IBM Security

Government of British Columbia Security Day

11/20/19

Cyber Security – There is No Silver Bullet

Sylvia B. Henson
Senior Data Security Sales Specialist

IBM

Disclaimer

Notice: Clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation. Clients are solely responsible for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the clients' business and any actions the clients may need to take to comply with such laws and regulations. The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability. IBM does not provide legal, accounting or auditing advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation.

IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM's sole discretion.

Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.

The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract.

The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.

None of the statements contained herein constitutes legal advice – it is process advice only.

Let the right people in
Keep the wrong people out

Challenge: People Can’t Protect What They Can’t See

74%

74% of non-IT executives have incomplete visibility into **data discovery**

- What are our most critical data assets?
- Where is the most critical data?

70%

70% of non-IT executives have incomplete visibility into **threat and vulnerability management**

- What will be the impact on the organization of losing data?
- What are the current risks to Data repositories?

70%

70% of non-IT executives have incomplete visibility into who is the **data owner**?

- What are our crown jewels?
- Who has access to data and who can approve access to data?

73%

73% of non-IT executives have incomplete visibility into **third party risk**

- Should we encrypt all data?
- Can the data be shared outside the bank?

Source: A commissioned study conducted by Forrester Consulting on behalf of Agile 3 Solutions, an IBM company

Challenge: Security Pros, Executives Speak Different Languages

IT Security Pros struggle to communicate **business relevant, security insights** to Non-IT Executives

67%

Of Security Pros struggle to **identify** the most useful data security and risk metrics for non-IT executives

66%

Of Security Pros struggle to **translate** data security and risk into business risk for non-IT executives

65%

Of Security Pros struggle to **communicate** real-time insight into critical data for non-IT executives

People Need ***business context*** to Improve Data Security

Common phrases we hear from People

Lead, Security Operations

"The FS-ISAC alert this morning reported on a Windows vulnerability that affect Windows Server 2012 and SQL Server 2015 with CVE-123456"

Chief Security Officer

"Our patch management process is mature. Every quarter, we patch 98% of our databases, 95% of our Web Applications, and 90% on Windows and Linux OS. I'm sure our data security practices are effective"

The missing context

- How critical are the Windows systems to the business?
- What is the business impact ($$) of the vulnerability reported?
- Who owns the applications?
- What is the criticality of the data on databases or applications not patched?
- Where do the applications reside?
- Are there any regulatory implications?

3 Guiding Principles of IBM Data Security

Dynamic Defense

- Can’t protect what you’re unaware of
- Volume of data makes manual threat hunting impossible
- Need dynamic and right-time data protection

Customer Trust

- Data Privacy increasingly important to organizations
- Regulatory requirements getting increasingly complex
- Need to be empowered to deliver on compliance and customer trust

Business Agility

- Need faster and more focused decision making
- Demonstrate greater ROI
- Require greater infrastructure flexibility

Empowering Human Interaction

Data Privacy Regulations

CISOs responsible for enforcing privacy controls

75%

consumers will not buy a product from a company if they don't trust the company to protect their data[1]

$2.6B

GDPR Spending on Security in 2019 - IDC

1.https://newsroom.ibm.com/Cybersecurity-and-Privacy-Research

Data Privacy Orchestration and Automation

1. Build a strong privacy program
2. Gain risk-based privacy insights
3. Automate privacy controls

Promote privacy, build trust, differentiate and grow

1

Build a strong privacy program

Implement a holistic, continuous, dynamic privacy foundation

- Assess risk and privacy controls
- Develop privacy readiness roadmap
- Conduct executive reviews
- Implement privacy and security measures

Risk and privacy assessment
Privacy readiness
Regulatory expertise

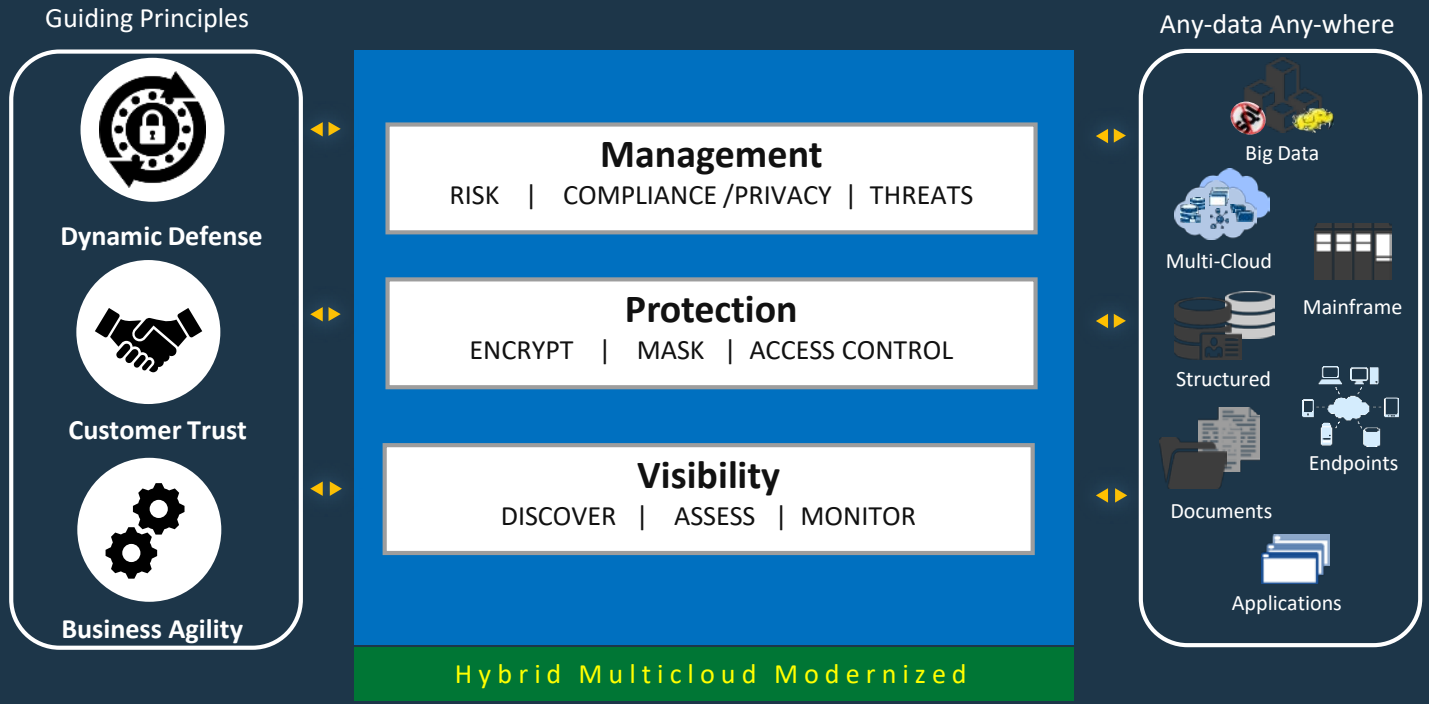
2 Gain risk-based privacy insights

Leverage risk-based visibility and privacy insights for actionable business impact

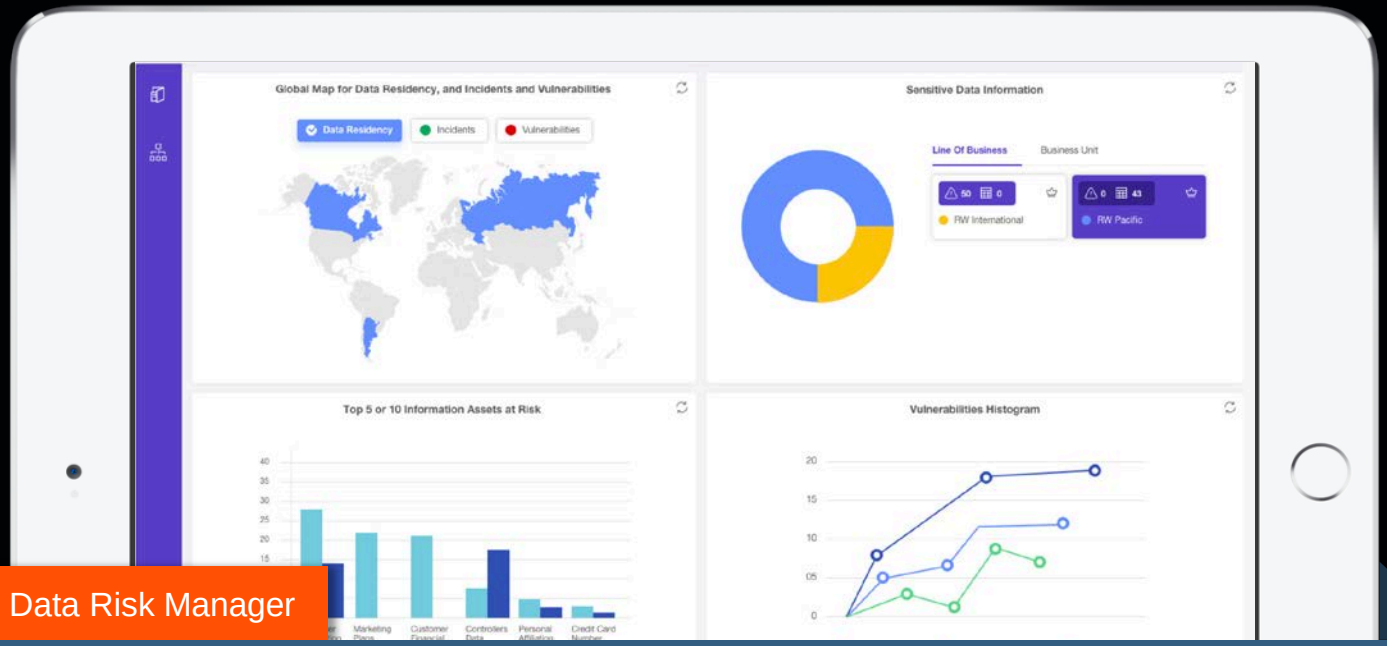
- View privacy and risk from a single dashboard
- Prioritize actions for risk mitigation
- Govern and control access to personal data
- Apply necessary security and privacy controls
- Prepare for privacy incident response

Data protection and compliance	Identity and access management	Incident Response Orchestration	IBM Services

NextGen IBM Data Security Platform



Get Closer to the Silver Bullet : Data Risk Manager



IBM Data Risk Manager

Uncover, analyze and visualize data-related business risks

- Identify specific, high-value, business-sensitive information assets
- Gain early visibility into potential risks to data and processes
- Inform executives with a business-consumable data risk control center

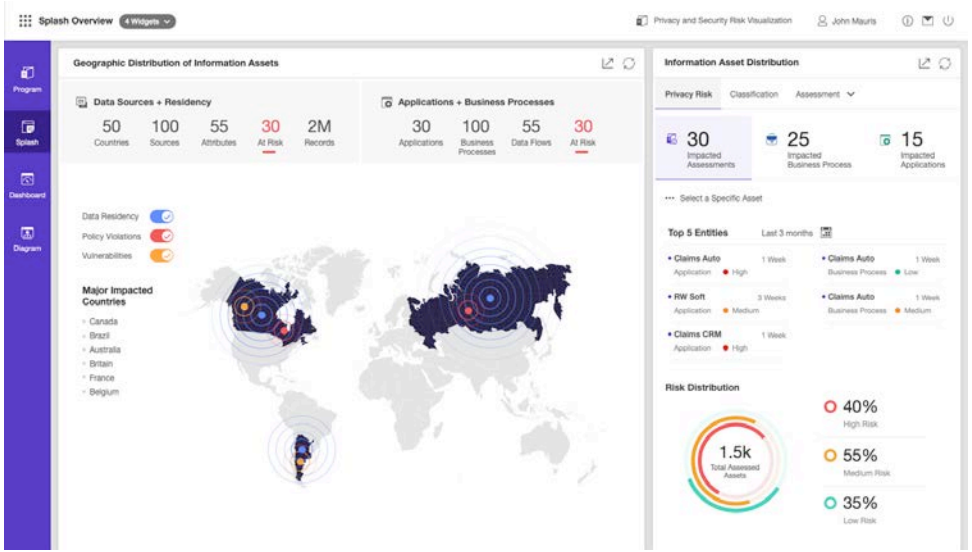
IBM Security Data Risk Manager

Identify – Visualize – Communicate

Data Risk Manager provides executives and their teams with a business-consumable data risk control center that helps to uncover, analyze, and visualize data-related business risks so they can effectively collaborate and take action to protect their business.

KEY BENEFITS

- **Identify high-value, business-sensitive information assets** that are at risk from internal and external threats, and provide an end-to-end view of business metadata associated with crown jewel data via an interactive data risk control center
- **Visualize potential risks with business risk evaluation modeling** that correlates threats, vulnerabilities, controls, and business attributes across information assets to highlight where the business is at risk & provides remediation recommendations
- **Communicate data risk information** across teams, business units, and technologies to your board of directors with an executive ready dashboard and reports



The missing business context addressed by DRM

Decision-enabling insights around critical data

What?

- Categories of data critical to the business
- Data subjected to regulatory and compliance requirements

How?

- Protection measures implemented for safeguarding data
- Effectiveness of data monitoring, encryption, vulnerability management and others

Where?

- Physical and logical location of the data store
- Location of users and applications accessing data from

Security?

- Security controls for data protection
- Assessment for evaluating data risk

Who?

- Stakeholders responsible for safeguarding the data
- Organization units involved in the data lifecycle

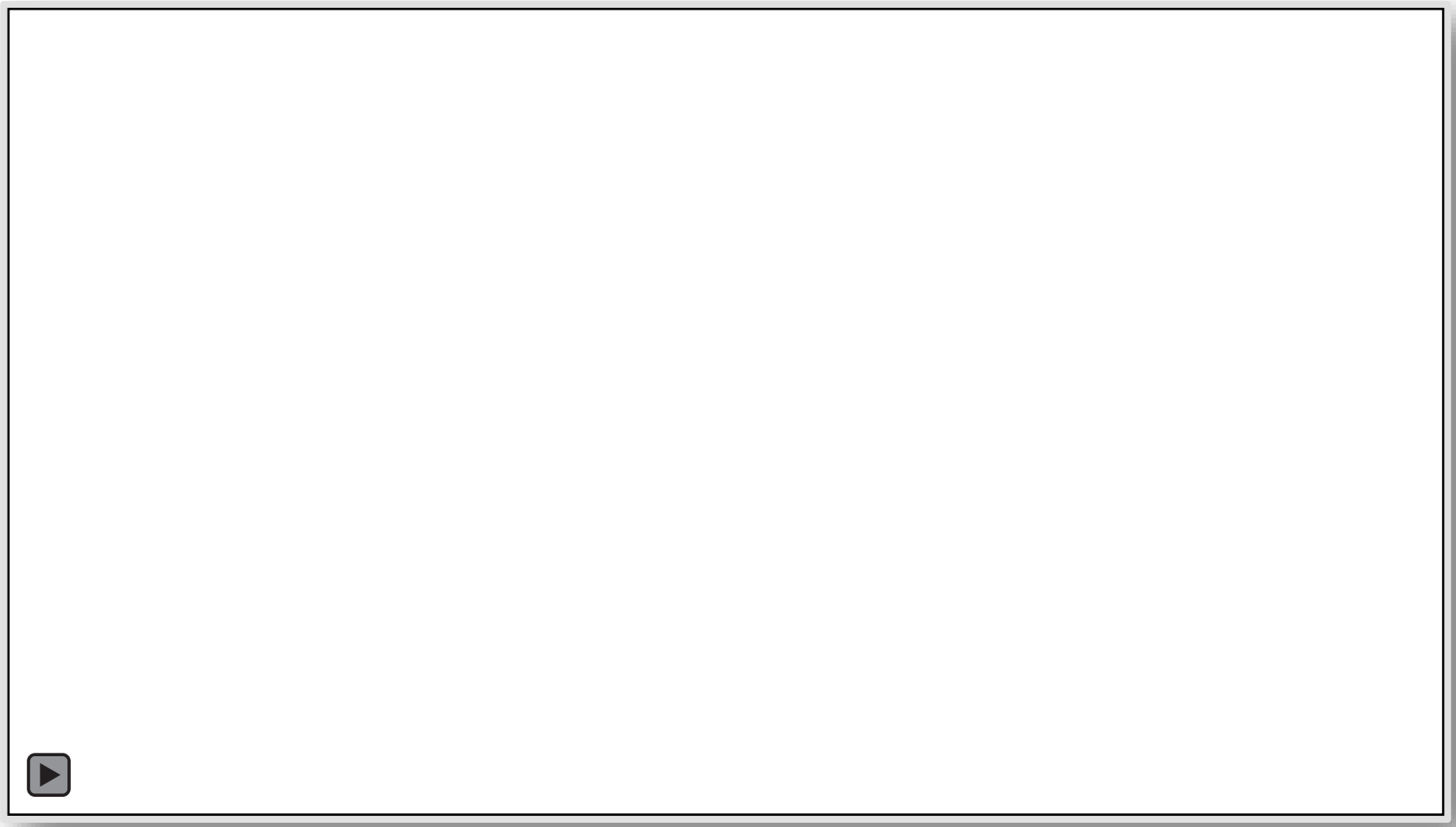
Governance?

- Risk and mitigation for identified data risk
- Action management for risk reduction

Why?

- Applications and Business Processes that rely on critical business data
- Business or compliance need for data usage, storage, retention

DRM Video



Q&A

IBM Security – a leader in its category:

Analyst Reviews

FORRESTER®

A leader in Forrester Wave report on Data Security Portfolio vendors

kuppingercole ANALYSTS

A leader in the Leadership Compass on Database and Big Data Security

Peer Reviews

G2

A leader for Summer 2019 in Data-Centric Security Software

IT Central Station

Ranked #1 in Database Security

IBM Security

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

IBM