IBM Security

Achieving comprehensive data protection and governance

IBM Cloud Pak for Data with IBM Security Guardium Data Protection

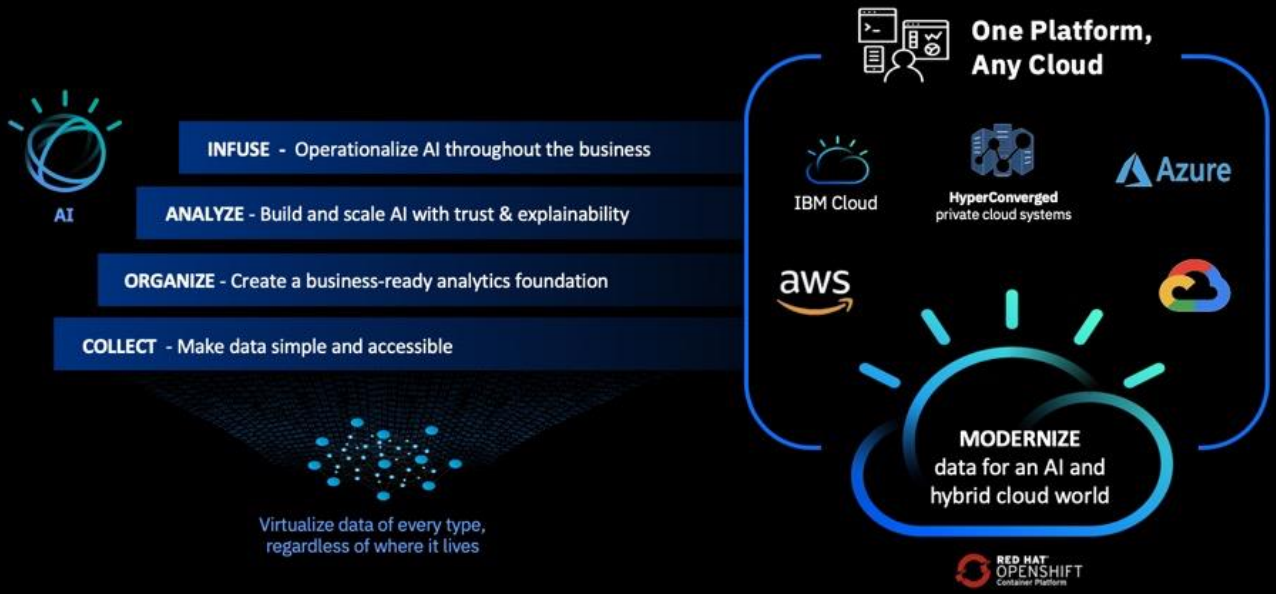
Businesses are embracing cloud-native platforms to facilitate advanced data analytics and AI, driving competitive advantage through innovation.

Despite these transformative efforts, organizations struggle with disconnected teams, fragmented IT tooling, and slow and expensive compliance auditing and reporting processes.

Cloud Pak for Data:

An open and extensible cloud-native platform providing a unified set of data and AI services

- Eliminate data silos, connect all data
- Automate and govern the data and AI lifecycle
- Operationalize AI with trust and transparency



Data governance and data security are interdependent

Data Governance	Data Security

Address compliance with industry and government regulations

Data Governance

Document policies and privacy rules for governance and enforcement

Discover and classify sensitive or regulated data stored across hybrid multi-cloud

Define user access rights to sensitive data

Data Security

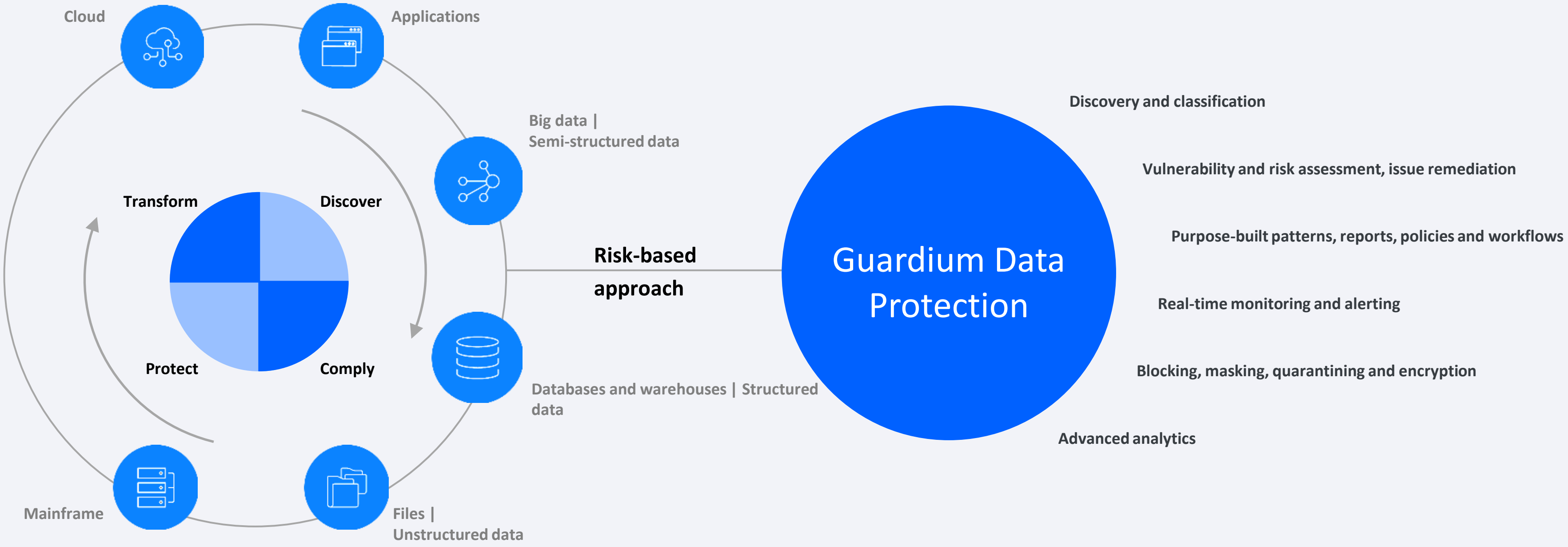
Monitor access to sensitive data in real-time

Detect and remediate insider threats

Protect workloads across hybrid multi-cloud deployments

Guardium Data Protection empowers you to meet your critical data protection needs with smarter capabilities

Complete visibility — **Actionable insights** — **Real-time controls** — **Automated compliance**



Getting specific

Securing hybrid multicloud environments with Guardium Data Protection

Dynamic

Active & passive monitoring for 30+ cloud-native data sources

- Agentless
- Agent-based

Minimize security blind spots and take real-time action with blocking and redaction*

Store data security and audit data to meet retention requirements and uncover unknown threats

Orchestrated

Centralized policy enforcement and management across hybrid multi clouds

Automate compliance workflows for audit reviews and approvals Orchestrate remediation and response with IT and SecOps tools

- ServiceNow, Splunk, QRadar, Resilient, and more

Modern

Uses cloud-native and containerized technology

Simplify and streamline deployment with cloud management frameworks, such as Kubernetes and OpenShift

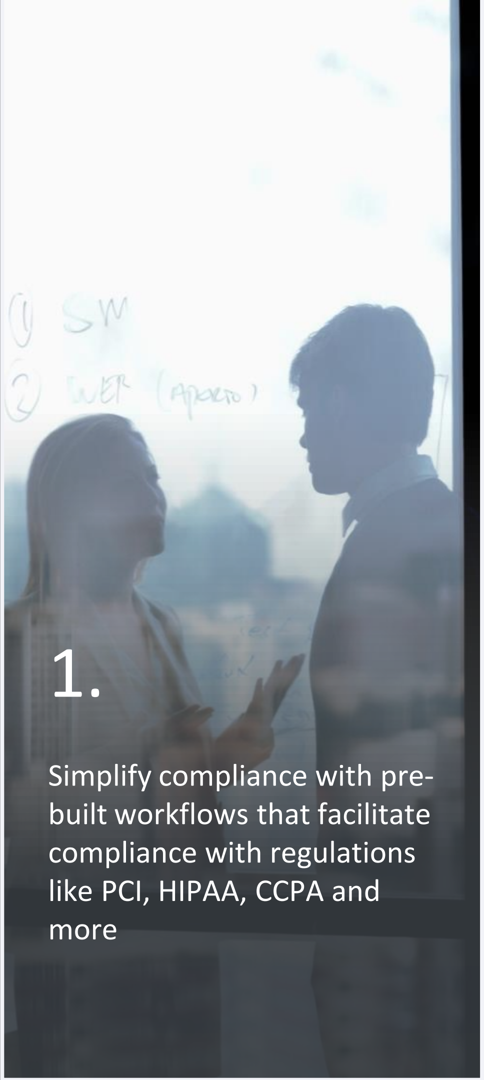
Elastic, scalable and resilient

*** Agent-based**

Cloud Pak for Data

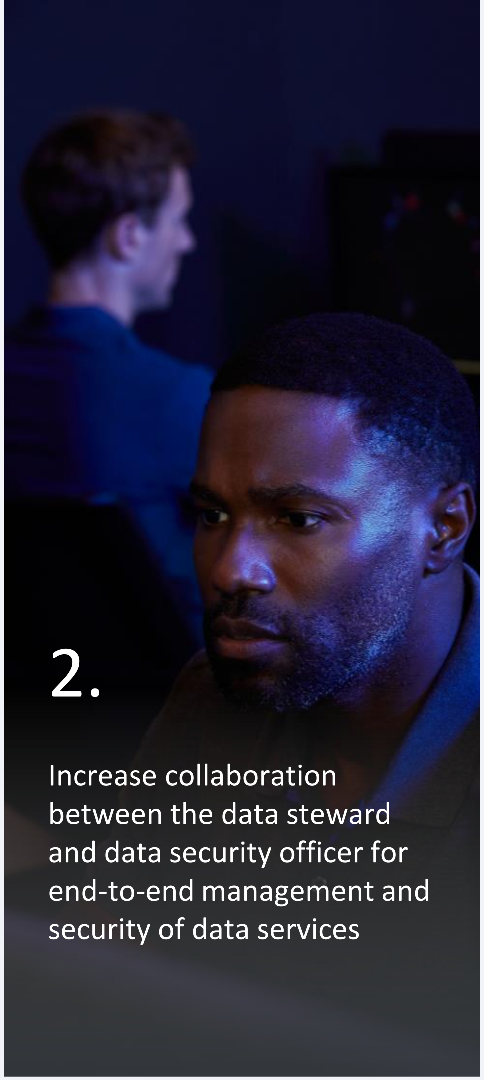
+

Guardium Data Protection



1.

Simplify compliance with pre-built workflows that facilitate compliance with regulations like PCI, HIPAA, CCPA and more



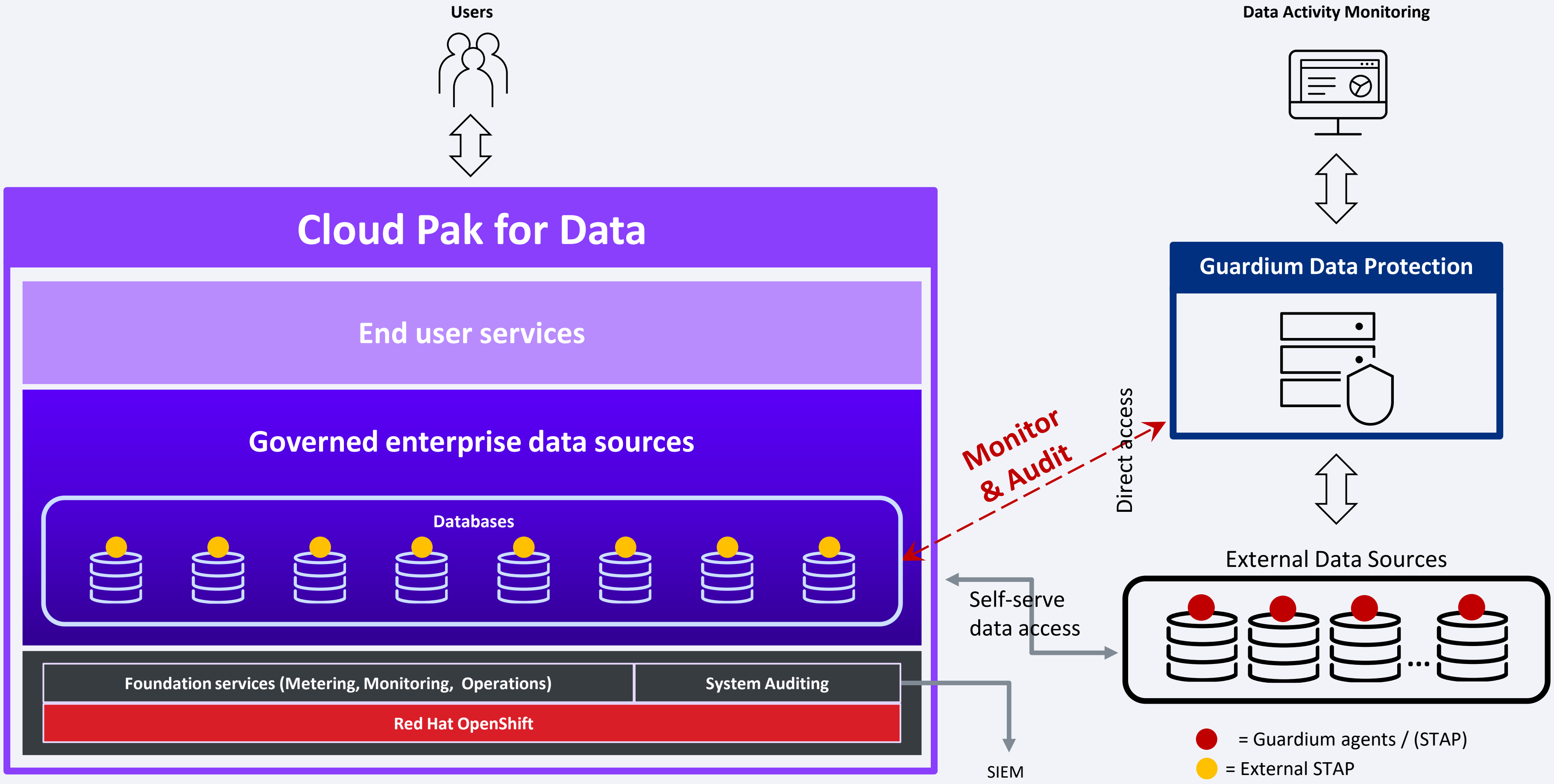
2.

Increase collaboration between the data steward and data security officer for end-to-end management and security of data services

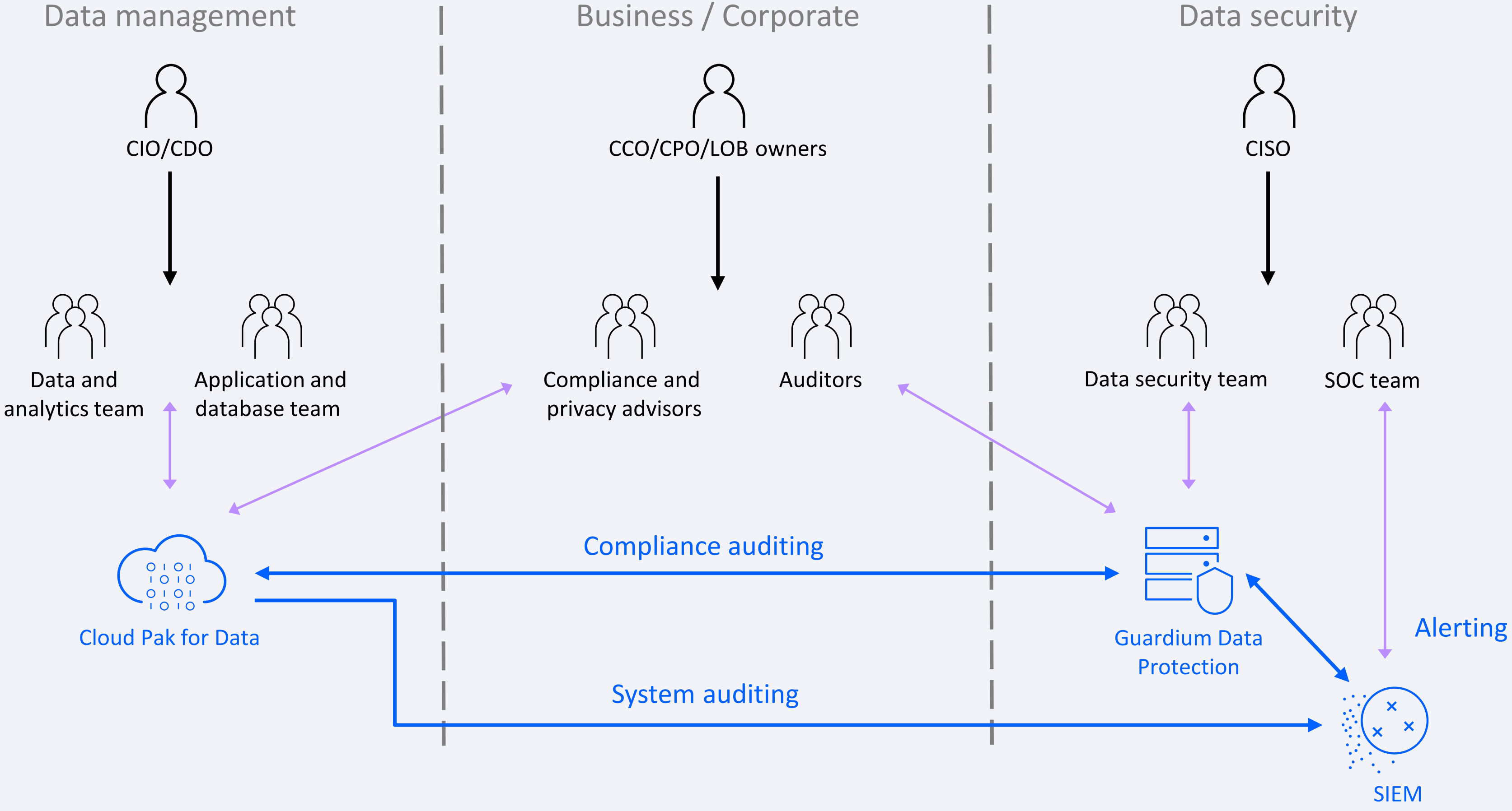
3.

Centralize and correlate data security through a single pane of glass to protect cloud-native and traditional database workloads in real time

Governed secure enterprise data plane



Breaking down silos with Guardium



Cloud Pak for Data with
Guardium Data Protection

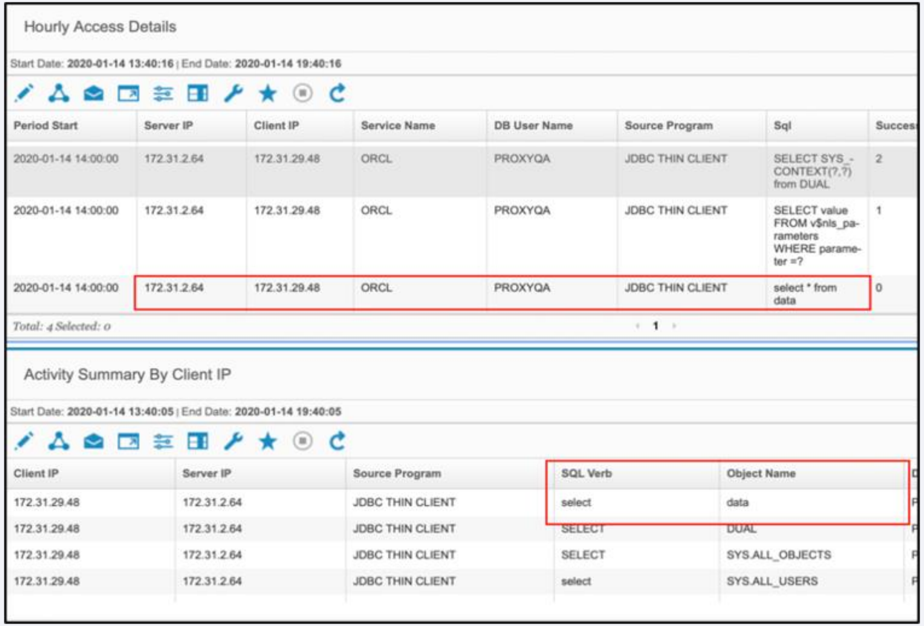
Data security that creates value

- ✓ Reduce time it takes to enable monitoring of sensitive database services **by 50%**
- ✓ Achieve compliance and privacy related process efficiency. Reduce the time required to prepare for a database audit **by 89%**
- ✓ Decrease the time to detect and respond to suspicious activities **by 42%**

Extend real-time database monitoring to containerized database environments

Guardium External S-Tap deployed as a light-weight auto-scalable microservice to simplify data protection across hybrid multi-cloud environments.

1. Organically built on S-TAP technology
2. Modern, container-based technology certified for Docker Hub and RHOS
3. Simplified operational management with Kubernetes
4. Fine-grained visibility into the encrypted database traffic, including local traffic*
5. Clear separation of duties between database access and the processes responsible to monitor behavior
6. Built-in high availability and resiliency (fail-over) with less than 2% latency
7. Support: Azure, AWS, Google Cloud, IBM Cloud, IBM Cloud Pak for Data



Hourly Access Details

Start Date: 2020-01-14 13:40:16 | End Date: 2020-01-14 19:40:16

Period Start	Server IP	Client IP	Service Name	DB User Name	Source Program	Sql	Succes
2020-01-14 14:00:00	172.31.2.64	172.31.29.48	ORCL	PROXYQA	JDBC THIN CLIENT	SELECT SYS_CONTEXT(?,?) from DUAL	2
2020-01-14 14:00:00	172.31.2.64	172.31.29.48	ORCL	PROXYQA	JDBC THIN CLIENT	SELECT value FROM v$nls_parameters WHERE parameter =?	1
2020-01-14 14:00:00	172.31.2.64	172.31.29.48	ORCL	PROXYQA	JDBC THIN CLIENT	select * from data	0

Total: 4 Selected: 0

Activity Summary By Client IP

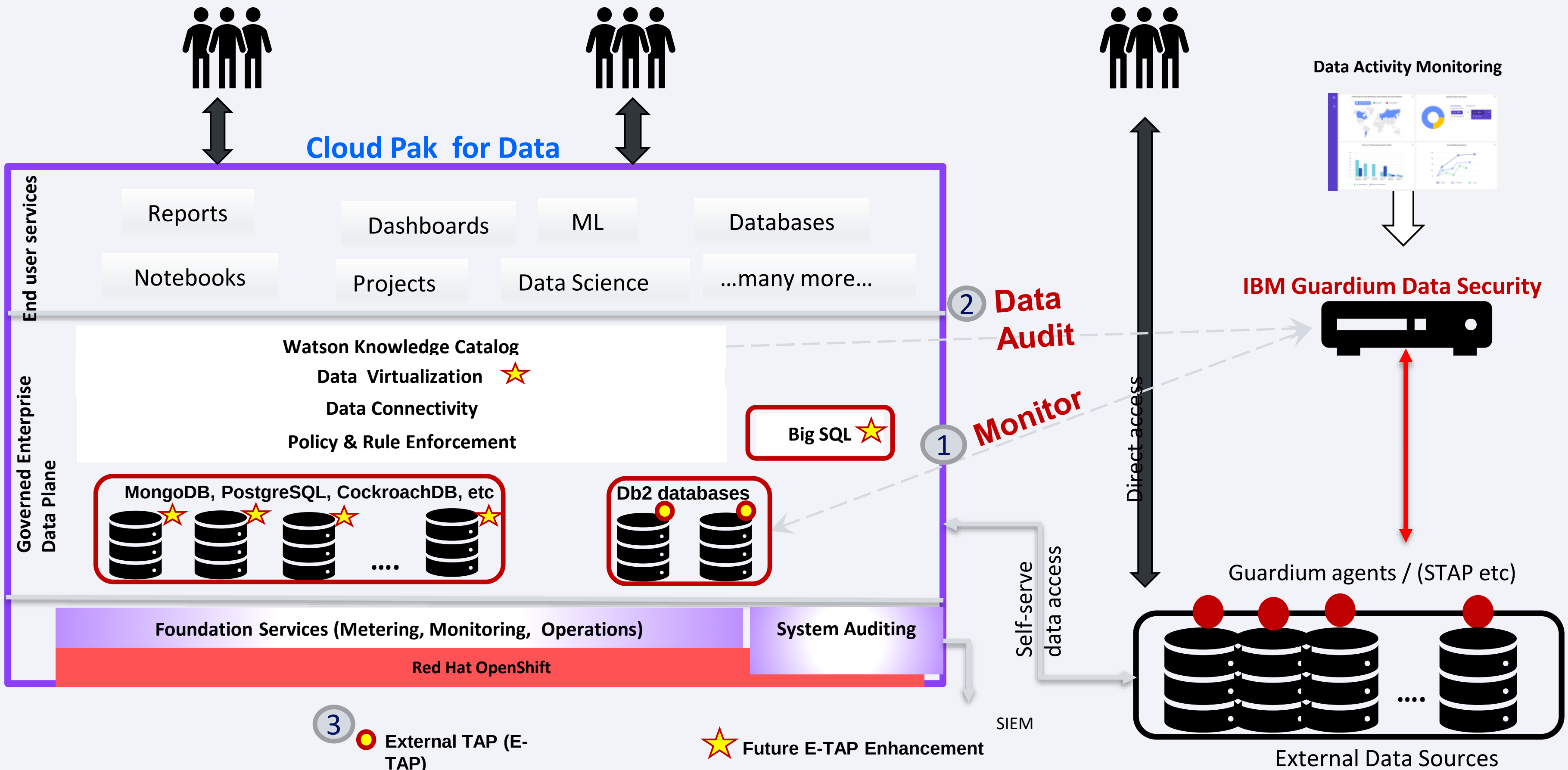
Start Date: 2020-01-14 13:40:05 | End Date: 2020-01-14 19:40:05

Client IP	Server IP	Source Program	SQL Verb	Object Name
172.31.29.48	172.31.2.64	JDBC THIN CLIENT	select	data
172.31.29.48	172.31.2.64	JDBC THIN CLIENT	SELECT	DUAL
172.31.29.48	172.31.2.64	JDBC THIN CLIENT	SELECT	SYS.ALL_OBJECTS
172.31.29.48	172.31.2.64	JDBC THIN CLIENT	select	SYS.ALL_USERS

* Requires configuration

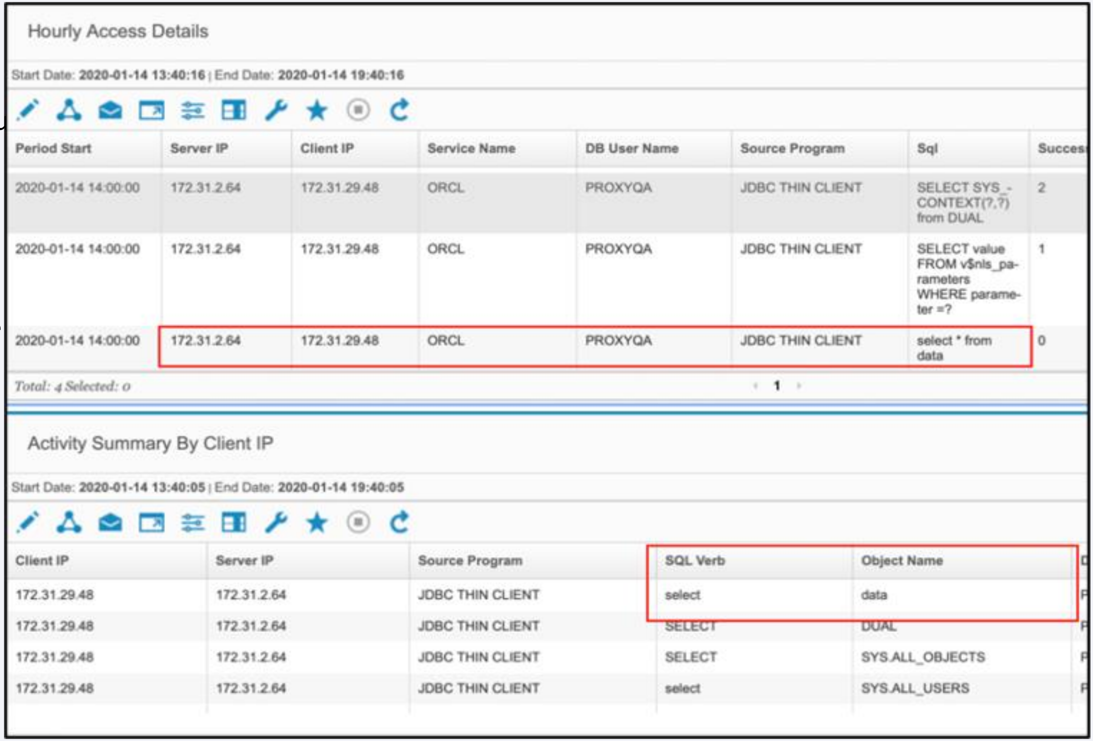
Governed Secure Enterprise Data Plane

Provide safe, trusted self-served data for Analytics



Guardium External S-TAP

1. Organically built on S-TAP technology
2. Modern, container-based technology certified for Docker Hu
3. Simplified operational management with Kubernetes
4. Fine-grained visibility into the encrypted database traffic, including local traffic*
5. Clear separation of duties between database access and the processes responsible to monitor behavior
6. Built-in high availability and resiliency (fail-over) with less than 2% latency
7. Support: Azure, AWS, Google Cloud, IBM Cloud


Hourly Access Details

Start Date: **2020-01-14 13:40:16** | End Date: **2020-01-14 19:40:16**

Period Start	Server IP	Client IP	Service Name	DB User Name	Source Program	Sql	Succes
2020-01-14 14:00:00	172.31.2.64	172.31.29.48	ORCL	PROXYQA	JDBC THIN CLIENT	SELECT SYS_-CONTEXT(?,?) from DUAL	2
2020-01-14 14:00:00	172.31.2.64	172.31.29.48	ORCL	PROXYQA	JDBC THIN CLIENT	SELECT value FROM v$nls_pa-rameters WHERE parame-ter =?	1
2020-01-14 14:00:00	172.31.2.64	172.31.29.48	ORCL	PROXYQA	JDBC THIN CLIENT	select * from data	0

Total: 4 Selected: 0 1

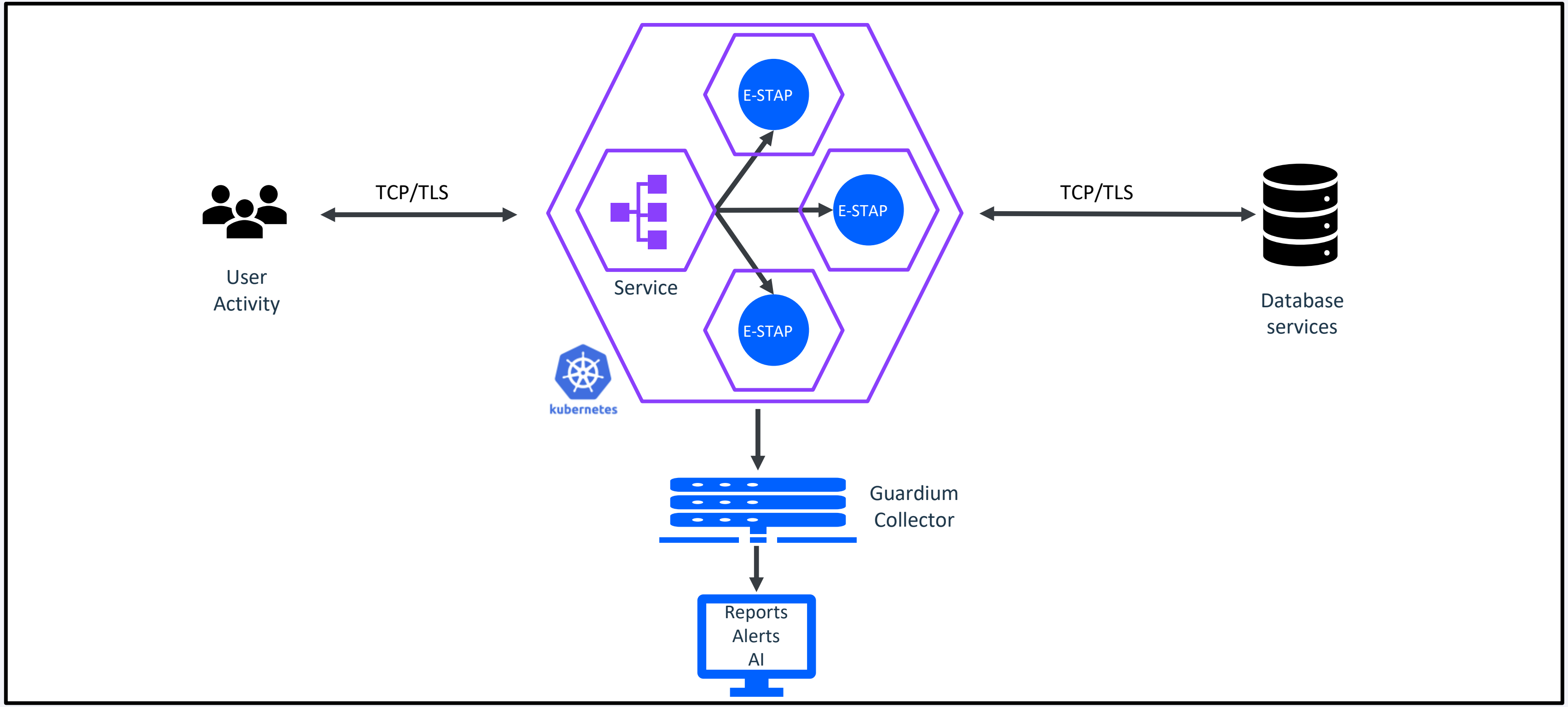
Activity Summary By Client IP

Start Date: **2020-01-14 13:40:05** | End Date: **2020-01-14 19:40:05**

Client IP	Server IP	Source Program	SQL Verb	Object Name
172.31.29.48	172.31.2.64	JDBC THIN CLIENT	select	data
172.31.29.48	172.31.2.64	JDBC THIN CLIENT	SELECT	DUAL
172.31.29.48	172.31.2.64	JDBC THIN CLIENT	SELECT	SYS.ALL_OBJECTS
172.31.29.48	172.31.2.64	JDBC THIN CLIENT	select	SYS.ALL_USERS

* Requires configuration

Guardium External-TAP V11.x deployment



IBM Cloud Pak for Data (CP4D 3.x) + IBM Security Guardium (v11.2)

1. Pre-built framework to secure database services
2. Proactively configure and monitor database services hosted on CP4D with External-TAP Service
3. Pre-built template can be used to configure and simplify the deployment of External-TAP on the CP4D platform
4. Fine-grained and real-time visibility into the encrypted database traffic (including local traffic) with ability to take proactive actions such as blocking and redaction
5. Clear separation of duties between database access and processes responsible to monitor
6. Expand the realm of data governance, and management into security by facilitating integration with broader security eco-system

1. External-TAP certified for OpenShift Container Platform
2. Data sources: DB2 WH, DB2