5 Questions to Ask Your Security Platform Vendor

Security platforms are evolving in response to customers' need to consolidate their vendor landscape and simplify security.

The following are important questions to ask when you're evaluating your options.

1. How is your platform different from a SIEM or SOAR?

Many vendors are calling their native SIEMs or SOARs "platforms" because they know the need for integration is so huge.

The main purpose of SIEMs and SOARs is to cut down on the number of alerts so response is more efficient. While they can automate incident investigation and response workflows, they don't enable you to take holistic, coordinated actions across your environment.

Even next-gen SIEMs and SOARs remain complex and tough to integrate. Without native connectivity between the backend control points and frontend workflows, you must divert limited staff resources to labor-intensive integration work.

Consider a vendor that offers a more sustainable platform approach that:

- Provides a full lifecycle dashboard — unifying visibility and control across all your security solutions from one central location.
- Streamlines workflows — enabling automated responses and coordinated actions to investigate and respond to threats more efficiently.
- Unifies workflows — enabling NetOps and ITOps to serve as an extension of SecOps, improving each team's productivity.

2. To which control points does your platform natively connect?

Your security solutions should work as a team, delivering consistent visibility and control across your entire environment.

A platform should provide coverage for all major threat vectors and natively connect controls across the network, endpoints, cloud, and applications, giving you one unified view.

This unified view enables teams to respond to threats from multiple angles and understand the full lifecycle of alerts, regardless of where they originate.

3. How many of my existing security components can connect to your platform?

There are incremental advantages to using multiple solutions from a portfolio-based platform vendor; however, wall-to-wall coverage isn't a realistic goal or expectation. You need to be able to leverage your current investments and easily integrate new solutions in the future.

Ask your vendor how they prioritize working with third-party technologies; do they use partnerships, out-of-the-box integrations, standards-based information exchange, or open APIs?

Their platform should be:

- SIEM/SOAR-agnostic — so you can connect the platform to any SIEM or SOAR one time to send fewer, higher-fidelity alerts from multiple control points.
- Cloud-agnostic — so you can keep network security policies consistent, whether you're using AWS, Azure, Google Cloud Platform, or on-prem control points.
- Infrastructure-agnostic — so you can connect your existing best-of-breed solutions to the platform.

4. How will your platform increase my efficiency?

When your teams get buried under repetitive, manual tasks, efficiency goes down and the probability of errors goes up. 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.

Find out if the platform can apply analytics to identify behavior anomalies across on-prem and cloud network traffic — even in encrypted flows. It should be able to do this while enforcing policies and automatically adapting network and application access for compromised endpoints.

At the same time, your automation should be nuanced enough to not get in the way of productivity — while a compromised endpoint should automatically have its access blocked, the individual user should still have access on a healthy device.

5. How will I know your platform is improving my security?

The right platform won't just help you improve your security across users, applications, and devices – it will help you measure and prove success. Does the vendor provide a unified, easy-to-consume dashboard with insights into how well your security program is mitigating risks?

Ask the vendor how easily the platform can create reports or show live views that measure how your security maturity is changing. If one of your objectives is to achieve a continuous improvement cycle, the platform should also provide metrics that map policy changes to the meaningfulness of alerts.

Unlock new potential in your investments today

Start the journey with SecureX

cisco.com/go/securex