# Your biggest vulnerability: The privileged user

## Even if you have a mainframe, security threats can get into your business through the front door

# Who are privileged users? Why are they a worry?

Every organization has privileged users—those employees, partners, even customers granted special access to data and applications. But these users may not be who you think they are. Their actions often come with high risk—and enormous consequences—to the security, integrity and availability of your services.

Privileged users may be humans or system-related identities. Either way, they have multiple needs and capabilities based on their role or function—from configuring mainframe security settings, to administering users or managing applications and databases. With such broad responsibilities—and a potentially large number of users—their user IDs can be a vulnerability for your organization.

Why is this? Because user IDs are prime targets for anyone seeking to impersonate legitimate users to compromise your applications and data. Even staff with privileged access can be a risk, as they carry out complicated, manual processes that can be prone to errors and security issues.

All of which means threats can come right through the "front door" of your business—with your trusted users—rather than via the hidden backdoors usually associated with crime.

The answer is to put into place simplified, secure, automated and integrated tools that protect the organization from cyber threats and protect users from their own actions.

▶ Learn more in the IBM infographic and IBM video about identity governance.

**Privileged users can be your biggest vulnerability. A recent report from IBM® X-Force® noted that insiders were responsible for 60 percent of all attacks in 2015, up from 55 percent in 2014.[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. http://www.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEW03133USEN&attachment=SEW03133USEN.PDF

# What steps should you take to control user-related threats?

When threats come from people, even the most secure technology infrastructure—including your mainframe—is not immune from compromise. In fact, mainframes have a particular user-related vulnerability: Administrators are highly skilled individuals who remain on the job for years. Over time, they can accumulate access privileges known as "entitlements" beyond their current needs—a condition known as "entitlement creep." If entitlements are not regularly reviewed and then removed when they are no longer appropriate, they can create security vulnerabilities.

But even when entitlements are correct, people make mistakes, and many breaches are accidental. Causes may range from a lack of training to broken processes that allow managers to incorrectly approve system changes. Regardless, the organization must protect the custodian of a privileged identity—the person who has been assigned privileges or who is empowered to log on with a privileged identity, for example, when using an emergency account.

Where possible, automated preventive or corrective controls should be established to block changes to the components critical to the security of your systems, applications and data. The reality is: Poor security is often implemented by the privileged user. So it is important to control what these users can do, even if they have the highest levels of privilege.

- **Learn more in the IBM webinar on entitlement creep and the IBM white paper on best practices.**

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

[1] "Ponemon Survey Indicates the Growing Threat of Insider Fraud Not a Top Security Priority for Organizations, Proves a Costly Mistake," *Ponemon Institute*, February 28, 2013. https://www.ponemon.org/news-2/49

# Best practices provide security beyond basic requirements

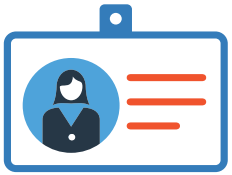
From corporate governance to regulatory compliance and legal requirements, it is typically mandatory to perform monitoring, auditing and entitlement reviews of privileged users and their roles. But today, with the risk of breaches on the rise, it's wise to go beyond what these requirements demand. For example, roles are no longer enough for governing user accounts. A better approach is to govern users according to specific, business-related activities and a granular view of entitlements.

To make this possible, the organization should follow best practices including:

- Establishing a baseline to determine who or what is supposed to have which privileges
- Limiting privileges to the least possible access with segregation of duties for each individual
- Monitoring and auditing the activities of privileged accounts, both individual and shared
- Establishing session recording to record privileged user activity in detail for forensics and compliance reviews
- Establishing and following a regular process for recertifying privileged users
- Understanding methods by which users bypass system security
- Establishing access controls that prevent privileged users from accessing sensitive resources
- Putting into place an acceptable use policy for the use of privileges
- Establishing preventive measures that block inappropriate changes that are implemented by superusers and security administrators
- Implementing strong authentication with multi-factor authentication mechanisms
- Implementing encryption for traffic pertaining to privileged users
- Challenging vendors who request powerful privileges for system accounts

**Learn more in the IBM video on risk management and the IBM white paper on mainframe security.**

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



[1] "Ponemon Survey Indicates the Growing Threat of Insider Fraud Not a Top Security Priority for Organizations, Proves a Costly Mistake," *Ponemon Institute*, February 28, 2013. https://www.ponemon.org/news-2/49

# To thwart abuse, deploy layered solutions for managing mainframe users

Your mainframe is integrated to seamlessly support both user-related and system security. But to protect against users, the next step is to add protection against threats such as segregation-of-duties violations that create conflict of interest, breaches and theft that take advantage of poorly managed user accounts, lack of recertification that fails to ensure users have only the access they need, and lack of strong authentication that fails to ensure only the people who have been granted access are the ones actually using it.

Three key layers of capabilities form the foundation for this comprehensive security approach:

**Privileged identity and access management**

- Administering and governing users' access permissions and roles
- Providing strong multi-factor authentication for privileged users

**Security intelligence**

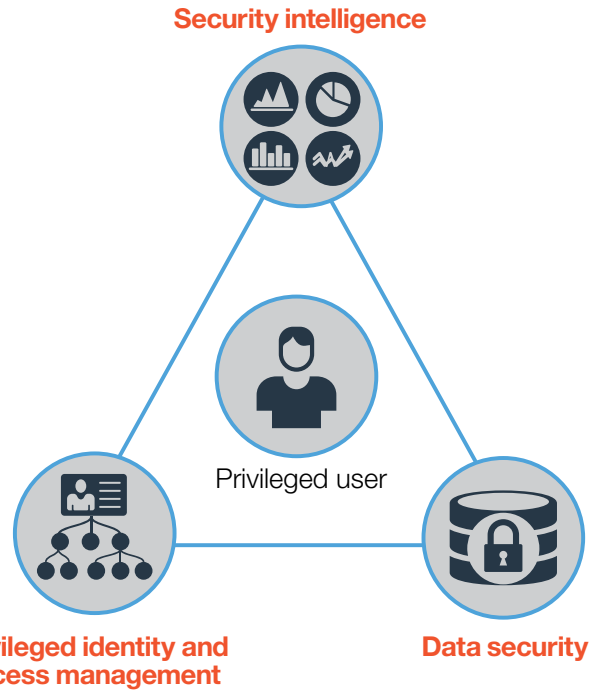
- Monitoring and auditing privileged user activity
- Identifying anomalous behavior
- Reporting on compliance policy adherence

**Data security**

- Discovering, classifying, protecting and monitoring sensitive data
- Encrypting user credentials
- Encrypting data at rest and data in motion

Learn more on the IBM web page on identity management and in the IBM video on layered solutions.

**Protection for privileged users**



# IBM delivers the full spectrum of user and access management

**Privileged identity and access management**—Governing, protecting and auditing users with elevated privileges to prevent unauthorized access

- IBM Security zSecure™ Administration—Manage users, clean up security databases and support compliance
- IBM Multi-Factor Authentication for z/OS® (IBM MFA)—Enforce strong authentication
- IBM Security Identity Governance and Intelligence—Consolidate roles and recertification
- IBM Resource Access Control Facility (IBM RACF®)—Administer privileges and access
- IBM Security Privileged Identity Manager—Manage privileged users and their access

**Security intelligence**—Correlating security data to uncover patterns of unusual activity; issuing real-time alerts

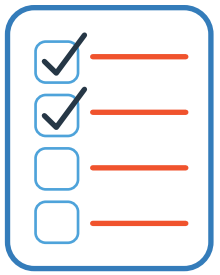
- IBM QRadar® Security Intelligence Platform, powered by IBM Sense Analytics Engine™—Monitor activity by privileged users
- IBM Security zSecure Compliance and Auditing—Audit privileged users, monitor activities and support compliance
- IBM Security Guardium®—Control database administrators and monitor their activities

**Data security**—Defending and protecting critical assets with encryption and intelligent data monitoring

- IBM Security Guardium—Protect data, control database administrators and monitor their activities
- IBM Security Key Lifecycle Manager—Centralize, simplify and automate encryption key management
- IBM Security zSecure Compliance and Administration—Audit administrators, limit access capabilities and support compliance

**Learn more in the IBM video on identity governance for z Systems.**

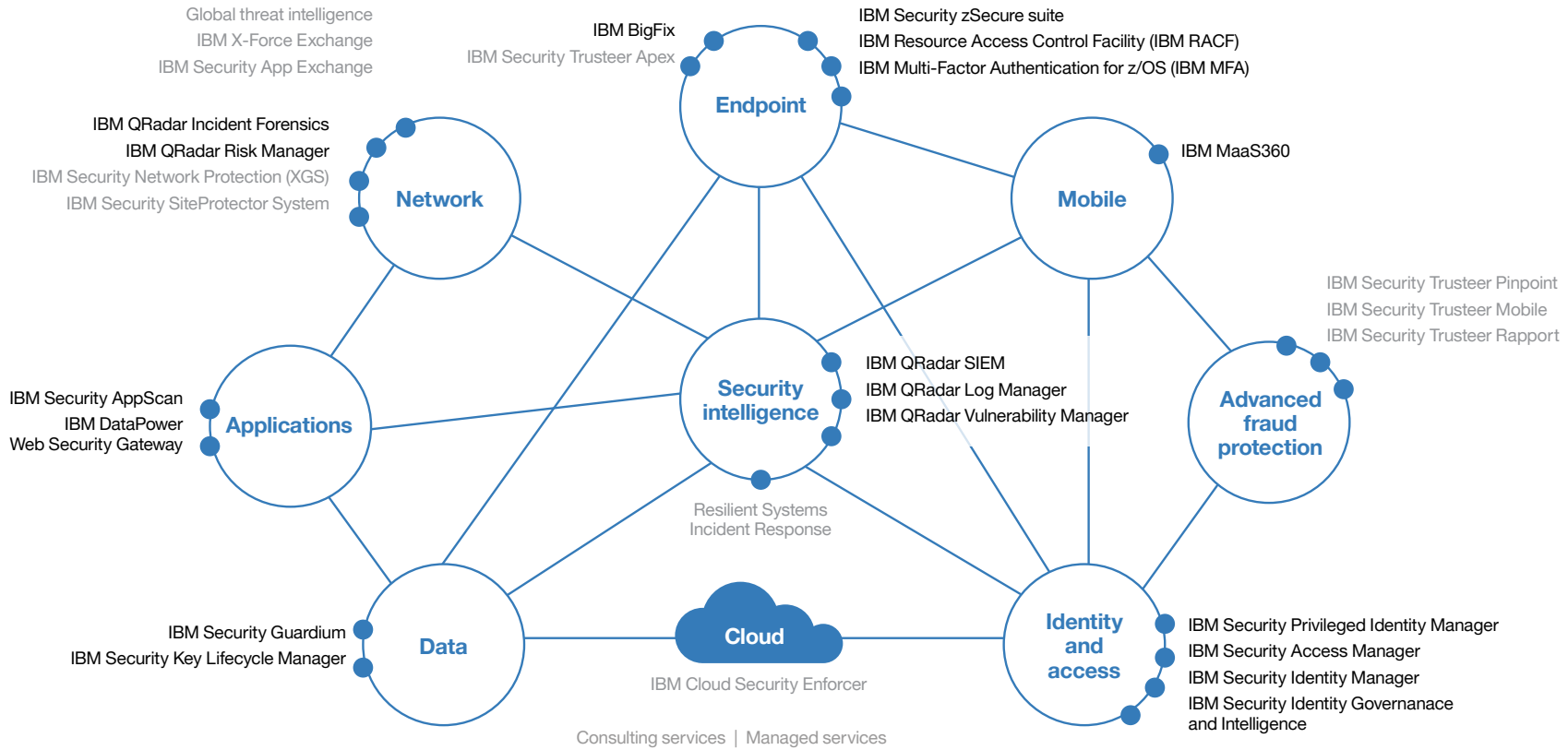
**69% fewer tasks are required to implement standard protection on z Systems.[1]**



[1] "Solitaire Interglobal Paper: Cyber Crime: Keeping Data Safe from Security Incursions – A Summary," *Solitaire Interglobal*, February 2016. http://www.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=ZSW03298USEN&attachment=ZSW03298USEN.PDF

# IBM solutions work together to detect and prevent attacks and user errors

**The broad and deep security portfolio for IBM z Systems**




Learn more in the IBM video about how one company used IBM solutions to improve its identity governance capabilities.

# IBM solutions: Control and authentication

The backbone of mainframe security is RACF, designed to assign privileged user roles, protect vital system resources and control what users can do on the operating system.

To provide higher authentication assurance for RACF users, MFA requires multiple authentication factors to protect access by privileged and highly entitled users. Both solutions help reduce business risk by enforcing strong security policy and best practices.

**RACF: Meeting security goals with centralized administration**

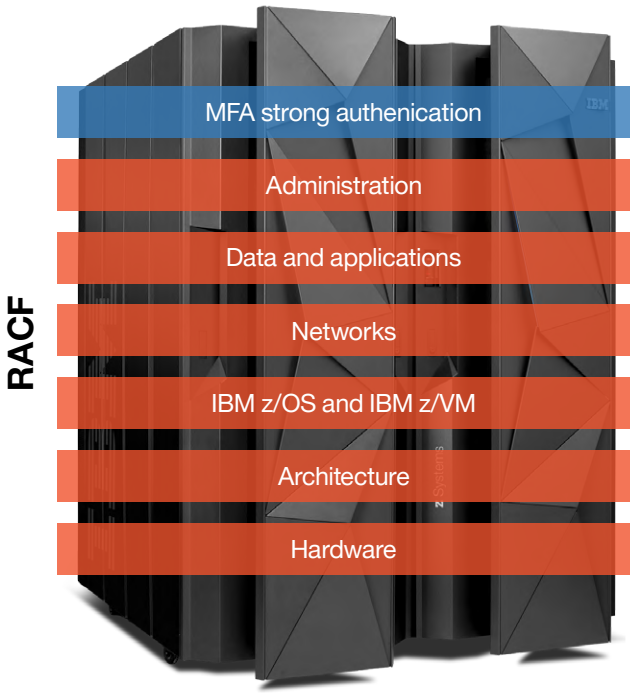
- Identifies and verifies system users, roles and groups of users
- Identifies, classifies and protects system resources
- Authorizes users who need access to protected resources
- Logs and reports authorized and unauthorized access attempts
- Enables application and database security without modifying applications
- Tracks activity to address audit and compliance requirements
- Establishes security policy and secure configuration settings

**MFA: Preventing unauthorized use of privileged user IDs**

- Requires privileged and highly entitled users to authenticate with multiple factors during logon
- Supports multi-factor authentication that is easy to deploy, manage and use
- Audits which factors are used during the authentication process
- Addresses regulatory and industry requirements for strong privileged user authentication
- Provides flexibility because it is not locked to particular authentication factors; new factors can be added as they become available without changes to the infrastructure

Learn more about RACF and the RACF library on the web, and MFA in the IBM solution brief.

**IBM Resource Access Control Facility (IBM RACF)**
**IBM Multi-Factor Authenication for z/OS**



# IBM solutions: Integrated, automated security capabilities

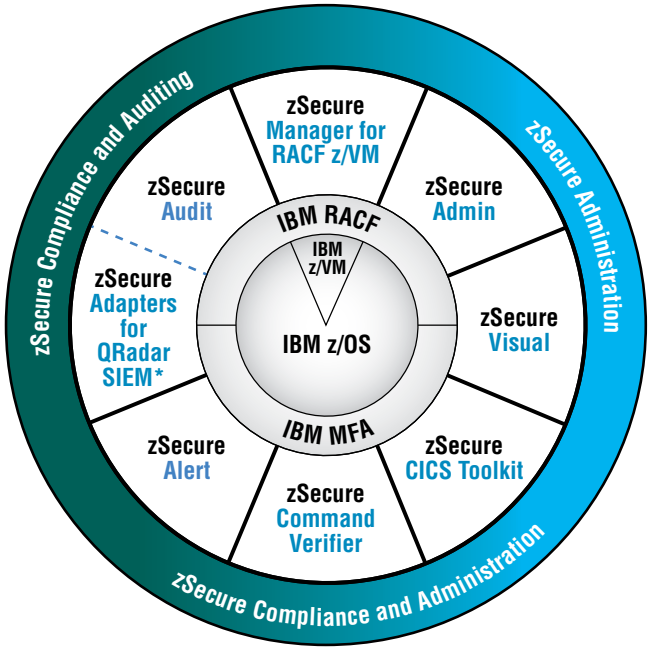
Designed to help detect threats, comply with policies and regulations, and reduce costs in mainframe environments, the zSecure suite delivers capabilities for administering mainframe security, monitoring for threats, auditing usage and configurations, and enforcing policy compliance—while helping improve the efficiency and manageability of the mainframe security environment.

**zSecure suite: Delivering comprehensive security for the mainframe**

- IBM Security zSecure Audit—Enables vulnerability analysis for the mainframe infrastructure; automatically analyze and report on security events and monitor compliance
- IBM Security zSecure Adapters for QRadar—Collects, formats and sends enriched mainframe System Management Facility (SMF) audit records for IBM QRadar SIEM integration
- IBM Security zSecure Alert—Provides real-time mainframe threat monitoring of intruders and alerting to identify misconfigurations that could hamper compliance
- IBM Security zSecure Command Verifier—Enables policy enforcement to help ensure compliance to company and regulatory policies by preventing erroneous commands by RACF administrators
- IBM Security zSecure Manager for RACF z/VM—Delivers combined audit and administration for RACF in the virtual machine environment, including auditing Linux on z Systems
- IBM Security zSecure Admin—Enables efficient and effective RACF administration, including cleanup, identity governance, tracking, and integration with IBM Security Identity Governance and Intelligence
- IBM Security zSecure Visual—Empowers help desks and decentralized administrators to perform RACF administration without deep technical knowledge using a Microsoft Windows–based interface
- IBM Security zSecure CICS® toolkit—Provides access to RACF command and application programming interfaces (APIs) from an IBM Customer Information Control System (CICS) environment, allowing additional administrative flexibility

**Learn more about the zSecure suite in the IBM data sheet, interactive white paper and video.**

**IBM Security zSecure suite**




* Product offers a subset of the capabilities provided by zSecure Audit

# IBM solutions: Access and identity governance

IBM Security Privileged Identity Manager is designed to protect, automate and audit the use of privileged identities with centralized capabilities to guard against insider threats, improve access control and reduce security risk.

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 and roles.

### IBM Security Privileged Identity Manager: Controlling credentials and activities

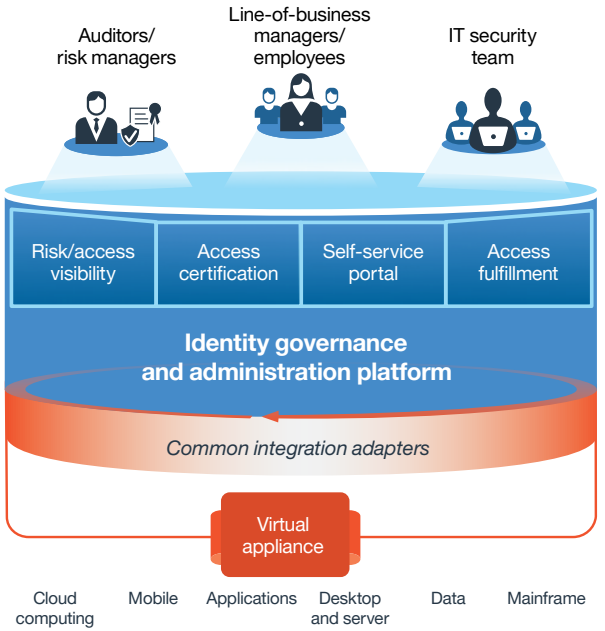
- Provides greater accountability with enhanced control of shared privileged user IDs
- Improves security with policy-based password management
- Eliminates the need to share passwords and hardcode passwords in applications
- Provides automated password management and single sign-on for high-risk account access
- Helps deter malfeasance by users and support compliance using session recording and replay
- Supports compliance with processes for approving and granting access permissions

### IBM Security Identity Governance and Intelligence: Enabling business-driven governance

- Enables a range of managers—including IT managers, auditors and business owners—to govern access from a business perspective
- Integrates intelligence-driven identity governance with management of the full user lifecycle
- Enables a business-activity-based approach to help determine segregation-of-duties violations
- Improves visibility and access control with algorithms for role mining, modeling and optimization

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

### IBM Security Identity Governance and Intelligence



# IBM solutions: Analytics for privileged data activity

QRadar Security Intelligence Platform with Sense Analytics Engine goes beyond conventional security information and event management (SIEM) approaches to address concerns including threat detection, risk assessment and management, vulnerability management, fraud discovery, forensics investigation, incident response and regulatory compliance.

IBM Security zSecure Adapters for QRadar SIEM help automate and integrate event analysis and compliance monitoring as they collect, enrich, format and send information on mainframe activity to QRadar. zSecure Alert provides QRadar SIEM with real-time critical alerts.

**QRadar: Providing visibility and clarity for the mainframe**

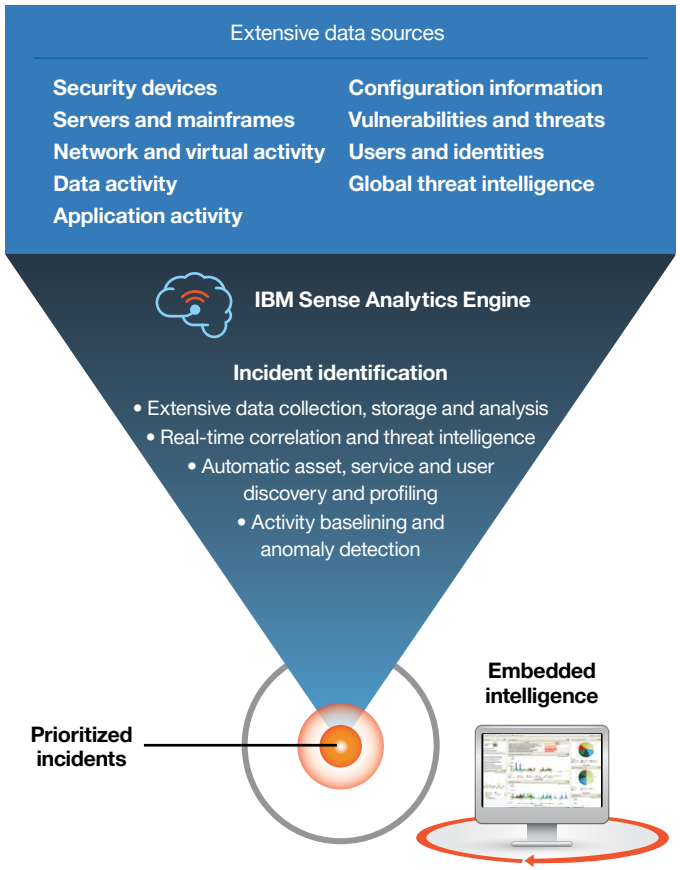
- Collects billions of events per day, on-premises or in the cloud, and integrates them to unify threat monitoring, vulnerability and risk management, forensics and incident response
- Uses its Sense Analytics Engine to sense change—including abnormal, risky behaviors across users, entities, applications and data—and attach context and meaning to the change
- Discovers low and slow threats in real time; finds and prioritizes weaknesses before exploit
- Enables intelligent incident prioritization and comprehensive insights by leveraging the power of threat intelligence and collaboration with IBM X-Force® and the IBM Security App Exchange

**zSecure Adapters for QRadar SIEM: Analysis and monitoring**

- Integrate and collect security events from many IBM z/OS sources
- Add enriched descriptive audit information about users and resources to help build intelligent reports

Learn more about QRadar, zSecure Adapters for QRadar SIEM, and zSecure Alert on the web; learn about Sense Analytics in the interactive white paper.

**IBM QRadar Security Intelligence Platform with IBM Sense Analytics Engine**



# IBM solutions: Insight for data compliance

Guardium empowers teams to protect against threats and loss by automatically finding and classifying sensitive data, analyzing access patterns, detecting threats, preventing unauthorized database access, and protecting data through real-time blocking, quarantining and encryption.

IBM Security Key Lifecycle Manager centralizes, simplifies and automates encryption key management to help minimize risk and reduce operational costs.

**Guardium: Monitoring user activity**

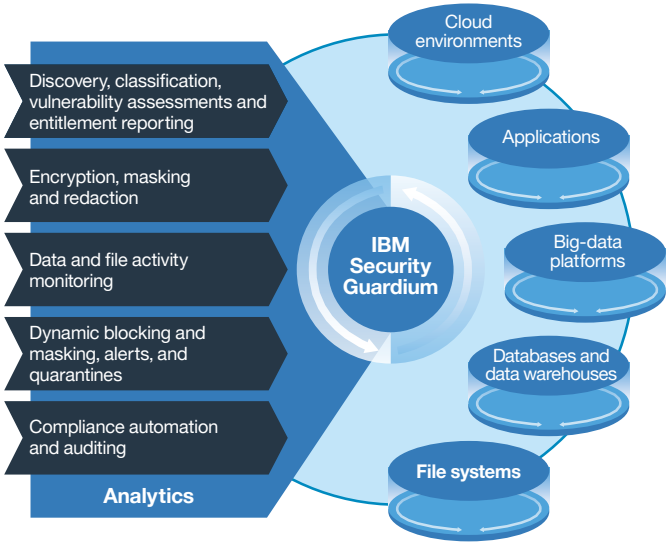
- Mitigates insider threat with real-time monitoring of privileged users' access to sensitive data
- Provides analytic insight and compliance by creating audit logs in a common format for comprehensive analysis and reporting
- Includes automated compliance workflows and pre-packaged templates to support mandates
- Supports a broad set of data sources including databases, applications, data warehouses, file shares and big data
- Provides automation and intelligence to help reduce total cost of ownership and improve manageability

**IBM Security Key Lifecycle Manager: Securing encryption keys**

- Provides centralized, simplified, transparent key management
- Addresses requirements for protection of encryption keys and control of management processes
- Helps reduce key management costs by automating the assignment and rotation of keys

Learn more about Guardium and IBM Security Key Lifecycle Manager on the web; learn about using Guardium for mainframe security in the white paper.

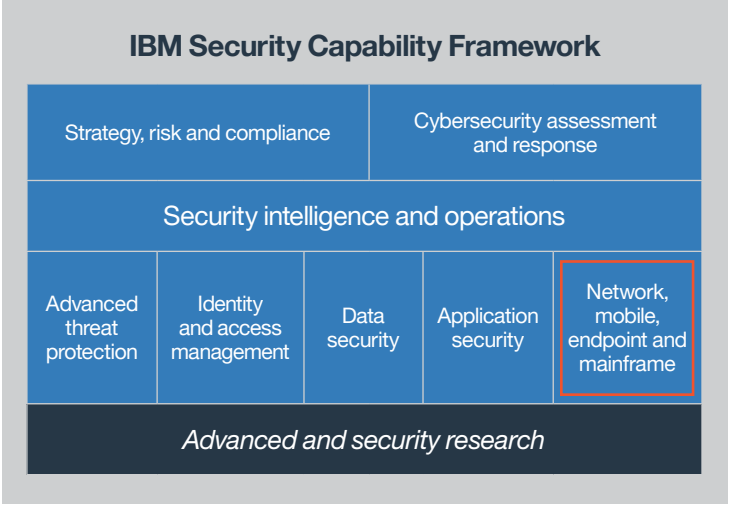
**IBM Security Guardium**



# Conclusion: Why IBM?

IBM helps organizations protect their business-critical data and mainframe infrastructures—and the people who use them—from threats and breaches. The layered, integrated IBM approach to security solutions addresses mainframe-specific concerns as well as overarching security issues such as identity and access management, security intelligence and data security across the enterprise.

The broad IBM portfolio of security solutions provides a comprehensive view of all mainframe and network user activity—including abnormal behavior—as well as potential system vulnerabilities, identifying threats and alerting administrators so they can take necessary action to prevent or remediate damage.



## For more information

To learn more about IBM solutions for protecting mainframe infrastructures, data and users, 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 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 can help you acquire the software capabilities that your business needs in the most cost-effective and strategic way possible. We'll partner with credit-qualified clients to customize a financing solution to suit your business and development goals, enable effective cash management, and improve your total cost of ownership. Fund your critical IT investment and propel your business forward with IBM Global Financing. For more information, visit: **ibm.com**/financing



IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
June 2016



WGW03223-USEN-00