IBM Security
Thought Leadership White Paper

January 2016

Protecting your critical data with integrated security intelligence

Automatically identify and control data breach threats through closed-loop security intelligence to and from the data layer

Contents

Introduction

The world depends more than ever on highly sensitive digital information—from customer credit cards to electronic health records to classified government data—and this confidential information is an increasingly attractive target for criminals. As a result, staying ahead of these sophisticated attacks requires a comprehensive, layered approach to data security that helps organizations identify anomalies and take action before any serious damage can occur.

By integrating data monitoring and vulnerability assessment with overall security intelligence, organizations can uncover hidden relationships within massive amounts of security data. The analytics can extend across the entire IT environment, so threats against traditional databases as well as unstructured "big data" and file system sources can be correlated with suspicious activity at the network, infrastructure or application level. This way, millions of security events can be reduced and correlated into a manageable list of prioritized incidents.

This white paper explains an integrated approach for extending security intelligence with data security insights—for example, by combining the industry-leading security intelligence capabilities of IBM® QRadar® Security Intelligence Platform with the broad, deep and feature-rich data security capabilities of IBM Security Guardium®. The result is a comprehensive solution that helps organizations prevent attacks, identify risk, ensure compliance and reduce the overall costs of security management.

The complexities of data security

In today's interconnected world, information security is expanding beyond its technical silo into a strategic, enterprise-wide priority. The reason? The cost of a data breach is on the rise—from an average of USD1.33 million in 2013 to USD1.57 million in 2015, according to a recent study by the Ponemon Institute.[1]

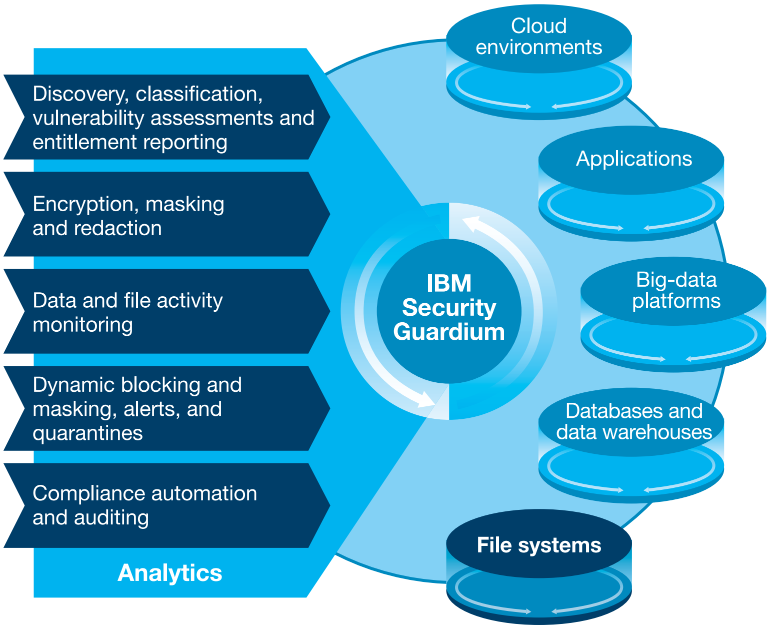
Some of the key operational and security challenges for ensuring data security involve understanding and having complete and immediate visibility into:

- Where sensitive data is stored
- Who has access to the data
- What data is being viewed, modified or deleted
- When a potential data breach or policy violation has occurred
- How to prevent data breaches and reduce exposure

Protecting data across the enterprise

Today's organizations are part of a new era of computing, where the variety and velocity of data is unprecedented. Social media feeds, video blogs, click streams, sensor data, log files and more can all be analyzed to create invaluable insights on improving customer satisfaction—which in turn creates more customer demand and requires still more openness for data. And as business data grows in value, the repositories holding that data are even more vulnerable to attack.

In addition, as organizations aggregate more data, they are subject to a growing body of security regulations, such as those protecting customer credit card, healthcare and financial information. This means that traditional, perimeter-based approaches to data protection are no longer sufficient. Organizations must tighten security controls closer to their databases, file systems and big-data platforms.


Discovery, classification, vulnerability assessments and entitlement reporting
Encryption, masking and redaction
Data and file activity monitoring
Dynamic blocking and masking, alerts, and quarantines
Compliance automation and auditing
Analytics
IBM Security Guardium
Cloud environments
Applications
Big-data platforms
Databases and data warehouses
File systems

IBM Security Guardium is a comprehensive data security platform that helps security teams secure and manage all types of sensitive data consistently, whether it is in big-data platforms, databases or file systems.

A holistic approach with real-time database monitoring, auditing and vulnerability assessments can help assure the privacy and integrity of trusted information in a transparent, non-intrusive and efficient way. Data security and compliance insights enhance the coverage of security intelligence solutions to better uncover possible risks. However, by combining data security capabilities with proven analytics, organizations can uncover insights hidden in large volumes of security data—even across operational silos—for immediate threat prevention.

Monitoring privileged users

Most IT environments require privileged users—such as database administrators, developers and even contractors—to manage, support or run critical resources. But these “super users” can easily bypass application- or network-level security control points because they have authorization to access the resources. By restricting access to data based on job responsibilities, or using other built-in data-source security controls, organizations can prevent end users from accessing sensitive data in data sources. But these measures cannot prevent privileged users from executing data-source commands on sensitive objects. Many organizations have no way to control what data-source administrators do with their most sensitive data, and they cannot detect if inappropriate activity is taking place.

Moreover, many of these privileged users may have jurisdiction over the security controls or tracking methods for their organization’s data resources. To enhance data security, organizations need a centralized, independent way to protect data integrity and prevent data breaches in real time—especially from privileged users—as well as get more insight into the security incidents that should be prioritized for response.

Identifying threats in real time

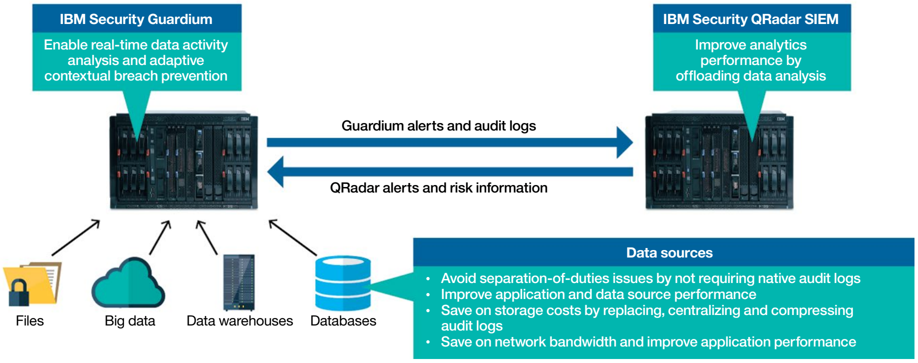
To immediately thwart unauthorized or suspicious access to sensitive data, even by privileged users, organizations need to be able to continuously monitor and analyze database activity in real time. However, according to the Ponemon Institute, in most data breaches, perpetrators have an average of 256 days to exploit the vulnerabilities before the breach is discovered.[1]

Many organizations understand that data security is important for ensuring regulatory compliance, as well as for building customer trust and brand reputation. But implementing a homegrown approach—as some organizations do—can be costly and ineffective. The native database logging employed by these solutions:

- Requires significant labor, time and expertise to extract audit logs from diverse systems, normalize data, correlate information, filter down to meaningful events and remediate identified issues
- Often significantly reduces the performance and stability of business-critical applications
- Leaves gaps in security because there is limited visibility in the information collected; even worse, collected data is not real time—giving attackers plenty of time to wreak havoc before the target organization even knows the anomaly occurred
- Fails auditors' requirements for segregation of duties, because database logging is not controlled by IT security personnel and can easily be circumvented by database administrators
- Limits the ability to enforce security policies enterprise-wide, since manual auditing of different systems can deliver inconsistent information

Rather than resorting to manual approaches, organizations need to be able to automatically monitor the entire data environment, detect suspicious activity and take preventive action, without sacrificing any performance.

IBM Security Guardium synergizes with IBM Security QRadar:
Optimize data security and expand the reach of security intelligence


IBM Security Guardium
Enable real-time data activity analysis and adaptive contextual breach prevention
IBM Security QRadar SIEM
Improve analytics performance by offloading data analysis
Guardium alerts and audit logs
QRadar alerts and risk information
Files
Big data
Data warehouses
Databases
Data sources

- Avoid separation-of-duties issues by not requiring native audit logs
- Improve application and data source performance
- Save on storage costs by replacing, centralizing and compressing audit logs
- Save on network bandwidth and improve application performance

Deployed together, IBM Security Guardium and IBM Security QRadar SIEM can provide significant risk prevention, performance and cost benefits for data environments.

Comprehensive data protection with Guardium

To secure databases, data warehouses, file servers and big-data platforms such as Hadoop or NoSQL, organizations are turning to Guardium for integrated technologies for managing the entire data security and compliance lifecycle. Guardium gives organizations the capabilities to automatically analyze what is happening across the data environment to help minimize risk, protect sensitive data from internal and external threats, and seamlessly adapt to changes that affect data security.

The Guardium approach is designed to help organizations understand the who, what, when, where and how of database, warehouse, file share and big-data system transactions. With full insight, organizations can understand data and application access patterns, prevent data leakage, enforce data change controls and respond to suspicious activities in real time.

By deploying Guardium, organizations can:

- Analyze data risk—Automating the discovery and understanding of sensitive data exposure can help organizations plan for appropriate mitigation strategies.
- Protect sensitive data—Identity and access governance capabilities can help protect sensitive data from both internal and external sources, including privileged users.
- Adapt to change—Expanding the data protection architecture is critical to grow security capabilities from regulatory compliance to comprehensive data protection.

While Guardium provides an effective data perspective on identifying anomalies and subtle indicators of attack, it also has the flexibility to meet a wide range of data security and protection requirements—from basic compliance to comprehensive data protection—with a multi-layered, automated approach to threat analytics, data protection and enterprise-wide visibility to adapt to change. As a result, organizations get prioritized, actionable insights into potential offense sources across the environment so they can:

- Enhance business agility and resiliency by automating security and privacy
- Improve data security and mitigate risk by reducing fraud and cost of compliance requirements
- Gain enterprise-wide security intelligence to defend against persistent threats

Enterprise-wide actionable intelligence with QRadar

For layered protection across the organization, Guardium integrates with QRadar Security Intelligence Platform solutions to detect and prioritize threats in real time. QRadar solutions dramatically expand visibility into network and security device log sources, network flows, user identities and activity, asset configurations, external threats and more. The solutions automatically correlate events and detect anomalies so organizations can rapidly respond to a dramatically reduced list of high-priority security incidents.

By implementing QRadar security intelligence solutions, organizations can:

- **Prevent threats**—By using detailed security insights and behavioral algorithms, organizations can intelligently prioritize threat alarms from thousands of security events and prevent targeted attacks against critical data resources.
- **Consolidate security log silos**—By collecting, correlating and reporting on security event and network telemetry data in one integrated solution, organizations can ensure smoother operations and facilitate compliance.

- **Detect insider fraud**—By extending security intelligence with identity management insights, organizations can quickly detect when privileged users or other trusted insiders attempt to steal or destroy data.
- **Predict business risks**—By automating security policy monitoring and evaluation of device configuration changes across a massive infrastructure, organizations can improve network visibility, understand and prioritize vulnerabilities, and reduce risks.
- **Address regulation mandates**—Using automated data collection and configuration audits, organizations can meet compliance mandates and make operational and security improvements that reach across the infrastructure.

Conclusion

By extending their security intelligence with data security insights, organizations can proactively identify, monitor and address the most sophisticated threats. They can analyze previous breach patterns to predict potential areas of attack, mine employee systems behavior to identify patterns of potential misuse and monitor the external environment for potential security threats.

IBM Security solutions, including Guardium and QRadar Security Intelligence Platform, are trusted by organizations worldwide for comprehensive, layered data and network protection. These proven technologies enable organizations to protect their critical resources from emerging threats and achieve peace of mind for years to come.

For more information

To learn more about Guardium, QRadar or other IBM Security solutions, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/security

© Copyright IBM Corporation 2016

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
January 2016

IBM, the IBM logo, ibm.com, Guardium, QRadar, and X-Force are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at **ibm.com**/legal/copytrade.shtml

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

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.

[1] Ponemon Institute, “2015 Cost of Data Breach Study: Global Analysis,” *Ponemon Institute LLC*, May 2015. http://www-03.ibm.com/security/data-breach/

Please Recycle