To protect your organization, know your users and your data

Most threats come from inside the organization. Take action now to better control access to your “crown jewels.”
Securing the perimeter is not enough—danger may also lurk inside

Threats to your digital assets are everywhere. They’re constant. So you build defenses to keep them out. But like a carpenter framing a new addition to a house, you want to regularly step back from working on the details for a full view of your work. Do the enterprise security measures you’ve built do a complete job of protecting against intrusions? Or have you left any gaps that allow bad actors an easy way in? When you check all the possibilities, you might be surprised.

Because despite the common image of cybercrime, threats don’t always come from lone hackers, organized crime, rogue states, politically motivated activists or other undercover external actors. Protecting against attacks from these sources is undoubtedly important. You don’t want to ease up on those efforts. But you’ll probably discover that you’re also at risk from the employee in the next office. In fact, recent surveys show you’re more likely to be the victim of an internal vulnerability or threat than one from outside your organization.

It turns out that even when you’ve built strong technology defenses to keep outsiders from accessing your business resources—the customer data, intellectual property and other “crown jewels” of information that are the foundation of your business advantage—it’s the people who regularly use your systems and who have legitimate access to these resources that most often are the weak link in your defense.

IBM® X-Force® finds that insiders account for 60% of all attacks.¹

To learn more about protecting your organization from insider threats, watch the IBM webinar.

¹ “2016 Cyber Security Intelligence Index: Reviewing a year of serious data breaches, major attacks and new vulnerabilities.” IBM X-Force Research, April 2016.
Who are your insiders? And why are they so dangerous?

The access insiders have to your resources is as diverse as the jobs they perform. So is the damage they can inflict. But the engineers in product development or the administrators in human resources have a key factor in common. They're not as mysterious as hackers. You see them every day.

Insiders likely to pose threats, in fact, can be divided into three familiar categories:

- **The unsuspecting:** Whether employees or trusted outsiders such as customers, they innocently create vulnerabilities that bad actors can exploit. Maybe it’s an honest mistake by the distracted IT staffer taking a phone call while configuring systems. Careless by a user leaving a password in plain sight where it can be easily copied. Or bad judgment by co-workers sharing passwords. But the damage can be just as real as if it were intentional.

- **The disgruntled:** Typically employees, they maliciously seek revenge or profit following a perceived or actual slight such as an unfavorable performance review. Or perhaps they’re planning to go to work for the competition—and take your trade secrets with them. They can be stealthy and hard to discover, in many cases altering and resetting application controls to make it look like nothing has happened.

- **The opportunistic:** Often trusted third parties who have been granted insider status, they methodically use their position to take advantage of your weaknesses—or to steal user IDs once they become familiar with your defenses. A former contractor might use access rights that were not revoked at the end of a project to turn a quick profit by reselling your customers’ credit card information. And because they’re using real, if unauthorized, permissions, their actions can be hard to discover.

**81%** of insider attacks used another person’s credentials to bypass controls or gain elevated rights.¹

Learn more about the risks associated with insider access in the IBM video.

How are organizations dealing with threats? Or not dealing with them?

When an attack—even an unintentional one—comes from inside, the organization can suffer significant financial loss, damage to customer relationships, noncompliance with regulatory mandates and reduced brand value. This is the same damage it can suffer when an attack comes from the outside. So if companies face the same—and actually more frequent—damage internally as externally, it would seem natural that they’d devote substantial resources to combating the damage from both sources of activity. But this is not necessarily the case.

While deploying solutions such as security information and event management (SIEM) tools to gather information on network activity, application-scanning tools to discover vulnerabilities in software, or network-intrusion protection systems to block unauthorized access to enterprise resources, many organizations overlook the weakness that humans and human error bring to their environments.

The amount spent on solutions that address security issues within the enterprise environment, in fact, typically does not match the amount spent on securing the environment’s perimeter. More than half—61 percent—of organizations do not monitor and audit the actions of privileged users—those with access to especially sensitive functions or data—more closely than ordinary employees. And a whopping 70 percent of organizations do not have a data security solution that helps them discover who has been granted entitlements to access which systems or information.

Even a breach innocently caused by human error takes an average of 162 days to discover, and 59 days to contain.

View the IBM infographic to help solve the mysteries of security challenges using identity governance.

Knowledge is the key to reducing the threat of insider attack

Because even an accidental, non-malicious data leak can be disastrous, it is essential to understand who your organization’s users are, what access they have to your crown jewels of information, how they use that access and what threats can occur if they abuse their privileges. Two steps are therefore critical to building defenses against insider threats: knowing your users and knowing your data. Here are the core questions you should answer as you lay your internal security foundation:

Know 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?

Know your data
- What data is sensitive? Where does it live?
- Is the right sensitive data being exposed?
- What risk is associated with sensitive data?
- Can you control privileged user access to sensitive data?

As organizations have moved to cloud-, mobile- and social-based workforces and customer interaction, it has become increasingly difficult to know who users are and what they are doing, particularly privileged users. The expansion of data that comes with these new IT domains, as well as with big data and the Internet of Things, makes it increasingly difficult to understand where your crown jewels are.

79% of insider attacks occurred when a privileged user altered and reset controls to avoid detection.¹

Learn more in the IBM blog about protecting your resources using identity governance and intelligence.

Make a strong start on the path to security—and then keep going

To help stop insider attacks and prevent information from being stolen or compromised, it is more critical than ever for your organization to control access to its crown jewels. You need to put into place security measures that help ensure all users have the access they need—and nothing more. For internal, external or third-party users alike, you need to provision access properly from the beginning, monitor how individuals use their access, recertify permissions accurately at regular milestones in the access lifecycle, and effectively de-provision access when users no longer need it.

The process can begin with a tool as simple as a spreadsheet that documents the type and location of sensitive data and user access to it. After gathering this information, ask: “Do all these people need access?” Chances are, the answer will be “No.” You’ll then be on the way to removing access—and risk—from people who don’t need it.

But comprehensive protection requires ongoing control and watchfulness. Data has to be protected, both at rest and in motion, in databases and in unstructured formats. Requiring the same strong, multi-factor authentication for all users that many organizations apply only to privileged users can help stop inappropriate access. Then actions have to be monitored, whether they’re by employees, business partners, contractors or customers. Threat-detection analytics can help you spot attack symptoms early and take real-time actions to prevent damage. Meanwhile, remember: Partial protection means gaps exist. And gaps mean the risk of an attack or data breach.

A scant 24% of companies make sure users are granted only the privileges they need.¹

View the IBM infographic to learn why compliance is only part of the journey toward security.

¹ “Privileged Access: Manage the Potential Risk to Safeguard Your Data,” UBM, May 2016.
You’ll encounter many threats—but you’ll have tools to deal with them

Not all access is created equal. The same is true of risk. An employee logging into your network from home during the day is not the same as a former contractor logging in from a coffee shop after midnight. Today, passwords aren’t enough. Context is vital. And the ability to dynamically authenticate users, assess the situation and block risky action is critical. To provide these capabilities, leading security solutions enable both the insight and control you need:

- **Dynamic access management**: The ability to control access to resources as users initiate actions seeking entry into your data environment. It determines whether the person requesting access is a valid user for the type of information accessed.
- **Comprehensive data security**: A solution designed to monitor access, analyze risk and prevent unauthorized or suspicious activities, protect sensitive data, and find and fix vulnerabilities in sensitive data repositories. Such a solution can discover and classify sensitive data—and uncover compliance risks—automatically.
- **Business-centric identity governance**: The ability to control the granting of access privileges and to prevent “entitlement creep,” the tendency for users to accumulate access privileges over time without shedding the ones that are no longer relevant to their work. Business centricity also includes the ability to provide information regarding user access in ordinary language to help managers understand what access they are certifying and why.
- **Intelligent integration**: Security solutions that work together for a more aggressive stand against threats in a smarter, safer environment.
- **Meaningful insight**: The ability to understand what’s normal and what’s anomalous behavior—and support preventive action—by creating a baseline of access commands executed in the past.

Only 39% of companies monitor privileged users more closely than other users.¹

Read this interactive white paper to learn how IBM can help you become compliant with the new General Data Protection Regulation.

---

¹ “Privileged Access: Manage the Potential Risk to Safeguard Your Data,” UBM, May 2016.
IBM Security Guardium: Spotting the symptoms of an attack

You can’t govern—or protect against threats—what you don’t understand. So for the insight and control you need in today’s increasingly risky data environments, IBM Security Guardium® provides specialized threat-detection analytics that spot and attack symptoms early to help stop attacks.

Operating in real time and in the background while your organization continues its business, Guardium is designed to mitigate insider threats by monitoring users’ access to sensitive data. Delivering key capabilities you need to protect against internal and external threats, Guardium automatically finds and classifies sensitive data, analyzes access patterns, detects threats, prevents unauthorized database access, and protects data through real-time blocking, quarantining and encryption.

Guardium applies machine learning and intelligence to determine who is accessing sensitive data and what actions they are taking in order to spot changes and anomalies in access patterns that can indicate risk. It uses policy-based, real-time monitoring that reveals behavior patterns over time, and analytics that provide context and meaning for those patterns. And when abnormal events occur, Guardium sends alerts for manual review by your security team or triggers automatic action in real time to stop threats based on policies you have in place. Importantly, Guardium can identify both SQL injections and malicious stored procedures, two of the leading causes of data breaches today. It can identify actions and risks that can make your organization noncompliant with the regulatory mandates of your industry.

Key Guardium features:

- Discovery, classification, vulnerability assessment and entitlement reporting
- Encryption, masking and redaction
- Data and file activity monitoring
- Dynamic blocking and masking, alerts, and quarantine
- Compliance automation and auditing

Learn more about Guardium on the web.
Identifying and stopping threats as they occur is critical to your enterprise security. But so is the other side of the coin. In addition to controlling the access of unauthorized users, it’s also necessary to manage how you grant access to authorized users and control that access. IBM Security Identity Governance and Intelligence gives you capabilities both for provisioning access privileges and managing access across the full user lifecycle. The right identity governance and intelligence solution should also have the ability to integrate with and enhance your current solutions—for example, to integrate with a privileged identity management solution and seamlessly recertify your privileged users’ access entitlements.

IBM Security Identity Governance and Intelligence gives you the tools you need to analyze user access and prioritize risk—with a business-driven approach to designing, reviewing and certifying user access. Additionally, IBM Security Identity Governance and Intelligence integrates with mainframe systems, where high-value information often resides, to govern user access.

The solution uses plain English rather than technical language to communicate among requestors and grantors of permissions so that business managers can understand the privileges they are giving their employees—to avoid overprovisioning privileges either by mistake or out of expediency.

Over time, users can accumulate access entitlements beyond their needs—entitlement creep. They also can accumulate toxic combinations of entitlements—violating segregation-of-duties policies. For example, a person with the authority to request a purchase may also have the authority to approve the purchase. By governing users based on their business activities rather than their roles—in other words what they do on the job rather than what their title indicates they do—the solution provides a major step toward preventing threats from either malicious or careless insiders.

Key IBM Security Identity Governance and Intelligence features:

- The ability to govern access from a business perspective
- Integration of governance with identity management across the user lifecycle
- Improved visibility and control to help avoid segregation-of-duties violations

Learn more about IBM Security Identity Governance and Intelligence on the web.

Learn more in this video about identity governance on the mainframe.
Other IBM Security solutions: Simplified, strengthened protection

IBM QRadar® Security Intelligence Platform with IBM Sense Analytics™ Engine goes beyond conventional SIEM approaches to address needs such as threat detection, risk assessment and management, vulnerability management, fraud discovery, forensics investigation, incident response and regulatory compliance. Collecting events both on-premises and in the cloud, QRadar can sense change—including abnormal, risky behaviors across users, entities, applications and data—and attach context and meaning to the change. It then integrates its findings to unify security activities.

As business activities continue to expand into cloud, mobile and social platforms—and the numbers of users accessing business resources increase as well—IBM Security Access Manager further extends capabilities for a unified approach to security while simplifying user access management. Responding to issues such as the complexity of hybrid cloud environments and the dynamic—and often insecure—nature of bring-your-own-device (BYOD) mobile device usage, IBM Security Access Manager simplifies the user experience with single sign-on across applications and protects assets with strong multi-factor authentication. In combination with IBM Security Privileged Identity Manager, IBM Security Access Manager can provide strong authentication (including multi-factor) of privileged users touching sensitive data from their web browsers and mobile devices.

Specifically addressing the need for greater security for insiders, IBM Security Privileged Identity Manager provides centralized, automated management of privileged users’ identities to reduce the risk that they might abuse their elevated access to sensitive data such as your customers’ financial information or your organization’s intellectual property. With the ability to monitor and record privileged users’ activities—“What did they do?” “Why did they do it?”—and manage shared access, the solution is designed to provide greater accountability and control while helping deter malfeasance and support compliance. IBM Security Privileged Identity Manager also supports integration with IBM Security Identity Governance and Intelligence for seamless governance and recertification of privileged user access.

Key IBM solution features:

- The ability to transform raw security data into meaningful insights
- Convenient and secure access to resources from mobile and cloud platforms
- Greater accountability with enhanced control of insiders’ IDs

Learn more about QRadar, IBM Security Access Manager and IBM Security Privileged Identity Manager on the web.
Why IBM?

IBM helps organizations protect their business-critical data and infrastructures—and the people who use them—from threats and breaches. The integrated IBM approach to security is based on a broad portfolio of security solutions that enable a comprehensive view of all network user activity, including abnormal behavior. An intelligent, adaptive approach to security and the ability to share findings and results enable IBM solutions to help stop insider threats aggressively with targeted actions.

IBM Security solutions further provide business and financial benefits ranging from reduced cost for monitoring data and users, and support for ensuring compliance with regulatory mandates and avoiding failed audits.

The Total Economic Impact™ of IBM Security Guardium, a study by Forrester Research, examined the Guardium approach to managing the data security and compliance lifecycle. The study identified benefits of improved process efficiency, lowered cost in recovering from a data breach, reduced likelihood of regulatory fines, and reduced cost for security labor—resulting in a typical return on investment of 218 percent, total benefits of USD2.6 million and a net present value of USD1.8 million.¹

“Investing in Guardium meant that these organizations could simplify their operations while improving the quality of their enterprise data security strategy.”¹

—Forrester Research

To learn more, read the Forrester study, The Total Economic Impact of IBM Security Guardium.

For more information

To learn more about IBM solutions for protecting against insider threats to enterprise resources, 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 provides numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit: ibm.com/financing