White Paper

Adopting a Next-Generation Data Security Approach

Sponsored by: IBM

Robyn Westervelt
March 2020

REGAIN VISIBILITY AND CONTROL OF SENSITIVE DATA

Businesses are increasingly turning to a hybrid mix of on-premises and cloud-based technologies to increase agility, remain competitive, and drive their organizations forward. This is resulting in an influx of cloud-hosted applications, databases, infrastructure, and services proliferating within the enterprise.

Attackers are seizing on the gaps, vulnerabilities, and weaknesses generated by the struggle of enterprise security teams to manage data security across complex hybrid and multicloud environments. Likewise, data security tools for discovering, classifying, monitoring, and protecting sensitive data are often designed for specific environments and narrow use cases. As a result, security teams are overwhelmed with limited data security visibility, fragmented compliance reporting, and disjointed workflows across their on-premises and cloud-hosted data stores.

The extent of an organization's security tool sprawl is often uncovered during data migration projects by security teams that quickly realize they have amassed a wide range of siloed tools in an effort to keep pace with rapid technology adoption trends and workflow and process changes.

Without a comprehensive data security strategy, security teams lack an efficient way to assess their organization's data security and compliance posture. Insufficient data security and compliance assessments often result in an inability to effectively prioritize investigation and response activities.

"When a new threat vector emerges, you often realize your coverage is inadequate," said the chief information security officer (CISO) at a large financial services firm who is investing in modern, cohesive security solutions to protect sensitive data and meet compliance obligations. "You quickly see the value of a centralized view and status of the data assets, and you gain a more efficient way to maintain an audit trail across the life cycle of the sensitive data you are protecting."

Several IDC studies have identified this continued lack of situational awareness and the ineffectiveness of existing security infrastructure to enforce data governance policies. The result is data exposure or worse. According to IDC's 2020 *Data Security Survey,* nearly 40% of respondents indicated their organization experienced four or more security breaches in the past three years. The survey, which reached 620 information technology (IT) and IT security professionals in North America and Europe, detailed the daunting challenge that today's security teams are experiencing. Nearly half of the survey respondents said their organization managed 3–10 on-premises datacenters, up to 6 private cloud environments, and a dozen or more public cloud environments. The more than 310 IT security practitioners that took the survey indicated a variety of approaches being used to protect the data. The survey found that generally 30–35% of the sensitive data is encrypted in these environments. Forward-leaning organizations used data discovery and classification tools to gain control of the most sensitive assets located in on-premises datacenters or in hosted private cloud environments. Cloud data loss prevention (DLP) was in use for software-as-a-service (SaaS) applications, with organizations using both native data loss prevention features from the cloud provider and a cloud security gateway to extend on-premises data governance policies to popular cloud applications. Security teams also indicated that managing the security features and products was onerous, with at least a quarter of IT security practitioners indicating that the biggest challenge was the integration of crypto keys with existing on-premises key management infrastructure.

IDC has found that breaches often stem from lost or stolen credentials, simple human errors, employees targeted in social engineering attacks, and system vulnerabilities that lead to data loss. When digital forensics investigators are asked about the challenges that lead to costly data breaches, their answers are all so eerily similar. Breached organizations often can't provide a complete accounting of the whereabouts of sensitive data, and many have invested in security products without ensuring that data discovery and policy enforcement can be applied holistically across disparate environments to protect their sensitive and regulated data from external attackers and insiders.

IN THIS WHITE PAPER

This white paper explores how organizations can adopt a next-generation data security approach to protect sensitive data across heterogeneous and highly distributed environments. It details why enterprise security teams must be equipped with modern solutions designed to take the complexity out of managing the entire data security life cycle from data discovery and classification to policy creation and enforcement, regardless of where data resides.

Today, a compromise is often made between the business' pace of technology adoption and the increased scale and complexity of securing the data environment. Likewise, the reduced effectiveness of existing security investments — in terms of limited visibility and control of corporate data — often stalls, prevents, or even reverses strategic technology initiatives.

A next-generation data security approach addresses the bottlenecks and inefficiencies that lead to data exposure and costly data breaches. It addresses the declining visibility and control over sensitive data as it spans across hybrid multicloud environments. Through a set of powerful, integrated data security components, security teams can gain a comprehensive view of security risks and take centralized action.

NEXT-GENERATION DATA SECURITY: THE STARTING LINE

At the core, a next-generation data security approach is about holistically visualizing and understanding the organization's security posture, quickly identifying areas of risk, and mitigating the highest risks to sensitive data, no matter where that data resides.

According to *Worldwide Data Replication and Protection Software Forecast, 2020-2023* (IDC #US45861919, January 2020), organizations need a starting point to effectively secure and maintain the integrity of corporate data, which is growing at a compound annual growth rate of 40-50%. This growth is influenced by digital business transformation strategies, a continuous process in which enterprises carefully analyze customer data to create new business models, products, and services that enhance the customer experience.

But data is everywhere. It can be replicated and deployed and can traverse across dynamic environments that incorporate a mix of mobile, social, and cloud architectures. The growing use and value of data are driving a corresponding heightened level of risk. Data must be secured because it provides productivity gains and competitive advantage, but also because its access, or use, may cause unintended consequences associated with an organization's financial and reputational losses as well as regulatory compliance requirements.

What data needs the most attention? According to IDC's 2020 *Data Security Survey,* account credentials were followed by credit card data, company financial information, strategic business plans, and trade secrets. The survey also found that securing sensitive customer data and employee pay and benefits information is also a top priority.

Security teams must work with data owners to identify the data that would cause catastrophic damage to the organization if it was lost or stolen. To that end, IDC's 2020 *Data Security Survey* respondents viewed the loss or exposure of intellectual property as the most impactful security events, followed by lost or stolen endpoints containing sensitive data. Next in line were ransomware, financial fraud, and business email compromises.

Survey respondents listed file encryption, full disk encryption, and email encryption as the most beneficial data security tactics. However, they frequently acknowledge that encryption is no panacea. Implementing encryption can't be done in a meaningful way without conducting data discovery and classification to help determine where the most sensitive assets reside and whether enough security controls are in place to mitigate the risk of theft or exposure.

That said, comprehensive data security and compliance projects are not a sprint — they're a marathon. It begins with identifying the assets requiring protection, the location of those assets, and determining who can access the information.

IDC studies have found that the most successful organizations take systematic steps when embarking on a next-generation data security approach. These steps may include establishing a data triage team consisting of all the key stakeholders that understand established business processes and typical workflows and may consider how existing security is applied to address data in motion, data at rest (stored in databases and data stores), and data in use (cached in places not intended for long-term storage).

A next-generation data security approach centers around protecting the entire data life cycle and requires a focus on the following controls, tools, and techniques:

- **Data discovery and classification:** Search the data stores throughout data environments on-premises and in the cloud, seeking all records and files that contain sensitive information based on patterns (e.g., regular expressions) and keywords. Determine the location and affiliation of sensitive data with users and applications. Identify and assign classification levels to data types within the organization. Start with regulated data that is privacy related or involves time-sensitive financial reporting.
- **Access control and encryption:** Practice a least-privileged strategy and allow access to data for the minimum necessary number of individuals. Ensure actions like redacting and masking and blocking access to data can be executed when risks are identified. Also, properly encrypt all data that traverses untrusted, public environments such as remote access networks and site-to-site communications.

- **Data governance:** Ensure data classification and protections are integrated into the risk assessment process. Review current data governance policies and update them to address workflow changes, public cloud services adoption (e.g., software as a service, infrastructure as a service [IaaS], and database as a service), and any perceived gaps if necessary.
- **Data monitoring and destruction:** Actively monitor when, where, and how sensitive data is being accessed and used to gain key insights into whether the data is being used legitimately or misused, either purposefully or mistakenly. Policies should outline data retention requirements and destruction processes for when data no longer needs to be retained. Adequate destruction requires the removal of information in a way that renders it unreadable or irretrievable.

IDC studies are increasingly uncovering gaps in data governance policy enforcement mechanisms. This trend is especially common in organizations with distributed environments and satellite offices where previous investments in security technology were spontaneous/on-offs to address a new regulatory requirement, a failed audit, a new technology adoption, or newly perceived risk.

Likewise, protecting disparate data environments with existing IT security infrastructure was cited as a top challenge by more than 30% of CISOs and IT security and data management professionals who responded to IDC's *Data Services for Hybrid Cloud Survey.* Cloud adoption and the use of file-sharing services also contributed to a lack of visibility and control over sensitive data and increased the complexity of adequately addressing legal requirements and restrictions.

INTEGRATE DISPARATE DATA SECURITY SOLUTIONS

A next-generation data security approach requires security teams to account for the importance of data discovery and classification, activity monitoring, vulnerability and risk assessment, threat hunting, and issue remediation. In addition, as more organizations face pressure to move not just their data but also their IT infrastructure to the cloud, the ability to deploy a comprehensive data security solution flexibly — across on-premises and multicloud environments — has become an important requirement to consider. Real-time activity monitoring, analytics, and user behaviors must be in place to provide holistic, real-time visibility into the organization's risk posture. Risk remediation capabilities must scale across data stores residing on-premises and in the cloud. In addition, it is critical to have a reporting framework in place for situational awareness that ensures compliance objectives are met.

Unfortunately, all too often, the breadth of these functionalities is delivered from disparate and disjointed tools.

To help ensure the success of a next-generation data security approach, it behooves security teams to utilize data security solutions that integrate and interoperate with the rest of the security and IT infrastructure and extend protection policies to data wherever it resides — or ends up residing. That includes solutions that can interoperate with SaaS, PaaS, and IaaS applications and cloud repositories to augment native data protection capabilities and ensure data governance policies remain consistent regardless of the location of sensitive data assets.

To be effective, the solution must incorporate the following:

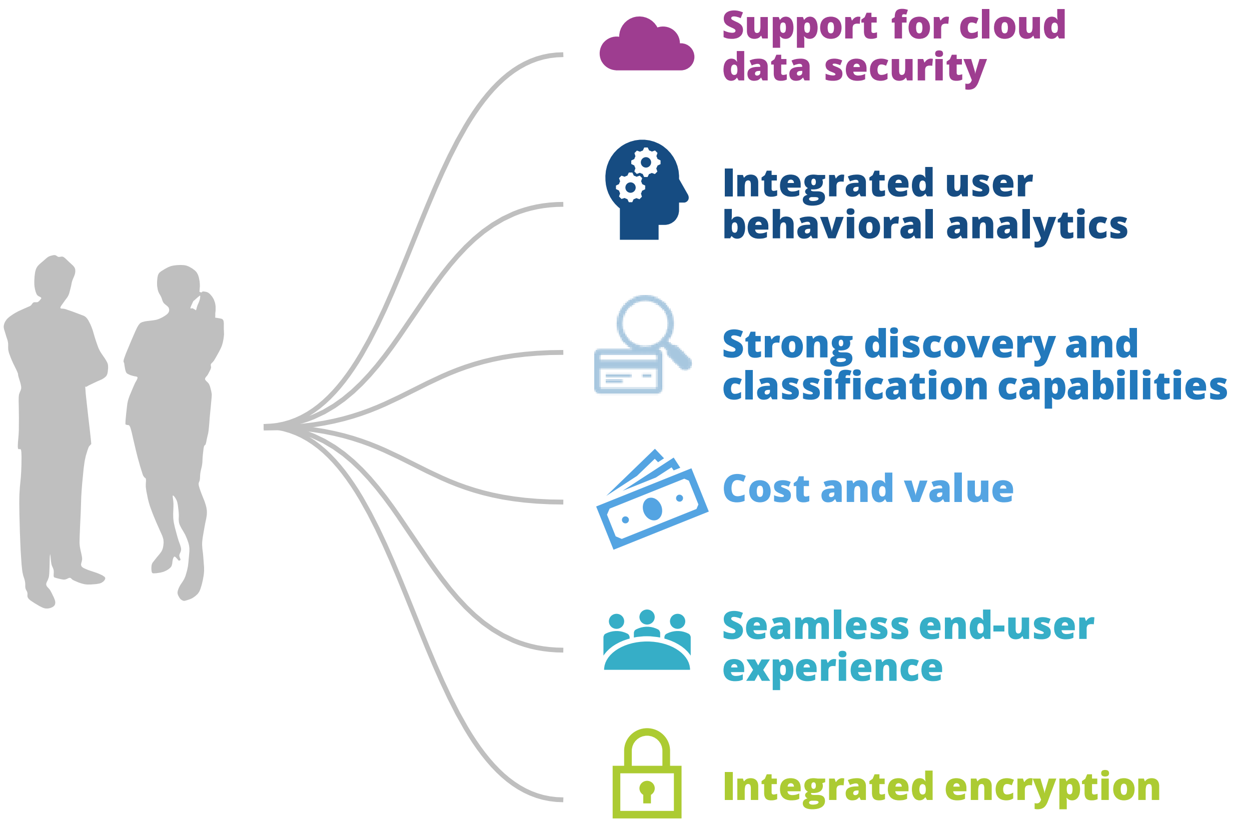
- Automated discovery and classification
- Ongoing vulnerability assessments
- Real-time activity monitoring

- Risk posture assessment and customizable key performance indicators (KPIs)
- Ability to protect data across environments
- Real-time and long-term security and compliance reporting

Figure 1 outlines key data loss prevention features and capabilities of a next-generation data security approach.

FIGURE 1

Top Next-Generation Data Security Features and Capabilities


Support for cloud data security
Integrated user behavioral analytics
Strong discovery and classification capabilities
Cost and value
Seamless end-user experience
Integrated encryption

n = 312 IT security practitioners

Source: IDC's *Data Security Survey,* January 2020

KEY BENEFITS OF A NEXT-GENERATION DATA SECURITY APPROACH

Enterprises successfully employing a next-generation data security approach can answer the question, "Do you know where your most sensitive data is and who has access to it?" Many of these organizations can now allocate data governance policy enforcement mechanisms based on the risk to the information being protected. This requires organizations to eliminate the silos of security solutions.

A next-generation data security solution provides protection over critical data residing in hybrid and multicloud environments. This represents the convergence of security information and event management (SIEM), privileged access management (PAM), and identity and access management (IAM) functionalities. A solution that supports a next-generation data security approach provides a single, unified policy engine; a single management console; centralized analytics; and a consolidated reporting framework. What's more, it provides security teams with simplified management and a mechanism to view and address the existing security posture from a single pane of glass.

Must-have capabilities of a next-generation data security solution include:

- **Situational awareness:** Centrally view your organization's data security and compliance posture across on-premises and cloud-hosted data repositories. Get the context necessary to make the right decisions and act on security risks to minimize any business loss or disruption that may occur due to an inevitable breach.
- **Automated response:** Enable organizations to set polices and take manual and automated responses across the entire data environment.
- **Gap visibility:** Identify and address significant gaps or disjointed security functionality across interrelated services containing sensitive data. Bridge point security solutions and incorporate them into existing workflows to enrich your existing security threat analytics.
- **Continuous monitoring:** Enterprises adopting a next-generation data security approach can protect critical data regardless of location. A solution that supports this approach provides continuous monitoring over data access, entitlements, and protection controls over sensitive data in on-premises and cloud-hosted data repositories. The once-siloed security solutions can now interoperate to execute automated or guided remediation workflows such as blocking suspicious users from accessing data and creating escalation tickets when suspicious activity is discovered.

Figure 2 highlights high-risk data channels and data types that require a systematic data security approach.

A next-generation data security approach enables organizations to implement the exact same security and policy controls regardless of where their data resides. Security administrators can use existing data classification or choose to classify data once and apply a consistent set of policies that are enforced at critical points across disparate environments. This convergence also creates cohesiveness by enabling the shared telemetry from once siloed security solutions to provide increased context behind newly detected threats and reduce false positives.

FIGURE 2

A Tale of Complexity: Protecting Corporate Data Requires a Systematic Approach

Highest-Risk Data Channels

- Internet access points
- Lost or stolen smartphones or laptops
- Employee remote access
- Wi-Fi sniffing of endpoints
- Email leakage
- Public-facing website

High-Risk Data Types

- Secrets, encryption keys, passwords
- Credit card data
- Personally identifiable information
- Personal health information
- Customer data (non–credit card)
- Strategic business plans

n = 620

Source: IDC's *Data Security Survey,* January 2020

CHALLENGES WHEN ADOPTING A NEXT-GENERATION DATA SECURITY APPROACH

Despite new and disruptive technologies and approaches, basic security best practices require information security professionals to gain situational awareness of the business' core assets, existing security policies, and workflow and the efficacy of the enforcement mechanisms already in place. Many data security projects examined by IDC found that success often hinges on execution of the following people and process issues:

- **Potential organizational and process changes:** Centralizing alerts and context from various solutions will require incident response workflows and process changes that should be assessed as early in a data security project as possible.
- **Participation of security and data owner:** Successful data security projects often require a thorough data discovery and classification exercise. Security teams must include all stakeholders for a complete picture of where key data assets are located and who has access to them.
- **Alerting and configuring prevention/blocking:** Automation to block malicious or compromised users or to block malicious code from executing should be considered. To minimize automated responses from disrupting legitimate actions and workflows, security teams should conduct a data discovery and classification exercise. This enables triggered responses to be associated with the classification level of the data and the context behind the user activity. A response can be as simple as alerting the end user of a potential policy violation.
- **Additional costs:** Some solutions will require managed security services, which can carry additional cost.

Also, to achieve the benefits of a next-generation data security approach, enterprises must identify security solution providers that support an open integration framework to enable integration and interoperability with third-party security products.

IBM SECURITY GUARDIUM

IBM Security Guardium discovers and classifies sensitive data residing on-premises and in cloud-hosted environments, enabling a comprehensive view of your data security and compliance posture.

With Guardium you can verify, define, and enforce data access entitlement policies based on up-to-date user privileges. Using advanced analytics, Guardium also analyzes and correlates long-term data security information from disparate security tools and monitors ongoing activity. When anomalous behavioral deviations are detected, Guardium can proactively take risk remediation actions such as blocking unauthorized access and shutting down user credentials. In addition, encrypting, tokenizing, or masking sensitive data deliver enhanced data protection without disrupting the ability of authorized users to perform their jobs.

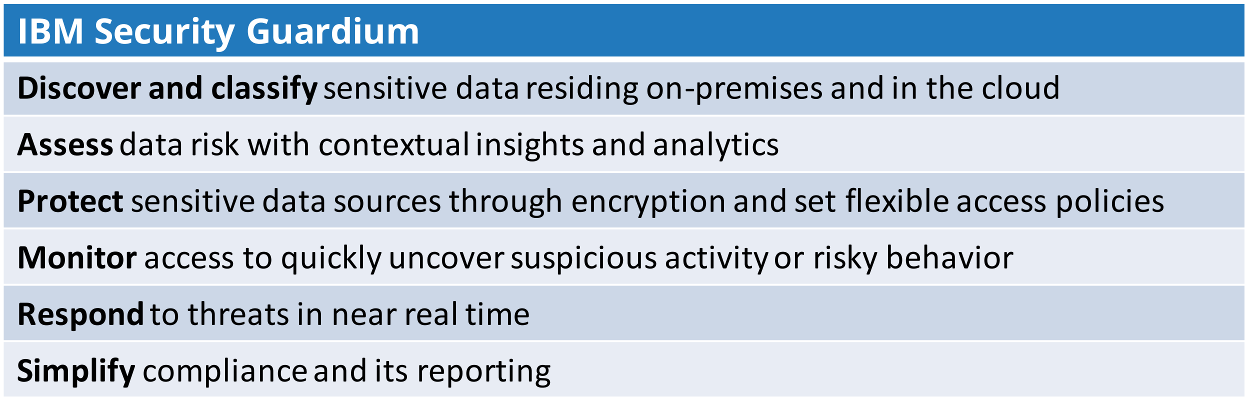
For example, IBM Security Guardium Insights integrates with a wide range of common data sources and products. These sources feed Guardium Insights with monitoring and audit-related data, and Guardium Insights retains that data, applies threat hunting analytics, and applies risk-based scoring to help data security administrators prioritize investigation and response. Data security admins can investigate and respond to issues and threats from the Guardium Insights console – whether that involves creating a report, investigating an anomaly, blocking a user, sharing an issue with a security analyst, or opening a ticket in ServiceNow.

Guardium Insights allows data security teams to centrally create reports and view, investigate, and take action to protect their on-premises and cloud-hosted data.

Figure 3 summarizes the smarter data security capabilities offered by Guardium.

FIGURE 3

IBM Security Guardium Enables a Comprehensive View of Data Security



IBM Security Guardium
Discover and classify sensitive data residing on-premises and in the cloud
Assess data risk with contextual insights and analytics
Protect sensitive data sources through encryption and set flexible access policies
Monitor access to quickly uncover suspicious activity or risky behavior
Respond to threats in near real time
Simplify compliance and its reporting

Source: IDC and IBM, 2020

CHALLENGES/OPPORTUNITIES

People and process issues often impede data security projects. Successful projects require buy-in from senior management and strong leadership to ensure project deadlines are met and changes can be incorporated with minimal impact to employee workflows. In addition, security buyers seeking solutions for discovering and classifying data should consider tools that can address both unstructured and structured data types. IBM Security Guardium has a long history of being a trusted specialist in securing structured data. IBM only recently began extending capabilities beyond structured data stores in 2018, beginning with network area storage and SharePoint solutions. IBM has continued to invest in user interface (UI) improvements via new policy and query builders in support of unstructured data. Today the platform supports interoperability with a wide variety of cloud repositories and on-premises environments.

CONCLUSION AND BEST PRACTICES GUIDANCE

There is no silver bullet when it comes to protecting sensitive data. No single security technology investment will eliminate the risk of data theft or a mistake exposing sensitive information. But security teams are learning that they need to collect and centralize security and compliance information from all the tools at their disposal to proactively defend against attackers.

Antimalware, data loss prevention, information rights management, native DBaaS security tools, and backup and recovery solutions are collecting valuable telemetry that can be used by security teams to regain visibility and control in this era of growing complexity. Maximizing the value of this information requires a solution that can provide comprehensive situational awareness and be the glue that turns siloed point security solutions into a cohesive security infrastructure.

The success of any data security project requires buy-in from senior management and a committed chief information officer (CIO) or CISO that can execute on the following activities:

- Ensure that data classification and protection are integrated into the risk assessment process.
- Conduct a data discovery exercise to crawl the data stores throughout the environment, seeking all records and files that contain sensitive information based on patterns (regular expressions) and keywords.
- Confirm that solutions extend discovery, monitoring, and protection mechanisms across hybrid and multicloud environments and support structured and unstructured data.
- Identify and assign classification levels to data types within the organization. Start with regulated data that is privacy related or involves time-sensitive financial reporting.
- Determine the location and affiliation of sensitive data with users and applications. Identify acceptable use cases based on this information.
- Work to integrate common protection policies and compliance monitoring to data wherever it resides and wherever it travels. Policies can be applied based on user identity, nature of the content, normal data access and usage patterns, and so forth. These controls must "follow the data" wherever it goes.

MESSAGE FROM THE SPONSOR

To learn more about how IBM Security Guardium can help your organization embrace a Next Generation Data Security Approach visit IBM Security.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.