Deloitte.

IBM

Platinum Partner

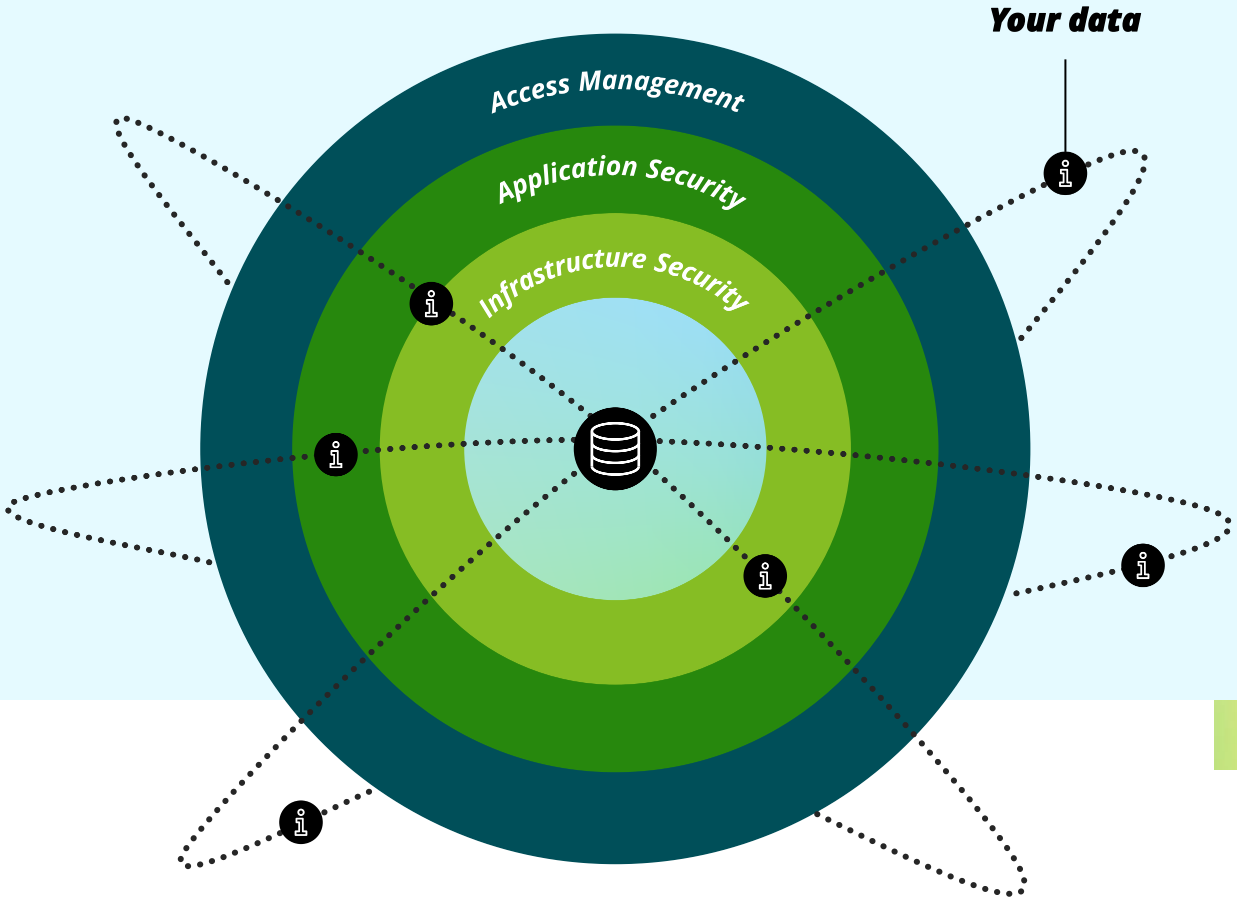
SEPTEMBER 2025

Deloitte Data Protection – Point-of-View (POV)

Powered by the IBM Guardium Suite

Data is the new perimeter

Data moves across applications and locations, making data-centric protection essential. With the advent of AI and Quantum computing, cyberattacks are growing in scale and complexity, and robust data security is no longer optional to help mitigate the potential risk against current and future threats.



- Cloud usage is increasing, and data is no longer confined to traditional perimeters
- Business objectives and next-generation technology require increased data flexibility
- Data continues to grow at an exponential rate
- Regulatory requirements and scrutiny are on the rise
- Cyber criminals are increasingly targeting data due to its value

Data-centric security aligns with business operations to safeguard critical assets in diverse environments and use cases.

Common challenges faced by organizations

AI-driven data growth and technological change demand adaptable security measures that can protect business data now and in the future.

01

Limited visibility into the organization’s data

Business leaders often have limited visibility into their organization’s data, forcing them to protect everything as if it were sensitive.

02

Siloed approach toward data protection

Data protection is often operated separately, instead of being integrated with data governance and privacy.

03

Data across different environments

Organizations are increasingly reliant on cloud services and sharing data with more third parties, which can boost productivity and innovation, but also increase data risk.

04

Embedded, integrated solutions for data protection

No single solution covers all data protection needs: an integrated set of solutions is required.

05

Negative perception from the business

Data protection can be seen as a burden or compliance activity instead of a mechanism to empower the business.

06

Unrealized data value

The growth and proliferation of data makes it increasingly difficult for organizations to manage and derive value from their data.

Data risks are not going anywhere

Cloud providers manage technology, but organizations remain responsible for their data, including its posture management, compliance, security and maintenance.

On-premise Data Center	**Public Cloud** Infrastructure as a Service (IaaS)	**Public Cloud** Platform as a Service (PaaS)	**Public Cloud** Software as a Service (SaaS)
■ Data	■ Data	■ Data	■ Data
■ Application	■ Application	▣ Application	□ Application
■ Operating System	▣ Operating System	□ Operating System	□ Operating System
■ Infrastructure	□ Infrastructure	□ Infrastructure	□ Infrastructure

■ Organization’s responsibility ▣ Organization shares control with service provider □ Service provider’s responsibility

Organizations need AI-powered data protection solutions based on today's threats

Modern cyber security solutions require dynamic identification and protection of sensitive information while continuously monitoring data movements, performing advanced threat analysis, and deploying rapid response for detected threats:

Discover

Continuously discover/monitor data across cloud and Software-as-a-Service (SaaS) environments; find sensitive, regulated, and shadow data across hybrid sources; classify data; map flows; and uncover vulnerabilities.

Artificial Intelligence/ Machine Learning (AI/ML) capabilities:

- Classify and label sensitive data
- Track data movements
- Detect vulnerabilities and compliance violations

Protect

Safeguard sensitive and regulated data, both in the cloud and on-premise using advanced protections, including real-time alerting, encryption, redaction, masking, and automated remediation across platforms and data sources.

AI/ML capabilities

- Define security and compliance policies
- Detect unauthorized access and suspicious activities
- Provide real-time alerts
- Enable dynamic data masking, redaction, blocking, and quarantining

Monitor

Uncover anomalous database activities and gain visibility into risky user behavior by continually monitoring activity and the behavior of privileged users for anomalies and outlier detections.

AI/ML capabilities

- Use outlier detection capabilities to monitor and identify abnormal user and server behavior
- Improved risk identification of possible breaches
- Facilitate investigations by reviewing detailed context of anomalous activities

Analyze

Evaluate real-time application connections, classify them by trust level, and provide real-time alerts for potential threats.

AI/ML capabilities

- Surface potential threats using advanced analytics
- Detect risky/untrusted database connections in real- time
- Continuously evaluate real-time application connections
- Classify connections and assign trust scores
- Provide real-time alerts

Respond

Use Artificial Intelligence (AI)-based analytics and context-based risk scoring to automate investigation and remediation, speeding up response times.

AI/ML capabilities

- Use AI-powered analytics and context-based risk scoring
- Tag results as high, medium, or low via a risk-scoring engine
- Automate remediation processes (e.g., opening tickets, cases, enriching playbooks)
- Share insights and threats with stakeholders for further investigation

A forward-looking approach to addressing challenges

Deloitte’s perspective looks at business and security objectives in today’s marketplace as intertwined.

Traditional data protection approach

Restrictive solutions that are applied in a blanket fashion, which can increase security but hamper the business.

Mandates and requirements (policies/standards) that are not accompanied by enabling capabilities.

Point solutions that solve specific use cases, but don’t integrate with the broader program, leading to missed opportunities.

Deloitte’s perspective

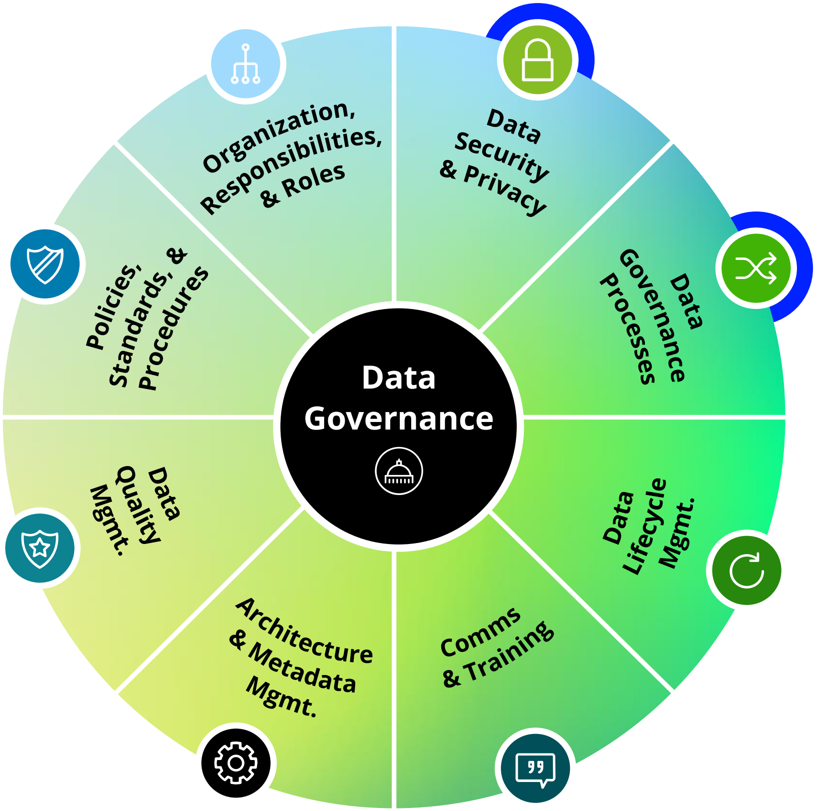
Team with the business to develop integrated solutions that contribute to business initiatives and security goals by design.

“Lighten the load” by deploying capabilities that help increase visibility, automation, and protection to address requirements.

Integrated capabilities that increase data management/security effectiveness, accuracy, and coverage when working in unison.

Data Security is a foundational component of effective Data Governance

Effective Data Security protects an organization's data from mismanagement, unauthorized access, breaches and misuse.


Data Governance
Organization, Responsibilities, & Roles
Data Security & Privacy
Data Governance Processes
Data Lifecycle Mgmt.
Comms & Training
Architecture & Metadata Mgmt.
Data Quality Mgmt.
Policies, Standards, & Procedures

Key Components of Data Security in Data Governance

Accessibility: Define and consistently enforce who can access specific data sets.

Discovery and Classification: Detect known and unknown sensitive data across hybrid environments, whether at rest, in motion, or in overlooked data sources.

Encryption: Protect data at rest and in transit using modern, flexible encryption technologies that can adapt to new threats.

Monitoring & Auditing: Leverage modern tools that improve audit readiness with integrated policies, automated workflows, and tamper-proof logging and reporting.

Data Masking: Apply automated techniques to scramble/obscure sensitive information in non-production environments or when sharing data externally.

Incident Response: Establish clear, actionable procedures for responding to data breaches or security incidents that include notification, containment and remediation steps.

Key Integration Points of Data Security with Data Governance Processes

Policy Development: Data Governance will define and maintain policies and standards for Data Security, such as Acceptable Usage, Data Retention, and handling Sensitive and/or Confidential Information.

Data Stewardship: Assign Data Stewards responsible for ensuring Data Security controls are properly implemented and consistently maintained for their respective data domains.

Risk Management: Identify, assess and mitigate risks to Data Security as part of Governance Risk Management procedures, prioritizing high severity risk mitigation efforts.

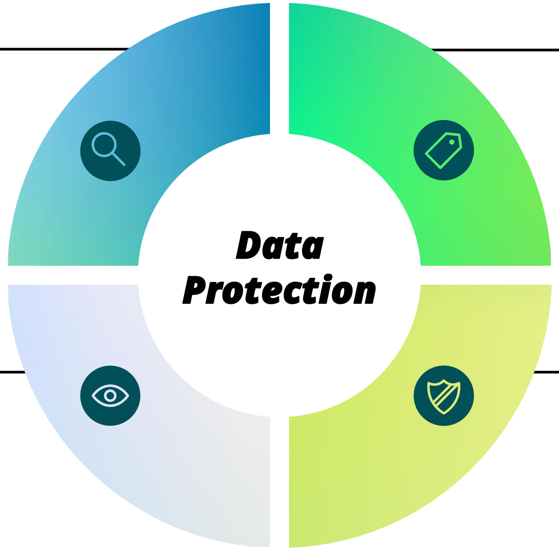
Compliance: Monitor and control Data Security activities, tools and outputs to confirm that they consistently meet regulatory requirements (e.g., General Data Protection Rule -GDPR, Health Insurance Probability and Accountability Act - HIPPA, California Consumer Privacy Act - CCPA) and industry standards.

The potential benefits of embedding data security into Data Governance:

- Reduced risk of data breaches
- More trust in the organization's data
- Strengthened regulatory compliance
- Improved operational efficiency

Deloitte's data protection framework enables data security

Deloitte organizes data protection into four (4) key pillars that work in tandem to improve efficiency, monitor and control capabilities, decision-making and overall data security:



Discover

Locate sensitive data to better target controls.

- Automatically discover databases or import assets manually. Define and map application data sources.
- 100+ data discovery patterns help to identify regulated data in your environment.

Classify

Classify sensitive data across on-premise and Cloud.

- Provides visibility and context into structured and unstructured data using network analytics, Artificial Intelligence, and Machine Learning.

Monitor/Enforce

Track sensitive data to spot and stop unauthorized activity.

- Reporting and Alerting
- Data Loss Prevention (DLP)
- Data Activity Monitoring (DAM)

Protect

Restrict sensitive data to approved users.

- Encryption, Tokenization, Masking, and Redaction
- Key and Certificate Management (KCLM)
- Data Access Governance (DAG)

Value to the Business

Risk mitigation

- Early detection and neutralization of security threats
- Continuous adherence to regulatory standards and requirements

Cost efficiency

- Lower expenses through automation and streamlined processes
- Reduced financial impact from potential data breaches

Comprehensive insight

- Complete overview of data security across environments
- Instantaneous tracking and analysis of security activities

Enhanced governance

- Consistent implementation of security policies across the organization
- Comprehensive systems for protecting sensitive data

The IBM Guardium Suite empowers Deloitte’s data security approach

Deloitte is teaming with IBM to deploy IBM’s Guardium Suite of products based on their enterprise-wide data protection capabilities and tight alignment with Deloitte’s data security approach:

Discover

Guardium Discover and Classify: Understand the location of sensitive data is an essential first step in data protection. IBM Guardium Discover and Classify classifies structured and unstructured data whether it is at rest or in transit. The platform automates the identification of sensitive data across both on-premise and cloud environments.

Guardium AI Security: Organizations are encouraged to secure their AI systems while assessing the risks associated with AI deployments and ways to address them. IBM Guardium AI Security is designed to help discover shadow AI, secure various AI models and use cases, to provide real-time protection.

Monitor/Enforce

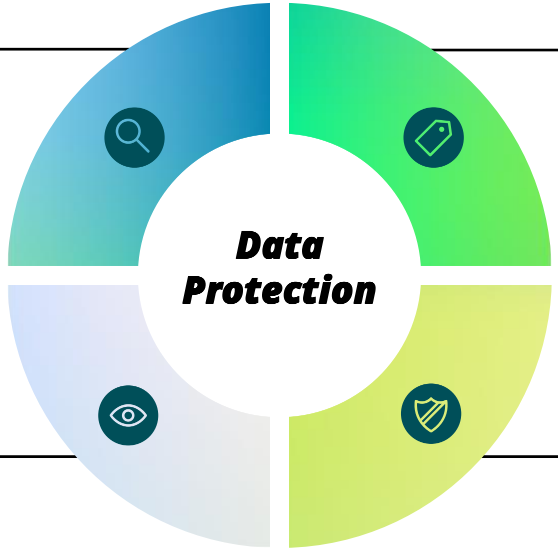
Guardium Data Detection and Response (DDR): Monitor critical data stores, detect threats, and leverage AI and SOC integration for robust monitoring capability.

Guardium DSPM: Analyze entitlements and logs to determine where data can go and is currently going. Detects vulnerabilities and provides automated remediation responses.

Guardium AI Security: Detect vulnerabilities, monitor classified and controlled unclassified information (CUI), data access, and integrate with IBM watsonx.governance.

Guardium Data Protection: Monitor privileged activities in on-premise and cloud data stores to detect violations and produce logging reports.

Guardium Quantum Safe: Track cryptographic posture and vulnerability remediation progress.



Classify

Guardium Discover & Classify: Understanding the location of sensitive data is an essential first step in data protection. IBM Guardium Discover & Classify locates known and unknown sensitive information across various environments. The platform classifies this data according to sensitivity and generates detailed risk assessments.

Guardium Quantum Safe : Classifies cryptography data in a Cryptography Bill of Materials (CBOM) by risk level

Protect

Guardium Data Protection: IBM Guardium Data Protection is a software platform designed to assist security teams in protecting sensitive data through automated discovery, classification, vulnerability assessment, and threat detection processes.

Guardium Data Compliance: Define and enforce custom data security policies and provide workflows and reports. Integrate with Cloud Pak for data to provide data masking while building a data fabric across a hybrid cloud landscape. Scan for vulnerabilities.

Guardium AI Security: The solution includes features to vulnerability scan Large Language Models (LLM’s) for vulnerabilities, provide real-time protection against malicious prompts, and detect policy violations.

Guardium Quantum Safe and Remediator: Identifies and addresses cryptographic vulnerabilities to protect your data and provide remediation recommendations and provides recommendations to mitigate cryptography vulnerability risks

IBM Guardium Key Lifecycle Manager: Provides encryption key management and centralized control for keys associated with IBM and non-IBM storage infrastructure, including cloud-based storage and applications, to help facilitate integration and enhance data security.

Why work with Deloitte for data security?

01

Regulatory, Industry, and Technical Experience

Deloitte's cyber teams possess deep experience assisting clients within regulated sectors to address compliance with complex frameworks such as GDPR, HIPAA, and SOX. Our technical specialists in data security and protection have supported organizations across various industries.

02

Enhancing Cyber Maturity

We work collaboratively to fortify an organization's security posture by evaluating existing capabilities, identifying areas for improvement, and implementing tailored solutions in collaboration with IBM.

03

Integrated Security Solutions

Deloitte facilitates the smooth integration of data protection suites into broader security infrastructures, including SIEM, digital identity, and endpoint management systems. Our approach can safeguard on-premise, cloud, hybrid, or multi-cloud environments, enabling visibility, control, and auditability.

04

Measurable Risk Mitigation: Deloitte's security solutions can deliver demonstrable reductions in risk, including:

- Lower likelihood of data breaches and regulatory sanctions
- Enhanced incident response and recovery capabilities
- Strengthened trust among customers and regulators
- Increased support for secure digital transformation initiatives

05

Trusted Advisor and Managed Services Provider

Ranked #1 by revenue in the Gartner® Market Share Analysis: Security Services, Worldwide, 2024 Report[1], Deloitte provides proactive, ongoing strategic guidance and support to its security clients as cyber threats and regulations evolve. We are committed to serving as your trusted cyber advisor, focused on helping you safeguard your enterprise security while supporting your business objectives.

[1] Gartner, Market Share Analysis: Security Services, Worldwide, 2024, Esha Bhatia, Shailendra Upadhyay, Tarun Rohilla, Bryan Haley, Travis Lee, Rahul Yadav, Ashita Joshi, 12 June 2025.

Gartner is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions on Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

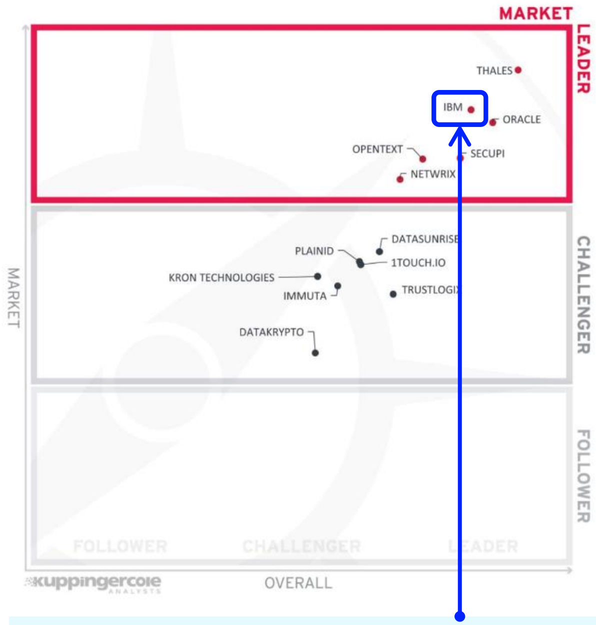
The IBM Guardium Suite provides flexibility and interoperability

The IBM Guardium Suite supports a choice of deployment models, a universal token system to be used across modules without advanced planning and enables the ability to easily explore and activate new models and scale by adding tokens as needed.

	Client-managed	***SaaS***
Discovery and classification	• IBM Guardium Data Protection • IBM Guardium Discovery & Classify (separate transaction)	IBM Guardium DSPM
Secure posture management	IBM Guardium Vulnerability Assessment	IBM Guardium DSPM
Risk detection & analytics	IBM Guardium Data Protection	IBM Guardium DDR (with GDP data)
Long-term data retention	IBM Guardium Data Protection	IBM Guardium DDR (with GDP data)
Compliance accelerators	IBM Guardium Data Protection	N/A
Data activity monitoring	IBM Guardium Data Protection	N/A
Discover and protect AI	N/A	IBM Guardium AI Security
Encryption	IBM Guardium Quantum Safe	N/A

The IBM Guardium suite is a market leader for enterprise data security

The data security market is fast-changing and competitive. Organizations need solutions that secure all types of data sources to help meet compliance requirements.



"IBM Guardium Data Security Center is a highly capable enterprise-grade data security solution, well-suited for large organizations requiring scalable, policy-driven security and compliance enforcement. Its comprehensive monitoring, broad integration support, and flexible deployment options make it an impressive option in the even-changing landscape of data security." [1]

IBM Guardium is a trusted leader in data security

4 of 5
Top global healthcare orgs

4 of 5
Top US banks

4 of 5
Top global insurance institutions

7 of 10
Top global telecom companies

4 of 5
Top global financial service orgs

3 of 5
Top US retailers

TrustRadius Awards[2]

TrustRadius Buyer's Choice 2025 ★★★★★

TrustRadius Top Rated 2025 ★★★★★

TrustRadius Trusted Seller

[1] KuppingerCole Analysts Leadership Compass for Data Security Platforms 2025, IBM, https://www.ibm.com/account/reg/us-en/subscribe?formid=urx-53611

[2] IBM Guardium, TrustRadius, https://www.trustradius.com/products/ibm-guardium/reviews

Data security requires quantum cyber readiness

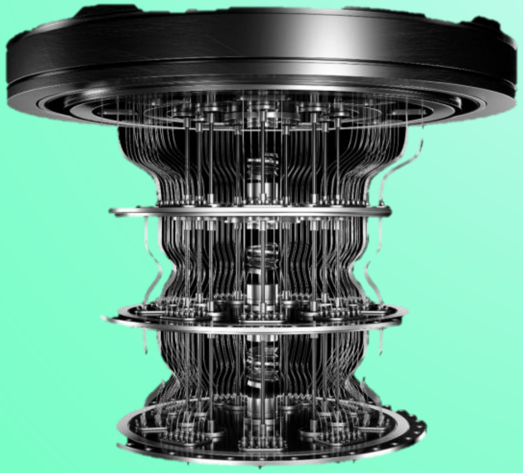
Modernized infrastructure and the advent of quantum computing necessitate a forward-thinking approach to cybersecurity. Quantum cyber readiness is at the forefront of this evolution.

The Next Frontier: Quantum cyber readiness

Quantum computing is no longer a distant dream. It may soon become a reality that, in the next 5 to 10 years, redefines how organizations across industries harness the power of data, run their businesses, and mitigate risk.

Quantum cyber readiness powered by IBM:

Deloitte's Quantum Cyber Readiness approach combined with IBM's Guardium Quantum Safe product prepare organizations for future challenges posed by quantum computing. IBM Guardium Quantum Safe provides organizations the ability to build an inventory of their encryption, analyze it to see if it is quantum ready, and provide remediation capability to address gaps found during analysis.



Strengthen cryptography today.

Become quantum cyber-ready for tomorrow.

Quantum cyber readiness with IBM Guardium Quantum Safe

Prepare your organization for quantum cyber readiness.

IBM Guardium Quantum Safe

Crypto inventory

Build a cryptographic inventory by comprehensively scanning and ingesting data such as source repositories and vulnerability scanners.

Evaluate posture

Evaluate your organization's posture based upon findings, such as library types, versions, cipher strengths, endpoints, and protocols employed.

Policy & vulnerabilities

Drill down into specific vulnerabilities, including remediation recommendations, opening tickets to put fixes into motion.

Track progress

Track the organization's posture over time by tracking progress of open vulnerabilities and policy violations.

Deloitte can support your quantum protection journey with an experienced team ready to help you better understand the risks and implement quantum-resistant cryptographic algorithms to protect your organization and data, now while also preparing for the future.

Cybersecurity in the era of Generative AI

Security for AI

Protecting foundation models, generative AI, and their data sets is essential for enterprise-ready AI.

- Secure the underlying AI input data by protecting it from data theft, manipulation, and avert compliance violations.
- Secure model development by scanning for vulnerabilities in the pipeline, hardening integrations, and enforcing policies and access.
- Secure the usage of AI models by detecting data or prompt leakage, and alerting on evasion, poisoning, extraction, or inference attacks.

AI for Security

Productivity gains from foundation models and Generative AI will reduce human bottlenecks in security.

- Manage repetitive security tasks such as summarizing alerts and log analysis, freeing teams to tackle strategic problems.
- Generate security content (detections, workflows, policies) faster than humans, expediting implementation and adjusting to changing security threats in real-time.
- Learn and create active responses that optimize over time, with abilities to find all similar incidents, update affected systems, and patch vulnerable code.

AI security with IBM Guardium AI Security

Guardium AI Security offers a robust solution to manage the security of your AI assets, including AI agents, and bring together security and governance teams on a single set of metrics, for secure and trustworthy AI.

IBM Guardium AI Safe

[1]Source: IDC MarketScape: Worldwide Artificial Intelligence Services 2025 Vendor Assessment, doc #US52978525, July 2025). This is the fourth time Deloitte has been recognized as a Leader by the IDC MarketScape in this market.

Shadow AI

Discover your AI deployments, including training and retrieval-augmented generation (RAG) data, models, and the applications that are utilizing these models.

Uncover vulnerabilities

Quickly determine if data and models are vulnerable to attack, poisoning, exfiltration, and manipulation, including mapping to the OWASP top 10.

Drill down and monitor

Drill down into training data, understand classification and sensitivities, and monitor ongoing access and entitlements to data supporting models, including prompt monitoring, leveraging an AI gateway to scan and protect prompts.

Govern with Watsonx

Import discovered AI inventories into watsonx.governance to fully manage the lifecycle of the model including bias, drift, tolerance, and more.

Deloitte is a named Leader in AI Services by the IDC MarketScape[1] and will leverage AI thought leadership and resources to help you custom design the right AI Security Program for your organization and business objectives.

Take the next step. Connect with our leaders.

Colin Soutar

Managing Director
Deloitte & Touche, LLP
csoutar@deloitte.com • LinkedIn

Dan Poliquin

Principal
Deloitte & Touche, LLP
dpoliquin@deloitte.com • LinkedIn

Scott Glover

Specialist Leader
Deloitte & Touche, LLP
scglover@deloitte.com • LinkedIn

Annamarie Hill

Managing Director
Deloitte Consulting, LLP
annhill@deloitte.com • LinkedIn

Deloitte.

IBM
Platinum Partner

Thank you.

This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.

Product names mentioned in this document are the trademarks or registered trademarks of their respective owners and are mentioned for identification purposes only. Deloitte is not responsible for the functionality or technology related to the vendor or other systems or technologies as defined in this document.

As used in this document, 'Deloitte' means Deloitte Consulting LLP, which provides strategy, operations, technology, systems, outsourcing and human capital consulting services; and Deloitte & Touche LLP, which provides audit and risk advisory services. These entities are separate subsidiaries of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.