

## IBM Advances Cloud Pak for Security to Manage Threats Across Tools, Teams & Clouds

- Open platform leverages AI and automation to streamline threat management across hybrid cloud environments and disparate security tools
- Industry-first ability to connect threat management, data security and identity within a single platform
- New turnkey security services to address cybersecurity skills shortage and remote workforce

ARMONK, N.Y., Oct. 14, 2020 /[PRNewswire](#)/ -- IBM (NYSE: IBM) Security today announced new and upcoming capabilities for Cloud Pak for Security, including a first of its kind data security solution that allows companies to detect, respond to and protect against threats to their most sensitive data across hybrid cloud environments. Designed to unify previously disconnected security technologies, IBM has expanded Cloud Pak for Security to include new data sources, integrations, and services that allow security operations teams to manage the full threat lifecycle from a single console.

With these upcoming capabilities,<sup>1</sup> Cloud Pak for Security will include access to six threat intelligence feeds, 25 pre-built connections to IBM and third-party data sources, and 165 case management integrations – which are connected through advanced AI to prioritize threats, and automation playbooks to streamline response actions for security teams.

As cloud adoption and remote work have dispersed the traditional IT perimeter, security response teams can benefit from deeper insights into security across hybrid cloud environments. User behavior, identities and data security have traditionally been siloed from threat management. With the upcoming new capabilities, Cloud Pak for Security will become the first platform in the industry to connect data-level insights and user behavior analytics with threat detection, investigation and response.

Today IBM is announcing capabilities to advance the Cloud Pak for Security even further, including:

- **Coordinated Threat Response + Data Security:** IBM has developed a new industry-first approach to provide security teams with visibility into data activity, compliance and risk, without needing to leave their primary response platform. The new built-in [data security hub](#), scheduled for general availability in Q4, allows analysts to quickly gain context into where their sensitive data resides across hybrid cloud environments, as well as who has access to it, how it is used, and the best way to protect it. Bridging the disconnect between data security and threat management can reduce the timeline for responding to data breaches, which currently take more than six months to identify and contain on

average for recently surveyed organizations.<sup>2</sup>

- **Access to Industry Leading Threat Intelligence:** Cloud Pak for Security is expanding its collection of threat intelligence, helping clients detect early warning signs of active threat campaigns impacting companies around the world. In addition to IBM's X-Force Threat Intelligence Feed, the platform will provide pre-built integrations for five additional threat intelligence feeds from third-party sources, including AlienVault OTX, Cisco Threatgrid, MaxMind Geolocation, SANS Internet StormCenter and Virustotal scheduled for general availability in Q4, and additional threat feeds expected to be added in 2021.
- **Dedicated Services and Support:** IBM is launching new dedicated security services to help organizations modernize their security operations with Cloud Pak for Security, leveraging a holistic approach connecting products and services. With a wide range of flexible service options, IBM experts can help clients deploy and manage Cloud Pak for Security across any environment, including end-to-end threat management, managed security services, as well as strategy, consulting and integration support.

*"Complexity is the greatest challenge facing our industry, forcing resource-strapped security teams to manually connect the dots between disparate tools and sources of security data," said Justin Youngblood, Vice President, IBM Security. "Cloud Pak for Security is built on open, cloud native technologies from the ground up to connect any tool within the security ecosystem. With these updates, we will be the first in the industry to bring together external threat intelligence and threat management alongside data security and identity, helping organizations to modernize their security operations and create the foundation for a zero trust security strategy."*

### **Open Connections Across the Security Ecosystem**

Cloud Pak for Security leverages open technologies to create an interoperable foundation and deeper connections between the IBM and third-party tools. For instance, the platform uses [STIX-Shifter](#), an open-source library that allows security analysts to search for threat indicators across all connected data sources with a single query. Additionally, Cloud Pak for Security is built on Red Hat [OpenShift](#), providing an open, containerized foundation that can be easily deployed across on-premise, public and private cloud environments.

This open approach allows Cloud Pak for Security to be more than simply a collection of security capabilities, but rather a platform to fully integrate security processes across tools and clouds. The platform uses advanced AI, analytics and automation to streamline the full lifecycle of threat management – including native capabilities for Security Information and Event Monitoring (SIEM), Threat Intelligence, User Behavior Analytics, Data Security and Security Orchestration Automation and Response. These capabilities are delivered through a single, unified user interface that connects the entire threat management process via end-to-end workflows, from detection through response.

Through IBM Security's participation in the [Open Cybersecurity Alliance](#), the company will continue to work with the community to advance the development and adoption of open technologies to make security more interoperable.

### **Unified Product and Services Approach**

Cloud Pak for Security's open framework makes it an ideal solution for collaboration between security teams and external service providers that augment companies' security skills and expertise. Cloud Pak for Security also supports multi-tenancy, enabling service providers to leverage a single instance of the platform to serve multiple companies and sub-organizations while keeping their data isolated.

The extensive capabilities of Cloud Pak for Security can be supported by and integrated with IBM Security Services, with unified offerings that connect technologies and services. Clients can take advantage of [X-Force Threat Management](#), an ongoing, end-to-end threat management service that uses a programmatic approach to help clients mature their overall threat management strategy over time. Companies can also leverage a wide variety of [IBM Managed Security Services](#), using Cloud Pak for Security to facilitate real time collaboration and visibility between clients and service teams. Alternatively, companies can leverage IBM Security [expert consultants](#) to help them plan for, deploy and integrate the Cloud Pak for Security with their existing security investments.

To learn more about IBM Cloud Pak for Security and stay up to date regarding its latest capabilities, visit the website [here](#). You can also register for the [webinar](#) which will take place October 29, 2020 at 11:00 a.m. EDT.

### **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](http://www.ibm.com/security), follow [@IBMSecurity](#) on Twitter or visit the [IBM Security Intelligence blog](#).

*Disclaimer: Statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.*

### **Media Contact:**

Cassy Lalan

IBM Security PR

m: 319-230-2232

[cjlalan@us.ibm.com](mailto:cjlalan@us.ibm.com)

<sup>1</sup> Scheduled for general availability within Q4 2020

<sup>2</sup> 2020 Cost of a Data Breach Report, conducted by The Ponemon Institute and sponsored by IBM Security

SOURCE IBM

---