
IBM Security
A data security strategy built for innovation
IBM

Section 1

A competitive data protection strategy

A data security strategy can propel your business towards agility and competitiveness.

Businesses are embracing hybrid multicloud IT deployments to become more agile and competitive. Yet, as they expand their data footprint across environments, their threat landscape expands as well.

Security and IT leaders must contend with new data security challenges, such as limited visibility, sophisticated cyberattacks and a growing skills shortage, all while working to meet compliance with regulations. Yet, every challenge is also an opportunity.

A holistic, comprehensive data security strategy can help protect your organization and propel it towards a cloud-based, innovative future.

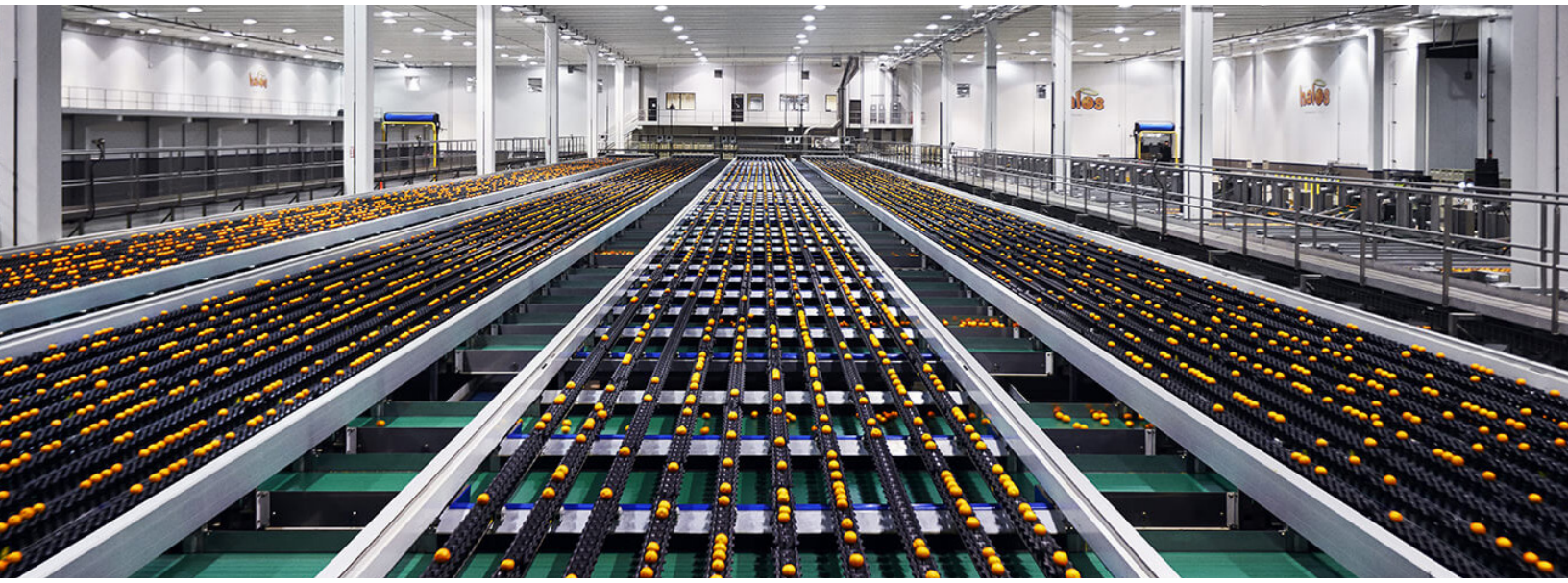
With a unified approach, your data security strategy can help you consolidate a range of tools focused on specific use cases that inundate teams and perpetuate siloed responses. It can help reduce operational

complexity with automated processes and offer your team full visibility on what kind of sensitive data you have, where it is located and who is accessing it, and defend against threats.

With more data created, shared, and stored than ever before, it's time for a smarter approach to data security in the emerging hybrid multicloud world, freeing your business to focus on innovation and strategic technological initiatives.

76%

of organizations predict that remote work increases the difficulty of responding to a potential data breach, which could result in costs of more than $3.8 million on average.[1]



[1] **Cost of a Data Breach Report 2020,** Ponemon Institute, July 2020

Section 2

Create a roadmap to a secure and agile business

Design a security strategy to help your business visualize risk, automate and scale protection.

Our security experts can help design and deploy a data security program that enables yourorganization to remain agile, responsive and secure. The ideal security offering enables your team to visualize risk across disparate environments, automate cumbersome processes and respond to suspicious activity – and is built on flexible architecture that scales as your organization grows.

With a new approach to security, you can:

Monitor data risk everywhere: Understand compliance and protection risk across all of your organization's data regardless of where it resides.

Automate with purpose: Pre-built workflows to simplify processes and mitigate the effects of an industry-wide skills shortage.

Scale to drive digital Transformation: Integrate with other solutions, platforms and infrastructure and reduce operational complexity as your business scales.

"As vendors expand their capabilities to approach data security in a holistic way, improved integrations and a range of granular controls that don't impede employee productivity will dictate which providers will lead the pack." [1]

IBM Data Security Services experts can help build a roadmap for your data security strategy.

Learn more →

[1] The Forrester Wave™: Data Security Portfolio Vendors, Q2 2019, Forrester Research, Inc., June 10, 2019.

Section 3

Leverage data security for digital transformation

A modern data security strategy helps progress, rather than impede technological advancements.

Data security and compliance concerns should not impede technology advancements across your business. In fact, a smarter approach to data security – one that provides full visibility and control over data stored on-premise and in the cloud – frees your organization to expand across the cloud and adopt modern tools for digital transformation.

As you evaluate your security needs, look for an offering that enables you visualize and understand risk holistically across disparate environments, leverage automation to uncover and respond to suspicious activity, integrate data security and compliance processes and tools, and is flexible enough to scale as your business seeks to capitalize on new innovations.

Pillars of a Modern Data Security Strategy:

Understand and visualize data risk:

With data stored on-premise and in the cloud, your team must be able to understand data security and compliance risk across your environment. In-depth correlated insights and analytics can assess risk and implications for your business and help you take informed action.

Automate and simplify:

Seventy-four percent of organizations surveyed report being negatively impacted by a cybersecurity skills shortage. Automation with pre-built workflows can simplify your processes and empower your teams, and automated detection of threats and suspicious activity can help secure your data.

Seamlessly scale to drive digital transformation:

To move or expand workloads across the cloud, support new regulations, adopt modern technologies or drive new innovations, your data protection must scale with your organization. It should integrate with other solutions, platforms, and infrastructures, as well as help to reduce operational complexity and streamline processes.

ESG Publication, The Life and Times of Cybersecurity Professionals 2018, April 2019.

Section 4

A foundation of visibility and automation

Use broad visibility and actionable insights to make decisions that support your data security journey.

A smarter data security strategy can provide you with a more adaptive and integrated approach to safeguarding your critical data across hybrid multicloud environments. With broad visibility and monitoring, actionable insights, and remediation controls, you can make decisions that support your enterprise's data security needs and innovation plans.

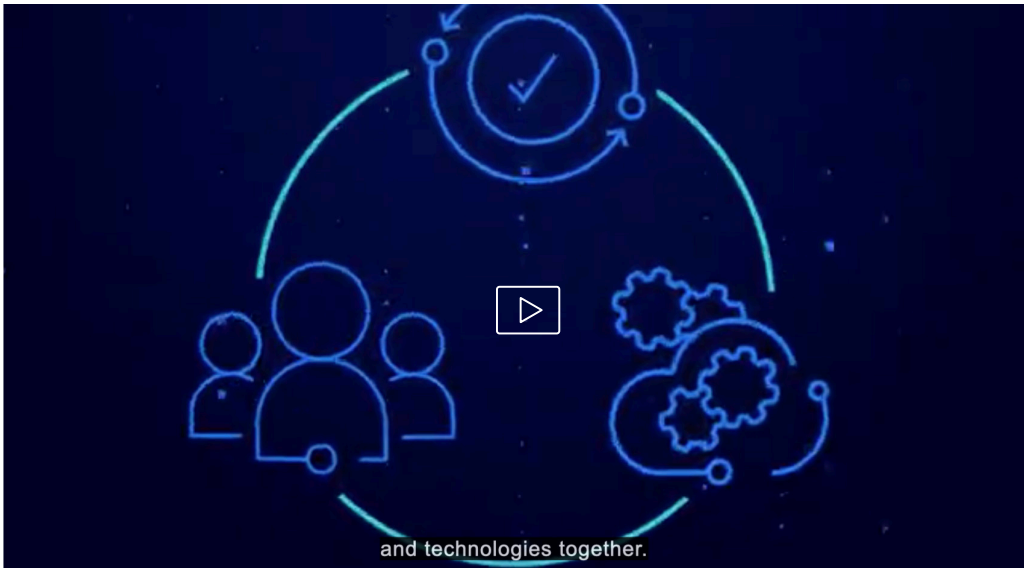
With IBM Security Guardium you can:

See with insight. Centrally monitor and view your data security and compliance posture across on-premises and cloud-hosted data repositories and assess your security and business risk across those environments. Create security and audit reports quickly to detect and examine suspicious activity and potential risk and threat activities.

Automate with purpose. Use guided automated workflows to help you set entitlements and access policies, detect, monitor, block risky behavior, create escalation tickets, and deliver comprehensive compliance reports.

Scale as you innovate. Flexible deployment models and built-in integrations can help expand your data security program to address new compliance requirements and migrate high volumes of data across hybrid multicloud infrastructures.

Watch the video →



[3] ESG Publication, The Life and Times of Cybersecurity Professionals 2018, April 2019.

Section 5

Protect data in the real world

As organizations move to the cloud, security professionals face a set of new challenges as they protect data.

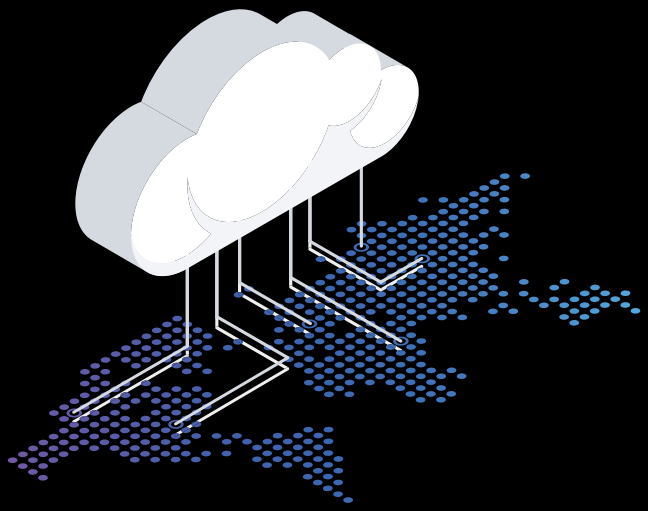
Migration to the cloud, everchanging data compliance requirements and an increase in breaches from inside organizations have changed the data security landscape. Visibility across all data storage locations, automated threat detection and advance analytics can help you identify and respond to threats, while automated and streamlined compliance can ensure you are up to date and compliant with the privacy mandates of each country your data is stored in.

Here's how Guardium's suite of data security solutions can help you navigate and leverage real world scenarios that can impede your data security and compliance journey:

Protect workloads across hybrid multicloud

Cloud deployments often mean your sensitive data is stored in multiple formats and locations. At the same time, you and your team are responsible for ensuring data is protected and in compliance with the industry and government regulations in effect wherever you do business. With a modern security strategy, you can centrally monitor data, identify, and remediate vulnerabilities to give your businesses the confidence to continue storing and accessing information on the cloud.

Guardium helps you manage security across on-premise and multicloud deployments, and provides a consolidated, centralized view of your risk profile and compliance posture. It supports a broad range of databases, which enables you to apply the same data security controls used on premise -- including encryption -- across your hybrid multicloud environment. As cloud computing becomes ubiquitous, Guardium can help you protect data and address compliance as you leverage on-premises and cloud data to drive your business forward.



We surveyed 183 US IT and IT security practitioners in organizations that used Guardium.

43%

reported an improvement in the ability to detect threats[1]

IBM Security Guardium Vulnerability Assessment

Scan for vulnerabilities in your data environment to keep your organization protected

Get started →

Simplify your data compliance journey

Companies are facing more data security and privacy regulations than ever before. Consumers are becoming more educated about their data privacy rights and have greater expectations of transparency, control and protection. Furthermore, penalties for non-compliance are increasing. Given potential negative financial and reputational impact to your brand if data is breached, protecting your sensitive data is more important than ever.

That said, compliance can be a time-consuming, manual process which could make it difficult to begin your compliance journey.

75%

of organizations surveyed identify data privacy as a strategic imperative.[2]

With workflows designed to guide you through requirements and simplify audit reporting, Guardium can help automate and accelerate your efforts to comply with regulations such as the GDPR, CCPA, HIPA.

Guardium can also help you gain visibility into your sensitive and personal sensitive data, wherever it resides, by providing insights into your database vulnerabilities, access entitlements, and configuration issues. Likewise, Guardium can provide detailed audit trails on user and application access to sensitive data sources, as well as manage access to sensitive data and flag unusual behavior.

Westfield CISO Kevin Baker discusses the data privacy and security challenges facing his organization and how the

Watch video →

Defend against insider threats

While threats against organizations are becoming increasingly complex, the majority of data breaches originate from within. Inadvertent insider breaches are often the result of human error such as a database misconfiguration or negligent behavior .

Meanwhile, malicious insiders and external actors are carrying out data theft, sabotage, espionage and fraud measures. Intentional or not, threats from insiders are difficult to detect as the perpetrators often have legitimate access to your sensitive data and can exploit security gaps within your organization. Visibility into potential insider breaches can help you prevent significant financial and reputational harm, and avoid costly compliance violations.

A comprehensive security offering gives you a broad view of your insider data security risk, enabling

$3.58 billion

Difference in the average total cost of a data breach for organizations without security automation deployed vs. organizations with automation fully deployed[3]

Guardium helps you identify and classify sensitive data and provides detailed visibility into your database entitlements and access rights. With Guardium, you can define and enforce entitlement policies based on up-to-date access privileges and remove or adjust outdated access rights to sensitive data.

Using advanced analytics, Guardium analyzes and correlates long-term database security logs from disparate security tools and monitors on-going database access activity. When behavioral deviations are detected, Guardium can proactively block unauthorized access to your data and suspend user credentials due to risky activity.

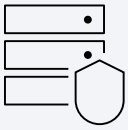
Detect threats with advanced analytics

As your enterprise continues to migrate across hybrid multicloud environments you may rely on disconnected tools to help protect data in all locations. As a result, your team may lack a comprehensive and consolidated view of security threats to your business, which can your ability to effectively identify and respond to threats.

IBM Security Guardium centralizes and correlates massive amounts of long-term data security logs from various tools, and applies built-in advanced analytics to help you uncover, interpret and prioritize threats and risk patterns in context. Likewise, Guardium allows you to create data security audit reports to surface hidden threats and potential risks.

Through Guardium's pre-built workflows, your team can take quick action on suspicious activities, such as blocking access and masking data to prevent a wide-scale breach.

maximize value throughout your data security journey. Coupled with a unified approach to data security, Guardium's advanced analytics IBM X-Force Threat Management Services can add clarity



Forrester Wave names Guardium a leader

See why Guardium is named a Leader in Forrester Wave™: Data Security Portfolio Vendors, Q2 2019 and is a good fit for buyers seeking to centrally reduce and man

Get Started →

and transparency detect advanced threats, as well as respond to and recover from disruptions. Guardium also integrates with SOAR systems such as IBM Security Resilient for intelligent incident response orchestration processes.

IBM Security Guardium Insights for IBM Cloud Pak for Security

Learn how in-depth analytics can help you quickly detect and respond to potential threats.

Learn more →

[1] **Ponemon Report: Client Insights on Data Protection with IBM Security Guardium,** Ponemon Institute, August 2019
[2] **Data Privacy is the New Strategic Priority,** Forrester Consulting, A custom study commissioned by IBM, May 2019.
[3] **Cost of a Data Breach Report 2020,** Ponemon Institute, July 2020

Section 6

IBM data security solutions and services

IBM products can help with data monitoring and encryption, analytics and provide a business perspective on risk.

As you advance in your data security journey, IBM data security solutions and services can help you leverage various data security tools to navigate potential threats – all while providing a consolidated and comprehensive view of your data risk and posture.

Identify, monitor access and protect your sensitive data

IBM Security Guardium Data Protection helps protect your critical data across the public cloud, hybrid clouds and multiclouds. It can discover and classify sensitive structured and unstructured data and identify database vulnerabilities to help provide an accurate picture of your data security and privacy risk. With Guardium you can assess entitlements, create and enforce access policies, and monitor, alert and block suspicious activity. Through its built-in workflows Guardium can help simplify and streamline data security and compliance requirements and reporting, while long-term contextual analytics can help you detect and protect critical data across hybrid multicloud environments.

Watch video →

Identify and centrally monitor access to your sensitive data with Guardium. →

Section 6 continued

Centralize data security insights, reporting and action

IBM Security Guardium Insights is a hybrid cloud data security hub designed to help you improve visibility into user data activity and risk, protect data more efficiently, and enhance IT flexibility as you embrace new business paradigms–such as moving data to the cloud. It centralizes data from Guardium Data Protection's connected data warehouses, databases, big data platforms, and unstructured and z environments to support streamlining your data security architecture, monitoring, protection and reporting. Insights also supports monitoring and protecting data in database-as-a-service (DBaaS) sources, so you can see, act and report on your data security and compliance posture, across on-premises and cloud hosted environments, from a central location.

Enhance your data protection with centralized visibility, reporting and analysis →

Obscure sensitive data with flexible encryption

IBM Security Guardium Data Encryption can deliver flexible encryption, tokenization and masking solutions to help protect file and database data from misuse and support compliance requirements. With cyberattacks increasing in sophistication and volume, Guardium's encryption capabilities provide an important line of defense without disrupting authorized users from performing their jobs.

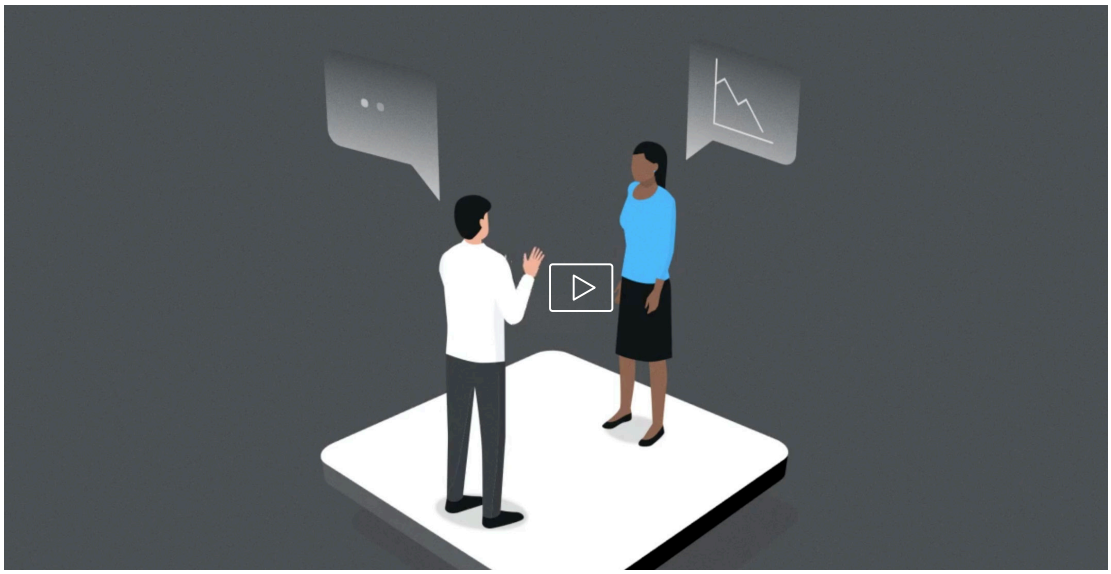
Use encryption to protect your data without disrupting authorized user access. →

Section 6 continued

Get a business perspective on data risk

Securing your organization's critical data starts with visibility and classification. IBM Security Guardium Data Risk Manager can help you provide executives and their teams with a data risk control center that helps uncover, analyze, and visualize data-related business risks and impact so you can take action to help protect your business processes, operations and competitive position.

Identify and protect your most critical data through a central data risk control center. →

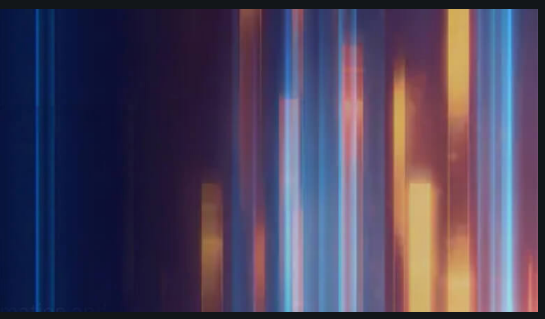


Experts who can help you discover, classify and protect your data wherever it resides.

As your organization's data grows exponentially, do you know where your data resides and how you are protecting it? IBM Data Security Services experts can help build your data security strategy - discover, classify, protect and monitor your most sensitive business data wherever it resides.

Start your data security journey with the help of IBM Data Security Services experts. →

Next steps

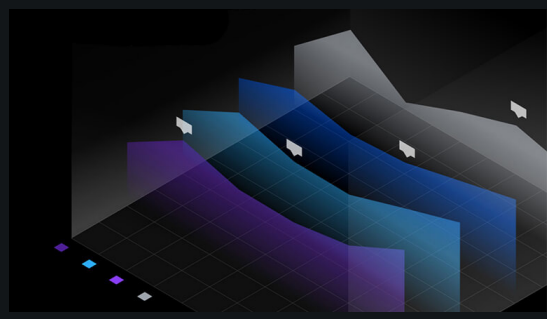


Explore the full suite of IBM Security Guardium products

Schedule a consult →

Transform your cybersecurity strategy with IBM Data Security Services

Talk to an expert →



Learn the true cost of a data breach

Dive Deeper →

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
November 2020

39035239USEN