

IBM Security and Thales

Presents a 4-part series:

Zero Trust and Your Data

Zero Trust and your Data – Session Schedule

Session 1

Securing Containers and Managing Access

June 16th, 2020 2:00 pm - available on-demand

<https://community.ibm.com/community/user/security/viewdocument/zero-trust-and-your-data-part-1>

Session 2

Securing Databases and Managing Vulnerabilities

July 14, 2020 11:00 a.m. - available on-demand

<https://community.ibm.com/community/user/security/viewdocument/zero-trust-and-your-data-part-2-s>

Session 3

Cloud Data Security and Cloud Keys Management

Aug 11, 2020 11:00 a.m. - available on-demand

<https://community.ibm.com/community/user/security/viewdocument/zerotrust-and-your-data-cloud-data>

Session 4 - Advanced Threat and Continuous Monitoring

Sept 17, 2020 1:00 p.m.



Businesses are embracing hybrid multicloud to gain agility, competitive advantage and drive their organizations forward.

However, expanding the data footprint increases the organization's attack surface, resulting in a host of new data security and compliance challenges.

Real world consequences

\$11.45M

Global average cost
of an insider threat

\$3.92M

Average cost
of a data breach

74%

of organizations are negatively impacted
by a cybersecurity
skills shortage

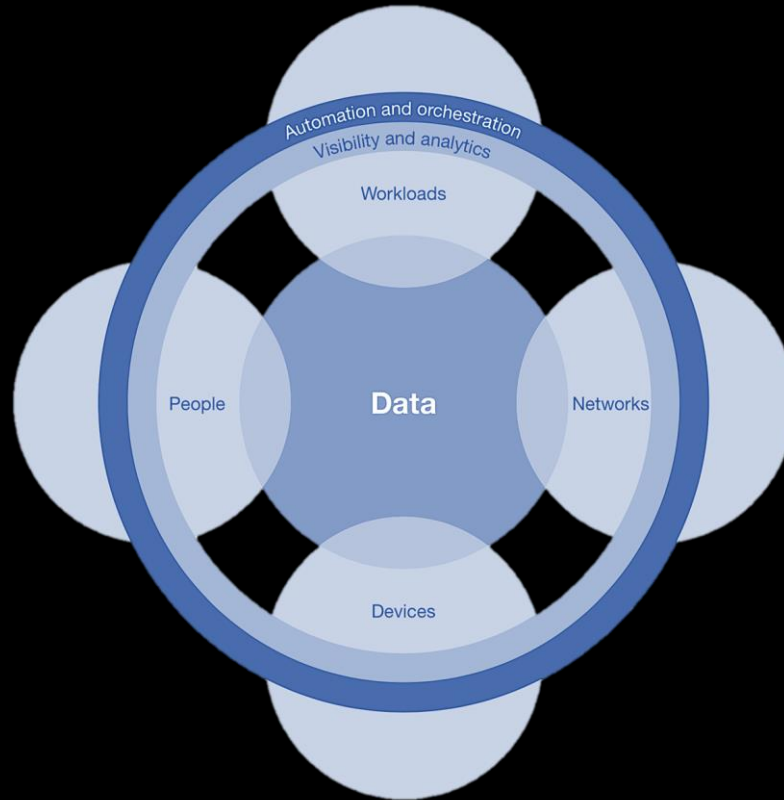
87%

are concerned with data security
adversely impacting the use of
public cloud services.

279 days

average time to identify
and contain
a breach

Forrester's Zero Trust Framework



Forrester's Zero Trust Framework

A conceptual and architectural model for how security teams should redesign networks into secure microperimeters, use obfuscation, limit risks associated with excessive user privileges, analytics and automation to improve detection and response.

Key tenants:



Data-Centric Approach
Security Travels with the Data



Never Assume Trust
Continuously Use Risk-Based Analysis

A Paradigm Not A Product

- Discover, classify and assess vulnerabilities for all data
- Darken multicloud apps from ALL networks
- Verify first then connect
- Least privileged, app-session access-based on context
- Encrypt everything
- Device-app and app-app micro segments
- Visibility and control inside and outside perimeter
- Continuous assessment

A smarter data security approach addresses key challenges across disparate IT environments

Discover your sensitive data across on premises and cloud data stores

Understand risk with contextual insights and analytics to quickly uncover suspicious activity

Respond to threats and share alerts and reports in real-time

Collaborate to share and gain access to critical threat information and remediate risk across teams



Environments and Data Sources

- Databases / structured data
- Cloud
- Containers
- Big data / semi-structured data
- Files / unstructured data
- Mainframes
- Applications
- IoT

Data security with IBM Security Guardium

Environments and Data Sources

- Databases / structured data
- Cloud
- Containers
- Big data / semi-structured data
- Files / unstructured data
- Mainframes
- Applications
- IoT

DISCOVER AND UNDERSTAND

- Guardium Insights
- Guardium Vulnerability Assessment
- Guardium Data Risk Manager

RESPOND

- Guardium Data Protection
- Guardium Data Encryption
- Guardium Key Lifecycle Manager

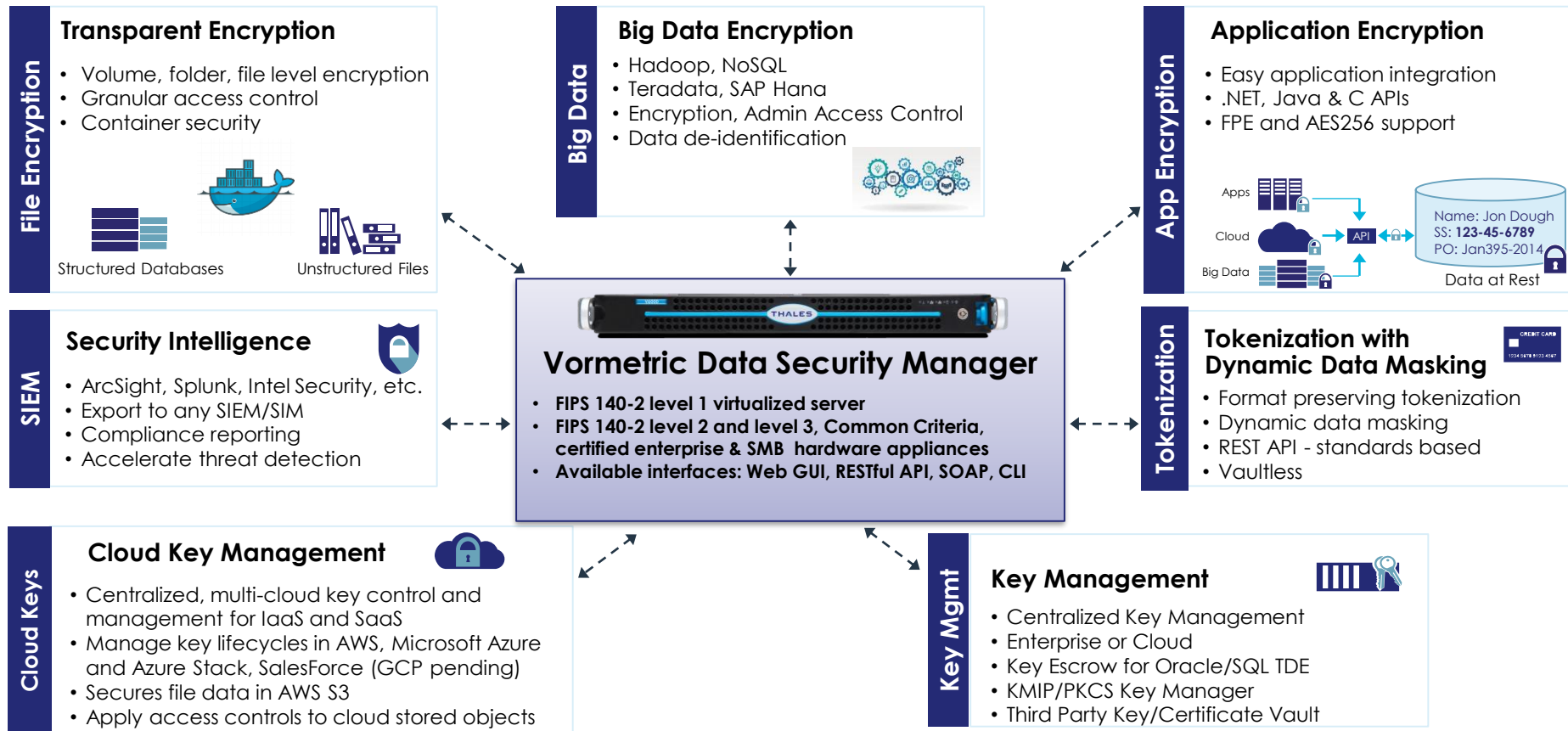
COLLABORATE

- Guardium Data Protection
- Guardium Insights

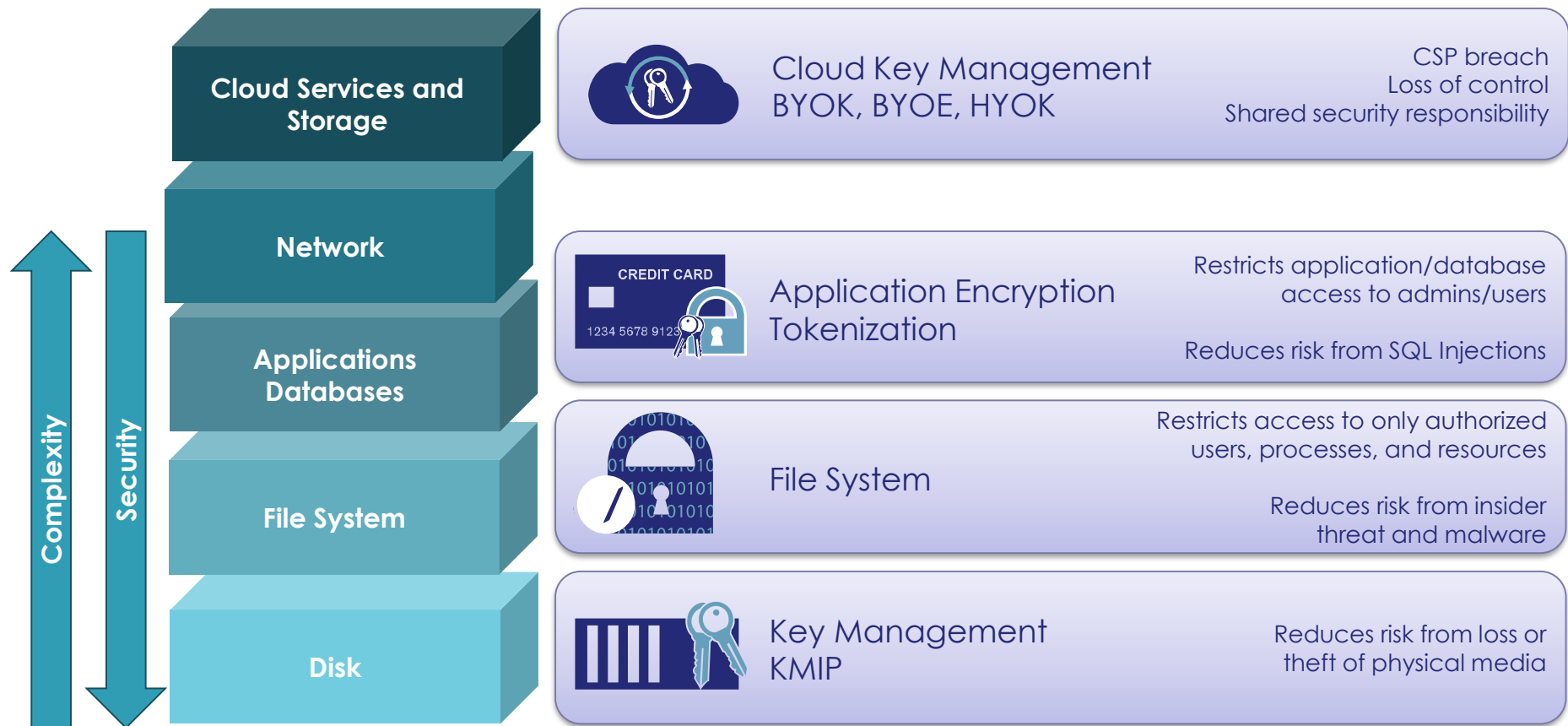
Integrations

- Data discovery and classification
- Security orchestration, automation and response
- Security information and event management
- Data leak prevention
- Identity and access management
- Privacy management
- Vulnerability assessment
- IT operations and service management
- Application security
- Auditing
- Archiving/backup restore
- Web Application firewalls

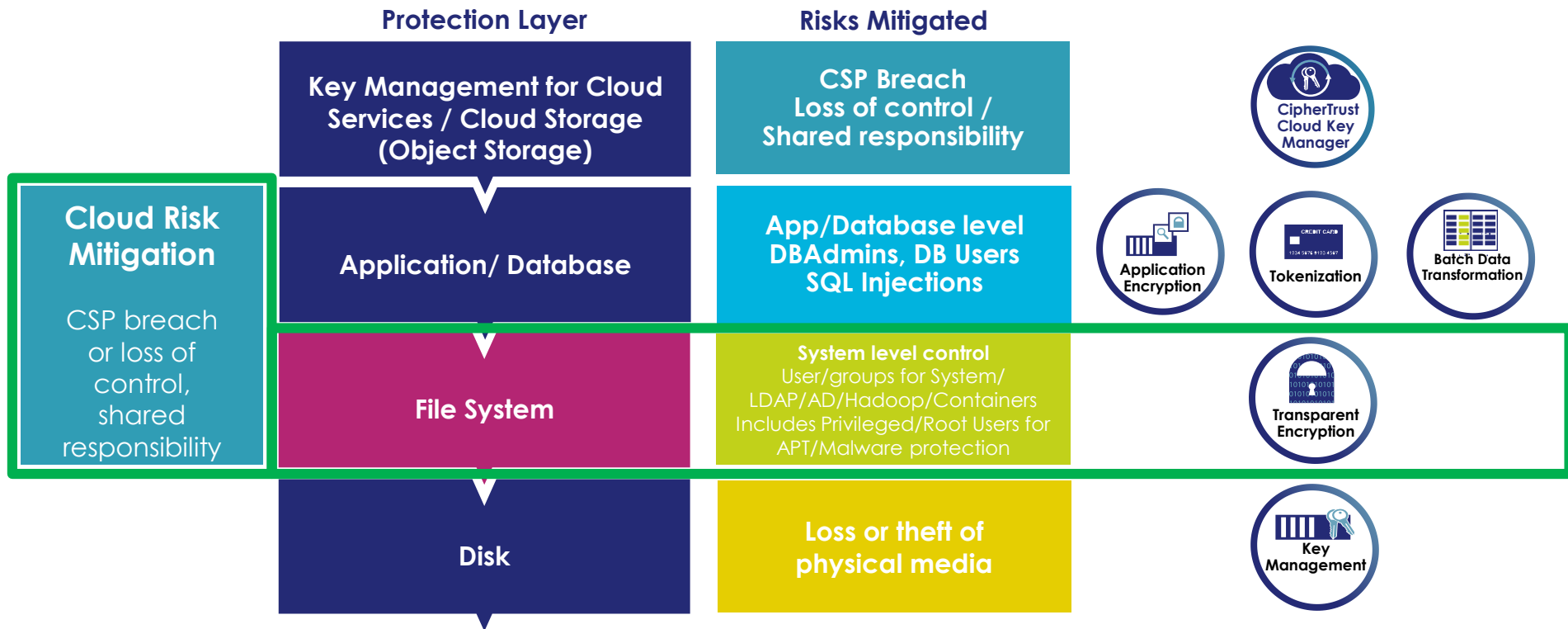
Vormetric Data Security Platform



Security Solutions for your Data Stack



Vormetric Transparent Encryption: Protection Layers



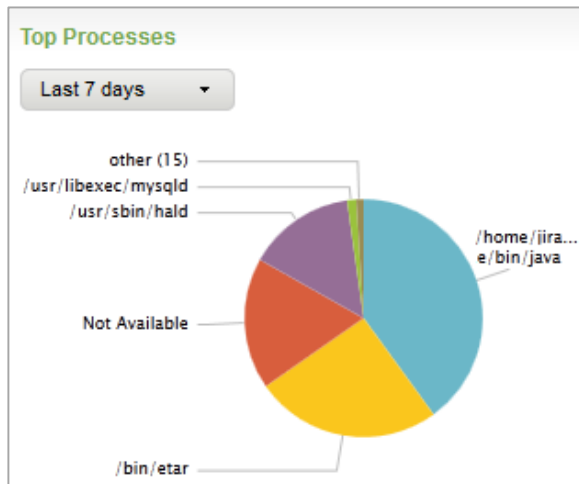
SIEM Integration: For Compliance Reporting

- Supports compliance reporting and audits
- Reveals unauthorized access attempts to protected data
- Identify compromised users, administrators and applications
- Identify attacks on data such as APTs or malicious insiders
- Invaluable for post-breach forensics

Top 10 Users

Last 7 days

uinfo	count
root,uid=0,gid=0root,bin,daem	459366
haldaemon,uid=101 (User Not	368313
jira,uid=1005,gid=100\users\	289836
mysql,uid=27,gid=27mysql	14082
root,uid=0,gid=0root	10280
root,uid=0 (User Not Authentic	980
SYSTEMWNT AUTHORITY	171
phenscheid\VORMETRIC	97
root,uid=0,gid=0root,bin,daemve,503)	19
apache,uid=48 (User Not Auth	15



Access Attempts from Unauthorized Agents

Last 7 days

shost	count	percent
PHENSCEID-WIN7.vormetric.com	31	38.27
fslpar215.i.vormetric.com	26	32.09
bob.i.vormetric.com	24	29.62

User Logins

Last 7 days

Name	Result	count	percent
User1	OK	199	95.2
anand	OK	5	2.39
User1	Failed	4	1.91
voradmin	OK	1	0.47



Our journey to a bigger and better data protection platform

IBM Security Guardium Insights
for IBM Cloud Pak for Security

Guardium Insights will help existing and new clients using Guardium Data Protection by:

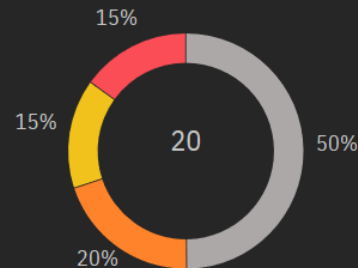
- Accelerating decision making using new, risk-based data security insight technology
- Reducing cost and complexity of collecting, managing and retaining data security and audit data
- Performing long-term reporting in seconds
- Enabling flexible deployment with on-prem, public cloud or private cloud installation options

Discover

Centrally store and visualize security and compliance data

- Quickly visualize data activity across on-premises and cloud-hosted data sources
- Produce pre-defined and custom data security and compliance reports in seconds
- Track how data is being accessed, shared, and interacted with using agent and agentless based monitoring
- Discover hidden threats and potential risks

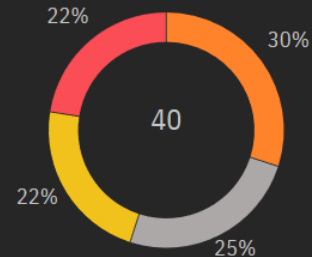
Data source risk



Score pending Medium Low High

[View all data sources](#) →

User risk



Medium Score pending Low High

[View all users](#) →

Recent anomalies

Name	Confidence score(%)	Status
Data Modification January 10th 2020, 8:06:06 pm	99	Read
Data Extraction January 10th 2020, 8:06:00 pm	99	Unread

Understand

Apply advanced analytics to uncover threats

- Advanced analytics learn logical operations in a business – and spot anomalies at the first occurrence
 - Uncover user behavior anomalies
 - Understand major deviations in database transactions
- Detect potential fraud or threat activities faster

Data Extraction

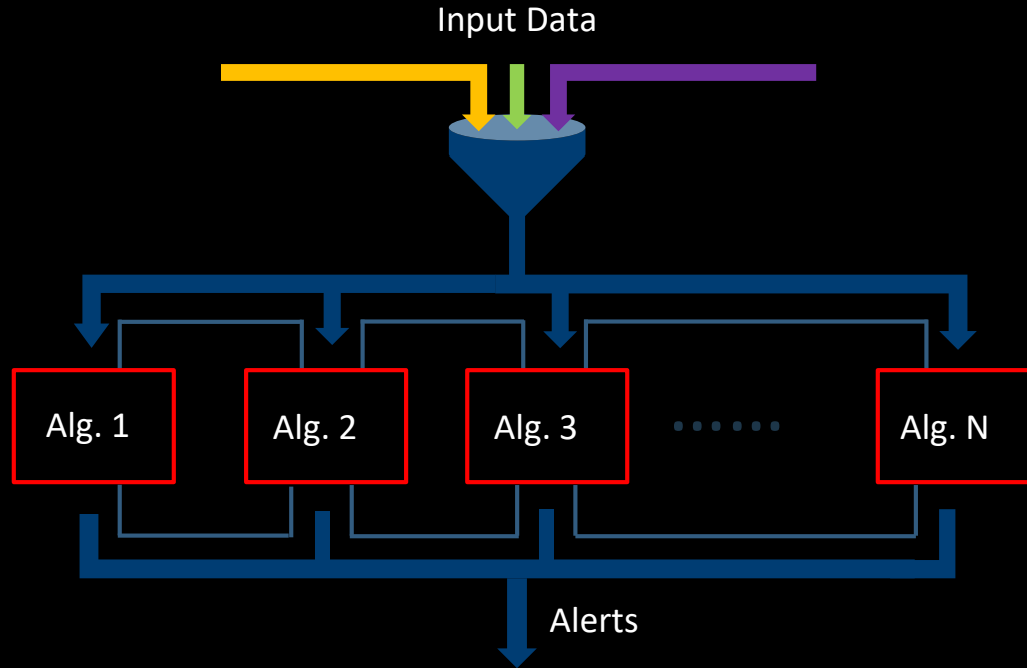
2019-10-08 11:00:00

Summary

A HIGH data extraction violation has been triggered by on , which violates the normal extraction on asset USER.

	Details	Timeline
Who	Actor: DB2INST1	
What	Database Name: DB2INST1	
When	Timestamp: 2020-01-10 20:06:00	
Where		
Why	Anomaly Type: Data Extraction	

Comprehensive analytics



Current Insights:

- Alg. 1: Classical outliers analytics
- Alg. 2: Sequence based predictive analytics

Sequence-based predictive analytics

Logical operation → Online money transfer

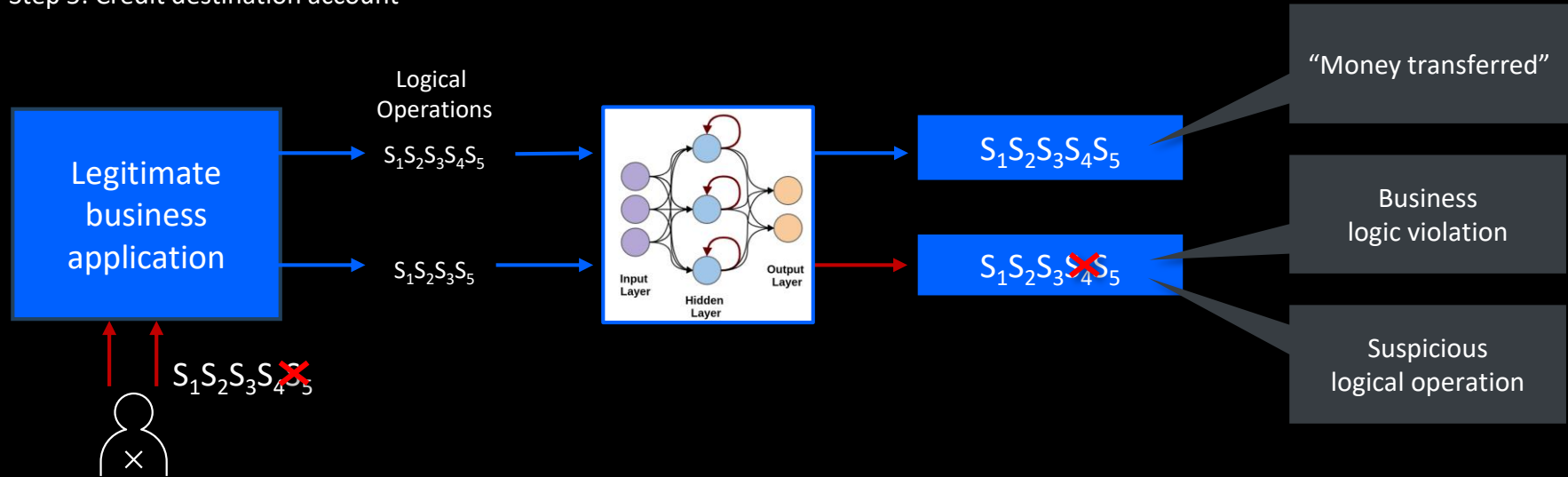
Step 1: Lookup source account

Step 2: Verify transfer limit

Step 3: Lookup destination account

Step 4: Debit source account

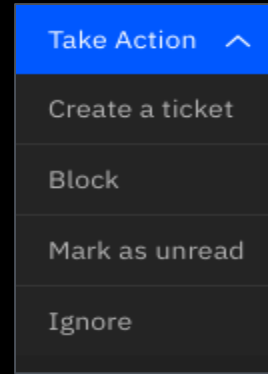
Step 5: Credit destination account



Respond

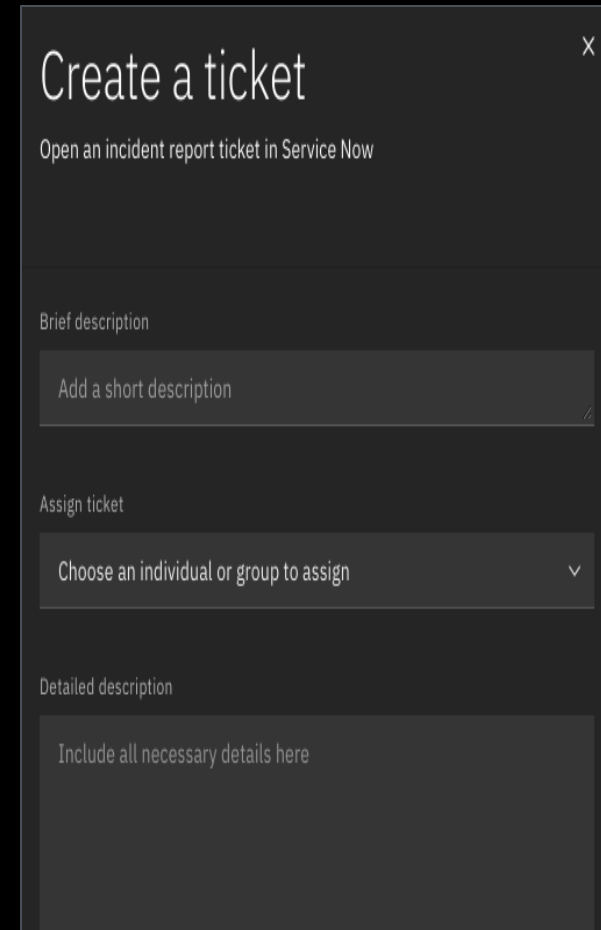
Tools at your fingertips to mitigate threats

- Standardized remediation workflows across hybrid multicloud environments
- Block unauthorized and suspicious users from accessing data
- Create tickets, enrich cases, and escalate issues
- Share insights and reports across teams



Take Action ^

- Create a ticket
- Block
- Mark as unread
- Ignore



Create a ticket X

Open an incident report ticket in Service Now

Brief description

Add a short description

Assign ticket

Choose an individual or group to assign

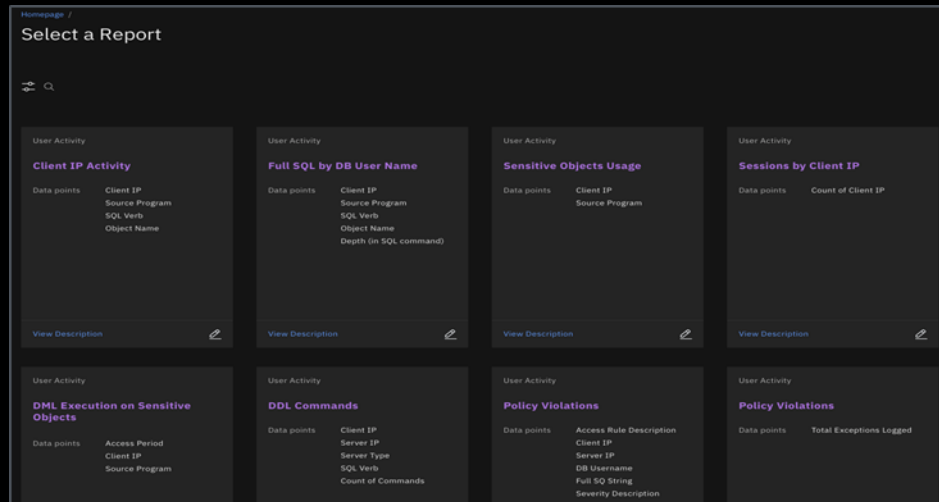
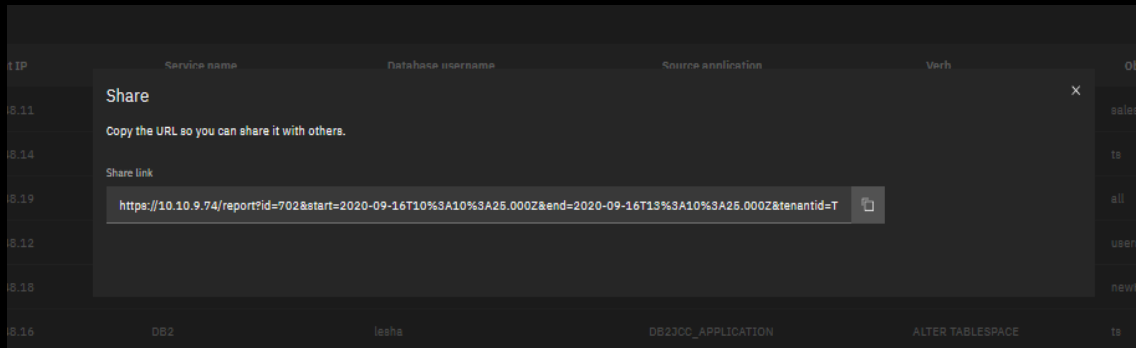
Detailed description

Include all necessary details here

Collaborate

Team up in the battle against threats

- Share out reports
- Customize reports to find repeating events
- Synchronized view and response to threats across teams

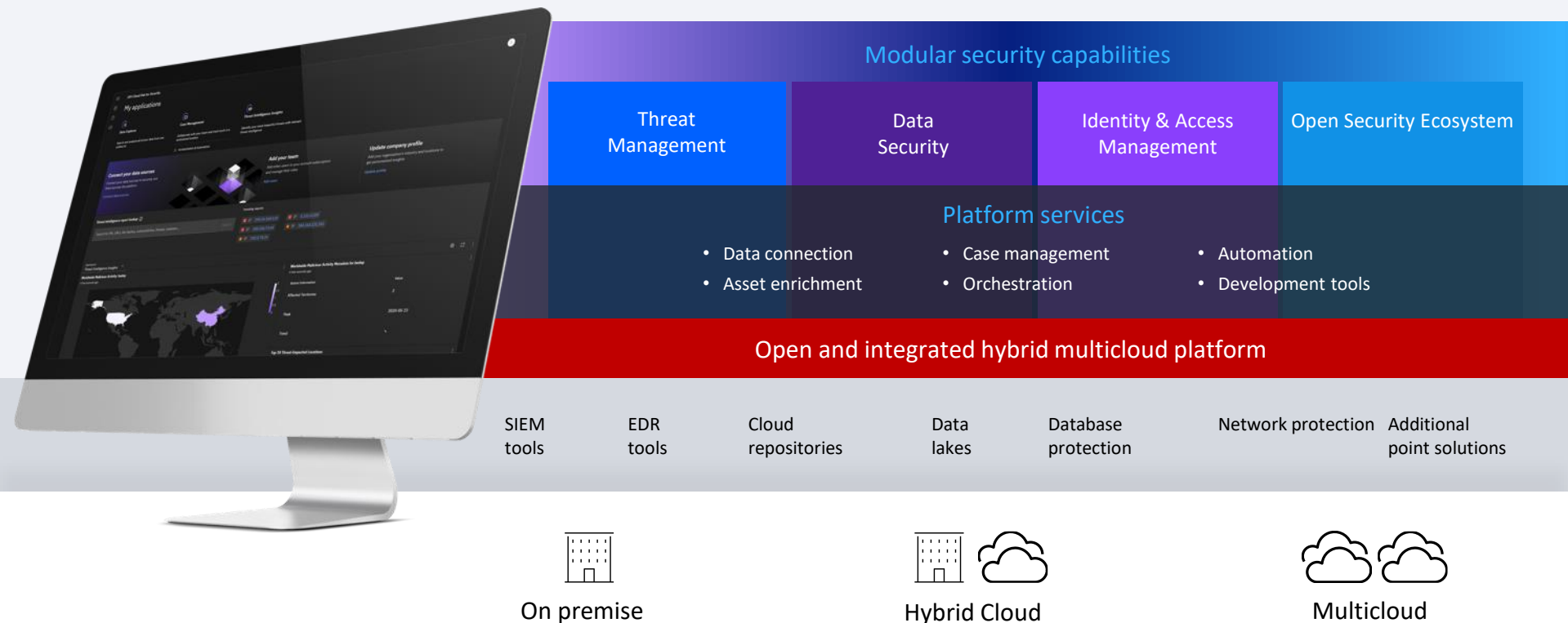


IBM Security Guardium Insights for IBM Cloud Pak for Security

Demo

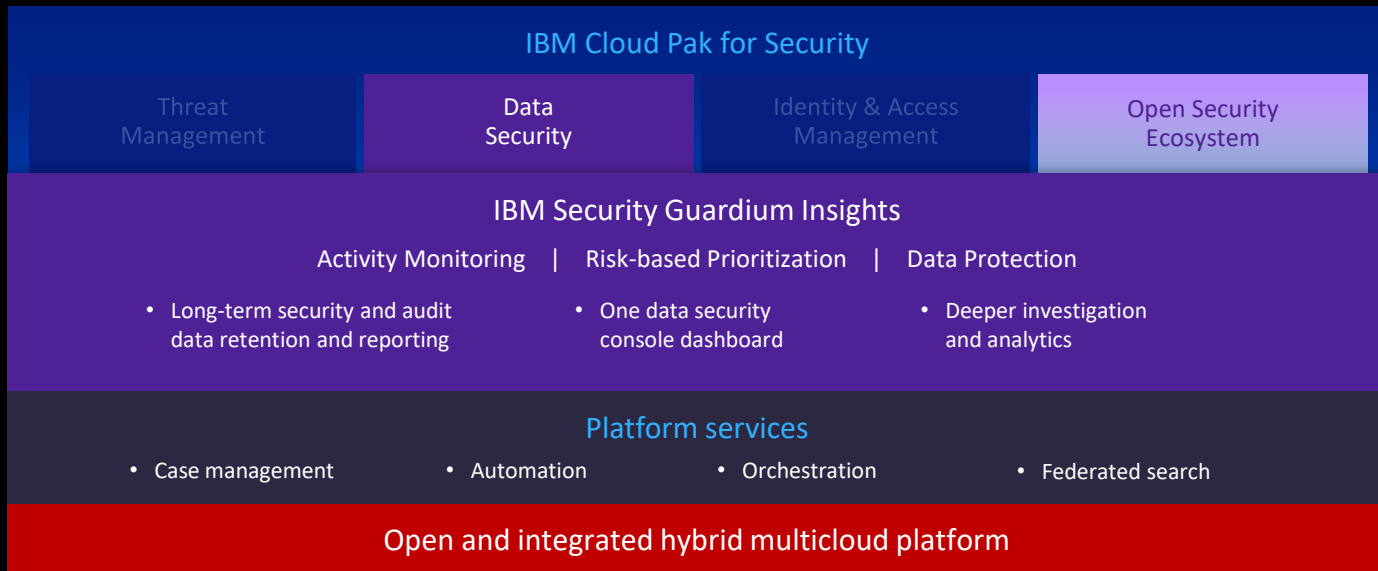
IBM Cloud Pak for Security

An open multicloud platform to gain security insights, take action faster, and modernize your architecture



IBM Security Guardium Insights for IBM Cloud Pak for Security

Collect, analyze and act on years of data security and audit data in the Guardium Insights for Cloud Pak for Security data security hub — whether that data comes from Guardium Data Protection via collectors or is streamed directly into the hub from Cloud sources in an agentless way.



IBM Security Guardium Insights for IBM Cloud Pak for Security

Data security becomes the latest addition to IBM Security's modern, open multicloud platform

Effective August 11th customers can purchase Insights with Cloud Pak for Security and the Red Hat OpenShift Container Platform

Use these resources to get in the know about this exciting news!

- [Security Intelligence Announcement Blog](#)
- [Community Post](#)
- [Product page](#)
- [Product Tour](#)
- [Data sheet](#)



Discover

Centrally store and visualize data security and compliance posture

Understand

Evaluate risk across hybrid multicloud data repositories

Respond

Centralize and accelerate responses

Collaborate

Unify critical threat information and workflows across teams

For additional information contact

- John Nestler
Thales Channels Manger
john.nestler@thalestct.com
- Enrique Gutierrez Alvarez
Digital Trust Security Leader
enrique_Gutierrez@us.ibm.com
- John Dombroski
Cyber Security Engineer
jdombros@us.ibm.com

Thank you

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube.com/ibmsecurity

© Copyright IBM Corporation 2020. 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.