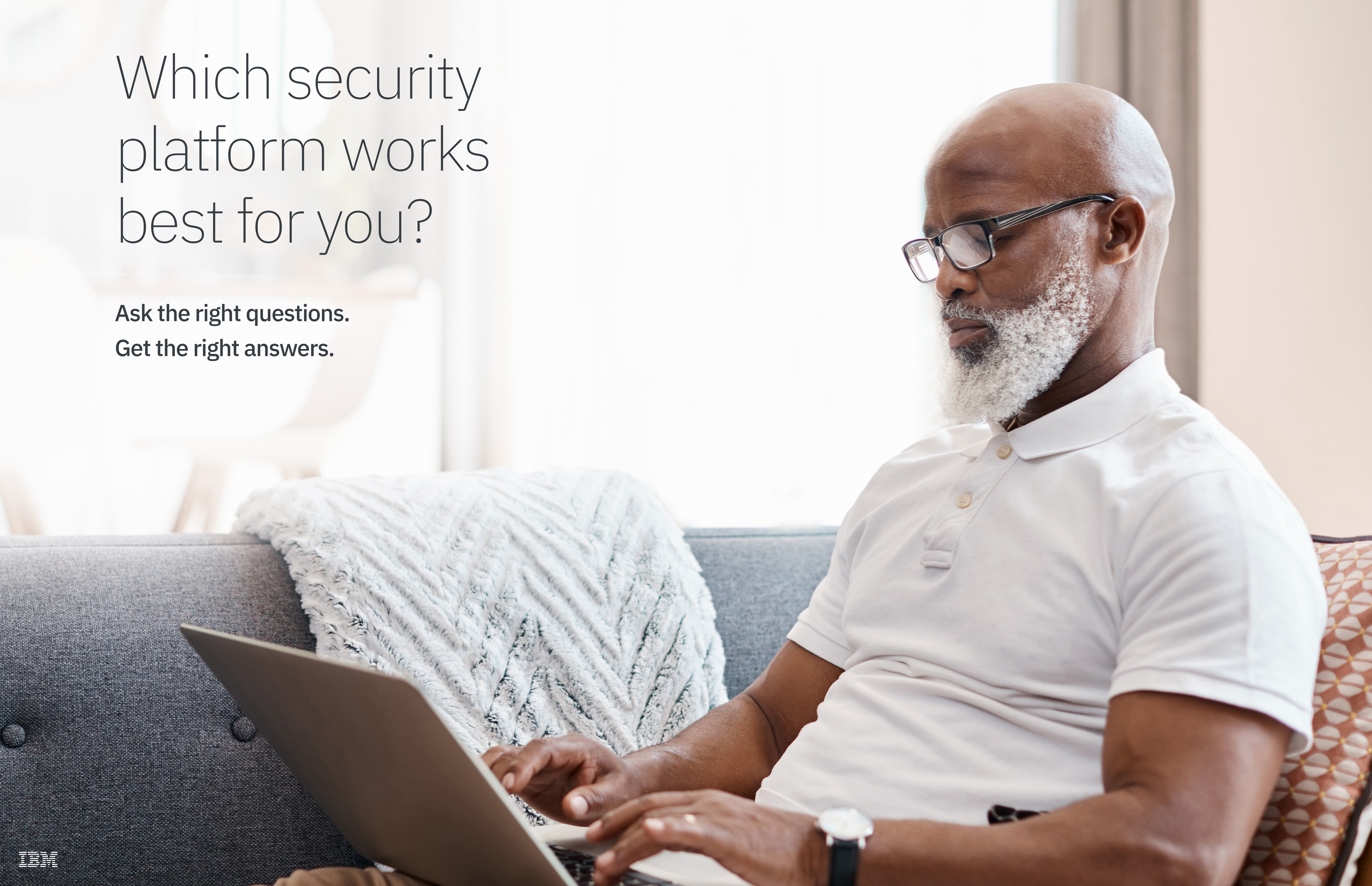
Which security platform works best for you?

Ask the right questions.
Get the right answers.



Choosing the right security platform

Finding a security platform for your organization can be a difficult task. In cybersecurity, the term "platform" has become overused, making it difficult to cut through the noise and understand which factors matter in choosing the best option for your business. The platform you choose today can act as a foundation for your security maturity posture for the next few years and should be chosen carefully.

Enterprise security teams are challenged by too much data, too many tools, and not enough resources. It's time for a different way to unify security data, tools, and teams, and there's a strong need to tie everything together in one place—the benefit of an integrated security platform.

What to look for in a security platform

To find a holistic, integrated cybersecurity platform that can be effective now and into the future, you should take into account:

- Considerations around moving your data
- Options for deployment
- Connections you'll need to other tools
- Openness and adaptability of the platform
- Orchestration and automation capabilities
- Threat intelligence integration
- Connecting SOC teams
- Risk management and dashboarding capabilities
- Services support

Consider the following key questions to help understand your options for choosing a security platform and determine which one may be best for your organization.

1. Do you have to move your data to get value?

Many security platforms require moving all of your data onto that platform to access it. While putting all your data in one place seems like a good idea, it can be complex and expensive. Furthermore, it can mean addressing important privacy and data residency issues.

From a cost and complexity perspective, it can be beneficial for a platform to connect to your data where it's already located, without the need to move it. This approach can complement your existing tools and help you maximize investments you've already made while still providing a centralized view and access to data already spread across various tools.

2. Can you deploy the platform on premises, in a public cloud, or a private cloud?

Many security platforms are available only as cloud-based software as a service (SaaS) solutions. While it may be the right approach for you, many organizations aren't ready for a cloud-only solution and may need the flexibility of a hybrid, multicloud architecture. With many organizations' workloads still on premises, a security platform offering the flexibly to run on premises, in a public cloud or a private cloud, or as a SaaS solution can be valuable. Rather than limiting yourself to one deployment option, look for a flexible architecture that can be deployed in hybrid, multicloud environments.

3. Does the platform support connections and integrations to third-party tools?

With the range of security tools organizations use today, it's unlikely that all of them will be from one vendor. Some security platforms are built to only integrate a specific vendor's tools and could be limiting. If you use security tools from many different vendors, look for a platform that supports open connections to a range of security and IT tools. Look for an option that includes:

- A large ecosystem of partners
- An open software development kit (SDK)
- Support services for adding your own custom connections

This approach can help determine whether the platform will work with your tools and help reduce the need to rip and replace existing tools.

4. Does the platform adapt as your security program changes?

When choosing a platform, it can be important to consider one that's open and flexible enough to support your security program as it changes. Consider whether it offers:

- Open standards
- Open source technology
- Open connections

An open platform connects to third-party tools and supports custom connections and development. This approach can help reduce vendor lock-in and promote interoperability with multiple security and IT tools.

5. Can it provide core orchestration, automation and response capabilities?

Security orchestration, automation and response (SOAR) solutions are often positioned as platforms themselves. But SOAR capabilities can be stronger when built into your main security platform, rather than offered separately. Look for a security platform that includes SOAR as a core function to help increase the efficiency of your security team across a range of workflows and security use cases. While SOAR has traditionally been focused on the incident response side of threat management, when it's built into a more comprehensive platform it can also provide benefits for other areas, like data security, and help bring together security operations center (SOC) and data security teams.

6. How does it support integrating threat intelligence?

Security analysts often use a variety of threat feeds and different products to comb through threat intelligence and inform their research and decisions. Consider whether the platform provides threat intelligence reports and how the intelligence is integrated with other capabilities as well as what threat intelligence vendors are supported. Integrating threat intelligence into your security platform can reduce a security analyst's workload and allow for more prompt and informed decisions.

7. Does the platform help connect disparate teams?

Many security platforms are geared primarily toward security operations and the security operations center (SOC). However, SOC teams often need to work with others, such as data security teams, to investigate and resolve incidents. When the platform can make it easier for these teams to collaborate and share information, it can increase their efficiency and decrease the time it takes to respond to a threat or breach. When evaluating security platforms, look for one that goes beyond the traditional SOC and can connect your organization's security environment and teams more holistically.

8. Does the platform provide risk management and dashboarding capabilities?

With dozens of security tools, security leaders can find themselves overwhelmed trying to process the disparate, subjective definitions of risk generated by their tools as well as prioritizing remediation. For security executives seeking to quickly and efficiently minimize their business's risk profile, they need a solution that normalizes and contextualizes risk data, facilitates prioritization and helps them determine the best course of action to reduce overall risk. Your security platform should be able to provide native risk management capabilities to collect and contextualize risk data from across your security environment.

9. Does the vendor offer services in addition to software?

While a security platform is a powerful tool, you may find that you need additional services specific to your organization or security program, whether that's upfront advisory or consulting around your security strategy, hybrid models to support where you need it most, or fully managed security services. Choosing a platform vendor that also offers additional security services can make it easier to add those services and integrate them with your security platform.

Understand your core security platform needs and wants

Platform approaches can be a way to streamline security data, tools, and teams. Yet with many different options available, it's important to understand the answers to these key questions when considering what security platform is right for your organization:

- Can you leave your data where it is?
- Can your deployment support hybrid, multicloud architectures?
- Will you want open integrations and connections to other security or IT tools?
- Can you easily adapt and adjust as your security program changes?
- Would you benefit from security orchestration, automation and response capabilities?
- How does it incorporate threat intelligence?
- How does it connect different security teams?
- Does it provide risk management and dashboarding capabilities?
- Can your vendor offer security services in addition to software?

IBM Cloud Pak for Security: Modernize your security with an open, multicloud platform

IBM Cloud Pak® for Security is an open, integrated security platform that provides deep insights into risks and threats across multiple environments now and in the future. You can search for threats, orchestrate actions and automate responses without migrating your data. The platform connects SOC and data security teams through case management, orchestration and automation, bringing threat management and data security teams together for greater visibility and faster remediation.

Through open standards and IBM innovations, IBM Cloud Pak for Security enables you to access IBM and third-party tools to search for threat indicators across cloud or on-premises locations. IBM has contributed open source technology used in IBM Cloud Pak for Security and forged relationships with dozens of companies through the OASIS Open Cybersecurity Alliance to promote interoperability and help reduce vendor lock-in.

IBM Cloud Pak for Security is comprised of containerized software pre-integrated with the Red Hat® OpenShift® enterprise application platform. This integration enables it to run on premises and in private or public clouds, giving organizations the flexibility to deploy where they choose.

Learn more about IBM Cloud Pak for Security

Visit the IBM Cloud Pak for Security web page to discover how you can uncover hidden threats and make informed risk-based decisions to respond faster to security incidents.

And, if you need additional talent and skills to support your team, tap into IBM Security services to help build a solid strategy and transform your security program.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
January 2021

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

It is the user's responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs. THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.