Security
Thought Leadership White Paper

January 2017

Protect your organization from the people you trust

Combining data governance and privileged identity management to secure your environment from insider threats

IBM

Introduction

According to the IBM 2016 Cyber Security Intelligence Index, the majority of data breaches are now caused by trusted insiders, including employees, third-party contractors and partners.[1] The research shows that insiders perpetrated 60 percent of data breaches in 2015—an increase of five percentage points over the prior year. While inadvertent actors are to blame in some cases, the majority of those data breaches were due to the willful misuse of access privileges by malicious users.

With more frequent attacks of this nature, it is important for organizations to take a closer look at how they manage privileged users—the individuals with access to the critical data or "crown jewels" of the organization.

Systems administrators, database managers and even corporate executives can cause major security breaches and jeopardize the safety of sensitive assets, unwittingly or on purpose. Because of the overarching access of these users, their privileged identities have extraordinary capabilities to control and exploit an organization's data, applications and endpoints.

Whether they are accessing data in insecure locations, deliberately exposing or downloading data, or even exposing their credentials to outside hackers, privileged users can wreak havoc on the most secure infrastructure. And if those privileged users aren't being properly tracked and monitored, security administrators have no visibility into their activities or the assets being compromised.

This white paper examines the reasons why insider threats are so common, presents approaches to address these threats, and discusses IBM solutions that organizations can deploy to help protect themselves from malicious or inadvertent actions by trusted insiders.

Insufficient control over privileged users

Research presented at Black Hat USA 2016 indicates that, when it comes to data breaches, the top concern of security professionals today is an attacker with inside access or knowledge of the organization.[2] However, despite the risk that privileged users represent to an organization, findings in a recent survey by UBM suggest that most organizations don't have sufficient control over privileged users to prevent a data breach—in fact, only 24 percent of survey respondents say they put significant resources into enforcing key the security principle of least privilege.[3] Why is that the case? There are three primary reasons.

Reason 1: Too much trust in privileged users

In many organizations, it might be unpleasant to view or refer to employees as a potential security threat. In fact, privileged users are provided sweeping administrative rights and trusted to keep passwords to themselves. Companies rely on these employees to meet strict privacy requirements when accessing and handling critical business assets.

However, companies must realize that without oversight, these "super users" have the power to create havoc by performing activities such as deleting user data, altering system configurations, modifying back-end applications or changing security settings—without leaving a trace.

Organizations need to finely balance the trust and access privileges they give to users in high-stakes business environments. While they want to trust employees, organizations must also monitor the activities that occur related to their most valuable assets—their intellectual property, financial data, product designs and other information that is vital to their business.

Your next attacker is likely to be someone you thought you could trust

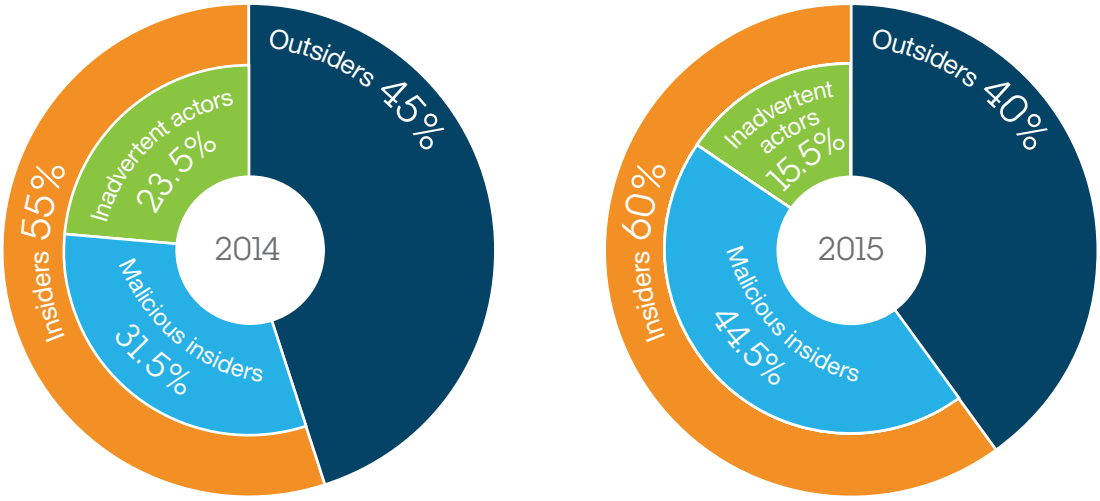

Figure 1. Insiders are increasingly responsible for data breaches, especially malicious insiders.
Source: "Reviewing a year of serious data breaches, major attacks and new vulnerabilities," IBM X-Force, April 2016.

Reason 2: Manually managing user privileges

With ongoing pressure to increase productivity and decrease costs, IT organizations continue to seek out new ways to more efficiently manage IT resources. These changes include tighter integration with business partners, increased levels of outsourcing, and leveraging virtualization and cloud computing.

Traditionally, organizations have used two approaches to manage privileged identities:

- Creating a set of shared accounts that all privileged users can access when needed
- Giving IT administrators their own individual accounts with privileged access to every application or system they support

But there are problems with each: The first approach lacks accountability and is often easily breached. The second can be complex and hard to scale.

With the emergence of global delivery centers, virtualization and cloud computing, the total number of unique IDs needed for each server has skyrocketed. Simply sharing privileged ID credentials does not address access problems either—this practice can make an organization's most sensitive privileged accounts its most vulnerable. When employees leave or change jobs, a shared password has to be immediately changed before it can be misused. In addition, the anonymity provided by a shared ID makes it difficult to tie an action or security breach back to a specific individual, virtually guaranteeing problems with regulatory compliance.

To top it all off, organizations are in a constant state of flux throughout the year, with projects and initiatives being started, finished, or abandoned, and new employees, contractors and suppliers being brought in and altering the data stored on different systems. And control only becomes harder as people change roles over time or leave.

Business leaders are left to wonder: How do we set up and maintain appropriate user access privileges for our sensitive resources? Do a privileged user's entitlements map correctly to the role he or she occupies in the organization? How can we enforce and demonstrate compliance with industry regulations and business policies designed to protect data privacy and integrity?

It is extremely important, as a result, that users, accounts, roles and privileges be in sync. Organizations should implement policies that can manage privileged accounts regardless of where they reside. They also need an approach that includes the ability to enforce policies, even with cloud providers. In this quest, identity and access management (IAM) tools that can monitor, report and proactively reduce user security violations are essential. An automated IAM solution can streamline the setup and enforcement of security policies across and outside the enterprise, helping an organization make the most of limited resources and tight budgets.

Reason 3: Lack of visibility from identity and data security solutions

Unusual activity around sensitive data is often the first indicator of an attack. While organizations may have formal data security policies that govern privileged users' access to IT systems, these organizations may lack the necessary enforcement controls or granular visibility into what's really going on.

Role-based access and other controls that prevent end users from accessing sensitive data in databases cannot stop privileged users who have the ability to execute virtually any database command. To make matters worse, privileged users often share database credentials, making it difficult to attribute a particular action to any user. In addition, application servers often use a generic service account to access databases, leaving no direct link to the user who initiated the transaction.

Server access using a generic service account

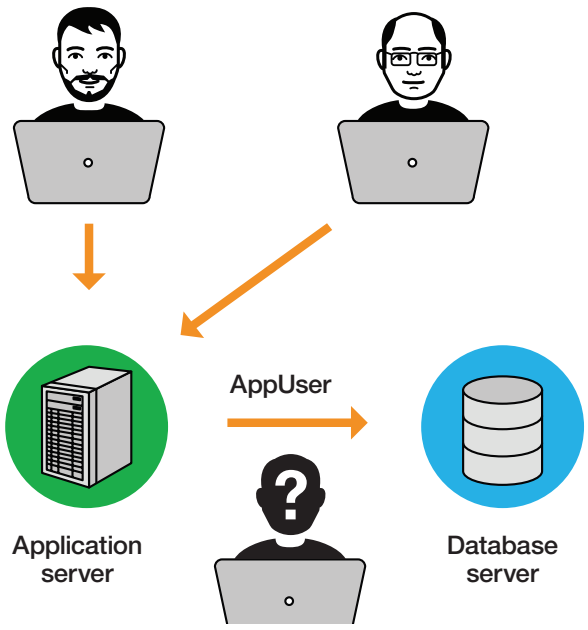

Figure 2. Application servers that use a generic service account (such as AppUser) to access the database make it very difficult to know which user initiated a given transaction.

Using native database logging to solve this problem may be impractical because it requires database changes that affect the performance and stability of business-critical applications such as enterprise resource planning and customer relationship

management. This approach also fails auditors' requirements for segregation of duties, because it is not controlled by IT security personnel and can easily be circumvented by database administrators.

By deploying a combination of monitoring and blocking capabilities provided by a database activity monitoring solution, activity in locations such as the network layer, database server, file server or big-data platform can be controlled, preventing information leakage at the source as well as unauthorized changes to critical data.

It is necessary to monitor all transactions in order to create a continuous, normalized, fine-grained audit trail that identifies the "who, what, when, where and how" of each transaction. Implementing fine-grained access policies is required for key regulations such as Sarbanes-Oxley (SOX), the Payment Card Industry Data Security Standard (PCI-DSS), the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, the Federal Information Security Management Act (FISMA), National Institute for Standards and Technology (NIST) Special Publication 800-53 and state/local data privacy and protection laws. As a result, it is extremely important that your data security solution integrate with your privilege identity management solution.

What is needed?

There are a number of approaches organizations can take to help mitigate the threat posed by privileged users. Stricter policy controls and improved user education are a good start. This means ensuring that staff members across the organization are aware of their responsibilities and accountability for particular activities—and know how to avoid attacks from inappropriate access. Firms also need to ensure that employees are kept up to date on regulatory and compliance requirements.

In addition, an organization should deploy an identity management solution that can provide a secure and convenient way for IT staff to automate the creation, modification and termination of user privileges throughout the entire user lifecycle, in addition to all the updating, monitoring and auditing that occurs in between.

Such a solution should:

- Centralize privileged identity management through a "single pane of glass" across all servers and users, increasing efficiency and ensuring a consistent approach across the organization.
- Authorize users based on the least access privilege they require. Granting privileged ID entitlements should be scrutinized and limited to only those who truly need the privileged access and who have the necessary credentials and clearances.
- Provide the capability to extend privileged user management to contractors, outsourced IT and other service providers. The solution should allow easy control and monitoring of activities of these privileged users without compromising on speed and ease of use.
- Enable organizations to effectively control shared access by centralizing the management of the pool of privileged user IDs.
- Provide a comprehensive, scalable and searchable audit and reporting solution to support expanding user populations, regardless of where they reside (in-house, virtual, web portal VPN, virtual desktop infrastructure or cloud-based services). The solution should be able to manage tens of thousands of identities across heterogeneous operating systems.

- Monitor and audit the activities associated with the IDs to highlight anomalies or misuse of the account's privileges. There is a growing realization that monitoring access is just as important as controlling systems access—if not more so. By combining user and application monitoring with application-layer network visibility, organizations can better detect meaningful deviations from normal activity, helping to stop an attack before it completes its dirty work.
- Provide a connected environment that can help administrators understand what, where and when sensitive data is accessed and reconcile privileged user access at the same time.

MyEyeDr.: Protecting against insider threats

MyEyeDr. optometry offers patients full-service vision care, a wide selection of prescription eyewear, and standard and specialty contact lenses. The number of MyEyeDr. practices has grown rapidly thanks to new location openings and collaborative acquisitions—and as a result the company now has nearly 2,000 employees in more than 250 offices serving approximately 1.8 million patients throughout the United States.

As a result of rapid growth, MyEyeDr. has a substantial number of new employees at any given time. In fact, 40 percent of the staff has been with the company for less than one year. But in addition to meeting PCI-DSS and HIPAA requirements, MyEyeDr. is committed to personally protecting and securing patient information, including protection from insider threats.

To that end, MyEyeDr. implemented an integrated identity solution from IBM Security. IBM® Security Privileged Identity Manager provides password management, including monitoring and tracking of administrator activity. IBM Security Guardium® provides data and vulnerability protection, including daily reports and alerts. IBM QRadar® provides security intelligence and analytics, including a holistic view of the entire security environment from a single dashboard.

IBM Security Privileged Identity Manager

IBM Security Privileged Identity Manager helps organizations manage the entire lifecycle of privileged identities. Administrators are granted privileged access only to the systems and resources needed to perform their job roles. When they change roles or leave the organization, their access rights are adjusted or revoked as necessary. From the user's standpoint, the process is simple and seamless.

When the user attempts to access a server or application, IBM Security Privileged Identity Manager transparently checks the required account credential and automatically inserts the credentials to authenticate the user at the managed endpoint. The user does not know the logon credentials, and the password can be changed when the user's login session is terminated so that the user cannot use the login outside the secured login process.

IBM Security Guardium

Guardium is a comprehensive data security platform that provides a full range of capabilities—including discovery and classification of sensitive data; vulnerability assessment; data and file activity monitoring; and masking, encryption, blocking, alerting and quarantining—to protect sensitive data.

Guardium helps secure sensitive data across environments—from databases to big data, cloud, file systems and more. Guardium also provides automated analysis to quickly uncover internal and external risks to sensitive data.

IBM QRadar SIEM

IBM QRadar SIEM provides comprehensive security information and event management capabilities, consolidating log events and network flow data from thousands of devices, endpoints and applications. It uses the advanced IBM Sense Analytics™ Engine

to baseline normal behavior, correlate system vulnerabilities with event and network data, detect anomalies, prioritize security incidents, uncover advanced threats and remove false positives. QRadar SIEM can also be integrated with IBM X-Force® Threat Intelligence, which supplies a list of potentially malicious IP addresses including malware hosts, spam sources and other threats.

IBM Security Identity Governance and Intelligence

IBM Security 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.

Conclusion

IBM Security solutions for identity and access management are trusted by organizations worldwide to safeguard, automate and track the use of privileged identities; improve identity governance; avoid the high cost of identity proliferation; and strengthen security across the entire enterprise. In fact, IBM won the 2015 Global Leadership Award for Identity and Access Management by Frost and Sullivan.[4] By extending privileged identity management with data security insights, organizations can proactively identify, monitor and address the most sophisticated insider threats.

An integrated combination of IBM Security Privileged Identity Manager, Guardium, QRadar SIEM, and IBM Security Identity Governance and Intelligence can help organizations protect their critical resources from insider threats and achieve peace of mind for years to come.

For more information

To learn more about the IBM Security portfolio of solutions, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/security

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 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.

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

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
January 2017

Please Recycle

[1] "2016 Cyber Security Intelligence Index," *IBM X-Force Research*, April 2016. http://www-03.ibm.com/security/data-breach/cyber-security-index.html

[2] "2016 Black Hat Attendee Survey: The Rising Tide of Cybersecurity Concern," *Black Hat*, July 2016. https://www.blackhat.com/docs/us-16/2016-Black-Hat-Attendee-Survey.pdf

[3] "Privileged Access: Manage the Potential Risk to Safeguard Your Data," *UBM*, May 2016. http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WGW03225USEN

[4] "Frost & Sullivan Honors IBM for Leading the Global Identity and Access Management Market," *Frost & Sullivan*, July 16, 2015. http://ww2.frost.com/news/press-releases/frost-sullivan-honors-ibm-leading-global-identity-and-access-management-market/

WGW03266-USEN-00