Announcements

IBM Launches Open Technology to Speed Response to Cyber Threats Across Clouds

Industry-first capability to hunt threats across security tools and clouds without moving data

ARMONK, N.Y., Nov. 20, 2019 /PRNewswire/ -- IBM (NYSE: IBM) today announced Cloud Pak for Security, featuring industry-first innovations to connect with any security tool, cloud or on-premise system, without moving data from its original source. Available today, the platform includes open-source technology for hunting threats, automation capabilities to help speed response to cyberattacks, and the ability to run in any environment.

Cloud Pak for Security is the first platform to leverage new open-source technology pioneered by IBM, which can search and translate security data from a variety of sources, bringing together critical security insights from across a company's multicloud IT environment. The platform is extensible, so that additional tools and applications can be added over time.

As businesses move further into cloud maturity, applications and data are frequently spread across multiple private and public clouds and on-premise resources. Attempts to protect this fragmented IT environment often require security teams to undertake complex integrations and continuously switch between different screens and point products. In a recent SANS Institute report, sponsored by IBM Security, more than half of security teams surveyed said they struggle to integrate data with disparate security and analytic tools and combine that data across their cloud environments to spot advanced threats.[1]

Three initial capabilities of Cloud Pak for Security include:

- **Run anywhere. Connect security openly** – IBM Cloud Pak for Security installs easily in any environment – on premises, private cloud or public cloud. It is comprised of containerized software pre-integrated with the Red Hat OpenShift, the industry's most comprehensive enterprise Kubernetes platform. Through the OASIS Open Cybersecurity Alliance, IBM has also forged partnerships with dozens of companies to promote interoperability and help reduce vendor lock-in across the security community through co-developed open source technologies.
- **Gain security insights without moving data** – Transferring data in order to analyze it creates additional complexity. IBM Cloud Pak for Security can connect data sources to uncover hidden threats and help make more-informed risk-based decisions, while leaving the data where it resides. Through the use of open standards and IBM innovations, clients can access IBM and third-party tools to search for threat indicators across any cloud or on-premise location. Via the Cloud Pak for Security's Data

Explorer application, security analysts can streamline their hunt for threats across security tools and clouds. Without this capability, security teams would have to manually search for the same threat indicators (such as a malware signature or malicious IP address) within each individual environment. Cloud Pak for Security is the first tool that allows this type of search without needing to move that data into the platform for analysis.

- **Respond to security incidents faster with automation** – IBM Cloud Pak for Security connects security workflows with a unified interface to help teams respond faster to security incidents. According to IBM Security estimates, security teams have to manage an average of 200,000 potential security events per day, and coordinate responses across dozens of tools. IBM Cloud Pak for Security allows clients to orchestrate and automate their security response so they can prioritize their team's time. The platform allows companies to orchestrate their response to hundreds of common security scenarios, guiding users through the process and providing quick access to security data and tools. IBM's Security Orchestration, Automation and Response capability integrates with Red Hat Ansible for additional automation playbooks. By formalizing security processes and activities across the enterprise, companies can react quickly and efficiently, while arming themselves with information to help address regulatory requirements.

"As businesses move mission-critical workloads to hybrid multicloud environments, security data is spread across different tools, clouds and IT infrastructure. This can create gaps that allow threats to be missed, leading security teams to build and maintain costly, complex integrations and manual response plans," said ***Mary O'Brien, General Manager, IBM Security****. "With Cloud Pak for Security, we're helping to lay the foundation for a more connected security ecosystem designed for the hybrid, multicloud world."*

IBM collaborated with dozens of clients and service providers during the design process, developing a solution to address critical interoperability challenges that permeate the security industry. The Cloud Pak for Security includes connectors for pre-built integrations with popular security tools from IBM, Carbon Black, Tenable, Elastic, BigFix, Splunk, as well as public cloud providers including IBM Cloud, Amazon Web Services[2] and Microsoft Azure[2]. The solution is built on open standards so that it can connect additional security tools and data from across a company's infrastructure.

"Organizations have rapidly adopted new security technologies to keep up with the latest threats, but are now juggling dozens of disconnected tools which don't always work well together," said ***Jon Oltsik, Senior Principal Analyst, Enterprise Strategy Group****. "The industry needs to solve this issue for customers by shifting to more open technologies and unified platforms that can serve as the connective glue between security point tools. IBM's approach aligns with this requirement and has the potential to bring together every layer of the security stack within a single, simplified interface."*

To further accelerate industry migration toward open security, IBM is also spearheading open-source projects

to make security tools work together natively across the security ecosystem. As a founding member of the Open Cybersecurity Alliance, IBM and more than 20 other organizations are working together on open standards and open source technologies to help enable product interoperability and reduce vendor lock-in across the security community.

Designed for the Hybrid, Multicloud World

Seventy-six percent of organizations surveyed report they are already using between two and 15 hybrid clouds, and 98 percent forecast they will be using multiple hybrid clouds within three years.[3] IBM's Cloud Pak for Security is built on open source technologies that support companies' cloud environments - including Red Hat OpenShift.

Creating Cloud Pak for Security on these open, flexible building blocks allows for easy "containerized" deployment across any cloud or on premise-environment. As companies continue adding new cloud deployments and migrations, Cloud Pak for Security can adapt and scale to these new environments – allowing clients to bring their sensitive and mission-critical workloads into the cloud while maintaining visibility and control from within a centralized security platform.

Cloud Pak for Security also provides a model to help Managed Security Services Providers (MSSP) efficiently operate at scale, connect security silos and streamline their security processes. Organizations can also hire IBM Security for a wide range of additional services, such as on-demand consulting, custom development and incident response.

IBM Cloud Pak for Security is now generally available worldwide – visit https://www.ibm.com/products/cloud-pak-for-security for more information.

About IBM Security

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, enables organizations to effectively manage risk and defend against emerging threats. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 70 billion security events per day in more than 130 countries, and has been granted more than 10,000 security patents worldwide. For more information, please check www.ibm.com/security, follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog.

Media Contact:

Cassy Lalan

IBM Security Communications

319-230-2232

cllalan@us.ibm.com

[1] SANS Institute survey, Effectively Addressing Advanced Threats, 2019.

[2] Available in Q4 2019

[3] IBM Institute for Business Value, 2018

SOURCE IBM