Partner acceleration guide for IBM Security Guardium

April 2021

IBM Security

IBM

Dear business partner,

As businesses move to the cloud and data protection becomes more critical, IBM Security Guardium offers companies a unified approach to data security challenges.

To accelerate your sales and marketing efforts we have created the partner acceleration guide. This guide was expressly developed to help you to build a successful data protection business with Guardium.

This simple, easy-to-follow guide captures the full value proposition for our partners to add Guardium into their portfolio, including market opportunity; solution description; client challenges and use cases; your investment required to build a practice; how to make money; and key enablement resources.

Here's to great outcomes and explosive growth throughout the year! Please let us know if there is anything else, we can do to support your success.

We thank you for your partnership with IBM.

Mary O'Brien
General Manager, IBM Security

David La Rose
General Manager, IBM Partner Ecosystem

Table of contents

Market landscape

Data security market opportunity snapshot

Market opportunity

$3.9B

Market CAGR

14%

Source: compilation of analyst data (GMV, Gartner, Forrester, IDC)

Key Value

Risk

- Secure and protect high-value data stores
- Identify risk and prompt remediation

Compliance

- Consistent enforcement of governance policies
- Demonstrate compliance
- Lower costs and effort, with no impact on existing business processes

Protection

- Protect sensitive data dynamically, on-premises and in the cloud, from unauthorized access, theft or changes
- Enable digital transformation by providing consistent protection as data environment evolves

Market landscape

Two macro trends driving the data security market

Trend 1:
Organizations embracing hybrid multicloud to gain agility, competitive advantage and drive their organizations forward.

However:
Need to ensure data is protected, and handled in compliance, throughout digital transformation and beyond.

Trend 2:
As organizations grow, the rate of new data, applications and users being added to ecosystem is increasing.

However:
Expanding data footprint increases an organization's attack surface.

Client pain point #1

Problem

I need to stop threats to my data before they disrupt my business

- Insider threats have a high potential to harm my organization
- External threats are growing in sophistication and frequency

Solution

Comprehensive data protection

- Advanced threat detection to identify suspicious user activity
- Real-time controls to block or quarantine users
- Closed-loop integrations with IT management and SIEM tools
- Data risk and vulnerability scans to harden infrastructure

Client pain point #2

Problem

I struggle to protect all sensitive data stored across my organization

- Data environments becoming more complex
- As data sprawls, becomes harder to track where sensitive data is, and who has access to it

Solution

Data security for modern landscape

- Consistent and comprehensive data protection across data environments (multi-cloud, on-premise, container, applications and more)
- Access and analyze years-worth of security data for more advanced security insights
- Robust, flexible encryption provides data-centric security

Client pain point #3

Problem

Reporting compliance is time consuming, expensive and resource-intensive

- Need to report on compliance on short notice, but traditional audit is time consuming
- Addressing compliance with regulations is unavoidable.

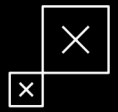
Solution

Simplified compliance

- Pre-built templates for most government and industry regulations
- Automated workflows reduce reporting and auditing process from months to weeks
- Access and analyze years-worth of compliance data for faster reporting

What is IBM Security Guardium?

Hybrid cloud environments exacerbate key data security challenges for organizations



Stop threats before they disrupt business

$5.52M

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

Keep up with the sprawl of data

$267K

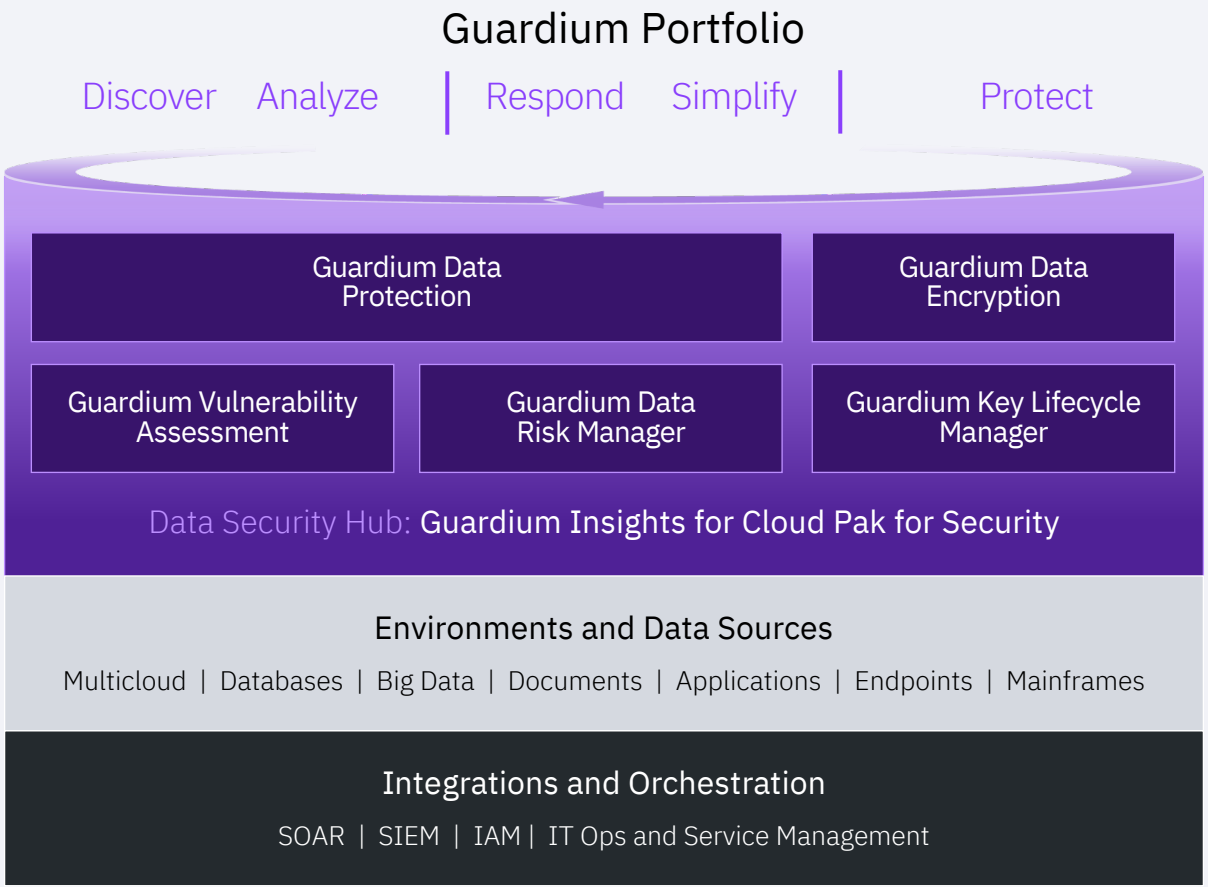
Average cost increase of a breach due to extensive cloud migration

Achieve regulatory compliance

$14.82M

Average cost of a failed audit for compliance with data protection regulations

What is IBM Security Guardium?



What is IBM Security Guardium?

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

Analyze

Analyze and assess risk with contextual insights and analytics

Protect

Protect sensitive data through encryption and access policies, and monitor data access patterns

Respond

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

Simplify

Simplify data privacy and security compliance

What is IBM Security Guardium?

IBM Security Guardium helps clients accelerate data discovery, improve accuracy, and save time

Discover

50%

increase in data classification accuracy.

Analyze

67%

increase discovering data source vulnerabilities and misconfigurations.

Protect

43%

increase in data threat detection accuracy.

Respond

42%

decreased time remediating data security issues.

Simplify

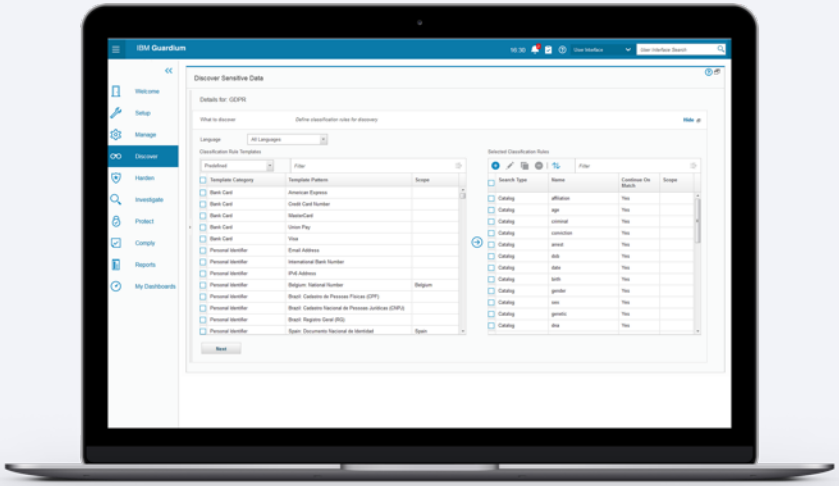
89%

reduced time spent preparing for an audit.

What is IBM Security Guardium?

Discover and classify your sensitive data

- Find data on premises and in the cloud
- Classify data subject to specific regulations
- Identify data access and entitlement rights
- Visualize the flow of sensitive data



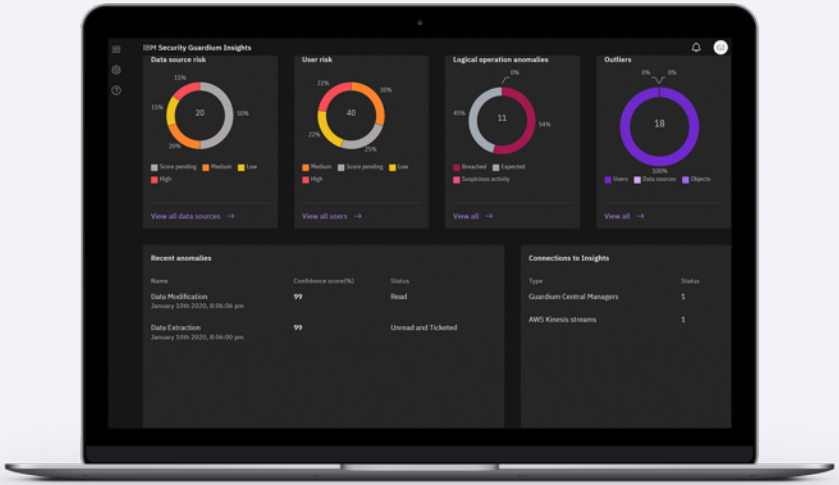
"Guardium is a huge product for us to utilize... prior to having that, there was a lot of mystery around what was happening with our data. What we've gained is a view into where our data's going and what it's being used for."

IT Security Domain Architect, Progressive Insurance

What is IBM Security Guardium?

Analyze risk with contextual insights and analytics

- Apply advanced analytics to uncover and analyze hidden risks
- Examine triggers and alerts
- Remediate, mitigate, and escalate issues
- Assess data risk and the business impact



"We can take advantage of that built-in functionality to give us a faster start, without having to build up things from scratch."

Senior Governance Specialist, Insurance Company

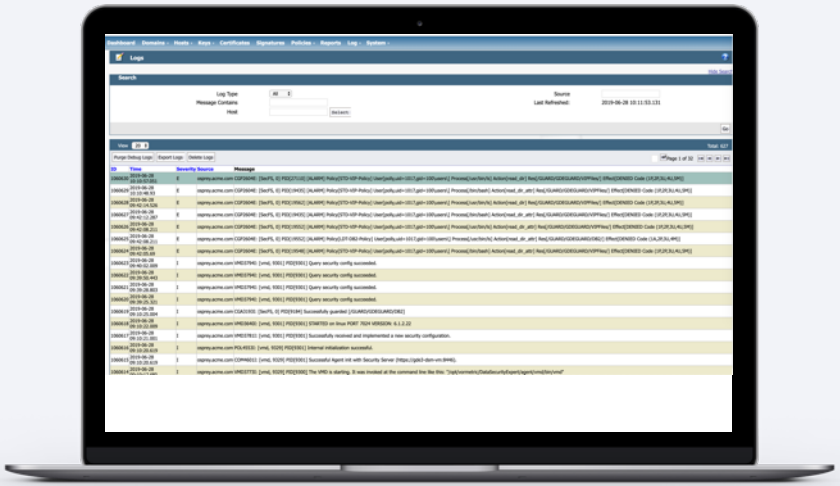
What is IBM Security Guardium?

Protect sensitive data sources

- Encrypt, tokenize, and mask data
- Manage encryption keys
- Refine and enforce user access policies
- Remove dormant accounts

Monitor data access to uncover suspicious activity

- See when, where, how and who is accessing data
- Detect anomalous activity and unauthorized access



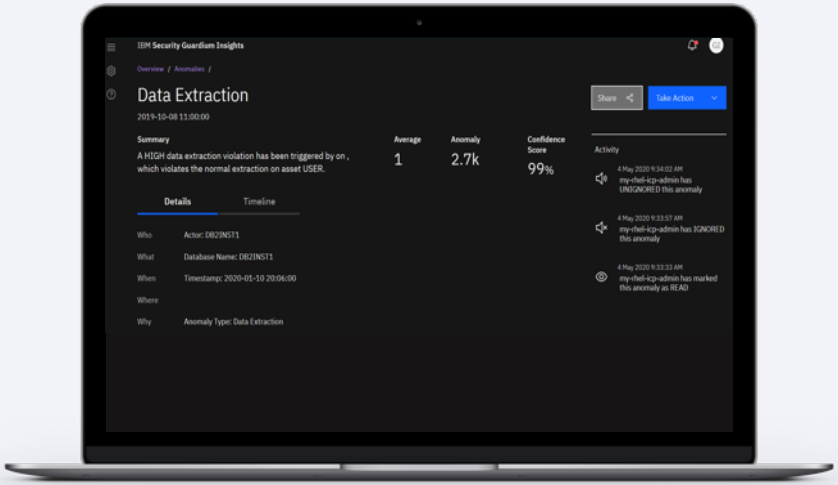
"This product has made it a lot easier to protect user information that has been sent or received."

Administrative Manager, Hospital & Health Care

What is IBM Security Guardium?

Respond to threats in real-time

- Block and quarantine suspicious activity
- Suspend or shut down sessions
- Ensure workflows
- Account for data privacy



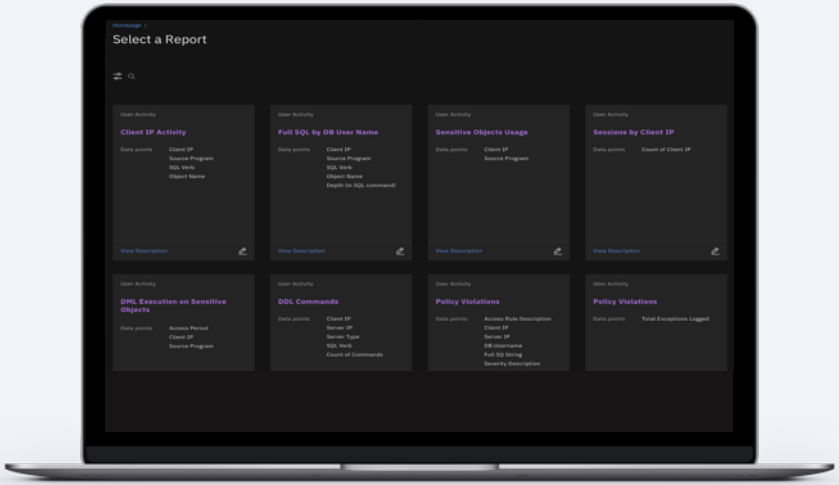
"Because we are using Guardium and it's monitoring 24x7, I sleep a lot better at night—and so does my management team."

Data Security Engineer, Westfield Insurance

What is IBM Security Guardium?

Simplify compliance and audit reporting

- Produce pre-defined and custom data security and compliance reports in seconds
- Confirm separation of duties through a continuous, fine-grained audit trail
- Integrate analytics from an open ecosystem of security products



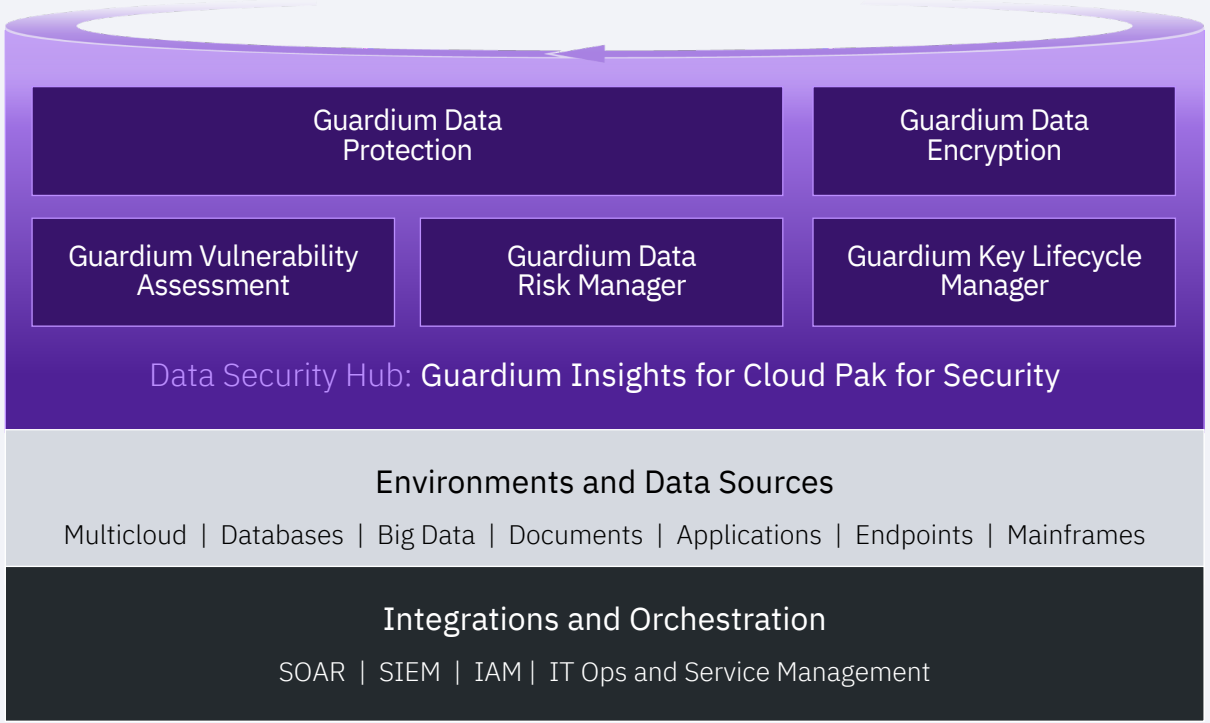
"When you consider the many challenges that hybrid multicloud poses for enterprises amidst their digital transformation, data security, data privacy, and compliance must be major areas of focus. IBM Security Guardium Insights for IBM Cloud Pak for Security solves many of these problems..."

Christopher Steffen - Research Director, Enterprise Management Associates

What is IBM Security Guardium?

Guardium Portfolio + Partner Services

Discover Analyze | Respond Simplify | Protect



Partner value-add services opportunities

- Data Security Strategy
- Data Discovery
- Data Security Governance
- Managed DAM
- Managed Data Encryption

Guardium differentiators

Proactive security controls

- Real-time and near real-time security controls use behavioral analysis and advanced analytics to stop or contain data security threats
- Data activity monitoring and compliance support for structured, semi-structured and unstructured data.

Secure modern data environments

- Platform-agnostic data security and compliance reporting capabilities, extensible across on-premise, DBaaS and hybrid multicloud data sources.
- Agent-based and agentless data collection options provide users flexibility in connecting to data sources.

Connected data security

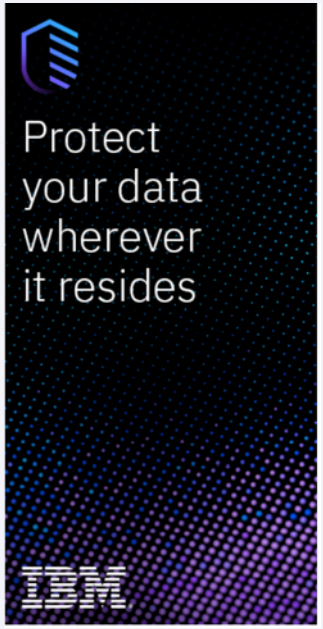
- Open ecosystem of APIs and technology partnerships (including automated integration with multiple commonly used security tools) IT ticketing systems, and modern platforms.
- Collaborate across security operations center by sharing data security event data with SOC tools and opening cases on Cloud Pak for Security

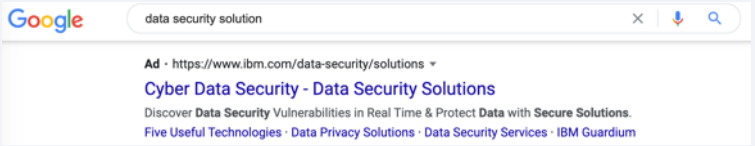
Simplified compliance auditing and reporting

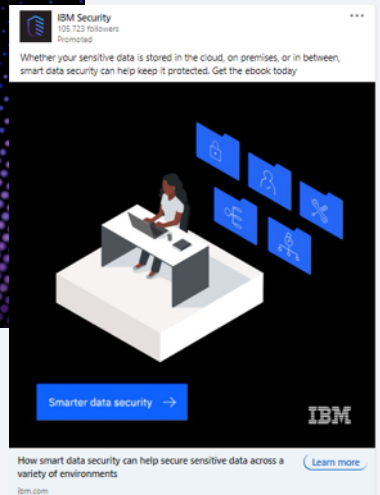
- Retain and analyze years-worth of security data for faster and enriched investigation
- Pre-built compliance templates accelerate auditing and reporting from months to weeks

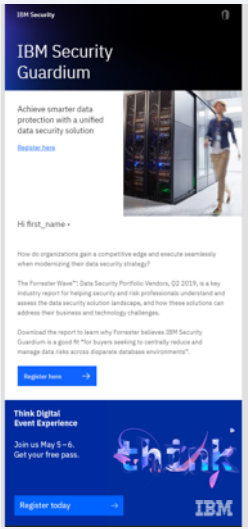
Demand generation for Guardium

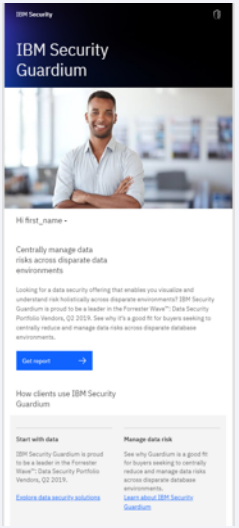
Paid social, paid search, competitive targeting, email nurture streams

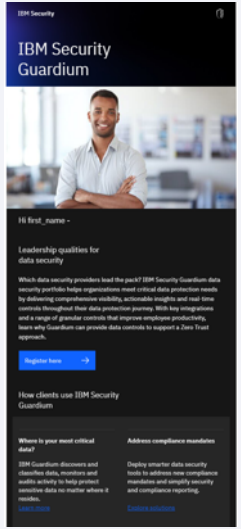












Your investment

Get started quickly and grow as fast as your time investments allow

Sign-up, start learning, start selling

- Register for IBM PartnerWorld
- Sign-up for Seismic
- Review interactive demos and tutorials

Build employee skills in as little as 3 weeks

- 2 technical credentials
- 1 sales credential
- Required to earn channel incentives
- Time Cost

Increase your rewards

- Complete advanced technical certifications
- Demonstrate sales success
- Achieve customer satisfaction targets

Can be accomplished concurrently

Guardium Data Encryption - new license example

Co-led/BP-led segment incentive rates

Partner incentive potential*

Average sale cycle: 3 - 6 months

Timing for initial deployment: Approx. 1 month

Incentive type	Incentive rates	Comments
Estimated Average Deal Size for Guardium - $150,000 for on-prem.		
Sales incentive	10%	Sales incentive rewards Business Partners for the opportunities they generate and the value they bring through the different stages in the sales cycle which result in the sale of IBM new license software to the end user.
Focus offering incentive	10%	Focus offerings incentive rewards Business Partners for selling eligible IBM product offerings which are core to IBM's strategy with value (applicable when transaction also received sales incentive or engagement incentive).
Growth client accelerator incentive (BP Led only)	15%	Growth Client Accelerator rewards Business Partner for selling in the BP-Led (Growth) customer segment with value (applicable when transaction also received Sales Incentive or Engagement Incentive).
Engagement incentive	10%	Engagement Incentive rewards Business Partners for their role and post-sales value-add activities they bring which result in the sale of IBM New License software to the End User and implementation and usage of the newly acquired IBM licenses.
Value-add distributor channel margin	Contact VAD	IBM Distributors have sole discretion to determine the amount (if any) of channel margin shared with the reseller. Resellers should discuss the channel margin with their distributors.
Potential margin on additional BP provided services	2x deal	Typical margin on services – varies by geography, complexity and BP expertise. Represents services included in a software deal. Additional/ongoing services revenue after the sale are typical.
Maximum potential margin	30% (Co-Led) 45% (BP-Led) +VAD margin	Earnings on your first deal may defray the cost of your time investment.

*For planning purposes only, incentives for GOE clients and VAD margin paid at time of transaction; incentives for non–GOE clients are paid back-end. Incentives above are worldwide rates; some Geos or Markets may vary. Refer to https://www.ibm.com/partnerworld/program/compliance/ibm-product-groups-exhibits for parts eligibility and https://www.ibm.com/partnerworld/incentives/ipe-software-new-license for detailed incentive descriptions

Guardium Data Protection - new license example

Co-led/BP-led segment incentive rates

Partner incentive potential*

Average sale cycle: 9 - 12 months

Timing for initial deployment: Approx. 4 months

Incentive type	Incentive rates	Comments
Estimated Average Deal Size for Guardium - $200,000 for on-prem.		
Sales incentive	10%	Sales incentive rewards Business Partners for the opportunities they generate and the value they bring through the different stages in the sales cycle which result in the sale of IBM new license software to the end user.
Focus offering incentive	10%	Focus offerings incentive rewards Business Partners for selling eligible IBM product offerings which are core to IBM's strategy with value (applicable when transaction also received sales incentive or engagement incentive).
Growth client accelerator incentive (BP Led only)	15%	Growth Client Accelerator rewards Business Partner for selling in the BP-Led (Growth) customer segment with value (applicable when transaction also received Sales Incentive or Engagement Incentive).
Engagement incentive	10%	Engagement Incentive rewards Business Partners for their role and post-sales value-add activities they bring which result in the sale of IBM New License software to the End User and implementation and usage of the newly acquired IBM licenses.
Value-add distributor channel margin	Contact VAD	IBM Distributors have sole discretion to determine the amount (if any) of channel margin shared with the reseller. Resellers should discuss the channel margin with their distributors.
Potential margin on additional BP provided services	2x deal	Typical margin on services – varies by geography, complexity and BP expertise. Represents services included in a software deal. Additional/ongoing services revenue after the sale are typical.
Maximum potential margin	30% (Co-Led) 45% (BP-Led) +VAD margin	Earnings on your first deal may defray the cost of your time investment.

*For planning purposes only, incentives for GOE clients and VAD margin paid at time of transaction; incentives for non–GOE clients are paid back-end. Incentives above are worldwide rates; some Geos or Markets may vary. Refer to https://www.ibm.com/partnerworld/program/compliance/ibm-product-groups-exhibits for parts eligibility and https://www.ibm.com/partnerworld/incentives/ipe-software-new-license for detailed incentive descriptions

Guardium go-to-market resources

Develop your strategy for delivering Guardium to your clients and/or prospects

Product overview	Review the latest about the solution
Product tour	Explore data security and compliance capabilities
Demo	Experience how to protect data at the source
Enablement	Build your sales and technical knowledge with a comprehensive roadmap
Competencies	Earn solution competencies to differentiate your skills in the marketplace
Community	Join our community to interact with IBM, clients and peers that leverage the solution
IBM Services	Available option to offer clients, if needed

Guardium go-to-market resources

Sales kits for data protection and data encryption

Data Protection Sales Kits	Data Encryption Sales Kits
Insights	File and database encryption
Data protection	Key management
Data risk manager	Tokenization
Vulnerability Assessment (coming soon)	Application Encryption

Demand generation

Drive demand and engage with your clients and/or prospects about Guardium

Co-Marketing Funding
Leverage IBM co-marketing funding to enhance your marketing plans

Digital Campaign
Drive leads through customized content throughout all stages of the buyer journey

Client facing assets and messaging
All content available to business partners

External client reference

SIRIUS

How can you improve public safety through large-scale open-source data analytics?

Read the full story

To improve citizens' quality of life, a government agency sought to turn information published on social media into actionable insight. Working with IBM Platinum Business Partner Sirius, Circinus architected and deployed IBM® Security and IBM Analytics solutions running on highly available IBM LinuxONE™ and IBM FlashSystem® technology, helping the client better understand the population it serves.

IT Infrastructure

Government

Protect citizens with the help of high-end intelligence and security analytics to scale up as demand grows, while keeping sensitive information safe and secure.

We have been able to create a powerful, reliable and highly secure analytics platform for our client, to help them use data to keep citizens safe.

Andy Kowal
Chief Technology Officer, Circinus

Solution Component:

IBM® Cloud Object Storage SW
IBM Cognos Analytics
IBM Security™ Guardium Data Protection
IBM LinuxONE Emperor II
IBM FlashSystem 9100
IBM Watson Discovery
IBM Watson Studio & Modeler
IBM Security i2 Intelligence Analysis

Contact Us!

Worldwide

Glenn Newlove, WW Channel Sales Leader
glenn_newlove@us.ibm.com

Traci Romero, WW Business Partner Marketing
traciromero@us.ibm.com

Prasad Raman, WW Ecosystem Offering Management Digital Trust
Prasad.S.Raman@ibm.com

Geo

North America

Randy Long, Security SW Sales Leader - Business Partner Ecosystem
randy.long@us.ibm.com

EMEA

Gonzalo de la Hoz, Security Partner Ecosystem Leader, EMEA
gonzalo_delahoz@es.ibm.com

APAC

Kittipong Asawapichayon, Security Partner Ecosystem Leader, APAC
kittipon@th.ibm.com

Thank you!

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube.com/ibmsecurity

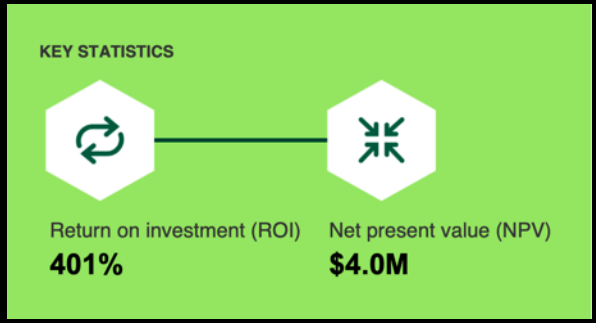
Appendix

Recent Forrester reports for IBM Security Guardium

The Forrester Wave™: Data Security Portfolio Vendors, Q2 2019

"IBM is a good fit for buyers seeking to centrally reduce and manage data risks across disparate database environments."

The Total Economic Impact™ of IBM Security Guardium



Key Findings

- Reduced likelihood of a breach by 40%
- Reduced effort to perform a data environment audit by 75%
- Increased ability to meet compliance regulations saving $1.1M
- Automation of database analysis processes saving approximately 1,000 hours annually