KuppingerCole Report

EXECUTIVE VIEW

by Martin Kuppinger | November 2019

IBM Cloud Pak for Security

IBM Cloud Pak for Security is an innovative solution that can run in a variety of deployment models that supports security analytics and incident response for today's complex, hybrid and multi-cloud environments. It provides a consolidated view on security and threat information across a range of sources from IBM and other vendors. It supports federated search across that data, plus consolidated workflows for incident response spanning multiple systems. With these capabilities, it is a tool that can deliver significant benefits to the efficiency of every SOC.

by **Martin Kuppinger**
mk@kuppingercole.com
November 2019

Content

1 Introduction 3
2 Product Description 4
3 Strengths and Challenges 6
4 Copyright 7

Related Research

Executive View: IBM MaaS360 with Watson – 79067

Executive View: IBM Cloud Identity – 79065

Executive View: IBM Security Access Manager (ISAM) – 79066

Leadership Compass: Identity as a Service (IDaaS) – IGA – 80051

Leadership Compass: Infrastructure as a Service – Global Providers – 80035

Leadership Compass: Access Management and Federation – 71147

Architecture Blueprint: Hybrid Cloud Security - 72552

1 Introduction

Over the past years, Cybersecurity has evolved from a technical challenge for the IT Security Division of businesses to a major concern for business leaders. Cybersecurity incidents cause massive damage to organizations from small businesses to global leaders. Understanding the current status of attacks across the entire IT landscape of businesses and being able to rapidly identify and respond immediately is essential to mitigate the potential damage they can cause.

On the other hand, the evolution of IT infrastructures from central, on premises data centers to hybrid IT environments running both on premises and in multi-cloud environments increases the complexity of gathering and processing the relevant data. DevOps environments also add a new element of volatility to the IT infrastructures. In addition, containerized environments – specifically if run in multi-cloud and hybrid scenarios – add to the complexity, where even critical business workloads are run in a very agile manner.

To add complexity, there is no one single tool for monitoring and analyzing data, or for automating the response to incidents. Most businesses have several such tools, one or more for each of the multiple environments in which applications run. There is a wide range of sources for security-relevant data in this hybrid world with few or even many tools consuming this data. Both the many sources of data for security and threat analytics, as well as the many systems consuming and processing that data and helping businesses to respond creates challenges.

It has become extremely difficult to create and staff process and to build infrastructures that support this complex environment. One such example is the SOC (Security Operations Center), which collects all relevant data from the hybrid, distributed, and volatile IT environments. In consequence, there is a risk that relevant data will be missed, incidents not identified in a timely manner leading to a failure to respond. Furthermore, with such a variety of such tools in place, it is also difficult to respond in a consolidated and efficient manner. Incident response, both from an organizational and technical perspective, becomes extremely complex.

Cybersecurity must deal with the reality and complexity of today's IT environments. Point-to-point integrations of data sources to analytical solutions and to incident response solutions fail – too complex, too costly, too slow. There is need for visibility across all the relevant source data, so that systems can build on that data to detect, identify and respond effectively to cyber incidents.

There is, as yet, no defined category for such solutions because, until now, there were no such solutions available. While some vendors have good integration within their own technology or provide interfaces to their analytical applications, a comprehensive integration framework with a broad range of out-of-the-box integrations to relevant sources and analytical tools has been lacking until now.

IBM Cloud Pak for Security is now the first open platform that supports the integration of existing security tools for generating insights into cyber events across hybrid, multi-cloud environments. It is one component of a series of such enterprise-ready, containerized software solutions, named Cloud Paks, that IBM has started to bring to the market.

2 Product Description

IBM Cloud Pak for Security is a platform intended to connect security-related data sources, from different tools such as SIEMs, EDRs, data lakes, and more. It can access data from a broad variety and sources and provide homogeneous access across all these sources. Based on that, it can deliver consolidated information back to security applications on the platform. Furthermore, it can orchestrate workflows for incident response and automate manual and repetive tasks. This helps security teams to work and respond faster and with better coordination, by working together based on all available data. IBM Cloud Pak for Security is intended to deliver the foundation for an integrated SOC and security teams, moving from uncoordinated processes using disparate solutions to a coordinated and integrated reponse. With a focus on fostering interoperability, IBM Cloud Pak for Security is not a replacement for existing tools as a "super tool", it enhances the value of those existing tools as an integration platform. Rather than providing a central data store it is a data federation platform providing consolidated access across multiple tools. This preserves existing investments and enables security teams to deal with the complexity of the heterogeneous IT landscape as well as the range of heterogenous IT security tools deployed. It enables a better coordinated approach to tackling the ever-increasing cyber-attacks.

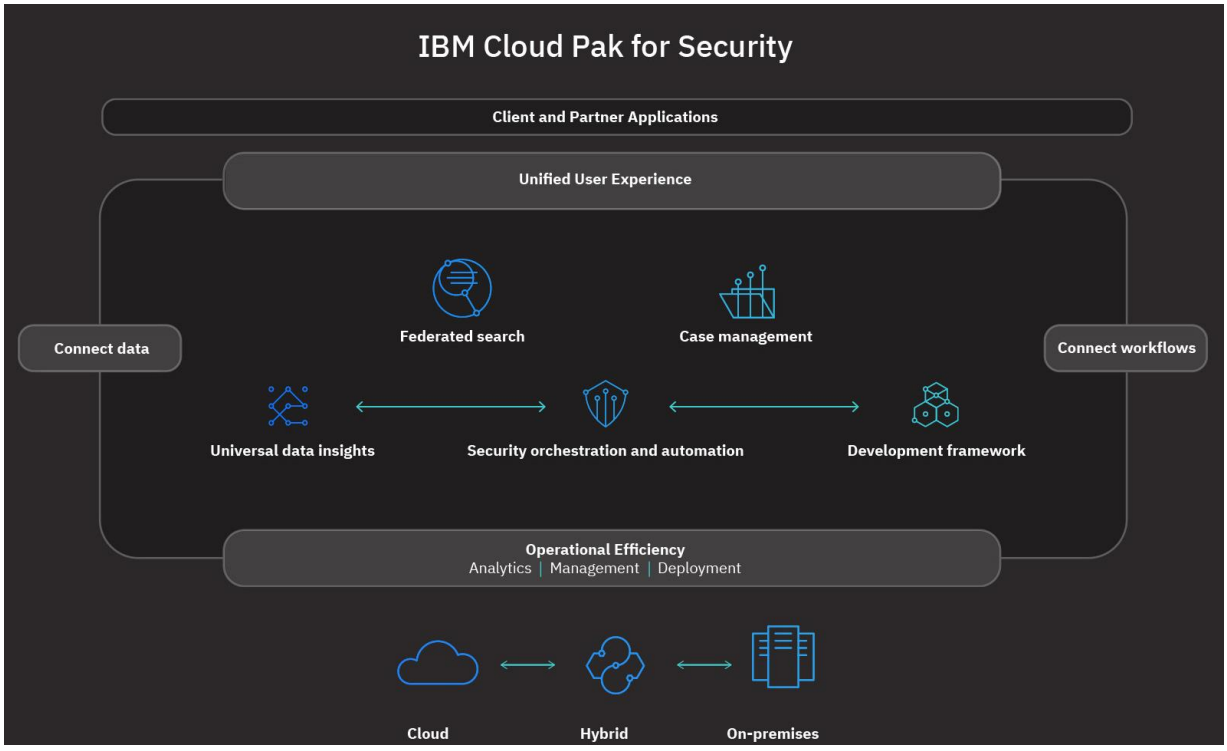

Figure 1: IBM Cloud Pak for Security Overview (graphic reproduced with permission from IBM)

IBM Cloud Pak for Security runs in hybrid environments – on-premise, private cloud or public cloud. It can access data from a variety of environments and source systems, and is an open environment, where multiple security tools can easily connect. It is focused on federating data investigations, as well as orchestrating processes and workflows across various security tools.

With the hybrid, multicloud approach, IBM Cloud Pak for Security aligns with other, recently published IBM Cloud Pak solutions. All these solutions are built on Red Hat OpenShift for the container platform and operational services and thus are one of the first concrete integrations that IBM has delivered since acquiring Red Hat. Based on that platform, Cloud Paks are micro-service based, containerized solutions that build on open source components whenever applicable, but extend and combine these into a comprehensive, packaged solution.

IBM Cloud Pak for Security will connect to a large number of tools. These cover many of the relevant vendors in the cybersecurity tools market, such as Splunk, Tenable, Carbon Black, Elastic, BigFix, AWS, or Microsoft Azure, to name just a few. All these 3rd party solutions can connect to IBM Cloud Pak for Security for access from the platform's unified interface. Security data is accessed leveraging the platform's universal data services and open source technology, and relevant findings can be further analyzed from one place.

Beyond integrating data sources, IBM Cloud Pak for Security also delivers unified access to that information, both via APIs and UIs. For API access, IBM Cloud Pak for Security provides its own SDK. Using that, businesses also can more easily build their own integrations and apps. The main focus of what IBM delivers out-of-the-box is on security workflows, orchestrating multiple existing solutions into integrated workflows, and supporting automation. These are intended to enable better and more efficient incident response, which is the key requirement for today's businesses and their SOCs.

Another key capability of IBM Cloud Pak for Security is the federated search, which is a natural consequence of unified access to security-related information. Based on this federated search, information can easily be extracted and analyzed across multiple tools. Again, IBM Cloud Pak for Security does not move data to a central store, but federates access to information. However, investigations across the complex IT landscapes of today's businesses are massively simplified when queries can be run across a variety of tools from different providers (and multiple instances of such tools), across all data centers and cloud services.

The broad support by other vendors from the very start of IBM Cloud Pak for Security is proof of the validity of this approach and the fact that this is a well-thought-out integration platform, not a replacement of existing investments.

IBM Cloud Pak for Security builds on open standards wherever feasible, which is in line with the Open Source foundation of the new solution. The solution can run on various platforms, including on premises environments, private clouds and public IaaS infrastructures such as AWS, Microsoft Azure, Google Cloud Platform, or for sure IBM's own Cloud.

3 Strengths and Challenges

With IBM Cloud Pak for Security, IBM delivers a major innovation to the Cybersecurity market, addressing three of the major issues:

- The increasing volatility of today's IT environments;
- The need to support complex, heterogeneous IT operating environments, that are hybrid and span multiple clouds;
- The multitude of cybersecurity tools that commonly exist in today's businesses, but lack integration of data and processes.

Based on the approach IBM has chosen, businesses can better integrate both their existing tools and data, in a way that easily builds on and extends their incident response processes. With the approach chosen by IBM, existing investments into cybersecurity solutions are preserved, while adding additional value.

We expect the network of partners supporting IBM Cloud Pak for Security to grow beyond the already impressive initial list of partners. From a competitive perspective, the biggest competition to IBM Cloud Pak for Security will come from vendors delivering incident response solutions. However, even those solutions can build on the integration and federated search capabilities provided by IBM Cloud Pak for Security.

In sum, IBM Cloud Pak for Security is a highly interesting solution for many businesses, specifically the ones running their own SOCs. It also appears to be of high interest to MSSPs (Managed Security Solution Providers) that need to integrate a range of solutions. We strongly recommend that customers evaluate IBM Cloud Pak for Security for use in their cybersecurity initiatives.

Strengths	Challenges
• Unique offering that allows for consolidated access to security and threat information across a wide range of systems; • Strong partner ecosystem, with support from the majority of leading security vendors; • No movement of data, but data federation, avoids the creation of new data siloes; • SDK and other options for developing additional apps and for creating flexible incident response workflows; • Runs in various cloud environments, supports multi-cloud and hybrid requirements; • Modern architecture, based on microservices and containerization.	• Confusion with existing incident response solutions, although built as a broader platform to work with any third-party solution • Successful federated search depends on availability of data sources.

4 Copyright

The Future of Information Security – Today

KuppingerCole supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision making processes. As a leading analyst company, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a leading Europe-based analyst company for identity focused information security, both in classical and in cloud environments. KuppingerCole stands for expertise, thought leadership, and a vendor-neutral view on these information security market segments, covering all relevant aspects like Identity and Access Management (IAM), Governance, Risk Management and Compliance (GRC), IT Risk Management, Authentication and Authorization, Single Sign-On, Federation, User Centric Identity Management, eID cards, Cloud Security and Management, and Virtualization.

For further information, please contact **clients@kuppingercole.com**

KuppingerCole Analysts AG
Wilhelmstr. 20-22
65185 Wiesbaden | Germany

Phone +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com