

Tech Data Market Moment / IBM Cloud Pak for Security

Integrate security tools to gain insights into threats across hybrid multicloud environments



Products featured

IBM Cloud Pak® for Security

Elevator pitch

As you move your business to the cloud, security data is frequently spread across different tools, clouds and on-premises IT environments. This process creates gaps that allow threats to be missed, resulting in the need for costly, complex integrations. In fact, more than half of the security teams surveyed stated they struggle with integration between security analytics tools and cloud infrastructure¹. IBM Cloud Pak for Security provides a platform to more quickly integrate your existing security tools and generate deeper insights into threats across hybrid multicloud environments. Using its infrastructure-independent common operating environment that runs virtually anywhere, you can quickly search for threats, orchestrate actions and automate responses—all while leaving your data where it is.

Customers

What are customers struggling with?

- Lack of visibility: security data in silos, spread across hybrid multicloud locations
- Too many manual processes
- Separate teams or use of different tools for on premises and cloud security
- Cost and complexity of consolidating data for better visibility
- Cost and complexity of managing point-to-point integrations
- Lack of resources and difficulty filling jobs

Who's interested and why?

- Small companies because they are more nimble and likely to appreciate the flexibility to run in any cloud environment
- Special attention to nascent security organizations to promote IBM Cloud Pak for Security as the connecting thread for their next-gen security programs
- Large organizations with a large security program and multiple stakeholders who struggle to manage their large hybrid multicloud environments
- Organizations interested in building and optimizing their threat detection and threat management programs
- Organizations that are standardizing their cloud deployments on Red Hat® OpenShift®, or at a minimum, on Kubernetes
- Customers using other IBM Cloud Pak solutions

Typical sponsors

- Chief information security officers (CISOs)
- Security operations center (SOC) directors
- Heads of security

Typical influencers

- Security analysts
- Incident responders

Partner targets

- IBM Business Partners that sell IBM® QRadar®, IBM Resilient® or other competitive SOC data security solutions for a cross-sell or upsell opportunity
- Red Hat Partners for customers with cloud deployments on OpenShift, or at a minimum, on Kubernetes



IBM solution

How we can help

IBM Cloud Pak for Security is a way to change the game in customer security. It drives wins, delights our customers, helps us make our targets and drives our strategic offerings. It helps us have conversations about security in multicloud environments—something customers are deeply concerned about. **IBM Cloud Pak for Security is connected security built for a hybrid multicloud world. It enables customers to connect data, connect workflows and connect anywhere—and unifies all the security functions vital to any enterprise.**

Value of our solution

- Gain security insights without moving data.
- Take action faster with orchestration and automation.
- Deploy on premises, in the public cloud or private cloud.
- Maximize existing investments.
- Deploy to meet needs with a flexible consumption model.

Key differentiators, competitive information

IBM Cloud Pak for Security is an integrated platform tying together threat intelligence; federated search; and security orchestration, automation and response (SOAR) capabilities.

- SOC analysts can detect, investigate and respond to threats, all in a single unified interface and without the need to move any data for point products and cloud environments.
- IBM Cloud Pak for Security is designed to install easily in virtually any environment on premises, on the private cloud or public cloud.
- The solution is built on open technologies that create a more flexible foundation to reduce vendor lock-in.
- New functionality provides a competitive advantage to any deal.

Marketplace highlights

- Measure and improve SOC effectiveness.
- Streamline security operations management.
- Establish standard incident response processes.
- Proactively manage incident response.
- Empower your security team.

Opportunity identification

Prescriptive actions

- Familiarize yourself with assets such as customer profiling, presentation decks, demos, and enablement tools and materials.
- Help ensure you are educated and enabled on IBM Cloud Pak for Security value selling.
- A flexible consumption model makes the solution attractive to a diverse set of customers to deploy as needed.
- Sales and technical badges with associated learning journeys are available.
- Identify your target customers and prospects and their pain points.
- Help progress the sale with demos and proofs of concepts.


Starting questions

- Are you struggling with multiple security products, such as endpoints or security information and event management (SIEM), from multiple vendors?
- Are you struggling to gain visibility across your security tooling?
- Do you have multiple instances of a single security tool and need visibility across those instances?
- Have you encountered challenges with managing integrations between products?
- Are you worried about missing threats in your environment?
- Have you encountered challenges with data migration or consolidation?
- What systems do you use for incident response today, and how are they working for you?

Average deal size

- Average deal size is USD 220,000. Software-to-services ratio is 1:2. Average sell cycle is 6 months.

Key assets and resources

IBM Cloud Pak
for sales
Seismic 

IBM Cloud Pak
for technical sales
Seismic 