Get smart to shut down insider threats

Reduce the risk of insider-related data loss with intelligent, integrated security from IBM

Fight the growing threats from trusted insiders

Security breaches are all over the news, and it can be easy to think that all the enemies are outside your organization. But the harsh reality is that more than half of all attacks are caused by either malicious insiders or inadvertent actors.[1] In other words, the attacks are instigated by people you'd be likely to trust. And the threats can result in significant financial or reputational losses.

Who represents an insider threat?

An insider, in this case, is anyone who has physical or remote access to your organization's assets. The threats can come from:

- Disgruntled employees—who decide to share sensitive information for personal gain or revenge
- Malicious employees—who intentionally misuse their access to networks, systems or data to cause harm
- Compromised employees—who unintentionally leave their systems open to attack or who make mistakes that open the door to malware (such as clicking on malware-laced emails that enable attackers to steal access credentials)
- Third parties (contractors, partners and clients)—who have trusted access to your sensitive data and represent the same types of threats as above

How can you fight back?

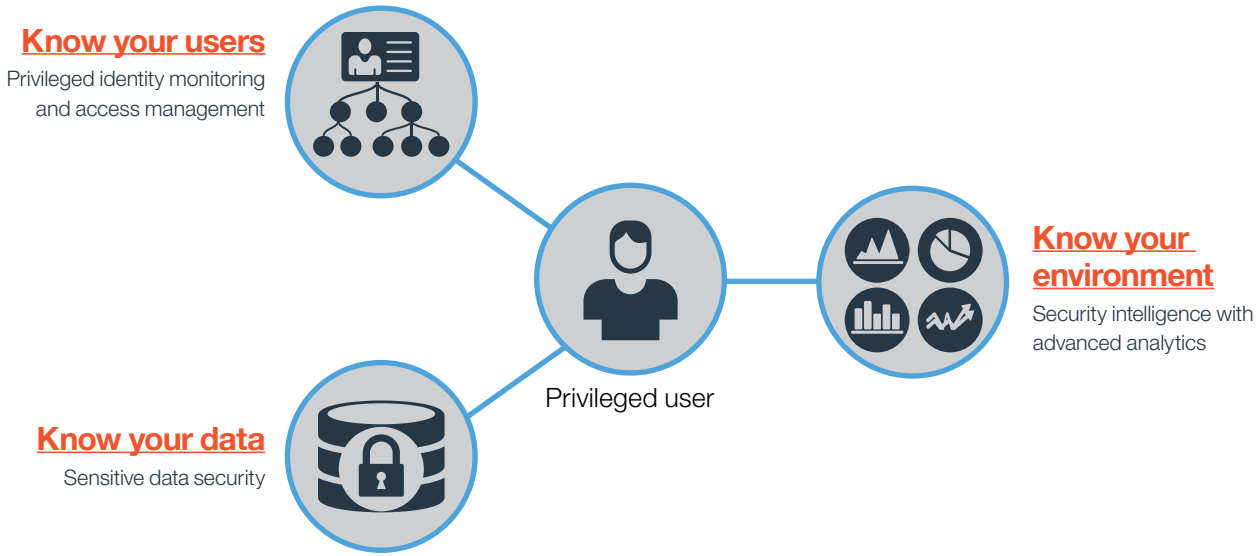
Educating employees about suspicious communications and potential risks is important. However, these efforts must be backed by integrated solutions that can proactively protect against emerging internal threats.

60% of attacks are carried out by those who have insider access.[1]

[1] "Reviewing a year of serious data breaches, major attacks and new vulnerabilities," *IBM X-Force Research: 2016 Cyber Security Intelligence Index*, April 2016.

Get started by understanding your users, data and environment

To protect against insider threats, you need to know what needs protection—and who to protect it from. The greatest risk comes from privileged users, who have special access to your most sensitive assets. So you need to control who has privileged access, monitor your sensitive data and analyze activities across the environment to help stop potential breaches.



61% of organizations do not monitor privileged users more closely than regular users.[1]

[1] "Privileged Access: Manage the Potential Risk to Safeguard Your Data," *UBM Report*, April 2016.

Get started: Know your users

When it comes to insider threats, even the most trusted relationships cannot be taken for granted. You need to trust privileged users to do their jobs—while verifying that these users are who they say they are, and that they are accessing only the information they need.

IBM® Security Privileged Identity Manager delivers a single integrated solution that focuses on securing, monitoring and auditing the use of privileged accounts. Designed to help thwart insider threats by automating and auditing the use of privileged identities, the solution helps centrally manage and audit a pool of privileged user credentials, providing centralized password management to help protect enterprise resources from insider threats.

To know your users—and what they are doing—IBM Security Privileged Identity Manager can help you:

- Monitor privileged user activities with session recording and playback support
- Control the check-out and check-in of shared accounts with an encrypted credential vault
- Eliminate the need to share privileged user credentials and hardcode passwords in applications
- Protect high-risk account access with strong authentication controls and single sign-on
- Deliver a cost-effective solution with shared policy management across your enterprise

See the infographic on combating insider threats with IBM Security Privileged Identity Manager.

Key questions for knowing your users:

- **Who has access to sensitive data?**
- **Who should have access?**
- **What are end users doing with data?**
- **What are administrators doing with data?**

Get started: Know your data

Your sensitive data is an attractive target for insiders—and you need to be able to protect it, wherever it resides. You need the right security for databases, data warehouses, file systems, big-data platforms and cloud environments. And you need to be able to track access, spot anomalies and prevent data breaches in real time.

IBM Security Guardium® is a comprehensive data security solution that enables you to understand the "who, what, when, where and how" of sensitive data access, across all major platforms. Designed to prevent unauthorized or suspicious activities, as well as vulnerabilities in sensitive data repositories, the solution can discover and classify sensitive data—and uncover compliance risks—automatically. What's more, Guardium includes advanced automated analytics to differentiate between normal and abnormal behavior, identify risks, and allow you to take action in real time, preventing data loss.

To know your data—and remediate risk—Guardium can:

- Perform continuous, policy-based, real-time monitoring of sensitive data repositories
- Scan data sources for vulnerabilities (missing patches, misconfigured privileges, etc.) and help you harden the environment against breaches
- Prevent unauthorized changes to data, data structures, configuration files, logs and more
- Analyze data to detect attack symptoms—such as SQL injections and malicious procedures—before they take root
- Protect data at rest and in motion through encryption, masking, redaction, blocking, alerting and user quarantines
- Support advanced behavior analytics to provide actionable protection in real time, including dynamic alerts, data masking and blocking, and user quarantines

▶ Check out an infographic on using Guardium to protect against insider threats.

Key questions for knowing your data:

- **What data is sensitive and where does it reside?**
- **Is the right sensitive data being exposed?**
- **What risk is associated with sensitive data?**
- **Can you control privileged user access to sensitive data?**

Get started: Know your environment

To stay ahead of threats, you must be able detect suspicious activities that are occurring across your environment—and take action. In addition to knowing your users and data, you need to have analytics capabilities to identify the "low and slow" threats that can persist for months. And alert security teams to enable rapid response.

IBM QRadar® Security Intelligence Platform, powered by IBM Sense Analytics Engine™, is designed to detect and prioritize threats in real time. QRadar helps eliminate threats by matching user behavior with log events, network flows, threat intelligence, vulnerabilities and business context. It enables security teams to focus on the most immediate and dangerous threats by finding clear signals within the noise—and guides them through remediation efforts to minimize any potential damage.

QRadar integrates data from Guardium, IBM Security Privileged Identity Manager and other solutions to provide a smarter approach to insider threat protection. QRadar can:

- Deploy rapidly across your entire network, including cloud-based resources
- Detect subtle differences in the environment, such as lurking intruders or rogue insiders
- Collect, normalize and correlate billions of events, prioritized to a handful of issues
- Identify the important vulnerabilities and risks to prevent a breach
- Support the rapid investigation of insider threats using forensics analysis

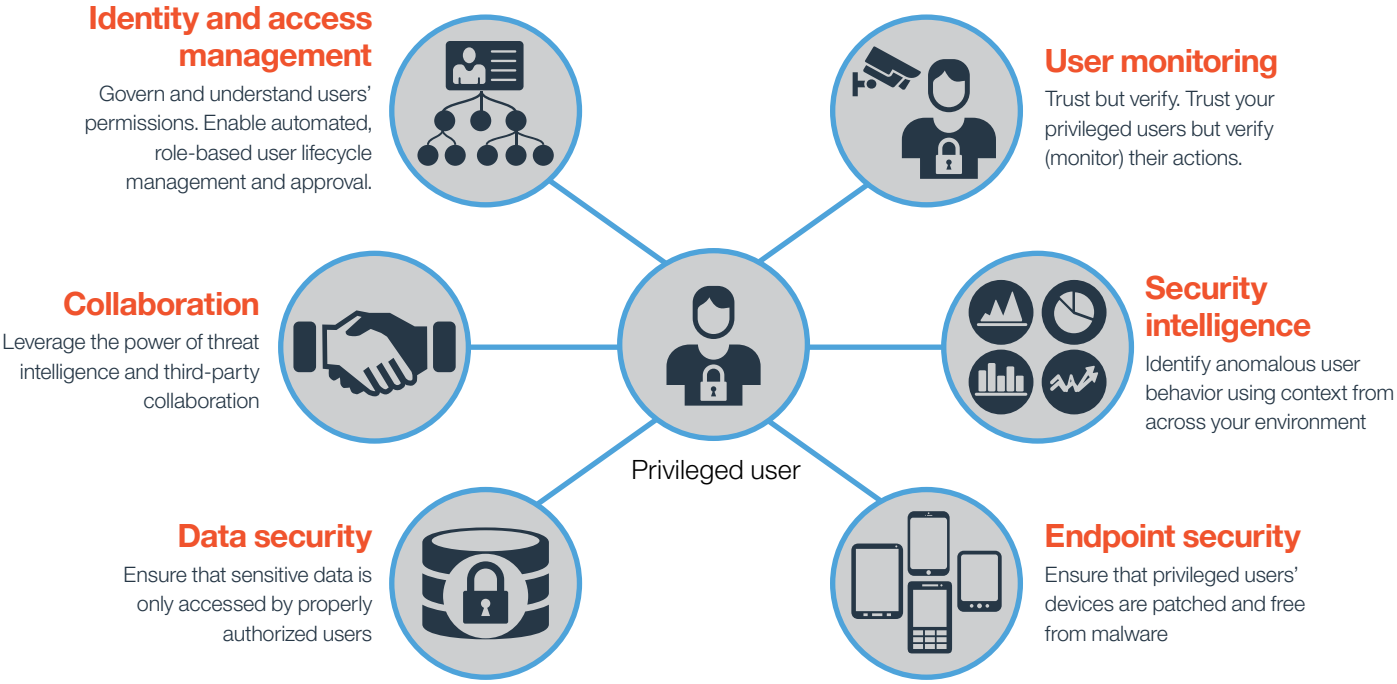
▶ Watch a whiteboard video on preventing attacks with QRadar analytics solutions.

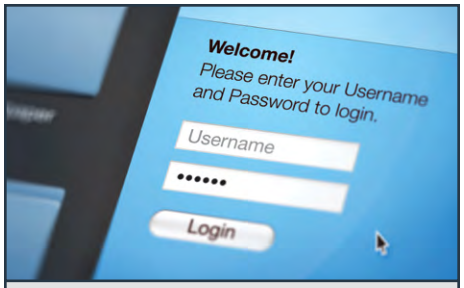
QRadar helps you get smart about:

- **Threat detection**
- **Risk assessment and management**
- **Vulnerability management**
- **Fraud discovery**
- **Forensics investigation**
- **Incident response**

Get smart: Put it all together for powerful protection

An integrated approach to insider threats is more important than ever. Deploying user monitoring and security intelligence tools together, for example, can provide critical capabilities for auditing user activities and detecting suspicious behavior. With a comprehensive view of all network activity and potential system vulnerabilities, your security teams can stay a step ahead of threats and block an attack before it completes.





81% of insider attacks used another person's credentials to bypass controls or gain elevated rights.[1]

[1] "Privileged User Abuse & The Insider Threat," *Ponemon Institute*, May 2014.

Get smart: Guard against privileged user breaches

By integrating identity and access management with data security solutions, your organization can spot meaningful deviations from normal activity—and stop data loss before it happens. For example, if confidential information is being inappropriately accessed, distributed or downloaded, you can block and/or quarantine the associated IDs.

IBM Security Privileged Identity Manager and Guardium are especially powerful in helping secure the use of shared IDs. Together, the IBM solutions provide nondisruptive, real-time data protection based on insight into access and data activity, control access and use of shared IDs, and help prevent unauthorized or suspicious actions by privileged users and attacks from outsiders.

IBM Security Privileged Identity Manager and Guardium empower you to:

- Verify the access of trusted users and continuously monitor access to high-value data sources, such as databases, big-data systems, file systems, etc.
- Validate whether access gained with a shared ID is within the scope of defined privileges
- Find users of an application using a generic service ID to access the data
- Assess whether an authorized user disclosed or shared credentials with an unauthorized user

Read this interactive white paper for insights on preventing threats by privileged users.

70% of organizations do not have a data security solution that supports entitlement reporting.[1]

[1] "Privileged Access: Manage the Potential Risk to Safeguard Your Data," *UBM Report*, April 2016.

Get smart: Stop data breaches before they take hold

To help you get a step ahead of breaches, IBM Security Guardium Threat Diagnostic Center includes specialized threat detection analytics that can scan and analyze audited data to detect symptoms of a database attack that is underway. Guardium can detect SQL injections and malicious stored procedures—coming from inside or outside the organization. (For example, a disgruntled administrator can use a stored procedure to disguise the dropping of an important table or the extraction of the table's contents.)

Unlike some solutions, Guardium does not rely on comparisons against a dictionary of attack signatures, which can change endlessly. Instead, it analyzes audit data activity for specific patterns of events that could indicate an SQL injection attack or malicious stored procedure. This approach is more flexible and does not require constant updating of signatures. In turn, Guardium can share this intelligence with QRadar, which can develop smarter, more targeted insights.

By integrating Guardium, IBM Security Privileged Identity Manager and QRadar, you can detect and prioritize threats in real time. The solutions automatically correlate events, detect anomalies and share information with each other—so you can rapidly respond to the highest priority threats.

- Read this white paper about protecting critical data with integrated security intelligence.
- Get the e-book to learn more about protecting sensitive data from insider threats.

After deploying Guardium, organizations see a 45% reduced likelihood of a breach.[1]

[1] "The Total Economic Impact of IBM Security Guardium," *Forrester Research*, September 2015.

Get smart: Take the next step

With data security, identity and access management, and security intelligence in place, your organization has powerful protection against insider threats. But the integrated portfolio of IBM Security solutions can help you go a step further in detecting threats, complying with policies and regulations, and reducing costs across the entire organization.

Additional solutions to consider include:

- IBM BigFix® endpoint security—Allows you to continuously monitor all your endpoints (from laptops, desktops and servers to point-of-sale devices) for potential threats, enforce security compliance and obtain real-time situational awareness for incident response
- IBM Security Identity Governance and Intelligence—Helps reduce access policy violations by connecting compliance, business and IT points of view and simplifying processes for designing, reviewing and certifying user access
- Collaboration via IBM X-Force® and the IBM Security App Exchange—Enables intelligent incident prioritization and comprehensive insights by leveraging the power of threat intelligence and collaboration via your industry peers

With IBM Managed Security Services, you can also take advantage of industry-leading tools, security intelligence and expertise that will help you improve your security posture—often at a fraction of the cost of in-house security resources.

▶ Find the apps and extensions you need by visiting the IBM Security App Exchange.

Integrated X-Force threat intelligence provides the context to quickly identify and remediate threats.

IBM solutions work together to crush insider threats

IBM Security solutions, including Guardium, IBM Security Privileged Identity Manager and QRadar, are trusted by organizations worldwide for comprehensive, layered data and network protection. The solutions work closely together to strengthen your defenses against all types of insiders, while also reducing overall complexity and total cost of ownership. 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 provides integrated solutions across diverse security domains to help you get the most value out of the solutions' capabilities. This gives you:

- **Integrated intelligence**—Correlating and analyzing siloed information from hundreds of sources to automatically detect and respond to threats
- **Integrated protection**—Enhancing security with solutions that interact across domains to provide cohesive, easy-to-manage protection
- **Integrated research**—Incorporating the latest information on vulnerabilities, exploits and malware to help you stay ahead of emerging threats and risks

As a strategic partner, IBM empowers organizations to reduce security vulnerabilities and manage risk across the most complex IT environments.

Inadvertent data breaches can take 158 days to identify, on average.[1]

- Learn more about Guardium on the product web page.
- Learn more about IBM Security Privileged Identity Manager on the product web page.
- Learn more about QRadar on the solution web page.

[1] "2015 Cost of Data Breach Study: Global Analysis," *Ponemon Institute*, May 2015.

For more information

To learn more about preventing insider threats with integrated IBM Security solutions, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/security

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned X-Force research, provides security intelligence to help organizations holistically protect their 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.

Additionally, IBM Global Financing can help you acquire the software capabilities that your business needs in the most cost-effective and strategic way possible. For credit qualified clients we can customize a financing solution to suit your business and development requirements. Fund your critical IT investment and propel your business forward with IBM Global Financing. For more information, visit: **ibm.com**/financing

© Copyright IBM Corporation 2016

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
June 2016

IBM, the IBM logo, ibm.com, BigFix, Guardium, QRadar, Sense Analytics Engine, 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 www.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.

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.

WGW03222-USEN-00