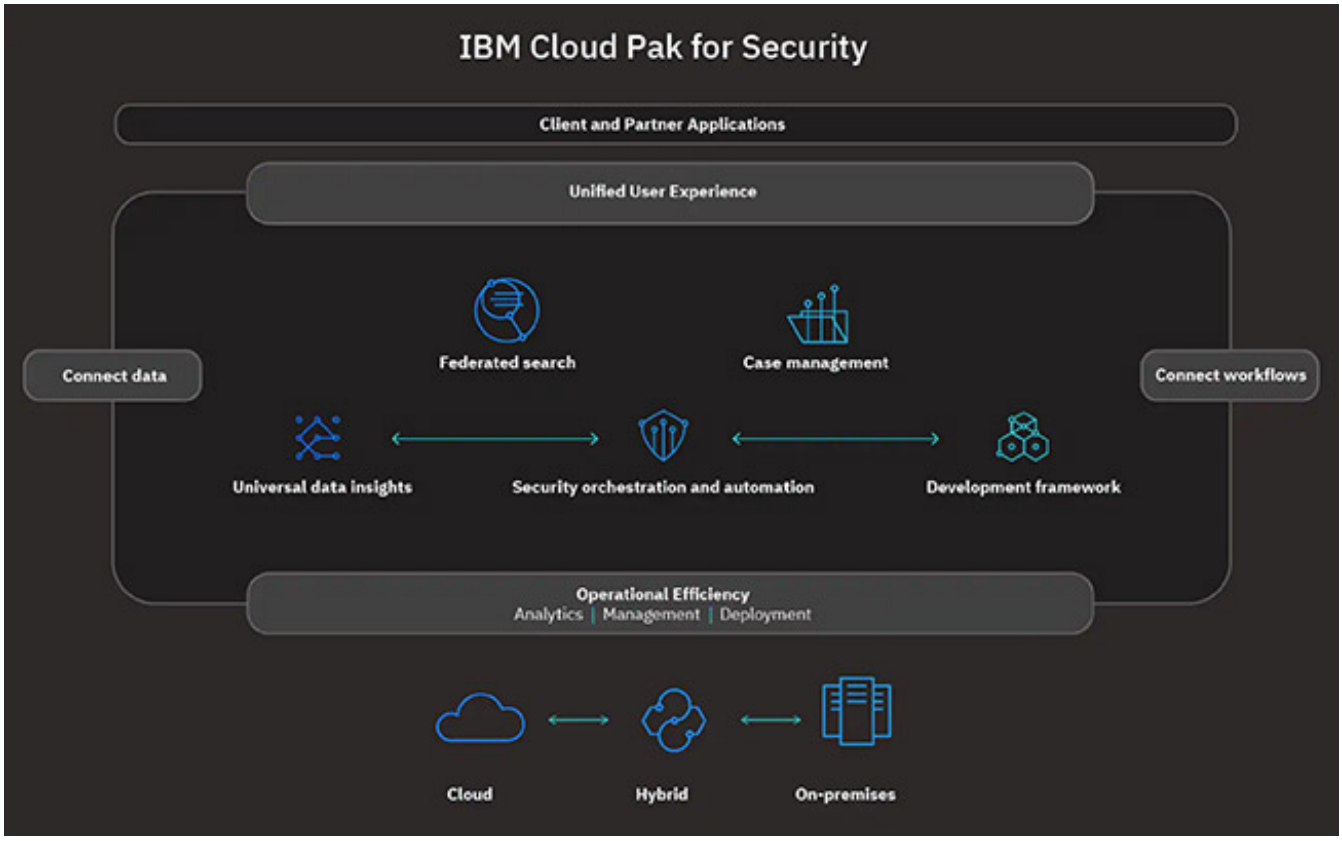
IBM announces Cloud Pak for Security-- a collection of "industry-first innovations" to connect with any security tool, cloud or on-premise system without moving data from the original source.



The platform uses open-source technologies to hunt threats, automation capabilities to speed response to attacks and the ability to run in any environment. As IBM puts it, Cloud Pak for Security can search and translate security data from a variety of sources, bringing together critical security insights from across a multicloud environment. It is also extensible, allowing the addition of tools and applications over time.

Cloud Pak for Security launches with three initial capabilities. It promises to install easily in any environment (on premises, private cloud or public cloud), and consists of containerised software pre-integrated with the Red Hat OpenShift Kubernetes platform. Partnership with the OASIS Open Security Alliance sidesteps vendor lock-in through co-developed open source technologies.

The platform connects data sources to uncover hidden threats, and helps make more informed risk-based decisions. The use of open standards allows customers to access IBM and 3rd party tools to search for threat indicators, while a Data Explorer application streamlines the hunt for threats across tools and clouds. In addition, a Security Orchestration, Automation and Response capability integrates with Red Hat Ansible to provide automation playbooks, formalising security process and activities across the enterprise.

Also included are connectors for built-in integration with security tools from Carbon Black, Tenable, Elastic, BigFix, Splunk and, of course, Big Blue itself, as well as public clouds such as the IBM Cloud, Amazon Web Services and Microsoft Azure.

Go IBM Cloud Pak for Security