IBM Security Risk Manager for IBM Cloud Pak for Security

Unified risk management

Organizations today deploy multiple security tools to protect their business's IT ecosystem from a variety of attacks, many of which provide their own definition of risk. With dozens of security tools at once, security leaders can find themselves overwhelmed trying to process the disparate, subjective definitions of risk generated by their tools as well as prioritizing remediation. For security executives seeking to quickly and efficiently minimize their business's risk profile, they need a solution that normalizes and contextualizes risk data, facilitates prioritization and helps them determine the best course of action to reduce overall risk.

IBM Security Risk Manager for IBM Cloud Pak for Security empowers security leaders to collect and contextualize risk data from across their security environment. By sourcing risk data inputs from a variety of vectors—including identity and access management solutions, data security solutions, and infrastructure security solutions—and running those inputs through a common risk engine, Risk Manager helps create a more complete image of activities and processes that threaten the integrity of the organization and providing business leaders the information they need to prioritize and remediate those risks.

Highlights

- Unified view of security risk metrics from across IT landscape through a single pane of glass
- Common definition of risk contextualizes organization's risk data
- Prioritize what actions to take to reduce overall risk posture
- Seamless integration with SOAR and other Cloud Pak for Security applications enables simple and rapid issue remediation

A common definition of risk

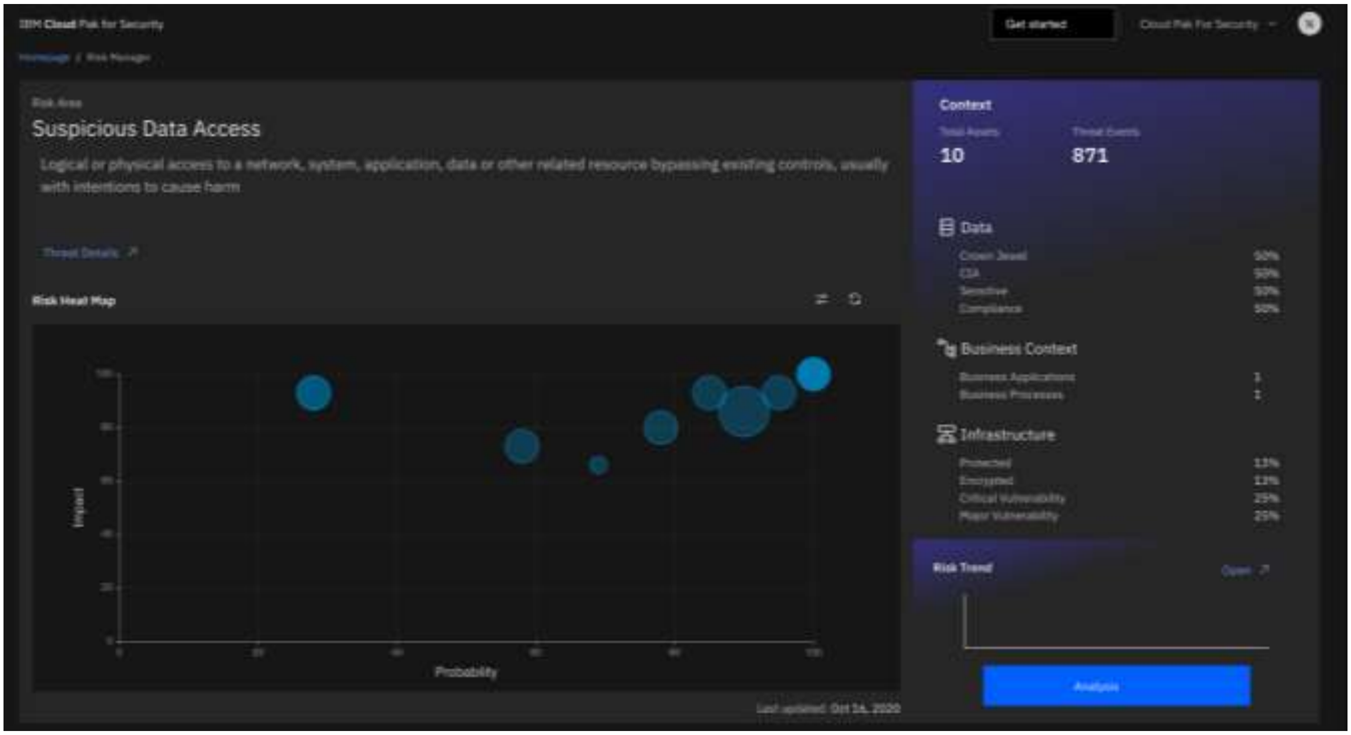
Risk Manager contextualizes an organization’s security risk data by processing it through a common risk engine consisting of three factors:

- Asset criticality: the relative value or importance of an asset to the business, whether it is a database, application server, network device, or personnel. The risk engine determines importance of the asset either by identifying the type of data stored, such as regulated data, or whether the asset is critical for execution of an important business function.
- Resistance strength: an indication of the organization’s overall control maturity or resiliency to attack. Resistance strength is usually associated with an asset, and it speaks to what types of defenses that a threat actor needs to overcome to lead to the loss or damage of the asset.
- Threats and their capabilities: the specific threat event or events and their probability of successfully exploiting known vulnerabilities in the system.

Security and risk leaders can easily compare the risk areas of their system once they have been processed by the risk engine and identify which risks have the biggest potential impact on their business, allowing them to prioritize remediation accordingly.

A unified, complete view of an organization’s risk

Risk Manager simplifies and accelerates the process of identifying a business’s most significant risks. By combining risk data from existing IT and security tools connected in the Cloud Pak for Security deployment, security leaders get a comprehensive and unified view of their risk posture that is driven by data and grounded in context.



Suspicious Data Access

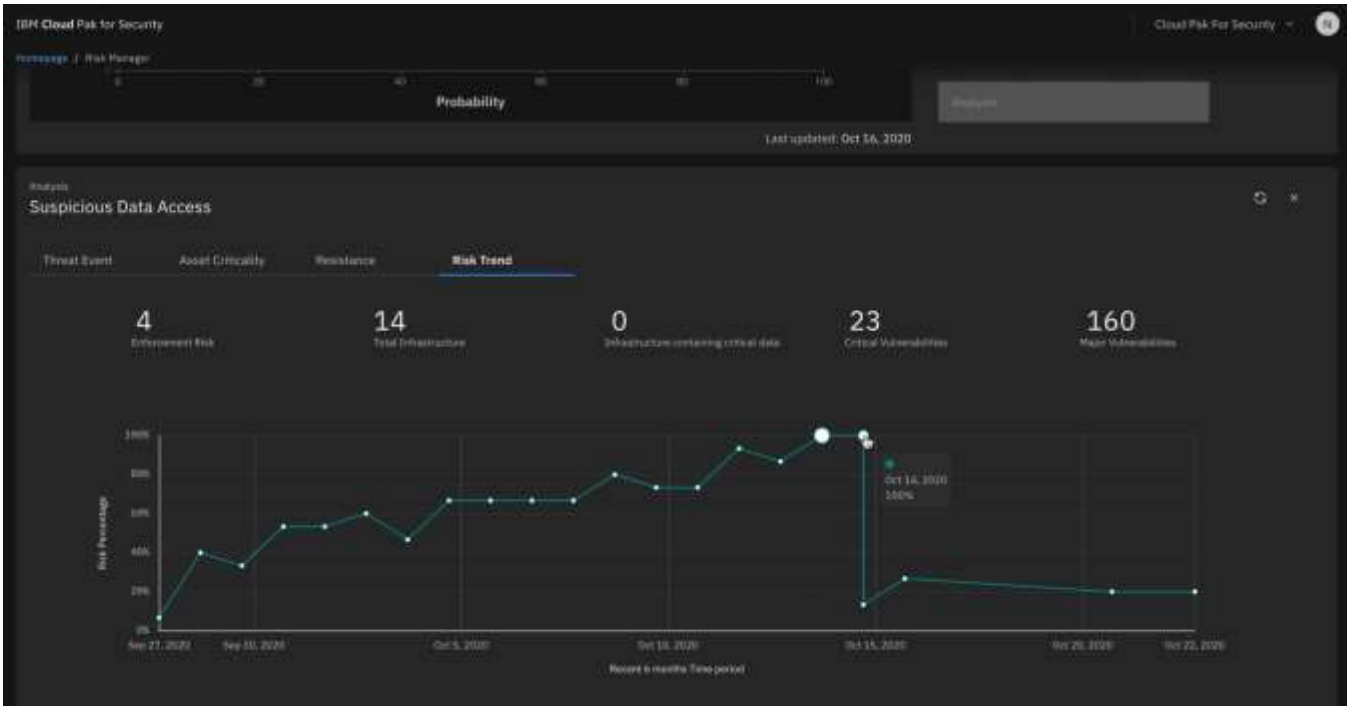
Logical or physical access to a network, system, application, data or other related resource bypassing existing controls, usually with intentions to cause harm

Total Assets	Threat Events
10	871

Data	
Crown Jewel	50%
CIA	50%
Sensitive	50%
Compliance	50%
Business Context	
Business Applications	1
Business Processes	1
Infrastructure	
Protected	13%
Encrypted	13%
Critical Vulnerability	25%
Major Vulnerability	25%

A user can explore their organization's sources of risk through the use of a heat map that charts risk along three dimensions: 1) the x-axis maps the probability of risk occurring; 2) the y-axis tracks the potential impact on business continuity; and 3) the size of each bubble indicates the number of assets contributing to the risk area. Risk Manager not only provides users with a fast and intuitive way to put risk into context, it can also help users uncover previously overlooked risks by correlating previously disconnected and subjective risk metrics.

Security analysts can use dedicated analysis panes within Risk Manager to investigate an area of risk along the three elements contributing to the risk engine: asset criticality; resistance; and threat event and capability. These drill-down tools allow the analyst to interpret the nature of their risk areas. The Threat Event view provides analyst with a view into the most significant threat events happening in your environment over time.



Asset criticality provides context into the types of assets at risk—such as data covered by regulations such as PCI, HIPAA, and CCPA—or deemed confidential by configurations set by the analyst. The Resistance view provides users with a view into the data sources at risk and the forms enforcement, such as activity monitoring or encryption, deployed to protect those sources. Finally, the Risk Trend view shows how an area of risk has changed overtime.

In the event that Risk Manager detects a critical risk in your environment, an analyst can easily open a case, through the Cloud Pak for Security's Cases application, to further investigate the issue across multiple siloed sources and achieve fast and simplified risk remediation from a single interface.

A Zero Trust approach to risk management

Risk Manager offers security teams with a modern approach to viewing and addressing security risk according to zero trust principles. It provides several elements critical to a zero trust strategy, including:

- Adding context to risk data produced by the organization’s security environment, allowing users to see and understand risks across their entirety of their security program.
- Integrating remediation strategies across the entire security program to maximize security with minimum impact to business using the Cases application
- Continuously improving the security posture of the entire organization by documenting risk remediation activities, and their impact, over time.

Powered by IBM Cloud Pak for Security

Risk Manager is an integrated application on IBM Cloud Pak for Security, IBM’s open security platform that connects to existing data sources and helps users generate deeper insights and faster response through automation. Risk Manager will come as a standard application on IBM Cloud Pak for Security version 1.5.

As part of the Cloud Pak for Security, Risk Manager integrates seamlessly with the platform’s other native applications, like Data Explorer and SOAR, further expanding the investigative and issue remediation capabilities of the solution.

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 Security Risk Manager for 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/risk-manager