IBM Cloud Pak for Security

Modernize your security with an open, multicloud platform

As organizations move their business to the cloud, security data is frequently spread across different tools, clouds and on-premise IT environments. This creates gaps that allow threats to be missed—that often are solved by undertaking costly complex integrations.

IBM Cloud Pak® for Security provides a platform to help integrate existing security tools quickly, in order to generate deeper insights into threats and risks across hybrid, multicloud environments. Using an infrastructure-independent common operating environment that runs anywhere, you are able to quickly search for threats, orchestrate actions and automate responses—all while leaving your data where it is.

- **Uncover hidden threats faster** by connecting and searching all data sources for a more complete view of your environment
- **Reduce the cost of security data** by connecting to your existing security tools through open standards, without moving the data
- **Reduce response time** by automating manual and repetitive tasks and driving investigations via third-party integrations
- **Run anywhere - on premise, public or private cloud** - with containerized software pre-integrated with Red Hat OpenShift
- **Increase security visibility** through a solution that connects to an open ecosystem of IBM and third-party data connectors
- **Expand your team's capabilities** with additional skills from on-demand consulting to custom development

Highlights

- Gain security insights without moving your data
- Respond faster to security incidents with AI and automation
- Modernize your architecture to run anywhere

IBM Cloud Pak for Security platform

IBM Cloud Pak for Security is an integrated platform that brings together tools, teams and data with a unified experience and seamless workflows. Different security functions, like the security operations center (SOC) and data security, are traditionally separate from each other, which decreases visibility and collaboration across the enterprise. IBM Cloud Pak for Security connects these previously siloed teams, enabling SOC and data security analysts to share incidents and artifacts through central platform capabilities.

Security leaders and analysts can gain visibility into their security operations with pre-built and custom dashboards that display high-level and drill-down metrics and analytics across the platform. They can easily build dashboards to include information across threat intelligence, security information and event management (SIEM) monitoring, case management, security orchestration, automation and response (SOAR) metrics, user behavior analytics, and risk management.

With open source technology and open standards built into IBM Cloud Pak for Security, the platform can connect to a range of IBM and third-party security tools and cloud solutions. By co-founding and committing open source technology to the OASIS Open Cybersecurity Alliance, IBM has forged partnerships with dozens of companies; through co-developed open source technologies, these partnerships promote interoperability and help reduce vendor lock-in across the security community.

How it works

The IBM Cloud Pak for Security platform is comprised of modular products and solutions for security teams to leverage. Products and solutions are tied together with a unified user experience and central case management to provide analysts with seamless integrated workflows across the platform. In addition, flexible licensing and non-volume-based pricing lets organizations choose the capabilities they need and easily add more, as their needs change.

IBM Cloud Pak for Security products and solutions

IBM Security Threat Intelligence Insights

Threat Intelligence Insights offers detailed, actionable threat intelligence that helps security analysts identify and prioritize the threats most relevant to their organization–based on their organizational profile. They can drive insights with X-Force Threat Intelligence from security investigations around the world and scan all connected data sources to see if a threat is affecting their environment. Once a threat is detected, a case is automatically created within the platform, and analysts can seamlessly investigate further across multiple siloed sources and remediate cyber threats by leveraging the integrated workflows of IBM Cloud Pak for Security.

IBM Security Data Explorer

Data Explorer enables analysts to perform federated investigations across IBM and third-party data sources. They can connect insights from security tools, such as security information and event management (SIEM), endpoint detection and response (EDR), and data stored in data lakes, such as Elastic. Additionally, analysts can gain insights from multicloud environments that SIEM tools like QRadar and Splunk are monitoring. Data Explorer helps significantly reduce time to investigate by enabling analysts to query multiple data sources using a simple query builder and one workflow. This allows SOC) teams to do more, faster and empowers analysts to search for indicators of compromise (IOCs) and threats across all data sources.

IBM Security SOAR

SOAR empowers security analysts by automating common security operations and incident response (IR) processes, guiding them through the necessary steps to resolve complex cases. They can access important security information quickly with the relevant incident context, enabling accurate decision making and decisive action. It leverages automation, 3rd-party integrations and dynamic case management to increase the

productivity of security analysts and improve the effectiveness of deployed technologies—alleviating the cybersecurity skills gap and alert fatigue.

IBM Security QRadar

QRadar unifies visibility with 500+ validated integrations for security and IT ecosystems with out-of-the-box support for hundreds of security use cases including insider threat, advanced threat, cloud security and more. SOC analysts can gain centralized insights across users, endpoints, clouds, applications and networks. QRadar's analytics engine uses a range of analytics to identify abnormal behavior and anomalous activity that indicate known and unknown threats. QRadar's analytics and models have been tuned and embedded with security best practices from our years protecting Fortune 100 companies.

IBM Security Guardium Insights

Guardium Insights is a data security hub built to simplify an organization's data architecture by delivering a unified view across data sources, storing compliance and audit logs for the long-term, and employing advanced analytics and machine learning (ML) to uncover hidden threats and anomalous behavior. Security professionals can derive key risk insights across their on-premises and cloud databases within seconds from years' worth of historical security data. Guardium Insights builds on the Cloud Pak for Security foundation to enable data security professionals to collaborate with SOC analysts and others within the IT and Security organization to uncover and act on data security events.

IBM Security Risk Manager

Risk Manager provides security leaders with visibility into their organizations' security risk posture by contextualizing risk data from across the IT environment and correlating insights across risk vectors and asset criticality. Security professionals can work across data security, SIEM, and identity to evaluate risk from multiple source products. They can quickly understand their risk posture from a business-consumable dashboard and

work with the broader security team and incident responders by creating a case and benefiting from the SOAR capabilities on Cloud Pak for Security.

Why IBM?

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, provides security solutions to help organizations drive security into the fabric of their business so they can thrive in the face of uncertainty.

IBM operates one of the broadest and deepest security research, development and delivery organizations. Monitoring more than one trillion events per month in more than 130 countries, IBM holds over 3,000 security patents. To learn more, visit ibm.com/security.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice and represent goals and objectives only.

For more information

To learn more about IBM Cloud Pak for Security, please contact your IBM representative or IBM Business Partner, or visit the following website: https://www.ibm.com/products/cloud-pak-for-security