Platform Buyer’s Guide
Navigating cybersecurity platforms like a pro
Understanding security platforms

Security needs a new approach

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 endpoints, 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.

What will a platform do for you?

You need more from the security solutions you already have, not additional solutions which will just make your infrastructure more complex. 72% of organizations say the complexity of the environment is their top concern. The majority believe they could improve operational efficiency and their security teams’ productivity through simplification.

This is where a platform approach comes in. A platform turns disparate technology, processes, and people into a unified, harmonious team whose components build on rather than stifle each other. A platform connects all the security tools to unify visibility, enables automation, and strengthens security across the network, endpoints, cloud, and applications. When your tools work as a team, security is simplified.

This buyer’s guide provides an overview of 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.
There are 3 main approaches to security platforms on the market

Vendors approach platforms from different vantage points, across solutions, technologies, and integrated portfolios, each offering their own benefits and challenges.

The types of security platforms

- **Solution-based**
- **Technology-based**
- **Integrated portfolio**

![Diagram showing the types of security platforms]

**Solution-based platforms**

The first type of platform you may want to explore is solution-based, which are typically built around individual solutions (usually network, endpoint, or cloud).

- **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. NGFWs don’t mitigate threats against all vectors in a heterogenous environment that interconnects networks, devices, users, and data.

- **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. Despite the addition of advanced capabilities, however, this solution is limited to endpoint visibility and control.

- **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. 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.

**Key challenges**

- Built around siloed solutions (typically either endpoint, network, or cloud)
- Provide limited visibility and context
- Cover single or limited control points

**Questions to ask**

- What solutions/products does your platform connect with out of the box?
- How much visibility can your platform provide me into my device inventory and userbase?
- How does your solution share context across all my endpoints, devices, network, and cloud?
Another type of security platform is technology-based, including SIEMs and SOARs.

**SIEM (security information and event management):** SIEMs offer visibility and meaningful insights by collecting, aggregating, and analyzing information from different sources. SIEMs focus on threat detection and incident response but leave blind spots because the data has limited context (e.g., 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 you still need to manually log into multiple systems to gather additional data when triaging events.

**SOAR (security orchestration, automation, and response):** SOARs are similar to SIEMs in that they aggregate, correlate, and analyze alerts. SOARs go a step further by integrating threat intelligence and automating incident investigation and response workflows based on playbooks developed by the security team. The biggest benefit of SOAR technology is prioritization of security activities and automation of response actions. One aspect to consider is the lack of backend architecture integration and native control points – SOARs don’t have the capability to holistically take coordinated actions across your environment.

Both technologies were designed to solve specific problems but lack native connectivity between the backend control points and frontend workflows, so you must divert limited staff resources from pursuing security outcomes to performing labor-intensive integration. Properly integrating the technology with external identity and infrastructure systems is often complex and resource intensive, which limits adoption.

<table>
<thead>
<tr>
<th>Key challenges</th>
<th>Questions to ask</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Require complex integrations</td>
<td>• What makes your platform different from a SIEM or SOAR?</td>
</tr>
<tr>
<td>• Leave blind spots</td>
<td>• How does your platform bring together information from all my other solutions?</td>
</tr>
<tr>
<td>• Lack native controls</td>
<td>• How can I orchestrate response actions and improve my MTTR?</td>
</tr>
<tr>
<td></td>
<td>• How does your platform contextualize data in a meaningful and actionable way?</td>
</tr>
</tbody>
</table>

Your third platform option is an emergent, portfolio-based platform.

These are open platforms, so security teams can easily integrate the products they use now, as well as cutting-edge products they’d want to use in the future. They provide the most broad and consistent end-to-end coverage across all major threat vectors and enhance efficacy.

**The most effective platform** is one that natively connects to the portfolio’s products, as well as providing easy integrations with 3rd-party products, covering different control points on the backend with a unified frontend workflow. The platform morphs the data generated by the backend into a dashboard that provides a meaningful user experience. This eliminates any work you’d typically do every time the vendor makes changes to the portfolio or you want to add 3rd-party solutions. Portfolio-based platforms do the work for you by enabling you to easily plug in your existing investments, reducing integration costs.

<table>
<thead>
<tr>
<th>Key benefits</th>
<th>Questions to ask</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Natively integrate the backend and front end</td>
<td>• How will your platform help my teams collaborate?</td>
</tr>
<tr>
<td>• Provide visibility across all control points</td>
<td>• How easily will your platform integrate with tools in my environment?</td>
</tr>
<tr>
<td>• Streamline workflows</td>
<td>• How will your platform strengthen my security?</td>
</tr>
<tr>
<td></td>
<td>• How will your platform simplify my security?</td>
</tr>
</tbody>
</table>
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. Let’s dive into your objectives and what to look for in an integrated platform approach.

Are these your objectives?

Then you might want to look for a more integrated approach to security.

- Simplify user experience
- Accelerate threat investigation and remediation
- Unify visibility across all control points
- Increase efficiency
- Increase collaboration between teams
- Mature security

What to look for in an integrated platform approach

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Look for...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection</td>
<td>Solutions that are broadly and globally deployed to cover every threat vector and access point</td>
</tr>
<tr>
<td>Intelligence</td>
<td>A large threat research team that has a broad customer base for effective threat intelligence and analytics</td>
</tr>
<tr>
<td>Integration</td>
<td>A platform that offers turnkey integration and openness at scale, allowing for unified visibility and control across backend and frontend</td>
</tr>
<tr>
<td>Transformation</td>
<td>A platform that delivers security transformation alongside XDR, like Secure Access Service Edge (SASE) and Zero Trust</td>
</tr>
</tbody>
</table>

This is a more sustainable platform approach that:

- Provides a full lifecycle dashboard for unified visibility and control across all your security solutions from one central location.
- Streamlines workflows with automated responses and coordinated actions to investigate and respond to threats more efficiently.
- Builds a unified toolset that extends across your ITOps, SecOps, and NetOps.
Cisco Secure

The Cisco Secure portfolio already has a built-in platform, SecureX

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, is a cloud-native, built-in platform experience within our portfolio and connected to your infrastructure. Every Cisco Secure customer is entitled to SecureX. It is integrated and open for simplicity, unified in one location for visibility, and maximizes operational efficiency to secure your network, endpoints, cloud, and applications.

Integrated and open for simplicity
Unified in one location for visibility
Maximized operational efficiency

Simplicity, visibility, and efficiency translate into unlocking value to:

- Reduce the dwell time of threats involved with countering attacks and staying compliant.
- Enable faster decisions with less overhead and better precision with less error.
- Deliver time savings and better collaboration by automating security across SecOps, ITOps, and NetOps teams.
- Realize more desired outcomes with measured, meaningful metrics.
- Speed time-to-value and reduce costs as you invest in more Cisco Secure products.
- Consolidate information from multiple device managers, endpoint detection and response tools, and other endpoint security products and then bring the details they provide into a unified view within SecureX.
- SecureX unifies data, analytics and automation across NDR, EDR, and beyond, to offer a simpler and broader approach to XDR.

To learn more about SecureX, go to cisco.com/go/SecureX