IBM Security

IBM Cloud Identity

Leverage risk aware actionable intelligence using Identity Analytics

Erika Weiler

IAM Offering Manager

Dinesh Jain
IAM Offering Manager



Security Impact of COVID-19

Key Findings from CSO Pandemic Impact Survey (March 2020)

- Three months ago, 16.5% of employees worked from home at least 60% of the time. As
 of March 23rd, that number climbed to 78%
- About 26% of organizations have seen an increase in the volume, severity, and/or scope
 of cyber-attacks since March 12th
- 73% of security executives believe that the impact of this pandemic will alter the way their business evaluates risk for at least the next five years



Leverage identity analytics to make smarter decisions and enforce principle of least privilege

Better Security Insights

Highlight anomalies

Increased Operational Efficiency

Support decisions

Quicker Response Time

Remediate risk

Challenges occur when there is a lack of risk visibility

View Risk Holistically

Enforce Principle of Least Privilege Reduce Human Error

"I'm unable to monitor risk across my IAM solutions so I'm not sure if I'm carrying compliance risk."

"My IAM processes inhibit me from being able to identify anomalies within peer groups."

"I need insights to make informed access and certification decisions or I'll just approve everything."

Healthcheck

Peer Group Analysis

Decision Support

Configure to what matters to your organization

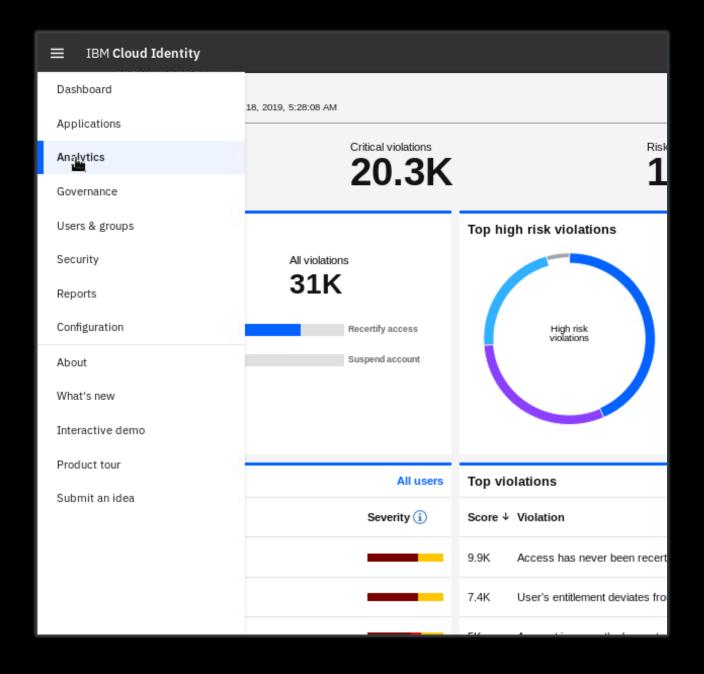
Identify anomalies within peer groups (geo, role, department, etc.)

Get additional support on which action to take via risk and confidence scores

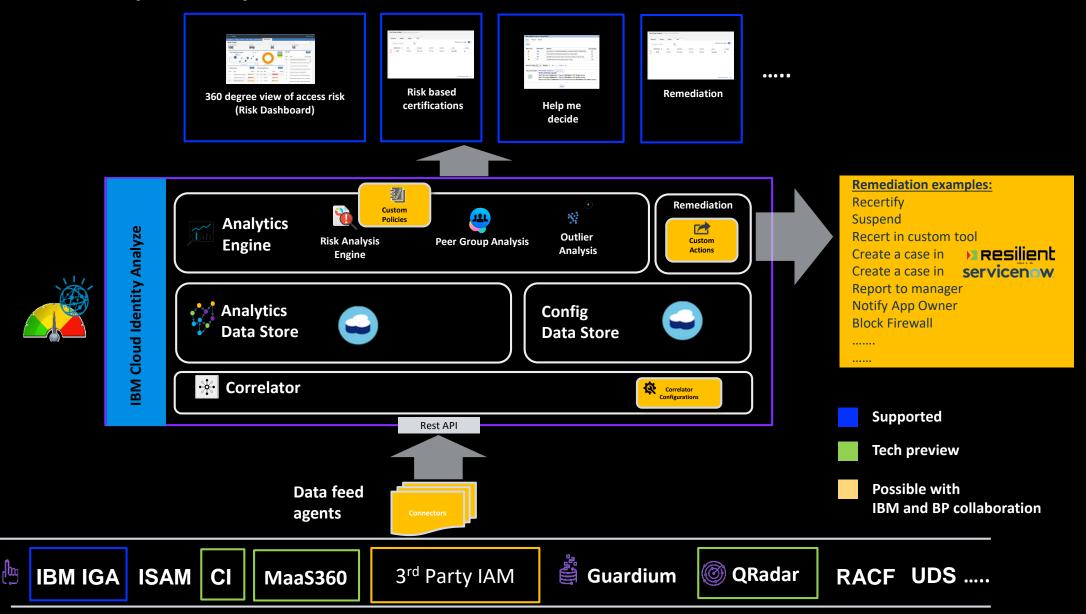
Introducing Identity Analytics in IBM Cloud Identity

A multi-purpose analytics engine that processes activity and entitlement data from a variety of sources, providing a holistic view of access risks with the ability to take action based on those risk insights

- OOTB support for IGI and ISIM
- Library of policies for identifying risk
- Extensibility for custom policies, workflows, data sources, and correlator configuration



Cloud Identity Analyze (CIA) - Platform Overview



Demo

Leverage Identity Analytics to stay secure in a time of crisis

Proactively reduce risk within your organization

Continuously monitor health to regularly ensure compliance

Leverage
Identity data in
conjunction with
other analytics
to increase
likelihood of
identifying
insider threat

Double the ROI by leverage identity analytics to 'clean up' IGA deployments

Thank you

Follow us on:

bm.com/security

securityintelligence.com

ibm.com/security/community

<u>xforce.ibmcloud.com</u>

@ibmsecurity

youtube/user/ibmsecuritysolutions

© Copyright IBM Corporation 2019. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

