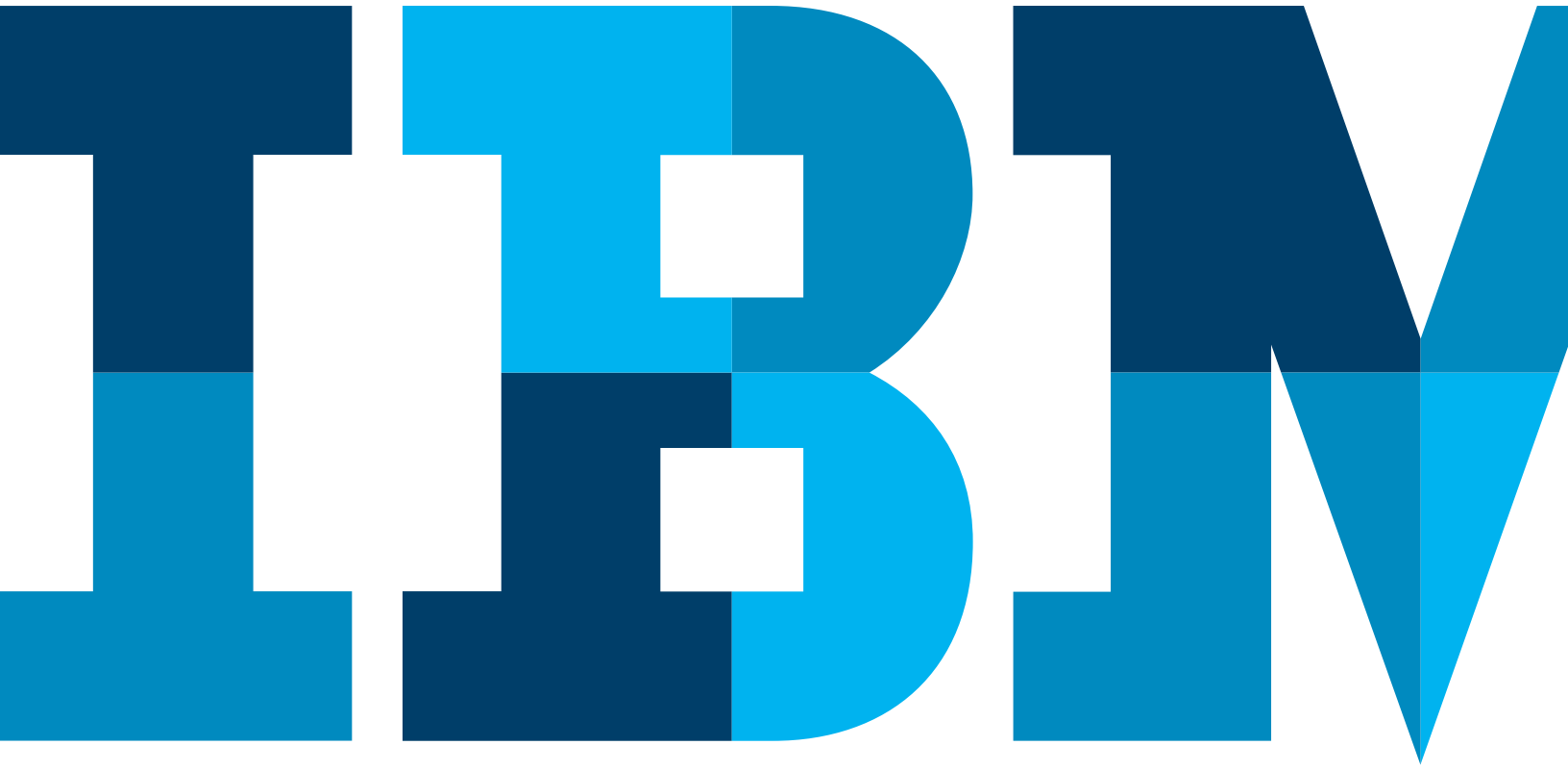
IBM Security
Thought Leadership White Paper

February 2016

Three guiding principles to improve data security and compliance

A comprehensive approach to data security across a complex threat landscape



IBM

Contents

Introduction

These days, data security breaches are more common than ever—and more expensive. The latest research shows that the average total cost of a data breach is now USD 5.85 million.[1] In the last year, we have seen a mounting 25 percent of company records stolen, resulting in loss of sensitive data, compromised brand reputation and huge costs incurred. The vast majority of value in most businesses rests in their intellectual property such as customer data, product designs, sales information, proprietary algorithms, communications, etc. The most damaging security incidents are those that involve the loss or illicit modification or destruction of sensitive data.

In response to this issue of persistent and increasing data breaches, regulations have been enacted around the world. Although the specifics of the regulations may differ, they generally exist to protect sensitive data (consumer, patient, etc.) and failure to comply can result in significant financial penalties, criminal prosecution, damage to brand and loss of customer loyalty and revenue.

In addition, the information explosion, the proliferation of endpoint devices, growing user types and volumes and new IT developments—such as cloud environments, big data analytics and the Internet of Things—create and proliferate new vulnerabilities. To secure sensitive data and address compliance requirements, organizations need to adopt a proactive and systematic approach.

Since sensitive data is the heart of most businesses, it is essential to ensure data privacy and to protect that data—no matter where it resides. Because of the dynamic, in-demand and distributed nature of data, organizations must take a comprehensive approach to safeguarding it by:

- **Understanding where sensitive data exists**: Organizations can't protect sensitive data unless they know where it resides and how it's related across the enterprise.
- **Safeguarding both structured and unstructured sensitive data**: Structured data contained in databases must be protected from unauthorized access, while unstructured data in documents, forms, image files and GPS systems also requires protection. All data types must meet various compliance requirements—all while still needing to be safely shared throughout an enterprise.
- **Protecting non-production environments**: Data in non- production, development, training and quality assurance environments needs to be protected, yet still usable during the application development, testing and training processes.
- **Securing and continuously monitoring access to sensitive data**: Enterprise databases, data warehouses, Hadoop and noSQL distributions, cloud environments and file shares require real-time monitoring to ensure data access is protected and audited. Policy-based controls determined by access patterns are required to rapidly detect unauthorized or suspicious activity, alert key personnel and stop the loss of sensitive data. In addition, sensitive data repositories need to be protected against new threats or other malicious activity and continually monitored for weaknesses.
- **Demonstrating compliance to pass audits**: It's not enough to develop a comprehensive approach to data security and privacy internally; organizations must also demonstrate and prove compliance to third-party auditors.

This paper will cover:

- Why there's a growing focus on data protection
- What the challenges are when protecting sensitive data
- Why you need a comprehensive approach to data security, rather than a mashup of point solutions
- How IBM—and our three guiding principles for data security—can help organizations achieve better security and compliance without impacting production systems or straining already tight budgets.

Why the growing focus on data security?

In 2015, Verizon published their latest report, 2015 Data Breach Investigations Report.[2] The headline for the paper was: "$400M. The estimated financial loss from 700 million compromised records shows the real importance of managing data breach risks." The Verizon report goes on to say "the year 2014 saw the term 'data breach' become part of the broader public vernacular with *The New York Times* devoting more than 700 articles related to data breaches, versus fewer than 125 the previous year."

Data security breaches are more common than ever—and more expensive. What's more, the loss of trade secrets, product designs or other intellectual property can spell financial ruin for an organization. Sensitive data is not only at the core of business interactions, it is also a highly valuable and attractive target for attack.

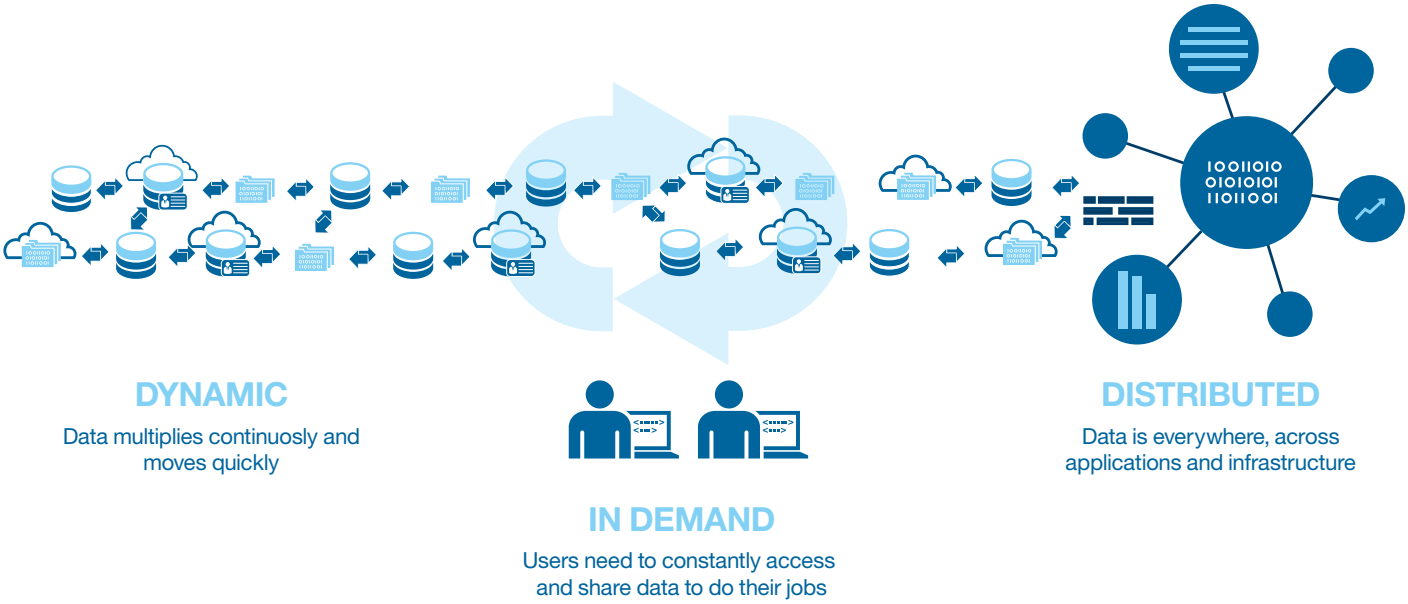


Figure 1: The dynamic, in-demand and distributed nature of data makes it challenging to secure.

Without a doubt, securing sensitive data is a challenging thing to do. When organizations try to tackle data-level security manually or with different tools to address different issues, they often get stuck. Securing sensitive data is challenging because data is difficult to control and pin down. It's dynamic—in different formats that constantly move and shift; it's in extreme demand by many different types of users; and it's highly distributed across the business environment, across applications, databases, cloud projects, big data projects and more (see Figure 1).

In spite of the growing frequency and costs of data breaches, prevention strategies at many companies are still immature. Frequently, organizations don't even know where their sensitive data is. Given that limitation, they certainly cannot stop abuse of data access privileges by authorized users. Additionally, many organizations admit to having sensitive data in non-production environments that is accessible to developers, testing and even third parties.

Changes in IT environments and evolving business initiatives

Security policies and corresponding technologies must evolve as organizations continue to embrace new business initiatives such as outsourcing, virtualization, Cloud, mobile and big data. This evolution means organizations need to think more broadly about where sensitive data resides and how it is accessed. Organizations must also consider a broad array of both structured and unstructured sensitive data, including customer information, trade secrets, intellectual property, development plans, competitive differentiators and more.

Cloud and big data projects often spin up on a departmental basis and are led by LOB executives, sometimes with little official IT department influence or control. In these scenarios, data security needs are often completely overlooked at a time when they are needed more than ever: Cloud and big data technologies are valuable to the business because they are fueled by sensitive data. However, Cloud and big data platforms often don't provide comprehensive data security capabilities—leaving low-hanging fruit for hackers to target.

Smarter, more sophisticated hackers

Many organizations are now struggling with the widening gap between hacker capabilities and security defenses. The changing nature, complexity and larger scale of outside attacks are cause for concern. Previously, the most critical concern was virus outbreaks or short denial-of-service attacks, which would create a temporary pause in business operations. Today, hackers are becoming more savvy and interconnected; they are part of organizations, leverage social networks, purchase pre-packaged "hacking" applications and some may even be state sponsored. By penetrating the perimeter and infiltrating the network, new advanced persistent threats (APTs) exploit employee knowledge gaps and process weaknesses. They also take advantage of technology vulnerabilities in random combinations to steal customer data or corporate data, such as trade secrets, resulting in the potential loss of billions of dollars, fines and lawsuits and irreparable damage to an organization's reputation.

Regulatory compliance mandates

The number and variety of regulatory mandates are too numerous to name here and they affect organizations around the globe. Some of the most prevalent mandates include the Sarbanes-Oxley Act (SOX), the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standard (PCI-DSS) (enforcement of which has firmly started expanding beyond North America), the Federal Information Security Management Act (FISMA) and the EU Data Privacy Directive. The number of regulatory mandates is made more complicated by the increasing pressure to show immediate compliance with mandates. Enterprises are under tremendous time pressure and need to show immediate progress to auditors—as well as to the business and shareholders—or face reputation damage and stiff financial penalties.

Insider threats

A high percentage of data breaches actually emanate from internal weaknesses or stolen priviledged use credentials. These breaches range from employees who may misuse payment card numbers and other sensitive information to those who save confidential data on laptops that are subsequently stolen. Furthermore, organizations are accountable for protecting data no matter where the data resides—be it with business partners, consultants, contractors, vendors or other third parties.

According to the latest IBM Security Services 2015 Cyber Security Intelligence Index, the insider threat continues to hold a top place in comparison to other attack types. While outsiders were found to be responsible for 45 percent of the attacks recorded in 2014, 55 percent of attacks were carried out by those who had insider access to organizations' systems.[3]

In summary, organizations are focusing more heavily on data security and privacy concerns. They are looking beyond developing point solutions for specific pains and toward building security and privacy policies and procedures into the enterprise. Building data security into business and IT policies is especially important to protect the business from regulatory risks and from the risk of data breaches.

Security versus privacy

- Data security and data privacy are related, but they are distinct concepts. Data security is the infrastructure-level lockdown that prevents or grants access to certain areas or data based on authorization. In contrast, privacy restrictions control access for users who are authorized to access a particular set of data. Data privacy ensures those who have a legitimate business purpose to see a subset of data do not abuse their privileges. That business purpose is usually defined by job function, which is defined in turn by regulatory or management policy, or both.
- Some examples of data security solutions include data activity monitoring and data repository vulnerability assessments. Some examples of data privacy solutions include data redaction and data masking. In a recent case illustrating this distinction, physicians at UCLA Medical Center were caught going through celebrity Britney Spears' medical records. The hospital's security policies were honored since physicians require access to medical records, but privacy concerns exist since the physicians were accessing the files out of curiosity and not for a valid medical purpose.

Common data security challenges

Businesses today operate infrastructures where data flows have multiplied because of the constant need that organizations have to better understand their customers, which leads to a tremendous increase in the data that's collected, managed and stored throughout the environment. Because sensitive data is critical to business success, it powers everything — from big data analytics projects to cloud projects to traditional database environments. What makes businesses flexible and smart can also make them very vulnerable.

The reality is that significant challenges and complexities exist. For one, there are numerous vendor solutions available that are focused on just one approach or one aspect of data protection. Few data security tools can cope with the full range of threats and data types and sources to deliver an intelligent and comprehensive strategy that can adapt as new threats arise and new technologies are embraced.

Additionally, few organizations have the funding or resources to implement yet another process-heavy initiative. Organizations need to build security and privacy policies into their daily operations and gather support for these policies across the enterprise including IT staff, business leaders, operations and legal departments. Privacy requirements do vary by role and understanding who needs access to what data is not a trivial task.

Finally, the manual or homegrown data protection approaches many organizations use today lead to high costs, higher risk and significant inefficiencies. Manual approaches typically don't protect a diverse set of data types in both structured and unstructured settings and do not scale as organizations grow. And, the rising number of compliance regulations with time-sensitive components adds more operational stress rather than clarifying priorities.

Organizations require a better approach to data protection — one that ensures they build security and privacy rules into their best practices and helps, rather than hinders, their bottom line. Numerous driving factors combined with high stakes make figuring out how to approach data security and privacy an important priority.

Use seven key questions to overcome data security challenges

In the past, teams tackling data security would either turn on database audit logs and perform labor-intensive and fallible manual reviews, or purchase separate point products to address different security-related challenges. Neither of these approaches is scalable or affordable enough to address enterprise-wide security and compliance requirements. Both of these approaches provide insufficient coverage and insight across the environment, leaving sensitive data exposed and vulnerable.

As attackers become more and more sophisticated and organized, organizations need an intelligent and comprehensive approach to data security more than ever. This approach must be able to adapt to protect diverse data types across physical, cloud and big data environments and support the protection of structured and unstructured data.

Leveraging a comprehensive approach helps focus limited resources without adding processes or increasing complexity. In addition to adaptability, a comprehensive approach also requires automation, which will help organizations support activities such as compliance in an automated and cost-effective way that doesn't interrupt critical business processes or daily operations.

To get started with comprehensive data security, organizations should consider seven key questions that will help teams focus in on the most critical and common data vulnerabilities:

1. Where does sensitive data reside across the enterprise?
2. Can you protect and monitor sensitive data — and audit access to it — wherever it resides (in databases, big data platforms, cloud environments, applications, file systems, etc)?
3. Can you protect sensitive data from both authorized users and unauthorized users?
4. Can confidential data in documents and files be safeguarded while still allowing appropriate business information to be shared?
5. Are the repositories that contain your sensitive data secured against attack, or are there exploitable gaps?
6. Do you have appropriate data encryption in place?
7. How can you reduce the cost of expanding data protection needs and meet audit compliance requirements?

The answers to these questions provide the foundation for a complete approach to data security that can scale appropriately. The answers also help organizations focus in on key areas they may be completely unaware of. Let's take a closer look at why the answers to those questions matter so much:

1. Organizations can't protect sensitive data if they don't know it exists — or where it's living. Sensitive data resides in structured and unstructured formats pretty much everywhere. And every time a new "important" project pops up, it's pretty safe to say there's probably sensitive data involved. Organizations need to document and define all data assets and relationships, no matter what the source. To be manageable, the data discovery process needs to be automated and must analyze data values and data patterns to identify the relationships that link disparate data elements into logical units of information, or "business objects" (such as customer identifier, patient record or invoice number).
2. Activity monitoring provides privileged and non-privileged user and application access monitoring that is, for example, independent of native database logging and audit functions. It can function as a compensating control for privileged user separation-of-duties issues by monitoring all administrator activity. Activity monitoring also improves security by detecting unusual database, data warehouse, file share or big data (Hadoop and noSQL) systems read and update activities from the application layer. Event aggregation, correlation and reporting provide audit capabilities without the need to enable native audit functions. Activity monitoring solutions should be able to detect malicious activity or inappropriate or unapproved privileged user access.
3. Data should be protected through a variety of data transformation techniques including encryption, masking and redaction. Defining the appropriate business use for enterprise data will dictate the appropriate data protection mechanism or policy. For example, a policy might need to be established to mask data on screen or on the fly to

prevent call center employees from viewing national identifier numbers. Or, you might need to mask revenue numbers in reports that get shared with business partners or third-party vendors.

4. Data redaction can remove sensitive data from forms and documents based on job role or business purpose. For example, physicians need to see sensitive information such as symptoms and prognosis data, whereas a billing clerk only needs the patient's insurance number and billing address. The challenge is to provide the appropriate protection while still meeting business needs and ensuring that data is controlled at a "need-to-know" level. Data redaction solutions should be able to protect sensitive information in unstructured documents, forms and graphics.
5. Data repository vulnerability assessment and remediation is important to address to ensure that your sensitive data repositories are secure and hardened against attack. Automated vulnerability assessment should be able to identify risks and security gaps in databases, data warehouses and big data environments that could be exploited by intruders and hackers to gain access to sensitive data. Data infrastructures are highly dynamic, with changes in accounts, configurations and patches occurring frequently. But most organizations lack the centralized control or skilled resources to systematically review changes and determine if security gaps have emerged. Look for vulnerability assessment capabilities that are automated, that can scan targeted systems on a scheduled basis to detect vulnerabilities and are able to create a specific, actionable remediation plan.
6. Data encryption is not a new technology and many different approaches to encryption exist. Encryption is explicitly required by many regulations including PCI DSS and also enables safe harbor provisions in many regulatory mandates. This means organizations are exempt from disclosing data breaches if the data is encrypted. It is challenging for an organization to identify the best encryption approach due to prolific offerings from various vendors. For encrypting structured data, consider a file-level approach. This will protect both structured data in the database management system (DBMS) and also unstructured files such as DBMS log or configuration files and is transparent to the network, storage and applications. Look for encryption offerings that provide a strong separation of duties and a unified policy and key management system to centralize and simplify data security management.
7. Compliance and data security are not one time events. Many organizations focus on compliance as the start of their data security journey, but both activities must be ongoing and will change and expand over time. It's important to find a solution that is able to meet a wide range of data security and protection requirements — from basic compliance to comprehensive data protection — in a cost-effective and scalable way that will work over the long term. IT environments will change and grow (adding technologies such as big data platforms, new databases, new applications, cloud environments, etc.), new users and different types of users will need to be added to the data security ecosystem over time and the solution will need to expand over time. So functionality such as automated load balancing and automated administration quickly become an important consideration. Determining how to keep costs down over time should be an important part of your selection criteria.

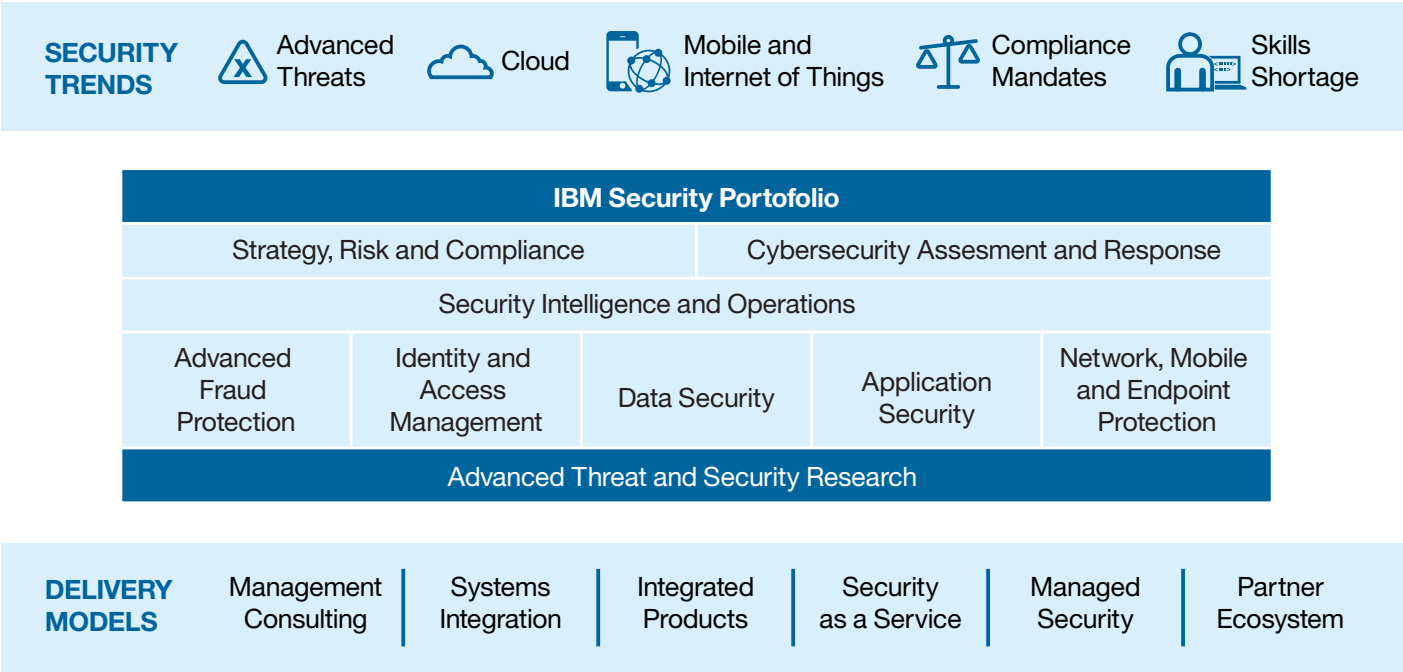


Figure 2: IBM Security provides an integrated portfolio, including technologies and services that are aligned to our client's security needs and are supported by industry-leading expertise and research.

IBM Security Framework

The goal of the IBM portfolio is to help organizations meet legal, regulatory and business obligations while keeping the overall total cost of ownership as low as possible. This helps organizations support compliance initiatives, reduce costs, minimize risk and sustain profitable growth. Read more about keeping costs low in the 2015 Forrester Total Economic Impact Study of IBM Security Guardium[4].

The alignment of people, process, technology and information separates IBM data security and privacy solutions from the competition. Data security and the IBM Security Guardium solution are key components within the IBM Security Framework (see Figure 2), which provides the technologies, best practices, expertise, data analysis and maturity models necessary to provide IBM clients with the opportunity to embrace security with confidence.

IBM® Security Guardium's Three Guiding Principles to Data Security

IBM® Security Guardium is a comprehensive data security solution designed to safeguard critical data, wherever it resides. Guardium capabilities support three guiding principles that help ensure comprehensive data security:

1. Analyze: Automatically discover sensitive data and uncover risks to take action and prevent data breaches.
2. Protect: Provide complete protection for sensitive data. This includes the ability to protect the data itself, to protect the business from risk by providing automated compliance support and the ability to control and manage access to sensitive data, including blocking unauthorized privileged user accesses.
3. Adapt: Seamlessly handle changes within your IT environment as you add new users and new technologies and need to adjust to the increasing volumes of data moving throughout the environment in a manageable and cost-effective way.

By leveraging a solution that follows these three principles, organizations can safeguard sensitive data and meet compliance mandates with confidence while containing costs and improving efficiency.

Analyze

For effective data security and before you can even begin to protect data, organizations first need to analyze. They need to identify their sensitive data and determine where that sensitive data resides across the enterprise. They also need to analyze to automatically uncover risks and threats to sensitive data throughout the enterprise in real time, as well as in right time.

Organizations must discover where sensitive data resides, classify and define data types and determine metrics and policies to ensure protection over time. Data can be distributed over multiple applications, databases, big data platforms, cloud environments, etc. Many organizations rely too heavily on system and application experts for this information. Sometimes, this information is built into application logic and hidden relationships might be enforced behind the scenes.

Finding sensitive data and discovering data relationships requires careful analysis. Data sources and relationships should be clearly understood and documented so no sensitive data is left vulnerable. Only after understanding the complete landscape can organizations define proper enterprise data security and privacy policies.

Guardium delivers value across a wide range of industries

- **A large insurance firm can now manage security for approximately 1,000 databases with just one full-time employee.**
- **A large utilities company achieved a 55 percent return on investment (ROI) in less than one year, helping ensure SOX and PCI compliance for 4.5 million accounts.**
- **A global bank can monitor more than 5,000 data sources, including big-data transactions, in real time—without impacting the performance of critical applications.**
- **An international telecommunications company is now able to centrally monitor and respond in real time to data access activity on thousands of databases dispersed in 16 data centers worldwide.**
- **An automotive manufacturer can monitor and audit 500 production databases to help increase security, while reducing its security staff requirements by 90 percent.**

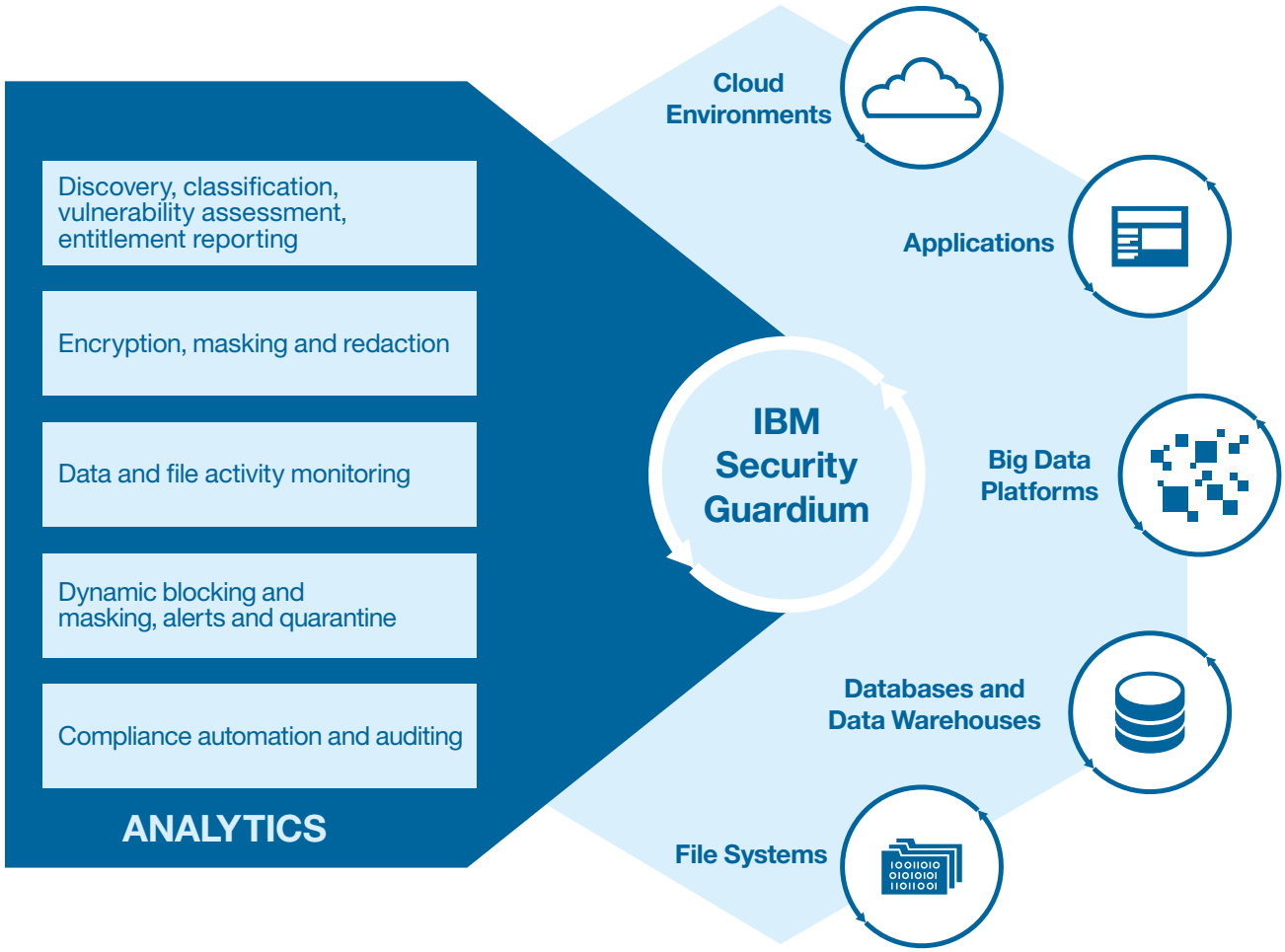


Figure 3: IBM Security Guardium delivers analytics, deep data protection capabilities and adaptability to support comprehensive data security

You need an automated process to identify data relationships and define business objects. Without automation, organizations can spend months or years performing manual analysis—with no assurance of completeness or accuracy. IBM Security Guardium is a comprehensive, intelligent data security solution. It can help discover sensitive data and automatically and accurately identify relationships and define business objects in a fraction of the time required using manual or profiling approaches. It accommodates a wide range of enterprise data sources, including relational databases, hierarchical databases, any structured data source represented in text file format, big data platforms—including Hadoop and noSQL, applications, file systems and cloud environments. Analytics capabilities are delivered across all the Guardium modules, making the solution more intelligent, making security teams more efficient, reducing risk and cost.

In summary, when it comes to automated discovery and classification, IBM Security Guardium can help organizations:

- Locate and inventory the data sources across the enterprise
- Identify and classify sensitive data
- Understand data relationships
- Define and document privacy rules
- Document and manage ongoing requirements and threats

IBM Security Guardium can also analyze the environment and automatically uncover internal and external threats. For deep analysis, Guardium offers outlier detection capabilities with the intelligence to understand risk based on changes in user behavior. It uses an advanced machine-learning algorithm to detect unauthorized actions based on detailed contextual information—the "who, what, where, when and how" of each data access attempt. With an adaptive learning process, it compares new normal activity patterns against new activities as they accumulate. Its intuitive user interface helps pinpoint anomalies, so administrators can drill down to investigate the root cause.

Protect

Data security and privacy solutions should provide complete protection. This means that the solution should be able to protect sensitive data via actions such as masking, encryption and redaction; but it goes further. A data security solution must also be able to protect the business from financial risk by providing automated compliance support to get the right reports to the right people at the right time.

Protecting the sensitive data and protecting the business from audit failure have a common point of intersection: the ability to support entitlement reporting—so you can successfully create compliance workflows and also successfully monitor and control access to sensitive data. Entitlement reporting is foundational to your ability to protect.

IBM Security Guardium helps protect sensitive data in ERP/CRM applications, databases, warehouses, file shares, Hadoop and noSQL based systems and also in unstructured formats such as forms and documents. Key protection capabilities include activity monitoring, data masking, data redaction and data encryption. Guardium provides enterprise-wide controls and capabilities across many platforms and data sources, enhancing the investments made in platforms, such as RACF on System z, that provide built-in security and VSAM. A holistic data protection approach ensures a 360-degree lockdown of all sensitive organizational data.

Different capabilities are required for different types of data (structured, unstructured, offline and online), but those capabilities need to integrate as part of a common platform for comprehensive data security. Keep in mind that various data types exist in both production and non-production environments.

Types of data

- **Structured data**
  This data is based on a data model and is available in structured formats like databases or XML.
- **Unstructured data**
  This data is in forms or documents which may be handwritten, typed or in file repositories, such as word processing documents, pictures, digital audio, video, GPS data and more.
- **Online data**
  This is data used daily to support the business, including metadata, configuration data or log files.
- **Offline data**
  This is data in backup tapes or on storage devices.

Keep in mind these four basic data types are exploding in terms of volume, variety and velocity. Many organizations are looking to include these data types in big data systems such as Hadoop or NoSQL for deeper analysis.

Let's take a closer look at how Guardium can help secure sensitive data:

IBM Security Guardium Vulnerability Assessment provides a security solution which addresses the entire data security and compliance life cycle with a unified web console, back-end data store and workflow automation system. IBM Security Guardium Vulnerability Assessment helps:

- By providing a scalable platform that helps protect and secure customer data repositories and manage PCI-DSS, SOX Audit and Compliance Mandates
- Enforce DoD STIG and CIS security best practice guidelines with specific tests and customization options for each data source type
- Deliver dynamic reports that provide recommendations on how to fix each data source vulnerability to remediate exposures and simplify security operations
- Support advanced user & role management (a.k.a separation of duties) to keep security and data administration separate. All operations completed by Guardium Vulnerability Assessment, including administration and configuration, are audited to maintain compliance controls. Security professionals can run reports without support from IT staff.
- Enable automated and built-in compliance workflows (review, escalation, sign-off) for Sarbanes-Oxley (SOX), Payment Card Industry Data Security Standard (PCI DSS) and Health Insurance Portability and Accountability Act (HIPAA) compliance mandates. An easy-to-use graphical user interface allows a wide variety of processes to be created to match the unique needs of the tasks and individuals involved. Numerous audit tasks are supported, including reviewing the results of automatically generated vulnerability assessments, asset discovery and data classification. Export reports to different formats including PDF, CSV, CEF, Syslog forwarding, SCAP, AXIS or custom schemas for better integration to SIEM solutions or for Business Intelligence reporting.

IBM Security Guardium Data Activity Monitor continuously monitors data access and protects data across the enterprise to help ensure the security and integrity of data in heterogeneous environments including databases, data warehouses, files, file shares, cloud and big data platforms such as Hadoop and NoSQL.

IBM Security Guardium Data Activity Monitor helps:

- Uncover risks to sensitive data through data discovery, classification and privileged access discovery to automatically take action or report for compliance
- Reduce data breach risk and extend security intelligence with in-depth data protection
- By providing a streamlined and adaptable solution for real-time monitoring of high-value data environments
- Minimize total cost of ownership with robust scalability, simplification, automation, analytics and transparency for a range of deployments—whether they are small, large or enterprise-wide
- By providing powerful analytic insights that enable you to centrally visualize and analyze data activity from a heterogeneous data environment using a single format. Apply leading-edge analytic tools to obtain actionable insights on data access behavior with tools such as Connection Profiling, Quick Search real-time forensics, Outlier Detection algorithms and an Investigative Dashboard
- Support automated compliance workflows by providing built-in customization capabilities as well as preset compliance accelerators (reports review, escalations, sign-offs, etc.). It creates custom processes by specifying your unique combination of workflow steps, actions and user and enables automated execution of oversight processes on a report line-item basis, maximizing process efficiency without sacrificing security. It ensures that some team members see only data and tasks related to their own roles and stores process results in a secure centralized repository. Supports SOX, PCI, HIPAA and more with pre-defined reports for top regulations. An easy-to-use graphical user interface allows a wide variety of processes to be created to match the unique needs of the tasks and individuals involved. Many different audit tasks are supported, including reviewing the results of automatically generated vulnerability assessments, asset discovery and data classification. Export reports in varying formats, which include PDF, CSV, CEF, Syslog forwarding, SCAP or custom schemas.
- With predefined security policies that allow you to create and manage your own data security policies based on audit data or leverage out-of-the-box predefined policies. The policies can be built to detect any threat scenario against the data utilizing the most common audit constructs such as who, from where, when, where to, on what, what action and other contextual information.

Traditionally, protecting unstructured information in forms, documents and graphics has been performed manually by deleting electronic content and using a black marking pen on paper to delete or hide sensitive information. But this manual process can introduce errors, inadvertently omit information and leave behind hidden information within files that exposes sensitive data. Today's high volumes of electronic forms and documents make this manual process too burdensome for practical purposes and increase an organization's risk of exposure.

IBM Security Activity Monitor for Files is built just like Guardium Data Activity Monitor, but it protects sensitive files and file systems. This Guardium module prevents unauthorized data access, alerts on changes or leaks to help ensure data integrity, automates compliance controls and protects against internal and external threats. Continuous monitoring and real-time security policies protect unstructured data across the enterprise without changes to file systems or applications or performance impact. It provides insight into your document and file contents, and usage patterns. IBM Security Guardium Activity Monitor for Files lets you discover, track, and control access to sensitive files on either local or networked file systems.

IBM Security Guardium Activity Monitor for Files can help you meet compliance obligations and reduce the risks of major data breaches by:

- Monitoring and auditing all file data activity across your enterprise file systems
- Enforcing security policies in real time — for all file access, change control and user activities
- Creating a centralized repository of audit data for enterprise compliance, reporting and forensics
- Supporting heterogeneous environments, including all leading platforms, file shares and operating systems

IBM Security Guardium Data Redaction protects sensitive information buried in unstructured documents and forms from unintentional disclosure. The automated solution lends efficiency to the redaction process by detecting sensitive information and automatically removing it from the version of the documents made available to unprivileged readers. Based on industry-leading software redaction techniques, IBM Security Guardium Data Redaction also offers the flexibility of human review and oversight if required.

IBM Security Guardium Data Encryption provides a single, manageable and scalable solution to encrypt enterprise data without sacrificing application performance or creating key management complexity. IBM Security Guardium Data Encryption helps solve the challenges of invasive and point approaches through a consistent and transparent approach to encrypting and managing enterprise data security. Unlike invasive approaches such as column-level database encryption, PKI-based file encryption or native point encryption, Guardium Data Encryption offers a single, transparent solution that is also easy to manage. This unique approach to encryption provides the best of both worlds: seamless support for information management needs combined with strong, policy-based data security. Agents provide a transparent shield that evaluates all information requests against easily customizable policies and provides intelligent decryption-based control over reads, writes and access to encrypted contents.

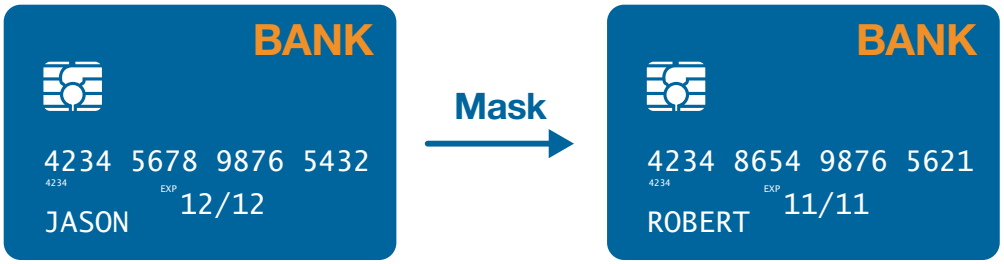


Figure 4: Personal identifiable information is masked with realistic but fictional data

This high-performance solution is ideal for distributed environments and agents deliver consistent, auditable and non-invasive data-centric security for virtually any file, database or application — anywhere it resides.

In summary, Guardium Data Encryption provides:

- A single, consistent, transparent encryption method across complex enterprises
- An auditable, enterprise-executable, policy-based approach
- Among the fastest implementation processes achievable, requiring no application, database or system changes
- Simplified, secure and centralized key management across distributed environments
- Intelligent, easy-to-customize data security policies for strong, persistent data security
- Strong separation of duties
- Top-notch performance with proven ability to meet SLAs for mission-critical systems

IBM InfoSphere Optim™ Data Masking Solution provides a comprehensive set of data masking techniques that can support your data privacy compliance requirements on demand, including:

- Application-aware masking capabilities help ensure that masked data, like names and street addresses, resembles the look and feel of the original information. (see Figure 4)
- Context-aware, prepackaged data masking routines make it easy to de-identify elements such as payment card numbers, Social Security numbers, street addresses and email addresses.
- Persistent masking capabilities propagate masked replacement values consistently across applications, databases, operating systems and hardware platforms.
- Static or dynamic data masking supports both production and non-production environments.

With InfoSphere Optim, organizations can de-identify data in a way that is valid for use in development, testing and training environments, while protecting data privacy.

IBM Security Key Lifecycle Manager helps IT organizations better manage the encryption key lifecycle by enabling them to centralize and strengthen key management processes. It can manage encryption keys for IBM self-encrypting storage devices as well as non-IBM encryption solutions that use the Key Management Interoperability Protocol (KMIP). IBM Security Key Lifecycle Manager provides the following data security benefits:

- Centralize and automate the encryption key management process
- Enhance data security while dramatically reducing the number of encryption keys to be managed
- Simplify encryption key management with an intuitive user interface for configuration and management
- Minimize the risk of loss or breach of sensitive information
- Facilitate compliance management of regulatory standards such as SOX and HIPAA
- Extend key management capabilities to both IBM and non-IBM products
- Leverage open standards to help enable flexibility and facilitate vendor interoperability

Adapt

Data infrastructures are constantly changing and growing—making it challenging to keep up with emerging and shifting data security gaps. Guardium gives organizations the power to:

- Support traditional and disruptive data technologies—such as Hadoop, NoSQL and cloud
- Easily expand the data protection architecture, growing from regulatory compliance to comprehensive data protection
- Reduce costs and improve results using a single data protection infrastructure—one that automatically load balances—across the entire data environment

Guardium enables organizations to adapt to changes in the data environment, expanding data protection to address new users, platforms and types of data. Guardium supports a very broad range of platforms, including traditional databases, cloud environments, Hadoop-based systems, NoSQL and in-memory systems, file systems and applications.

Guardium also provides agile control that can be deployed for specific security requirements and then can be easily scaled to provide additional protection as business needs evolve. Guardium is architected to support changing IT environments and infrastructure requirements and includes centralized and automated system and load management to make teams more efficient and reduce the cost of data security.

Unlike other solutions, Guardium supports heterogeneous integration with other industry-leading security solutions, vulnerability standards, applications and more. Guardium also provides best-of-breed integration with IBM Security solutions, such as IBM Security QRadar® SIEM, for proactive data protection. Guardium sends its events and database discovery/classification information to QRadar SIEM, enabling more effective correlation of threat activity. In addition, Guardium can receive status and alert notifications from QRadar SIEM to help defend against rogue IP sources, rogue users and new vulnerabilities, whether in applications, operating systems or other data sources. For example, the Guardium and QRadar integration can help organizations protect against potential attacks through applications; detect database attacks (such as through SQL injection) and block them before data can be extracted; and identify vulnerabilities at the application layer for virtual patching remediation.

Conclusion: Comprehensive data security for peace of mind

Securing sensitive data and protecting privacy is a detailed, continuous responsibility. All businesses need to secure sensitive data against a breach and ensure they are able to respond quickly to minimize loss and damage in the event of a breach. By providing capabilities that follow the three guiding principles, IBM Security Guardium is able to provide a comprehensive data security solution that is integrated, intelligent and automated to safeguard sensitive data.

Securing data requires a 360-degree, comprehensive approach. With deep and broad expertise in the security space, IBM can help your organization define and implement such an approach. IBM solutions are open, modular and support all aspects of data security, including structured, semi-structured and unstructured data, no matter where it resides. Guardium supports virtually all leading enterprise databases and operating systems, including IBM DB2®, Oracle, Teradata, Netezza®, Sybase, Microsoft SQL Server, IBM Informix®, IBM IMS™, IBM DB2 for z/OS, IBM Virtual Storage Access Method (VSAM), Microsoft Windows, UNIX, Linux and IBM z/OS®. IBM also supports key ERP and CRM applications — Oracle E-Business Suite, PeopleSoft Enterprise, JD Edwards EnterpriseOne, Siebel and Amdocs CRM — as well as most custom and packaged applications. IBM supports access monitoring for file sharing software such as Microsoft SharePoint and IBM FileNet and supports sensitive file data (VSAM z/OS data sets, FTP, Linux, Windows, Unix, etc). IBM also supports Hadoop-based systems such as Cloudera, Hortonworlks and IBM InfoSphere BigInsights, as well as NoSQL platforms such as MongoDB, Cassandra, Couch DB, Pivotal, etc.

About IBM Security solutions

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 15 billion security events per day in more than 130 countries and holds more than 3,000 security patents.

For more information

For more information on IBM security, please visit: **ibm.com**/security. To learn more about IBM Security Guardium, please contact your IBM sales representative or visit: **ibm.com**/guardium. To learn more about the new IBM DB2 for z/OS security features, download the Redbook at www.redbooks.ibm.com/Redbooks.nsf/RedbookAbstracts/sg247959.html

IBM Corporation
IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
February 2016

1 *2015 Cost of Data Breach Study: Global Analysis*, Ponemon Institute LL, May 2015 (**ibm.com**/security/data-breach)

2 *2015 Data Breach Investigations Report*, Verizon, (www.verizonenterprise.com/DBIR/2015)

3 *IBM X-Force Threat Intelligence Quarterly, 2Q 2015*, IBM, June 2015 (**ibm.biz**/X-Force_Threat_Intelligence)

4 *The Total Economic Impact™ Of IBM Security Guardium*, Forrester Study commisioned by IBM, September 2015 (**ibm.biz**/TEI_Of_IBM_Security_Guardium_2015)

Please Recycle

IMW14568-USEN-06