An integrated approach to insider threat protection

SAFEGUARD AGAINST HARMFUL INSIDER ACTIONS WITH TRUSTED SECURITY EXPERTISE, ACTIONABLE INTELLIGENCE AND POWERFUL TECHNOLOGY
As organizations battle multiplying complex threats to their data and sensitive information, they are forced to face an unsettling fact: in many cases, the threat originates from the inside, with a trusted user. These attacks can cause irreparable damage to a well-established brand, and undo in seconds the reputation painstakingly built over years of doing the right thing. It can lead to customers losing trust in the company, eclipsing in comparison the immediate financial value of the stolen information.

To make matters worse, harmful insiders are almost impossible to detect, because they have legitimate access to valuable data in the normal course of their jobs. And, any clues of wrongdoing they do leave behind often fall through the cracks because security products work in siloes, producing mountains of disconnected data. As a result, these tools are not able to interconnect the data from various sources to detect abnormal behavioral changes of legitimate users, and insiders continue to operate undetected.

An integrated approach to insider threat protection can provide actionable intelligence to stop insider threats, allowing organizations to regain control and reduce their risks. Bringing together data security, identity governance, and user behavior analysis enables organizations to detect insider threats and reduce their exposure to them. As a result, they can anticipate the risk of malicious actions before they occur and respond when breached. Additionally, they are able to secure their sensitive data and tightly govern their user identities.
Today’s security solutions need to do more than just “let the good guys in and keep the bad guys out.” That’s because an increasing number of security breaches are the result of actions by insiders, whether malicious or inadvertent. When employees share passwords or lose corporate data—or third parties put information at risk with inadequate safeguards—even the “good guys” pose a security risk.

An IBM X-Force® report found that insiders were responsible for 60% of attacks surveyed in 2015, compared with 55% in 2014. Of those, 23.5% were inadvertent actors. Often unwittingly “recruited” to aid the cause of others with malicious intent, they are becoming key players in carrying out highly damaging—and potentially prolonged—attacks. And because they’re insiders, they manage to do so without arousing any suspicion, by logging onto a social media site from a corporate network-attached device or opening an email attachment sent by a legitimate-looking business contact.

Then there are the malicious insiders, making up the remaining 31.5%, whose actions are not at all innocent. These insiders are especially dangerous, because they know they have access to valuable information – the loss of which can inflict great damage to the organization. This malicious intent, coupled with legitimate access to sensitive data, makes these insiders all the more dangerous. The unsettling truth is that just because they’re considered to be “insiders,” doesn’t mean they can be trusted. So it’s important to remember that situations and relationships can change over time—and not always for the better.

While the incidence of insider threats is on the rise, the consequences of a successful attack are also getting worse for organizations. A breach can cause financial damage, lead to costly interruptions to business operations, and affect reputation for years to come.

In a 2016 study, IBM and the Ponemon Institute calculated that on a global average, the cost of a data breach totals USD 4 million. This figure shows that the effects of a data breach ripple far beyond the monetary value of the stolen information – itself is omitted in that estimate.

Such a loss causes irreparable damage to an organization's brand, and shakes the trust of its customers. An estimated $1.63 million, or about 41% of the total cost of a data breach, is due to lost business. Customers lose trust in the brand, are harder to convince to return or remain with the organization, and have more turnover, increasing customer acquisition costs. The other 59% of the cost of a data breach are spent on response to the breach: notification to victims and regulators, detection and escalation, and ex-post response.

Knowing that such a costly attack is more likely than not to involve an insider, it becomes crucially important to protect crown jewel data from those who would abuse it. In today's information-driven economy, however, many different types of data fall into that category, and many different types of users gain access to it.

Components of the $4 million cost per data breach

**Lost business cost $1.63 million**
Abnormal turnover of customers, increased customer acquisition cost, reputation losses, diminished goodwill

**Detection and escalation $1.09 million**
Forensics, root cause determination, organizing incident response team, identifying victims

**Notification $0.18 million**
Disclosure of data breach to victims and regulators

**Ex-post response $1.10 million**
Help desk, inbound communications, special investigations, remediation, legal expenditures, product discounts, identity protection service, regulatory interventions

As the global economy relies more and more on valuable information, protecting crown jewel data from theft or inappropriate access has become increasingly complex. In truth, both the information itself and the users accessing it have evolved over time to complicate the issue.

Long gone are the days when "privileged users" were solely the network administrators. While these users do have exceptional privileges relative to the majority of users, and continue to need to be treated differently, many other types of users have joined their ranks. Executives carry with them access to extremely sensitive information. Engineers, researchers, and scientists all have access to valuable intellectual property, trade secrets, and patented information. Financial traders and brokers can access financial information, and HR employees have access to employee records, full of valuable personal information. Doctors, insurance agents, and other healthcare professionals have access to HIPPA protected patient records and other highly private and protected information. Sales managers have access to customer data, which can be extremely valuable to a competitor.

Another important complexity is that some of these users are no longer just typical employees. They are third parties, contractors, and partners. They have legitimate insider access, yet are not always well known or even managed by the organization who owns the data they access.

The types of crown jewel data and sensitive users vary by industry, but this much is true for nearly every organization: many different types of crown jewel data need to be protected, and many different types of end users need to be given legitimate access to it in order to do their jobs. Given these circumstances, many security solutions have been developed to protect crown jewel data. Yet, in many cases, malevolent insider actions still fall through the crack.
Insiders, malicious or not, who are putting valuable company data at risk of theft or compromise often act undetected. While their legitimate access to the information does make it more difficult to spot anomalies, the few clues they do leave behind generally fall through the cracks due to failures in an organization’s security program. Many factors compound to cause this to happen:

- **Where are my crown jewels?** Many organizations do not understand the sensitivity of their information, and where it resides. Therefore, they aren’t able to classify it appropriately and put the right access controls in place, which exposes it to more users than is necessary. Additionally, it is impossible for the organization to monitor access, since they don’t know what information to keep an eye on.

- **Processes? What processes?** In some cases, processes are either lacking or ineffective. These processes might affect data classification, as discussed above, identifying how sensitive a piece of information is. Or, they might affect user risk: third parties may be labeled more risky than employees, for example. The risk labeling could also be more dynamic, and include data around employee satisfaction, promotion rates, or HR status.

- **The right tools still don’t work.** While many organizations have many tools in place to address insider threats, they still fall through the cracks. One reason is that these technologies operate in siloes. They produce the necessary information, but security specialists are not able to connect the dots to derive meaning from it and take action. The same problem exists with the individuals who all know something about the users and their access. The application manager, business manager, IT security specialist, and internal auditors all hold a piece of the puzzle, but without putting them together they fail to see the big picture.

- **But you could be missing anomaly behavior detection methods or tools.** Since users are using their legitimate access, it can be hard to spot instances when they are abusing their privileges. Anomaly behavior tools can spot changes in users’ established patterns, indicating that some of their transactions were not done for typical reasons.

- **You are focusing on the wrong users.** Many tools now exist to manage and control privileged user lifecycle and access, but they generally focus on infrastructure-level administrators. However, other golden users with access to highly valuable information should be given the same scrutiny, including executives and users with access to financial or proprietary data.

- **Your employees might not trust you**—many times, the relationship between the manager and the workers cause the threats to go undetected. To avoid any consequences from whistle blowing (potential mistreatment by the manager or other co-workers), suspicious by-standers might not speak up.
Because insider threats can cause so much damage to an organization, and because they are so difficult to identify and stop, it is important for security teams to dedicate an integrated program to specifically address these types of threats – especially for organizations that rely on privileged information to create value for their customers, their shareholders, and their employees. It is important to take an integrated approach across many different technology and business areas with two important goals in mind:

<table>
<thead>
<tr>
<th>Identify</th>
<th>Protect</th>
<th>Detect</th>
</tr>
</thead>
</table>

**Reduce your exposure:** the more end users have access to sensitive information, the greater the chance that someone will put it at risk, either maliciously or by mistake. Ensure you are limiting access to only those users that absolutely need it, and that your controls stay current as your user population changes and evolves over time. Similarly, the easier the information is to access, and the more places it resides, the higher the chances that an insider, or an outsider with stolen credentials, will be able to gain access for the wrong reasons. Ensure that your sensitive data is appropriately protected, and has the right access controls in place to assure the identities of your legitimate users.

**Detect threatening insider behaviors:** For those users that remain and truly necessitate access to your privileged information, monitor & record their transactions and their risk levels. Understand both what constitutes a normal interaction with your crown jewel data for each individual users, and how likely this user is to become disgruntled. This will help you anticipate the risk of malicious actions before they occur so you can respond promptly in case of a breach.

These results can be achieved with an integrated approach. First, identify crown jewel data, where it is located, how it is accessed, and by whom. Then, protect your critical information with appropriate access controls and user governance for all of your privileged users – not only the infrastructure level administrators, but anyone who has access to valuable data, such as executives. Lastly, detect suspicious activity to stop bad actors by analyzing privileged and golden user behaviors.
An important component of an effective insider threat program is to **identify** crown jewel data, where it is located, how it is accessed, and by whom. This allows organizations to make sure they are protecting the right information, and that no crown jewel data falls through the cracks. They can then answer the following questions: Are the right access controls in place for my sensitive data? Are the right user groups accessing the information? To effectively achieve these goals, the following steps are necessary:

- **Standardize your information classification** – ensure your sensitive information is appropriately and consistently protected by putting in place the business processes to classify your information relative to its sensitivity. This will allow you to set access control and data security policies for various risk levels so a repeatable method is in place. Once this structure is implemented, company data can be inventoried and classified, accurately identifying the most sensitive information the company possesses.

- **Map out the access pathways of your most sensitive data** – Discover if your sensitive data is exposed to unnecessary risks by understanding the ways in which your users access it. Map sensitive information to the database table, authorization object, transactions, and roles. Additionally, a comprehensive, end-to-end mapping of sensitive information, whether that information is structured or unstructured data, includes looking at business and IT transactions or operational activities which may expose it.

- Then, determine the access path to the information or the transactions. For each piece of data, figure out where that information is located, how it can be accessed and by whom.

### Key questions for identifying 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?
Once your sensitive data has been identified and classified, it becomes possible to protect it in order to reduce the chances that it will be taken for a nefarious end. This includes both appropriate identity and access management, to govern the users accessing the information and their rights, as well as data protection.

The key is to minimize the risk of suffering from insider threats by controlling the ways users can access your sensitive data and making sure only those who truly require the access are granted permissions – without inhibiting legitimate users from doing their jobs and creating value for your organization. This step reduces the pool of potential insider threats, so you can focus on the few users who retain legitimate access. This provides an important, controlled foundation to enable behavioral analytics to further protect the crown jewels.

- **Set up access policies to ensure your data is accessed only in safe circumstances.** For example, don’t let your crown jewel data be accessed off network, from an unmanaged device, with only user name and password. The right access policies should allow you to control how your data is access – in what circumstances, from what devices, networks, etc. Appropriate identity assurance can also be used to enable remote access, if it is necessary. For example, an executive who’s always on the road might need access to sensitive data, but strong authentication can be put in place and access can be limited to corporate-issued smart devices. Granular authorization levels can also add another layer of protection, by controlling what users can do with the data once they access it. Will they have print rights? Will they be able to copy, or share via email? Is their access read only?

- **Make sure your controls are clear and measurable.** Security policies covering the access control should include appropriate access control models, ensuring least privileged and segregation of duty controls are being followed.

- **Keep your authorized users current.** Make sure the users who have access to your crown jewels still need it. This involves setting appropriate identity and access governance policies, to ensure you have a good handle on who is accessing your data. Coupled with periodic access recertification and user access removal controls, this can allow you to make sure you are making the list of users with access as small and restricted as possible.

---

<table>
<thead>
<tr>
<th>Key questions for protecting your data:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Who has access to sensitive data?</td>
</tr>
<tr>
<td>• Who should have access?</td>
</tr>
<tr>
<td>• What are end users doing with data?</td>
</tr>
<tr>
<td>• What are administrators doing with data?</td>
</tr>
</tbody>
</table>

---

The rise of insider threat

Integrated solution

How IBM can help

For more information

Identify

Protect

Detect
### Key questions for detecting inappropriate activity:

- What do normal transaction patterns look like between the user and your sensitive data?
- How much can you trust each individual user?
- When should a deviation from “normal” be cause for further investigation?

After identifying your crown jewel data, and protecting it to reduce your exposure to threats, it becomes possible to focus on the few legitimate users who are granted access to detect any suspicious activity that could lead to insider threat. To be able to anticipate nefarious behavior, it is critical to maintain a comprehensive understanding of your users’ behaviors, their satisfaction with your organization, and their relationship with your data:

- **Develop a risk score for employee satisfaction.** HR has a lot of data that can give you a sense of how likely an employee is to become disgruntled. Did their department recently undergo a restructuring exercise? When was their last promotion? How long have they been with the company? Have they been handed a termination notice? These types of data points can be aggregated to create a risk profile for each employee. The result is a classification that can help you prioritize the investigation of transactions that have been flagged by the other indicators described below.

- **Understand your employee’s relationship with your data and baseline behavior.** Determine what the normal usage patterns are for all of your users. Analyze historical logs and consider a broad set of data such as user actions, accessed resources, access time, geo-location, network activities, session duration, connectivity, and typical peer group behavior. Prioritize anomalies against your employee risk scores for follow-up investigations.

### User behavior analytics and privacy concerns

Many organizations in the world are concerned about the privacy implication of monitoring users’ activities. However, there are ways to protect the privacy rights of individuals while benefiting from the power of behavior analytics.

- **No access to personal communications:** UBA tools are focused on security/operation logs, vulnerability data and identity information. In other words, current UBA tools are not designed to intercept telephone communications or read personal emails to monitor the user activities. Instead, they will monitor system access and privilege activities to identify unauthorized access to the organizations’ crown jewels.

- **Employees vs. customers PII data:** The majority of organizations do not have the same level of privacy restrictions for their employees and customers, and in some countries like the United States, the privacy laws are more relaxed on employees especially if they are using corporate assets. In these situation, UBA tools can be configured to only consume the employee information while fully protect the customers’ privacy.

- **Data obfuscation:** In order to provide more restrictions around data privacy, some UBA tools also support data obfuscation and all the analysis will be done on obfuscated user information. In order to support this capability, the UBA tools should be able to convert the Personally Identifiable Information (PII) to unique hash codes that can be reverted back to original values by the legal team during high-profile incident investigation.
Safeguard against harmful insider actions with trusted security expertise, actionable intelligence and powerful technology from IBM

IBM Security is uniquely positioned to help customers design and execute an integrated insider threat program that will allow them to:

- **Detect insider threats**: Anticipate the risk of malicious actions before they occur and respond when breached.
- **Reduce their exposure**: Secure their sensitive data and govern their user identities.

Explore how IBM can help you combine the right identity and access management, data protection, security information and event management (SIEM), and user behavior analytics tools to identify your crown jewel data, protect it, and detect deleterious user behaviors. Leverage IBM Security Services experts to turn a collection of powerful technologies into an integrated program capable of detecting and stopping your most unnoticeable insider threats. Trusted IBM security specialists can offer the business, data and IAM security experience to help you evaluate intelligence, draw more meaningful conclusions and prepare for next steps.
Integrate your approach with insider threat protection services from IBM

IBM’s identity-focused, integrated program provides actionable intelligence to address the security gaps that skilled and knowledgeable insiders exploit:

- Prioritize compliance and security actions with risk-based insights from end-to-end mapping of your critical information’s access pathways.
- Analyze distributed data on user behaviors from SIEM, data protection tools, HR, and other sources to detect suspicious activities for further investigation.
- Trusted IBM security specialists can offer the business, data and IAM security experience to help you evaluate intelligence, draw more meaningful conclusions and prepare for next steps.

IBM® Identity and Access Management Services for insider threat protection offers an integrated approach to your organization’s defense. It grants greater insight into how and why insider attacks occur by focusing on user identity and behavior as they access your data. This helps ensure you are adequately protecting your data, governing user identities and understanding users who hold the potential for the greatest damage. Guarding against insider threat means preserving brand value and customer trust, defending your business from financial losses and costly interruptions.

Take advantage of unparalleled IAM expertise

With virtually unparalleled identity and access management (IAM) and data security expertise, IBM can provide the benefits of a trusted advisor to augment your security staff. Backed by IBM research and development resources, the large data set of IBM X-Force® command centers and managed security services clients, IBM Security specialists can offer the business, data and IAM security experience to help you evaluate intelligence, draw more meaningful conclusions and prepare for next steps.

Are you just getting started?

While an optimized insider threat program integrates many tools, people and processes, some organizations have not deployed complex systems to tackle insider threat.

Insider threat protection services from IBM can help you take the first step in the fight against insider threat by providing this integrated program, scaled down to only your most important apps or pieces of data. This can allow you to quickly and efficiently discover vulnerabilities and protect the data that matters most.
Identify your sensitive data with IBM Guardium

IBM 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
### Provision, audit and report on user access and activity with IBM Security Identity Governance and Intelligence

Identity Governance and Intelligence provides functionality to cover enterprise user lifecycle management, including access risk assessment and mitigation using business-driven identity governance and end-to-end user lifecycle management. Governance and Intelligence helps organizations mitigate access risks and access policy violations by using intelligence driven, business-driven identity governance integrated with end-to-end user lifecycle management.

IBM Security Identity Governance and Intelligence offers:

- An identity governance platform that lets IT managers, auditors and business owners govern access and ensure regulatory compliance
- A business-activity-based approach to facilitate communication between auditors and IT staff and to help determine segregation of duties violations across enterprise applications, including SAP.
- Better visibility and user access control through consolidating access entitlements from target applications and employing sophisticated algorithms for role mining, modeling and optimization.
- User lifecycle management including provisioning and workflow capabilities, along with integration with IBM Security Identity Manager and third-party tools.

### Protect your sensitive information by ensuring that your legitimate users are who they say they are, and that they are accessing only the information they need, with IBM® Privileged Identity Manager

IBM® 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 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
Detect suspicious activities that are occurring across your environment with IBM QRadar® Security Intelligence Platform

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 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

QRadar Security Intelligence Platform: Provides visibility to insider threats and cyber criminals exploiting compromised credentials

Add the QRadar User Behavior Analytics app to monitor risky activity to identify and manage insider threats. This app is free of charge and provides at-a-glance visibility to individual users and anomalous behaviors that could be signs of an insider threat. The IBM QRadar UBA app extends the capabilities of the QRadar Security Intelligence Platform and adds a user-centric view. It shows number of monitored users, high risk users, risk categories, security events and offenses, system status, and a user watch list. It’s dashboard is an integrated part of the QRadar console.

The QRadar UBA App extends the capabilities of IBM QRadar Security Intelligence Platform with user behavior analytics and an integrated dashboard exposing top user-centric security threats. It includes new out-of-box correlation rules that detect behavioral changes and anomalous conditions, and improves security analyst productivity by compiling risk scores and rank ordering suspicious or compromised users. QRadar UBA simplifies the creation of user watch lists and provides a free-text ability to add explanatory notes to any suspected incident. It produces results and user insights in less than a day after the initial deployment, and downloads quickly and easily as a free application from the IBM Security App Exchange.
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 hold more than 3,000 security patents.

Additionally, IBM Global Financing can help you acquire the IT solutions that your business needs in the most cost-effective and strategic way possible. We’ll partner with credit-qualified clients to customize an IT financing solution to suit your business goals, enable effective cash management, and improve your total cost of ownership. IBM Global Financing is your smartest choice to fund critical IT investments and propel your business forward. For more information, visit: ibm.com/financing

© Copyright IBM Corporation 2016

IBM Security
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
November 2016
All Rights Reserved

IBM, the IBM logo, ibm.com, IBM X-Force, IBM Guardium, and IBM QRadar are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at ibm.com/legal/copytrade.shtml Other company, product and service names may be trademarks or service marks of others.

References in this publication to IBM products and services do not imply that IBM intends to make them available in all countries in which IBM operates.

Other company, product and service names may be trademarks or service marks of others.

This document is current as of the initial date of publication and may be changed by IBM at any time.

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.