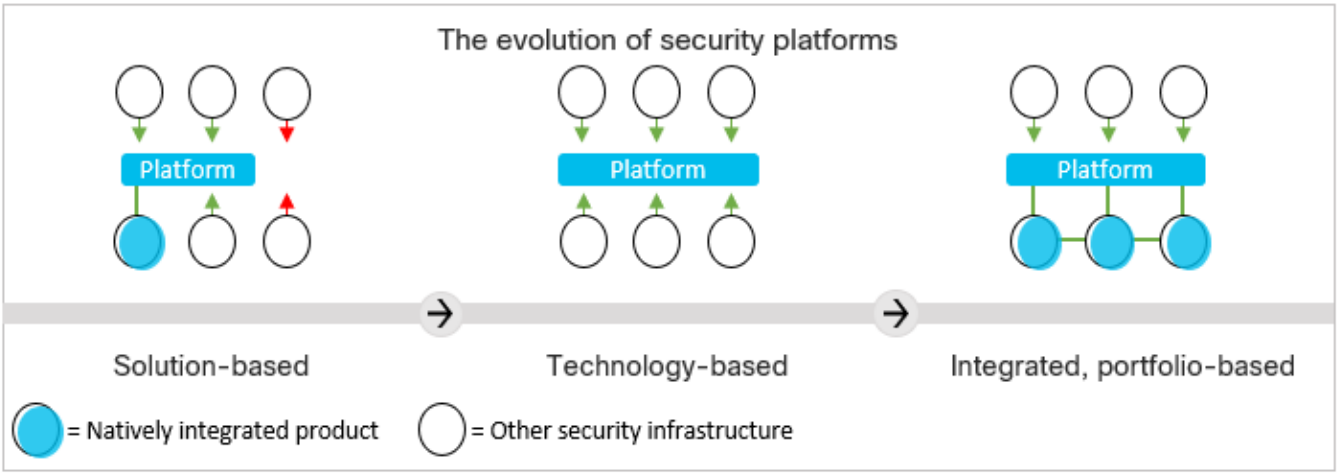
But not all platforms are created equal. Various vendors use the term platform to describe different approaches to security. While these approaches generally share some common goals, such as enhanced effectiveness through integration and openness, some offer a more limited number of control points and functionalities.

Another important distinction is whether the integrations come out of the box from the vendor, or you need to do this complex work yourself. If your team is spending a tremendous amount of time on it, they're diverting their attention from their core role of hunting and containing threats to mitigate breaches – and the value of an integrated platform is greatly diminished because you're no longer simplifying security.

> I look at security solutions as an ecosystem and how things work together. I don't want to spend time and energy integrating things, I want to do security.
>
> Steve Martino, Chief Information Security Officer, Cisco

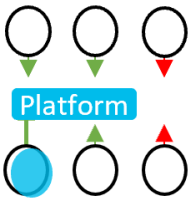
Three Approaches to Security Platforms

These are currently the three main types of platforms on the market.



Solution-based platforms

The first type of platform you may want to explore is solution-based. Within this category, there are three primary options: network, endpoint, and cloud. Naturally, each option has unique benefits and drawbacks.



Solution-based platforms

- Built around siloed solutions
- Provide limited visibility and context
- Cover single or limited control points

Network

Next-generation firewalls (NGFWs) combine the functionality of traditional firewalls, like stateful traffic inspection, with intrusion prevention, application awareness and control, integrated threat intelligence, and beyond. They're an effective solution for protecting against breaches between network segments and the internet, providing comprehensive network visibility, control, and protection. Although they're foundational for network security, NGFWs don't mitigate threats against all vectors in a heterogenous environment that interconnects networks, devices, users, and data.

If a malicious file comes via email, the NGFW can't quarantine the file on the affected endpoint. Conversely, it won't prevent a compromised user from logging on to a cloud app from a personal device. Additionally, NGFWs are less efficient as virtual firewalls in a cloud environment like AWS.

Endpoint

An endpoint protection platform (EPP) prevents file-based malware and unwanted or malicious applications from running. Many EPP solutions also offer endpoint detection and response (EDR) capabilities for ongoing protection against threats that evade initial controls. An integrated EPP and EDR solution can decrease an endpoint's attack surface, support proactive activities such as threat hunting, and protect against fileless malware and ransomware.

Despite the addition of advanced capabilities, however, this solution is limited to endpoint visibility and control. For instance, even if the EPP identifies a malicious file, it doesn't remove the email from Microsoft Exchange nor will it quarantine the potentially compromised endpoint. An important consideration is whether these platforms give you enough control points and visibility to defend your environment effectively.

Cloud

Cloud security solutions, sometimes known as secure internet gateways, combine a range of technologies including a layer 3-7 firewall, secure web gateway, and DNS-layer security. These solutions enable you to accelerate your cloud and SD-WAN adoption by providing a scalable solution that includes complete visibility, control, and protection of internet traffic and SaaS usage.

While effective against threats in a mobile world where users can connect to your network from anywhere, cloud security doesn't provide visibility into endpoints, emails, and internal or IaaS network activity.

If your cloud security solution detects command-and-control activity, for example, it can stop the "call home" communication – but it doesn't necessarily give you the data to determine where the threat came from and what else it interacted with. Additionally, it will not detect inside actors gaining unauthorized access to critical assets. Ask yourself whether a cloud security solution provides complete protection for all your use cases to be considered a true security platform.

Technology-based platforms

Another type of security platform available is technology-based. These platforms include SIEMs, SOARs and the next-generation equivalents.

SIEM (security information and event management)

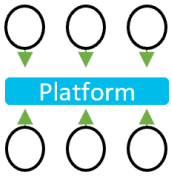
SIEM technology offers visibility and meaningful insights by collecting, aggregating, and analyzing information from different sources. When first introduced more than a decade ago, SIEM technology was considered revolutionary, but many vendors' solutions had closed ecosystems that didn't integrate well and proved to be very complex and labor intensive.

Newer generations have brought improvements, as well as expanding capabilities with analytics. While SIEM has shifted from a compliance focus to threat detection and incident response, blind spots remain because the data has limited context. For example, a SIEM solution typically doesn't include external threat intelligence. A well-tuned SIEM improves efficiency by cutting down on the number of alerts and enabling rudimentary actions like blocking activity, but it doesn't provide automated workflows for response. You still need to manually log into multiple systems to gather additional data when triaging events.

SOAR (security orchestration, automation, and response)

An emerging market category, SOAR technology is similar to SIEMs in that they aggregate, correlate, and analyze alerts (but without a data lake). SOAR technology goes a step further by integrating threat intelligence and automating incident investigation and response workflows based on playbooks developed by the security team.

.



Technology-based platforms

- Require complex integrations
- Leave blind spots
- Lack native controls

Strengthening Security with Harmonized Policy Management

Today, as multiple micro-perimeters have replaced the singe network perimeter and control point, maintaining strong security requires consistent policies across on-premises firewalls and into the cloud.

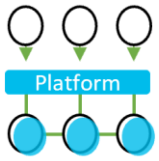
This is harder than it sounds. While 95% of organizations believe it's important to have consistent policies across all network security control points, 94% are concerned that increasing their network's complexity makes them more vulnerable.

That concern is not surprising. For example, take the move of apps from on-premises infrastructure to the cloud. At a typical organization, cloud-native firewalls are in siloed interfaces that provide no visibility and use different methodologies. Converting on-premises policies and firewalls to cloud ones could take hours of manual work for NetOps and leaves the door open to errors – and consequently, vulnerabilities.

The right platform can simplify policy management and provide visibility into policies across the hybrid environment, enabling NetOps to quickly define and harmonize policies, and reduce the time to protect against threats from hours to minutes. For all on-premises and cloud-native firewalls connected to a central interface, NetOps can see intrusion attempts, coordinate actions to block them, and quickly make access policy changes everywhere to block the threat.

The biggest benefit of SOAR technology is prioritization of security activities and automation of response actions, leading to faster detection and response through a unified dashboard. One aspect to consider is the lack of backend architecture integration and native control points – SOAR doesn't have the capability to holistically take coordinated actions across your environment. Like SIEM, properly integrating the SOAR technology with external identity and infrastructure systems is often complex and resource intensive, which limits adoption.

Integrated, portfolio-based platforms



Integrated, portfolio-based platforms

- Natively integrate backend and frontend
- Provide visibility across all control points
- Streamline workflows

Your third platform option is an emergent, portfolio-based platform. With an open platform, security teams can easily integrate the products they use now, as well as cutting-edge products they'll want to use in the future. To provide the most broad and consistent end-to-end coverage across all major threat vectors, as well as greater efficacy, these platforms help you:

- Secure every business endeavor to meet the security needs of today and tomorrow
- Unlock new potential from your security investments and cascade them across your entire infrastructure
- Effectively secure your business by making the right decisions with a meaningful view across every control point
- Strengthen your security across network, endpoint, cloud, and applications
- Realize desired outcomes informed by measurable, meaningful metrics and analytics
- Accelerate time to detect and remediate threats with human error minimized
- Optimize operational efficiency and precision across your security practice
- Speed up responsiveness to security changes with lower overhead
- Advance your security maturity level using your existing resources
- Deliver shared outcomes that ITOps and NetOps care about
- Collaborate better than ever across shared workflows and teams

The most effective platform is one that natively connects to the portfolio's products and services, covering different control points on the backend with a unified frontend workflow. Without this combination, you're left to do a lot of complicated work to morph the data generated by the backend into a dashboard that provides a meaningful user experience. This is work you'll have to do every time the vendor makes changes to the portfolio or you want to expand your capabilities in response to new threats and challenges. Portfolio-based platforms do the work for you by enabling you to plug in your existing investments, reducing integration costs.

Why Integrated, Portfolio-Based Platforms are Ideal

For many organizations, a natively integrated, portfolio-based platform delivers more value than solution-based or technology-based platforms. Integrated, portfolio-based platforms simplify and strengthen your security by unifying visibility and enabling automation. They provide value by:

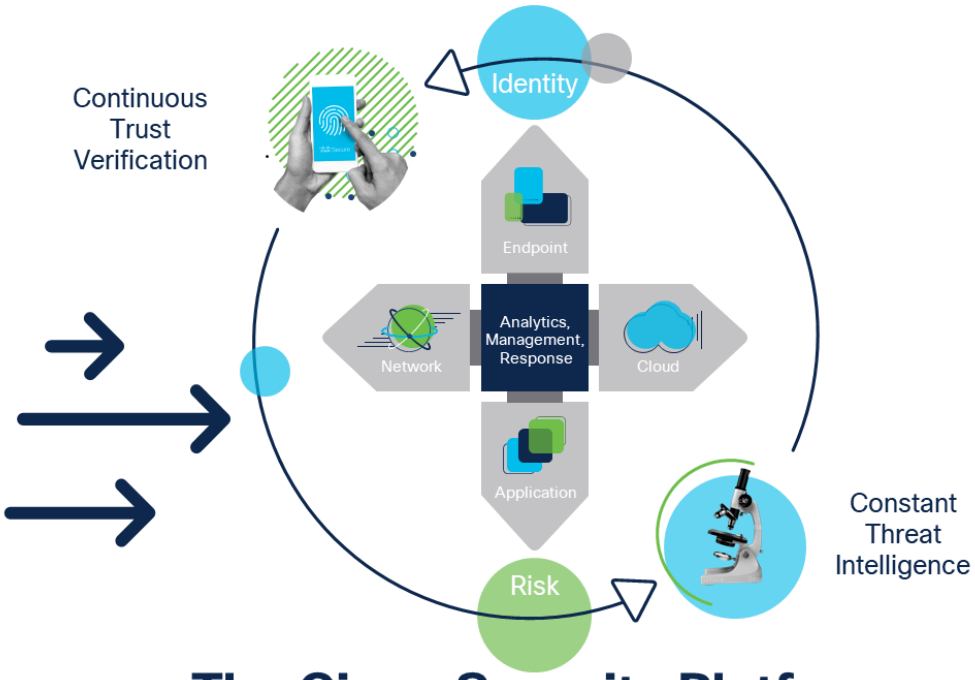
- Unifying visibility across all parts of your infrastructure—regardless of which vendor's products you have—to enable better decision making based on comprehensive threat detection, meaningful security analytics, and network security policy management
- Reducing complexity by integrating security products with out-of-the-box interoperability
- Automating security workflows like threat investigation, hunting, and remediation to strengthen operational efficiency and precision, lowering operational costs
- Accelerating time to value to give you real benefits in 15 minutes
- Changing how security teams interact with products to solve problems
- Emerging organically from your products and tying them together to a virtuous cycle of increased value from a central location
- Following you to maintain contextual awareness wherever you are in your threat investigation
- Accelerating responsiveness across the security lifecycle with lower overhead to better support evolving business and technology needs while staying ahead of an ever-changing threat landscape
- Sharing context to strengthen collaboration across security teams and workflows, including network security and policy harmonization

This list is by no means exhaustive – these callouts are just some of the ways that integrated, portfolio-based platforms provide value to businesses. However, there is one more important capability to call out: integrated, portfolio-based platforms help businesses address their talent shortage by enabling new levels of collaboration between security teams and simplifying security across the data center, network, cloud, internet, email, and endpoints.

Businesses have many security needs:

- Unlimited devices
- Transition to the cloud
- Distributed workforces
- Digital transformation
- *Any future needs*

They need a **robust platform** to integrate their entire security infrastructure.



The Cisco Security Platform

Breaking down siloes between SecOps, ITOps, and NetOps

For the CISO juggling business and security risks – amidst new regulations, rising board mandates, changing budgets, and growing emphasis on risk management – it's imperative to empower teams to move fast. The right platform makes it possible for:

- SecOps to quickly gather context from across the entire environment, scope the attack, and find the root cause in seconds or minutes, as well enable automation – so if a threat is detected in Mumbai, a worker in Milan and a datacenter in Montreal are protected almost instantly.
- ITOps to streamline and accelerate troubleshooting through collaborative workflows with SecOps and NetOps – so detecting and blocking unapproved apps can be done in minutes, not hours.
- NetOps to manage policies across thousands of network security appliances and virtual control points from one cloud-based location – so achieving consistent security is as simple as a few clicks.

By empowering NetOps and ITOps to become an extension of SecOps, the platform helps erase the boundaries that have historically existed among these teams. The collaborative workflows and shared context eliminate bottlenecks that these teams create for each other (when siloed) and improve productivity and outcomes for everyone.

Simplifying Security Visibility and Creating Collaborative Workflows

The security talent gap is affecting many organizations. In a recent ESG/ISACA survey[7]:

- 74% of cybersecurity professionals said the talent shortage has impacted their organization
  - 66% of these respondents said they increased the workload on existing staff
- Nearly 50% said the talent shortage inhibited their business's ability to fully learn or use the security technologies they had in place

One solution is to improve the productivity of teams by adopting a platform that enables more collaborative workflows, unifies visibility, and shares context across SecOps, ITOps, and NetOps.

For example, let's look at a typical workflow for an IT help desk when receiving a ticket about a slow-running computer:

1. The IT desk technician connects remotely into the server and sees an app using up memory but lacks visibility to identify the root cause.
2. IT involves SecOps and NetOps to gain more context. Since those teams don't share information, they may not be able to pinpoint the exact issue quickly either.
3. After an hour or more of troubleshooting and working with SecOps and NetOps, the technician decides to reimage the slow computer.

Now imagine if ITOps could share a workflow and context with SecOps and NetOps:

1. The IT desk technician uses the security dashboard – with access to a list of all users, devices, and apps – and an automated playbook to quickly investigate the app using too much memory. They are prompted to isolate the endpoint.
2. After identifying the problem – let's say it's cryptojacking – the technician blocks the malicious app.
3. The technician accesses the computer remotely to confirm that the cryptomining app connection was terminated and then simply reconnects the endpoint to the network.

The entire sequence takes just 10 minutes instead of an hour or more, and the technician has the right information to investigate without involving SecOps and NetOps. Furthermore, disruption to the end user is minimal.

How to Evaluate your Platform Options

When weighing the pros and cons of different platform approaches, you may start by looking at the tools you already have. For example, it's reasonable to ask: if I already have a SIEM, do I really need a portfolio-based platform?

The simple answer is: it depends on your objectives and the problems you're trying to solve.

When you have to rely on multiple vendors for integrations, or manually architect your own (as is the case with SIEMs and SOARs), the task will become more complicated as security evolves over time and you need to add more solutions. If your objective is to simplify security while getting unified visibility and controls across the network, endpoints, cloud, and applications, an end-to-end platform with built-in integrations is more effective and sustainable. Plus, you can leverage your SIEM as part of this approach by contributing fewer, higher-fidelity alerts across a portfolio-based platform to your SIEM to save significant operational costs.

Implementing an end-to-end platform approach doesn't mean replacing all your best-of-breed products with one vendor's wall-to-wall portfolio. Rather, it allows you to build on what you have while positioning you for changing needs in the future.

Accelerate Threat Investigation and Remediation

When your SecOps receives an alert – for example, blocked lateral communications, and command and control (C2) attempts – does it take an analyst half a day to investigate it, trying to correlate conflicting information? Without enough visibility and context, the analyst may have to reach out to other teams to find the source of a suspicious file. It can take more than five hours and multiple communications with ITOps or email teams for the SecOps analyst to finally understand the scope of the attack, contain it, and update the impacted users. In the meantime, users' personal or corporate assets were exposed, putting them at risk, while new alerts were ignored.

This inefficiency is often caused by the sprawling number of security solutions. A majority of surveyed IT and security professionals say threat detection and response is a challenge due to multiple independent point tools (66%[8]) or because of too many manual processes (67%[9]). A platform approach solves these challenges and accelerates threat detection, investigation, and response by simplifying and automating the SecOps workflows.

In our scenario, a platform would cut the analyst's response and remediation time to less than half and give SecOps the right context without looping in other teams. The analyst would immediately isolate the endpoint as a precaution; use a unified security dashboard to see a list of all users, devices, and applications; and quickly see that the root cause is an executable file making phishing and authentication attempts. The analyst would additionally see that other users were targeted and block the file across all threat vectors without engaging additional teams. And once the initial endpoint is back to its normal state, the analyst would connect it back to the network.

The backend and frontend integration discussed earlier should be one of your top criteria when evaluating portfolio-based platforms because it's required for unified visibility and native controls. There are a few other differentiators to consider when evaluating your platform options and the portfolios they are built on:

Criteria	Look for...
Protection	Broadly and globally deployed solutions that cover every threat vector and access point
Intelligence	A large threat research team that has a broad customer base for effective threat intelligence and analytics
Integration	A platform that offers out-of-the-box integration and openness at scale
Zero Trust	A platform and portfolio that offer a comprehensive approach to Zero Trust

Additionally, consider the vendor's ecosystem of partners and third-party integrations. While the vendor's portfolio should provide a solid foundation for your platform, their partnerships, along with information exchange based on internet standards and well-documented APIs, will help you get the most out of your existing architecture.

Final Thoughts

The demands on securing the future of your organization will continue to escalate. The security industry needs to do better to take you from overwhelmed to empowered, fuel progress, and help you reduce risks.

The platform approach is not a new idea. But in the face of growing complexity, the market is evolving to a new level of native integrations across a portfolio that enables better outcomes. This new approach is well positioned to solve the security conundrum and transform security from complex to cohesive.

Cisco's Security Platform

Cisco's vision for a security platform is built from a simple idea that we mentioned earlier - security solutions should act as a team, learning from each other, listening and responding as a coordinated unit. Our platform, Cisco SecureX, connects the breadth of Cisco's integrated security portfolio and your entire security infrastructure for a consistent experience that unifies visibility, enables automation, and strengthens your security across your network, endpoints, cloud, and applications.

SecureX rapidly unlocks new potential within your security teams, regardless of their size or maturity. It does this without requiring you to rip-and-replace components of your security ecosystem or invest in new technology – SecureX is built into the Cisco Security solutions you already have. This makes it possible to do more with less. It delivers a unified view of your entire security infrastructure and reduces complexity by integrating security products together with out-of-the-box interoperability. With a consistent ribbon across the entire interface, your teams can leverage shared context that follows them wherever they go in their environment, enabling new levels of collaboration. A single sign on account with authentication makes it easy and secure for users to log in while reducing backend complexity for IT. All of this is brought together with automated workflows that increase precision and make your teams more efficient so they can focus on what matters most – threat hunting and remediation. SecureX empowers your teams with measurable, meaningful metrics and analytics to make more informed decisions and accelerate threat response times: 95% of customers report that the platform helps them quickly take action and remediate threats[10].

Isn't it time to transform security from a blocker to an enabler?

Unlock new potential in your security investments today. Start the journey with SecureX at www.cisco.com/go/securex.

Sources

[1] 2020 CISO Benchmark Study." Cisco

[2] "Bridging the Cyber-Risk Management Gap," Enterprise Strategy Group blog, July 2019

[3] "Voice of the Enterprise: Information Security Worldwide," 451 Research, 2018

[4] "Cybersecurity Talent Crunch to Create 3.5 Million Unfilled Jobs Globally by 2021," Cybersecurity Ventures, October 2019

[5] "Complexity in Cybersecurity Report," Forrester/IBM, May 2019

[6] "Worldwide Spending on Security Solutions Forecast to Reach $91 Billion in 2018, According to a New IDC Spending Guide," Marketwatch, March 2018

[7] "The Life and Times of Cybersecurity Professionals 2018," Enterprise Strategy Group/ISACA Report, April 2019

[8] "Threat Detection and Response Landscape," Enterprise Strategy Group Report, 2019

[9] "Threat Detection and Response Landscape," Enterprise Strategy Group Report, 2019

[10] "TechValidate Research on Cisco Threat Response," TechValidate, 2019