Modern Cybersecurity solutions for today's business challenges

Valia Demesticha
Senior Sales Representative, IBM Security Software – Technology Unit, IBM Greece

Katerina Zervonikolaki
CyberSecurity Sales Engineer, Performance Technologies

IBM Security

IBM

Business priorities are driving digital transformation

Users and Endpoints
Accessing from anywhere
using any device

Data and Apps
Data is a shared resource
for users and apps

Infrastructure
Servers and networks distributed
across hybrid cloud environments

Security needs to safeguard these key transformations, but that can be a challenge...

Traditional security can't keep pace

Too much to do

- Meet with CIO and stakeholders
- Nail down third-party risk
- Manage GDPR program with privacy office
- Respond to questions from state auditors
- Update CEO for board meeting
- Update budget projections
- Write security language for vendor's contract
- Make progress on the never-ending identity project
- Review and updated project list
- Edit communication calendar
- Update risk rankings on security roadmap
- Clarify policies governing external storage devices
- Provide testing and encryption tool direction
- Provide data handling best practices
- Send new best practices to development teams
- Review logs for fraud ongoing investigation
- Help with insider threat investigation
- Determine location of sensitive data in cloud
- Investigate possible infection of new app
- Continue porting of new business mobile app
- Help architect network instance
- Answer security policy email
- Format security status report for executives
- Meet with recruiter to discuss staffing
- Write test plan requirements for new products
- Meet regarding improving security of facilities

Too many vendors

Too much complexity

Too many alerts

Too many silos

Identity and Access Management → Data Security → Application Security → Network Security → Endpoint Security

Organizations need a modern, open, Zero Trust approach to security

Security Challenges

| Cloud Security	Advanced Threats	Compliance and Privacy	Skills Shortage	Mobile, Edge and IoT / OT

IBM Solutions

IBM Security

Align
your security strategy to your business

Protect
digital users, assets, and data

Manage
defenses against growing threats

Modernize
your security with an open, multicloud platform

IBM Differentiation

Deep Expertise   AI-Driven Technology   Open Platform   Largest Ecosystem

Hybrid multicloud environments exacerbate key data security challenges for organizations
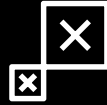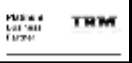
Stop threats before they disrupt business

$5.33 M

Average total
cost of a breach
at enterprises
of more than 25,000
employees

Achieve regulatory compliance

$2.30 M

Average difference in
cost of a breach
at organizations with
high level vs. low level
of compliance failure

Keep up with the data sprawl

$1.66 M

Average difference in
cost of a breach
at organizations with
high level vs. low level
of cloud migration

287 days

Average time to identify and contain
a data breach

A smarter, continuous approach is needed to address data security challenges

Discover
Discover and classify your sensitive data across on-premises and cloud data stores

Protect
Protect sensitive data through policies and data activity monitoring

Analyze
Analyze and harden against risks and vulnerabilities with advanced analytics and assessments

Respond
Respond to threats in real-time and send actionable alerts to security operations systems

Comply
Comply with data privacy and security regulations, and simplify auditing and reporting

IBM **Security** Guardium Data Protection

Guardium Data Protection accelerates data discovery, improves accuracy, and saves time

Discover

50%

increase in data classification accuracy

Protect

43%

increase in data threat detection accuracy

Analyze

67%

increase in discovering data source vulnerabilities and misconfigurations

Respond

42%

decreased time remediating data security issues

Comply

**89%**

reduced time spent preparing for an audit

Guardium Data Protection

Discover and classify sensitive data across on-premises and cloud environments

- Automatically discover databases or import assets manually. Define & map applications to their data sources

- 100+ data discovery patterns help to identify regulated data in your environment

Protect sensitive assets with data activity monitoring

- Define rule-based policies to monitor, log, report & alert on unauthorized data access

- Customize or use predefined policy templates to meet your audit & compliance requirements

- Variety of agent-based and agentless options to protect data on-premises & in the cloud
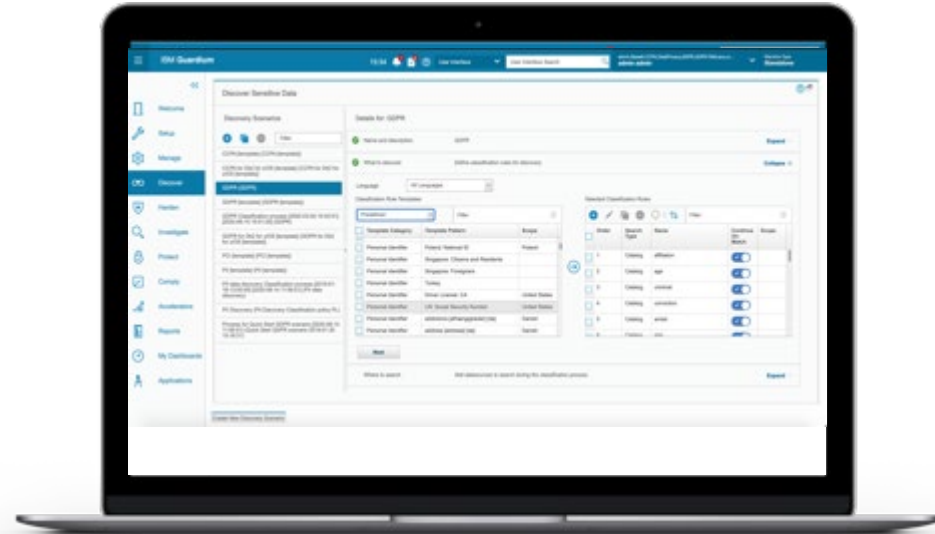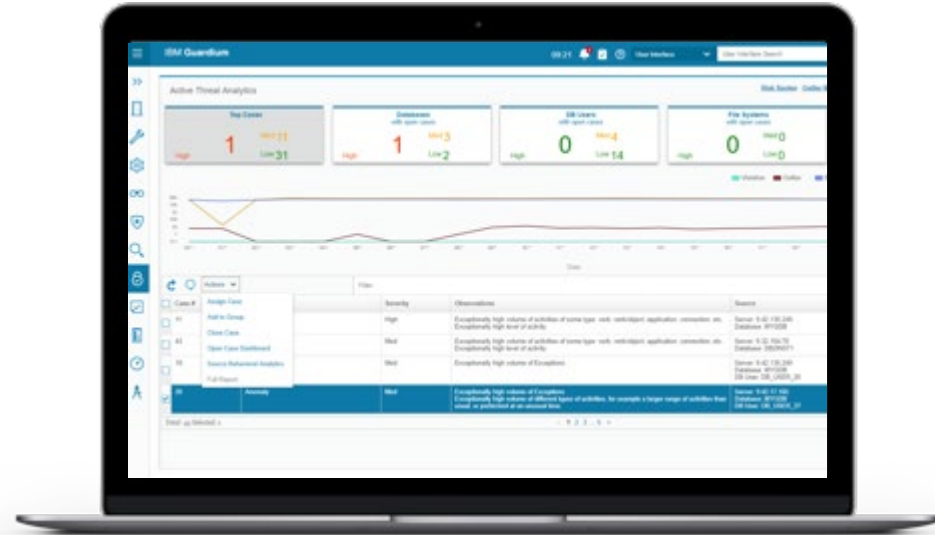
Guardium Data Protection

Analyze and harden your environments for vulnerabilities

- Proactively scan for vulnerabilities across heterogenous platforms using more than 3000 assessments

- Investigate user risk details to determine the "Who?", "What?", "When?" and "Where?" of an event with threat analytics

Respond to threats in real-time

- Quickly uncover and respond to suspicious user activity and external threats by blocking or quarantining suspicious users in real-time

- Initiate remediation of security gaps by integrating with security operations solutions to close the loop on exposures

Guardium Data Protection

Comply with regulations and simplify auditing and reporting through automation

- Automate tracking and reporting for regulatory compliance with pre-built templates for a quick start

- Add tagging to multiple policies and rules to enable easier and faster policy management

- Track progress towards compliance on all selected regulations from a single interface

- Accelerate audit activities and confirm separation of duties through a continuous, fine-grained audit trail
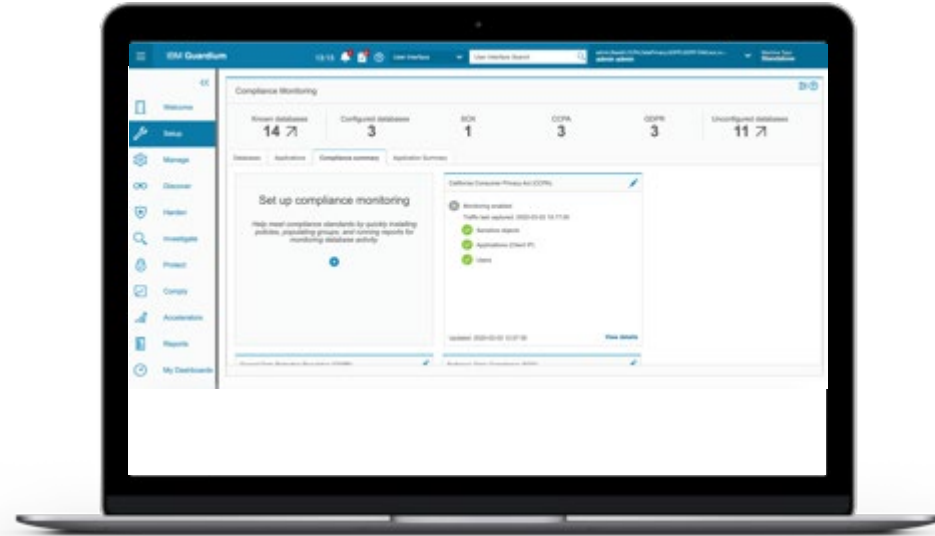
Compliance Key use cases
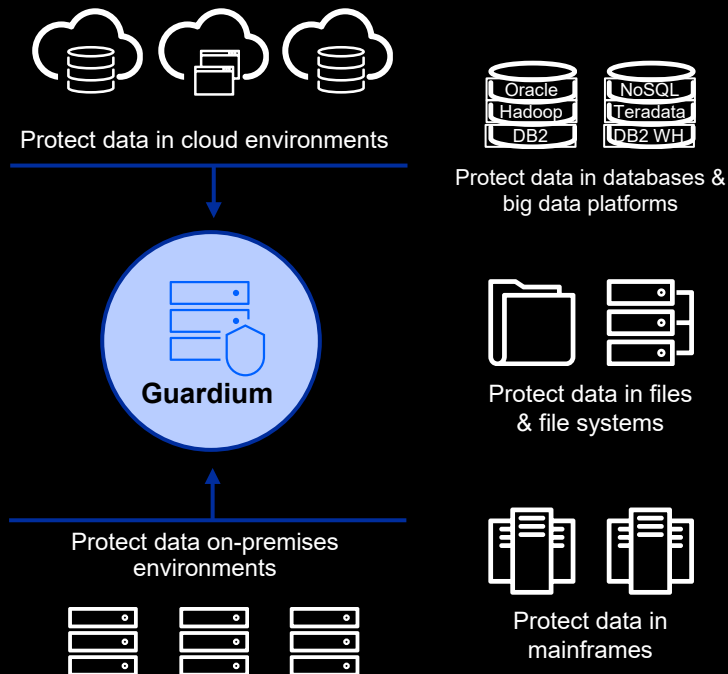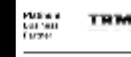
- Audit Requirements

- **PCI compliance**

- **GDPR compliance**

- Security best practice

Audit Requirements	PCI DSS	COBIT (SOX)	ISO 27002	Data Privacy & Protection Laws	NIST SP 800-53 (FISMA)
1. Access to Sensitive Data (Successful/Failed SELECTs)	✓		✓	✓	✓
2. Schema Changes (DDL) (Create/Drop/Alter Tables, etc.)	✓	✓	✓	✓	✓
3. Data Changes (DML) (Insert, Update, Delete)		✓	✓		
4. Security Exceptions (Failed logins, SQL errors, etc.)	✓	✓	✓	✓	✓
5. Accounts, Roles & Permissions (DCL) (GRANT, REVOKE)	✓	✓	✓	✓	✓

Capabilities	Basel II	GDPR	HIPAA	PCI	PII	SOX
Data discovery	X	X	X	X	X	X
Monitoring	X	X		X	X	X
Reports		X		X	X	

Built to protect data on-premises, in the cloud and everywhere in between

Protect data in cloud environments

Oracle Hadoop DB2 / NoSQL Teradata DB2 WH

Protect data in databases & big data platforms

Guardium

Protect data in files & file systems

Protect data on-premises environments

Protect data in mainframes

✓ Supports hybrid multicloud data protection with consistent data security policies across environments holistic risk views

- Databases and data warehouses
- Big Data
- Files
- Mainframe and z/OS
- Cloud: AWS, Azure, Google Cloud, IBM Cloud, Oracle Cloud, Database-as-a-Service

Supported Platform Database for Data Activity Monitoring →

✓ Broad platform support and massive scalability for the largest on-premises and cloud environments

Detailed system requirements and supported platforms →

Start taking a modern, Zero Trust approach to data security

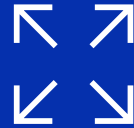## IBM **Security** Guardium Data Protection
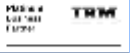
Intelligent

Empower your team to quickly discern and focus on the most significant threats in real-time

Adaptive

Evolve your data security as your data and IT infrastructure change and grow – while reducing costs

Connected

Break down silos to accelerate response and streamline compliance to reduce risk to the business

Clients see results with Guardium Data Protection

IBM SECURITY GUARDIUM BY THE NUMBERS

Reduced probability of a breach by **40%.**

Increased automation saves **79 hours** during database analysis.

Effort required to complete an audit decreased by **75%.**

VOICE OF THE CUSTOMER

"When we use IBM Security Guardium in our database analysis we are able to create reports and custom tables in a matter of minutes."

"I was able to short cut all the manual work we used to have to do for an audit. The compliance templates provided by IBM Security Guardium saved me a lot of time and kept the auditors happy."
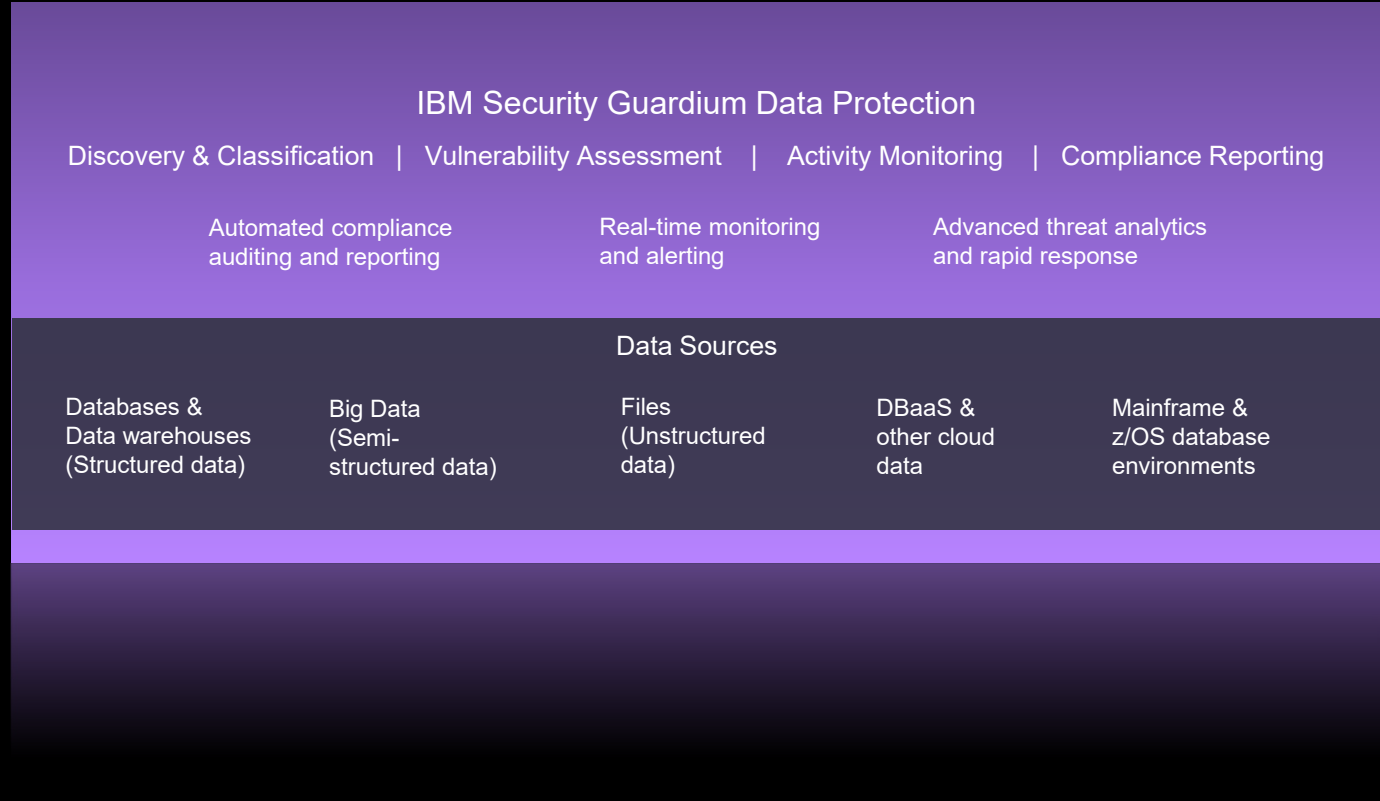
IT security engineer, energy & utilities

IBM Security Guardium Data Protection
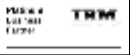
- Discover and classify sensitive data, regardless of whether it's stored on-premises or in the cloud

- Harden your infrastructure with vulnerability scans

- Uncover and respond to threats in real-time
- Use pre-built templates to accelerate your compliance journey

IBM Security Guardium Data Protection

Discovery & Classification | Vulnerability Assessment | Activity Monitoring | Compliance Reporting

Automated compliance auditing and reporting

Real-time monitoring and alerting

Advanced threat analytics and rapid response

Data Sources

Databases & Data warehouses (Structured data)

Big Data (Semi-structured data)

Files (Unstructured data)

DBaaS & other cloud data

Mainframe & z/OS database environments

Thank you!