IBM Z Security Interactive Guide

IBM Security

As the value of data extends from Z throughout the enterprise, IBM Security is ready

In an intensely distributed, data-driven era, the IBM Z® enterprise platform continues to deliver new enterprise workloads with the highest performance and availability. Hybrid cloud, AI, blockchain, and IoT are pushing Z to the forefront of digital transformation. Compliance requirements such as the General Data Protect Regulation (GDPR) mandate ever stronger data protection and privacy controls.

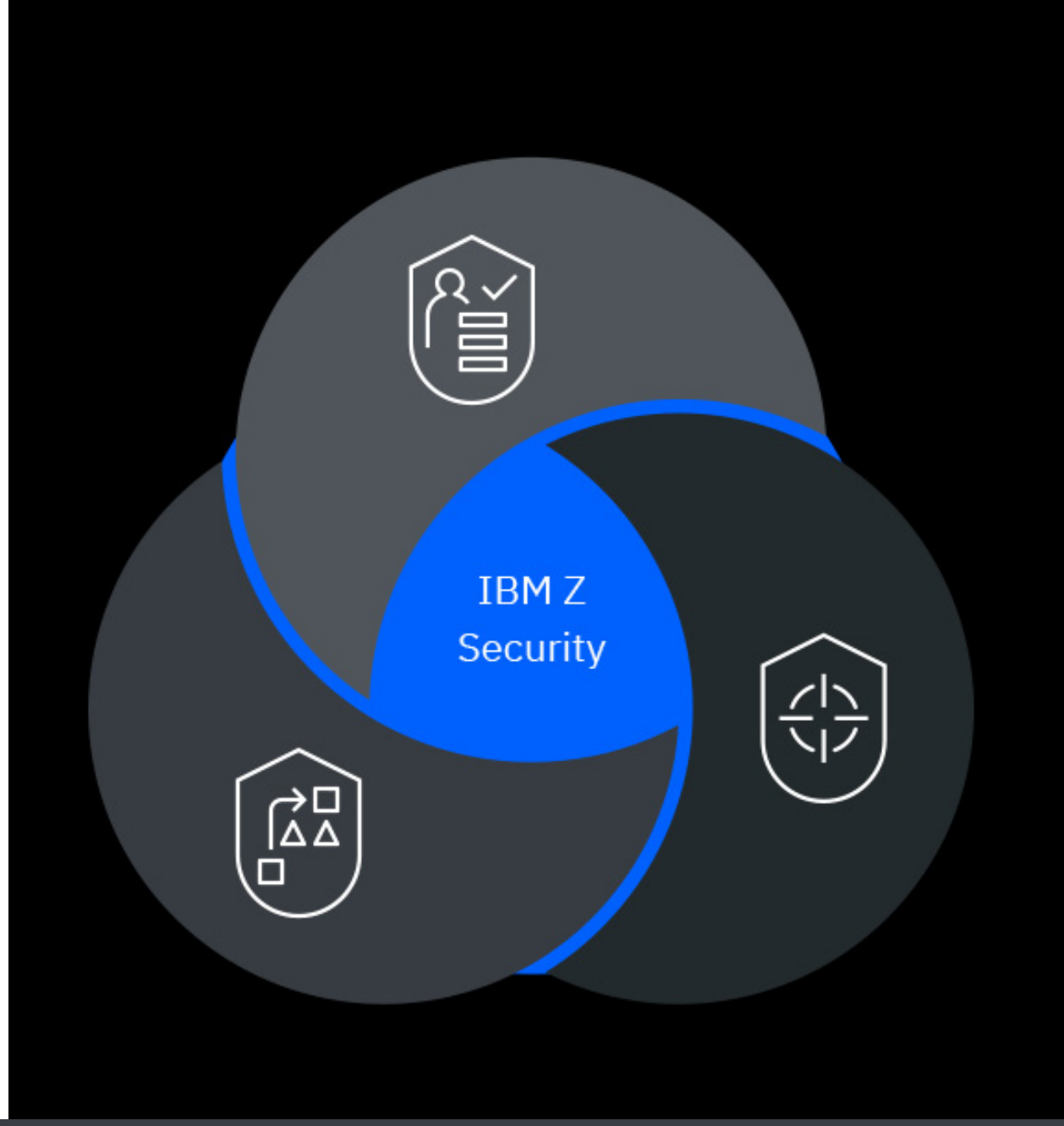
As with other essential computing platforms, IBM Z® environments are targeted by cybercriminals who exploit historical weak points such as application vulnerabilities and credentialed users with access levels beyond their needs. Modern techniques like phishing and hacking, which once were considered incapable of penetrating mainframes, are now being adapted and directed at IBM Z.

To grow your business, you need to counter these threats and address compliance needs. A cybersecurity strategy with new rules can help you to reduce risk, build confidence, and thrive. IBM Security™ provides solutions for Z that can help you achieve your objectives.

Digital Trust
Data protection
Identity governance
Advanced authentication

Threat Management
Automated threat detection
Enterprise orchestration
and security intelligence

Strategy and Risk
Regulations, policy and standards
Security strategy and maturity
Security testing and hygiene



Tools to help you grow your business and build digital trust

From protecting cloud, mobile and big-data applications, to simplifying provisioning, governance and authorization, IBM Z Security offerings are designed to help you detect threats, maintain compliance with policies and regulations, and reduce costs. Whether you want to modernize security across your mainframe environment or focus on a specific initiative, IBM Z Security offers a richly featured, integrated suite comprising point products that that are designed to be deployed quickly.

This interactive guide shows you how IBM Security zSecure suite, IBM Z Multi-Factor Authentication (MFA), IBM Security Guardium®, IBM Security QRadar® and complimentary tools can address your mainframe security needs.

Browse this this guide to read about the entire Z Security portfolio, or click on individual products to see specific capabilities and benefits.

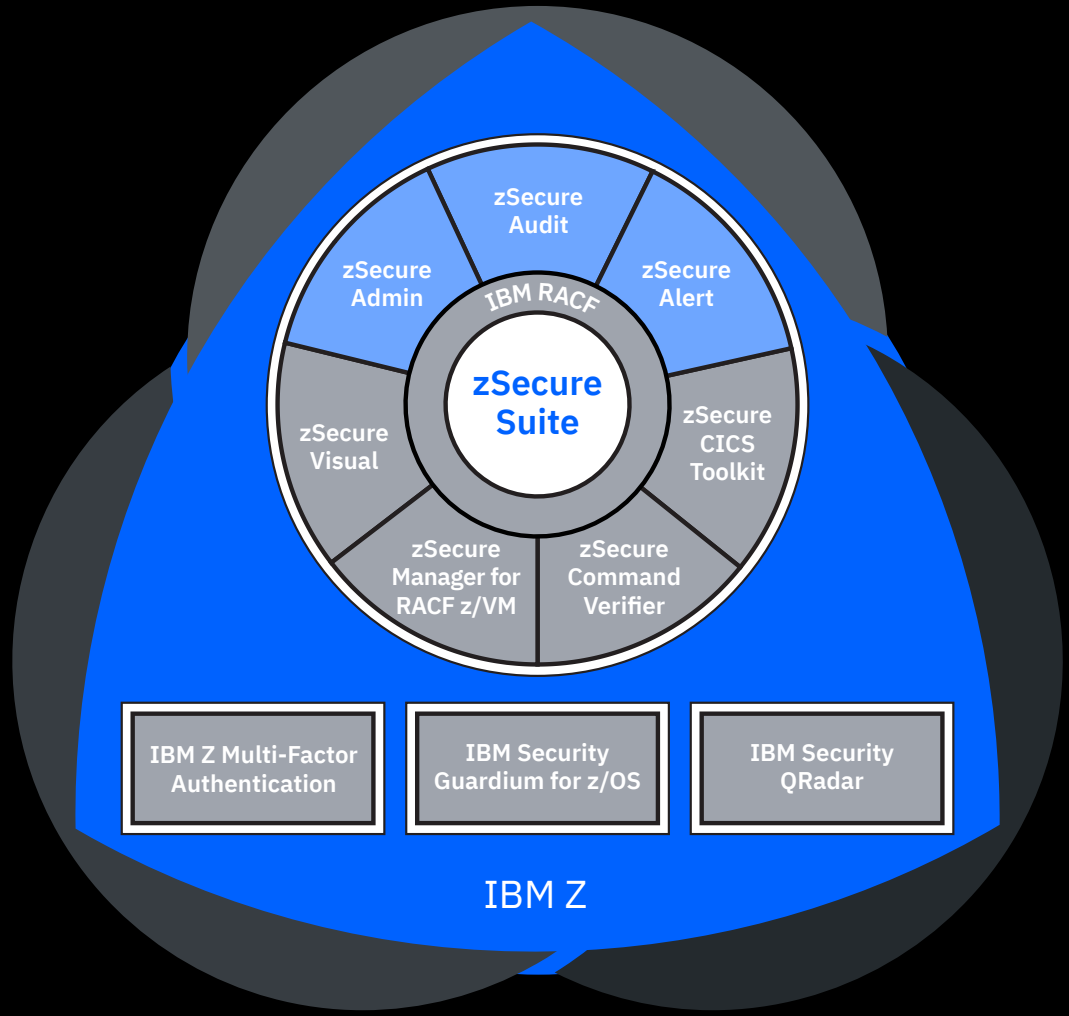
Find more information, videos, infographics and white papers at these web resources:

- IBM Security zSecure suite
- IBM Z Multi-Factor Authentication
- IBM Security Guardium family
- IBM Security QRadar Security Intelligence and Event Management (SIEM)
- IBM Resource Access Control Facility (RACF®)
- IBM Z enterprise security, including pervasive encryption, cryptography, Secure Service Container, and cloud and mobile solutions

View blog posts, webinars and videos that cover tips and tricks, strategic insights and more:

- Security Intelligence analysis and insights
- IBM Z Security community
- IBM Systems infrastructure blog
- Enterprise Knights of IBM Z videos

IBM Z Security



Click on the product names above for more information.

IBM Security zSecure Administration

Simplify IBM RACF security administration, minimize outages and streamline opeerations with IBM Security zSecure suite products that automate:

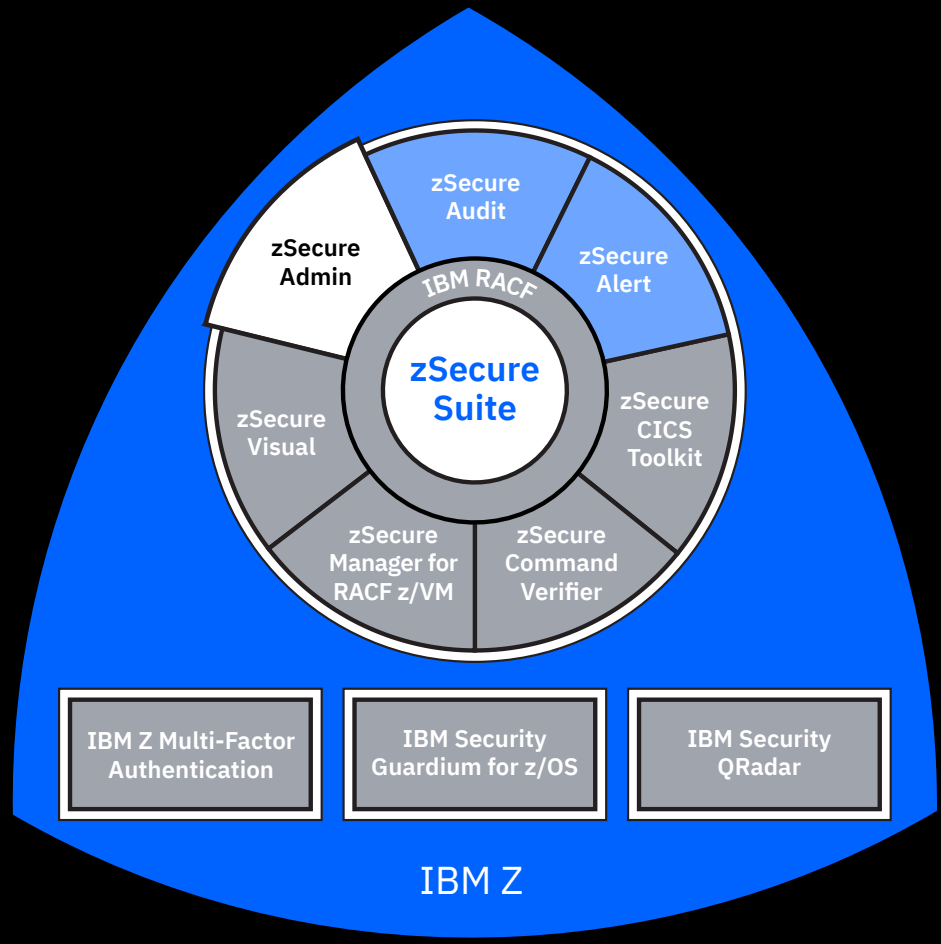
- Recurring, routine and time-consuming RACF tasks, which can help manage identities, control access, delegate tasks and provide statistics
- Identification and prioritization of security exposures and misconfigurations based a pre-defined set of best practices
- Security database cleanup to help improve security posture, such as enforcing least privilege

Other capabilities include:

- Synchronized management, merging, cleanup, testing and monitoring of multiple or remote RACF databases
- Ability to search for security related system management facilities (SMF) events
- Customizable reporting based on business requirements

For more information, visit the web page.

IBM Z Security



Click on the product names above for more information.

IBM Security zSecure Auditing

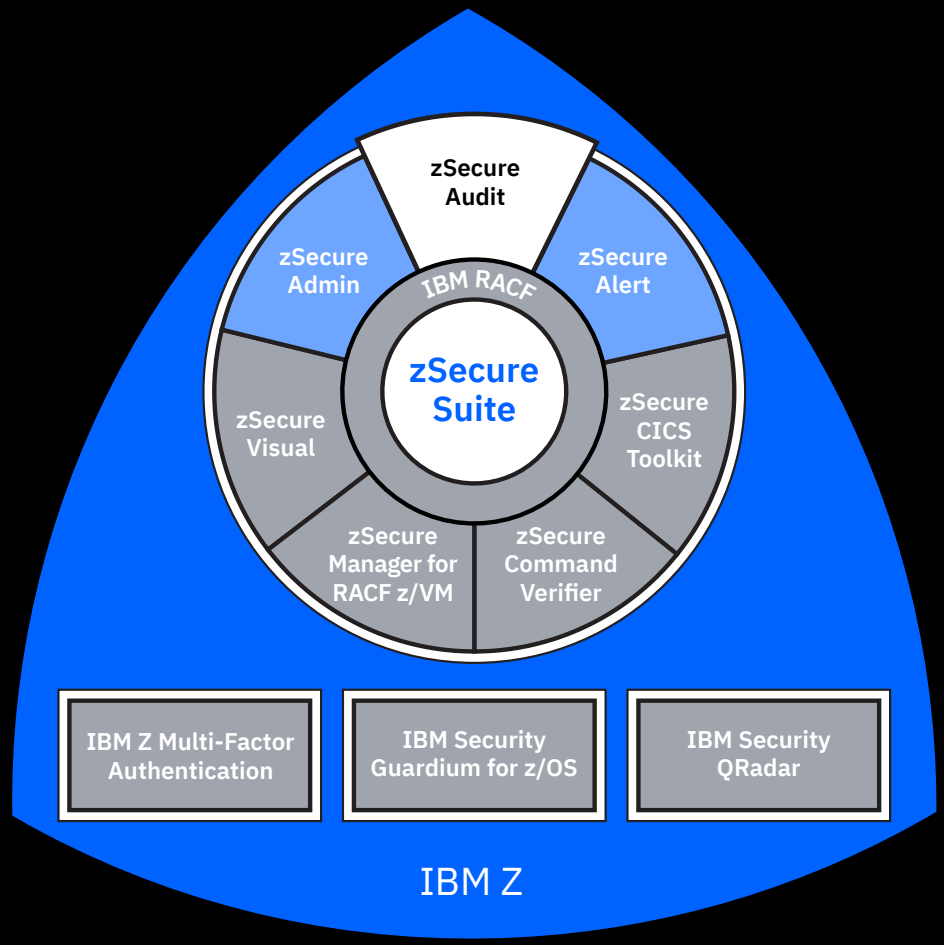
Simplify vulnerability detection, improve compliance monitoring and help reduce risks by automating:

- Security scans compared against policy and best practice baselines that generate prioritized security configuration vulnerabilities
- Analysis through a built-in knowledge base, which can improve the completeness of audits
- Detection of concealed and complex risks through data analytics
- Compliance framework testing and reporting for the below, and others:
  - The Payment Card Industry Data Security Standard (PCI DSS)
  - Security Technical Implementation Guides (STIGs)
  - Privacy regulations such as the GDPR
- File integrity monitoring with Secure Hash Algorithms (SHA-2 and SHA-3)

Other capabilities include:
- Ability to send near real-time, security-related SMF events to SIEM tools
- Customizable reporting based on business requirements

For more information visit the web page.

IBM Z Security



Click on the product names above for more information.

IBM Security zSecure Alert

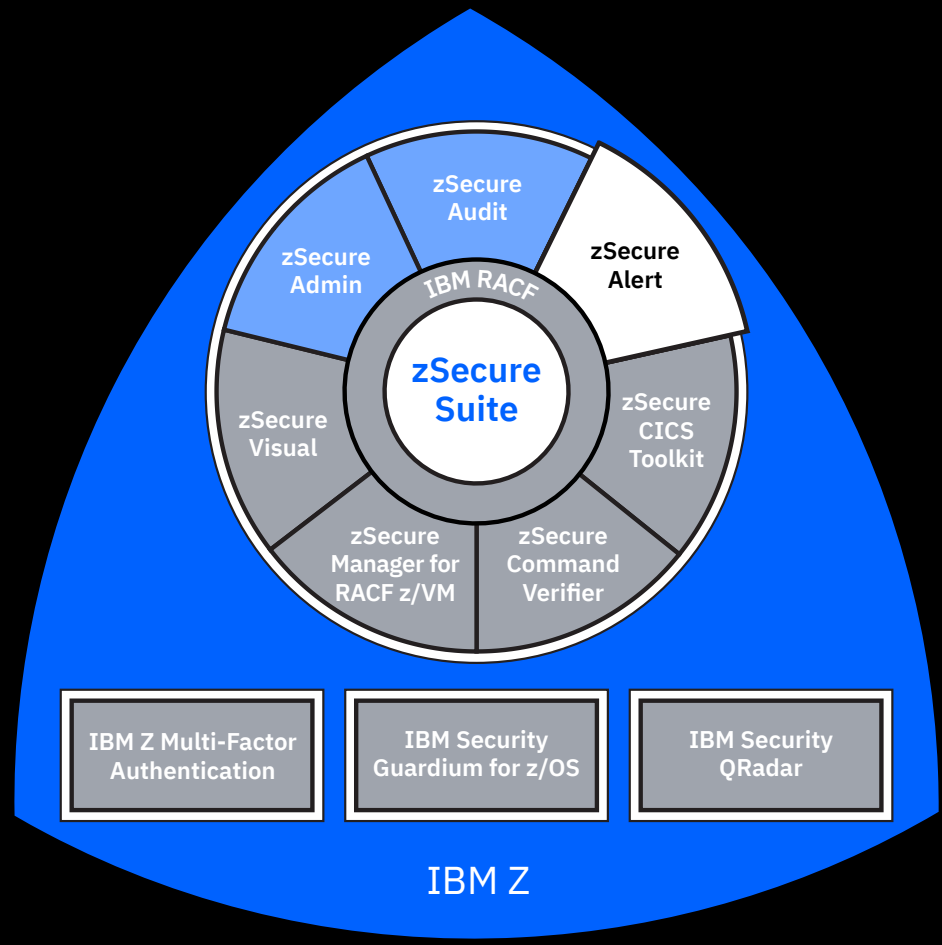
Near real-time monitoring for specific conditions and triggers that automate alerts and corrective actions through:

- Built-in alerts for common conditions
- The ability to customize predefined alerts match your operational model and business requirements
- Automated responses upon the detection of an event, such as remediation for intrusion attempts
- Monitoring of critical data to detect changes, which can help maintain data integrity, including PCI DSS data and other sensitive resources
- The ability to send near real-time alerts to your security operations center (SOC) team by integrating with enterprise SIEM tools, such as IBM Security QRadar SIEM

Alert functionality is compatible with RACF and CA ACF2 software.

For more information, visit the web page.

IBM Z Security



Click on the product names above for more information.

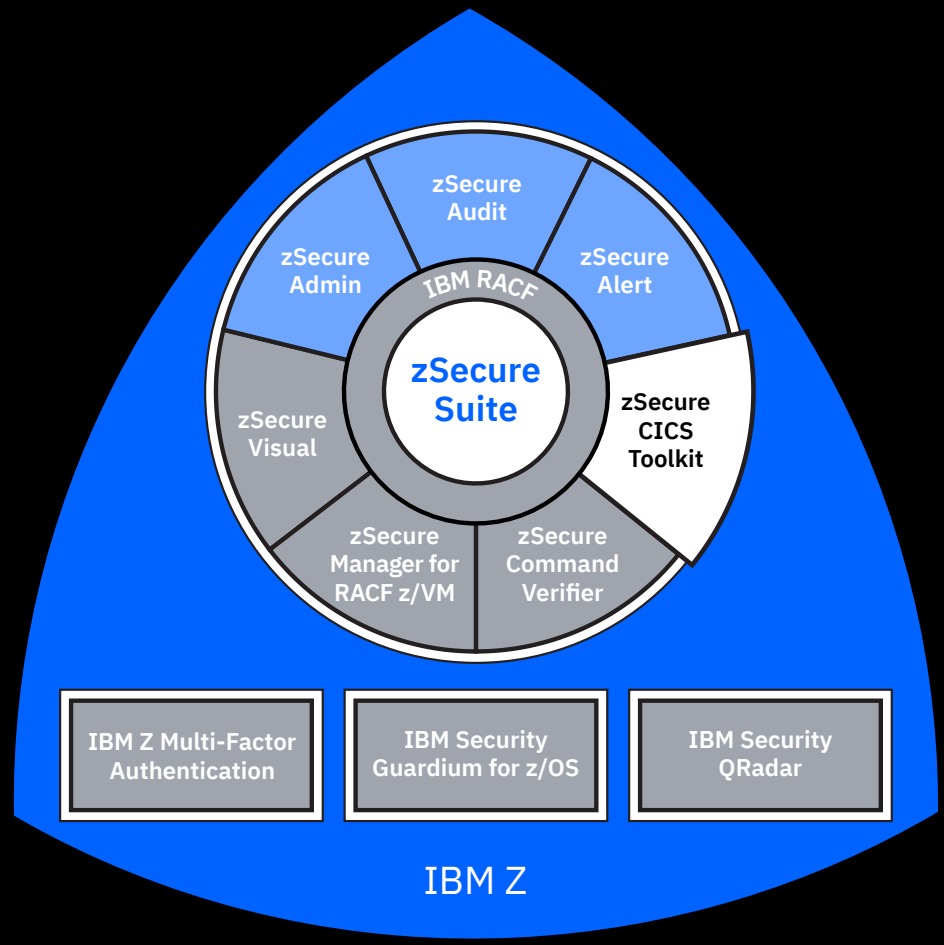
IBM Security zSecure CICS Toolkit

Capabilities
- Identify and verify system users and groups of users
- Identify, classify and protect system resources including data sets, files, tapes, IBM Db2® fields, transactions, MiniDiscs, volumes and commands
- Authorize users who need access to the resources you've protected
- Control the types of access to these resources
- Log and reports authorized and unauthorized attempts to gain access to the system and protected resources
- Administer security to help meet the security goals of your installation
- Support IBM z/OS and IBM z/VM operating systems

Potential benefits
- Provide visibility across your entire IBM Z infrastructure, enabling you to administer and report on system security
- Synchronize and consolidates security across multiple RACF databases
- Provide extensive auditing of security events for analysis that helps identify risks
- Help delegate and decentralize administration to optimize labor utilization
- Help eliminate outages and enhance availability by providing a broad coverage of audit control points and security event records
- Helps reduce business risk by enforcing security policies and best practices
- Integrate with IBM Z MFA, IBM Security zSecure, IBM Security QRadar SIEM, IBM Security Identity Governance and Intelligence and IBM Security Guardium solutions

For more information, visit the web page.

IBM Z Security



Click on the product names above for more information.

IBM Security zSecure Command Verifier

Automates proactive and remedial compliance for complex IBM RACF commands

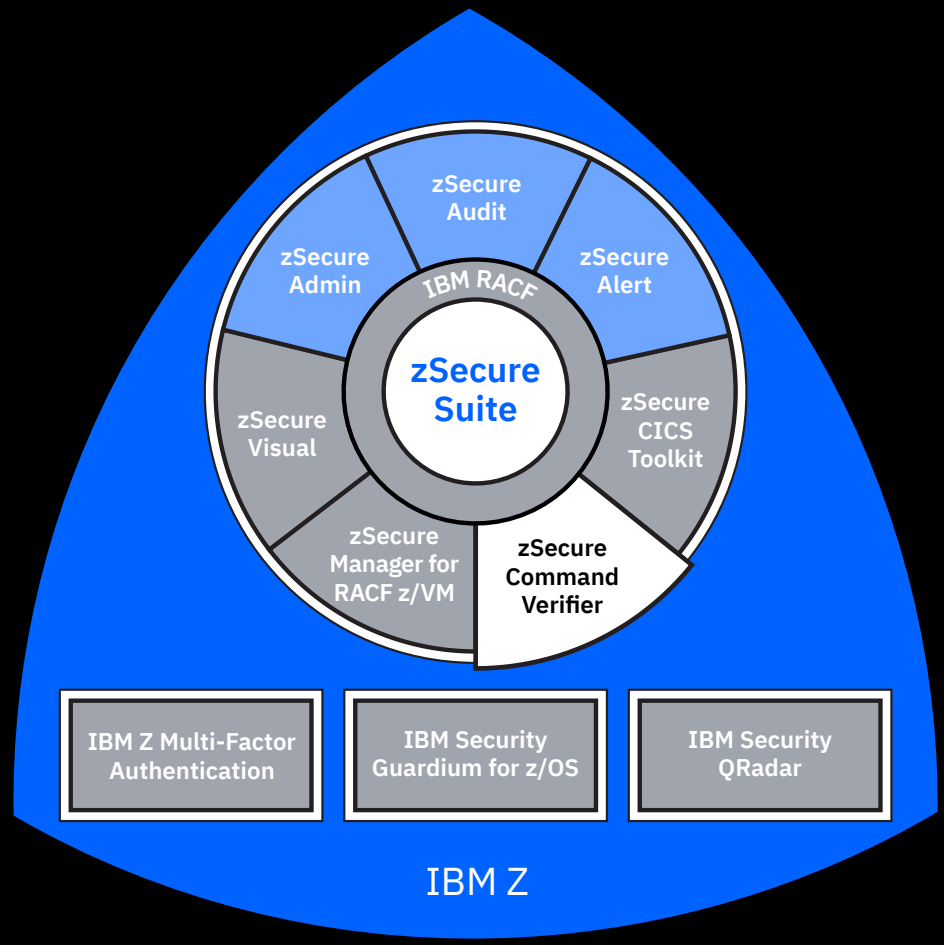
Capabilities
- Proactively enforces security policies by monitoring and blocking noncompliant RACF commands, such as those prohibited or representing high risk
- Helps reduce errors by automatically correcting miscoded RACF commands as they are being issued
- Separate duties by ensuring administrators can perform only the tasks that are permitted by their job role
- Aggregate security profile changes into a consolidated, easy-to-read list
- Ensures cleanup work that improves security cannot be undone
- Limit ability of new hires to implement high-impact changes
- Control who can set new and pervasive encryption options using command verifier policies

Potential benefits
- Helps reduce effort associated with audit remediation
- Helps reduce errors and enforces separation of duties
- Give users greater control by setting policies, alerts and defaults that enforce security policies and standards
- Help maintain the availability of critical systems and applications by preventing incorrect actions
- Integrate with RACF

IBM Security zSecure Command Verifier is included in the IBM Security zSecure Compliance and Auditing and IBM Security zSecure Compliance and Administration solution packages

For more information, visit the web page.

IBM Z Security



Click on the product names above for more information.

IBM Security zSecure Manager for RACF z/VM

Automates audit and administration, and includes auditing of Linux on IBM Z mainframes

Capabilities

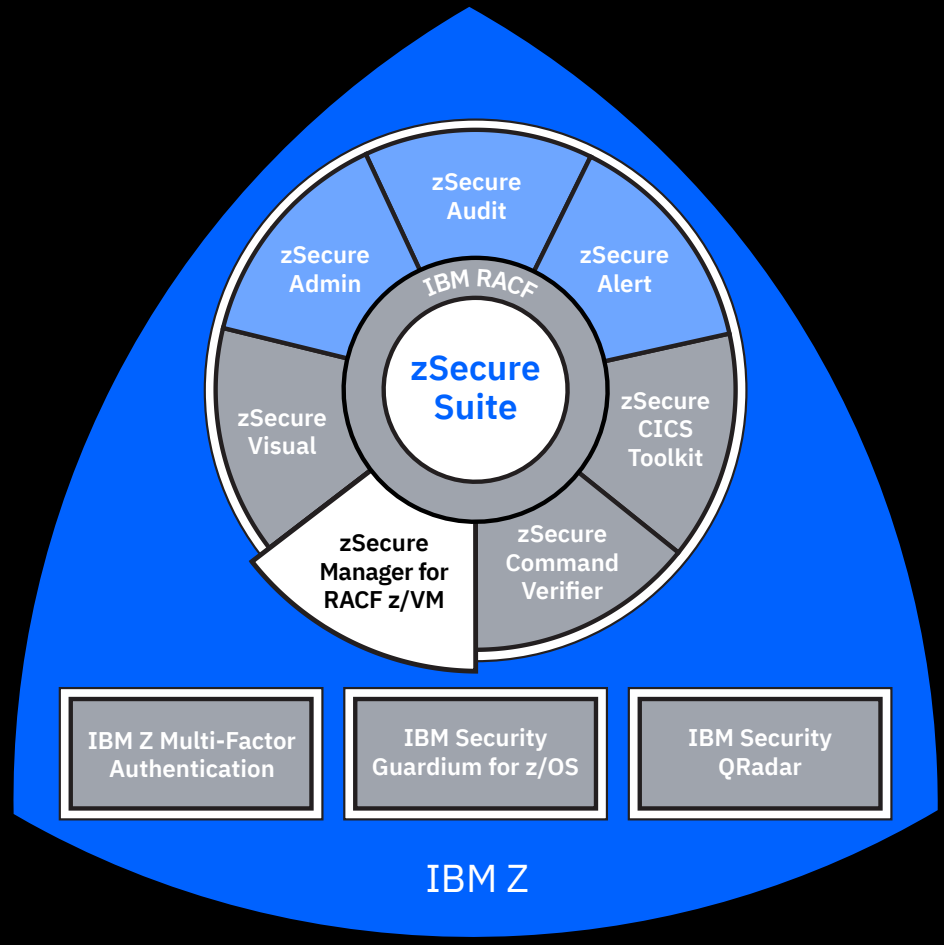
- Enhance and simplifies user management and provisioning for the IBM z/VM® environment
- Automate complex, time-consuming z/VM security management tasks with simple, one-step actions that can be performed without detailed knowledge of IBM RACF command syntax
- Extend auditing capability by reading the RACF database, analyzing SMF records generated by RACF z/VM, and providing user privileges from both RACF and the virtual machine directory
- Support ease of management, auditing and monitoring of the Linux guests if they use RACF for authentication while running in the z/VM environment
- Allow users to generate and view customized audit reports with flexible schedule and event selections
- Measure the effectiveness of controls using the solution's automated Compliance testing framework

Potential benefits

- Improve the functionality of the IBM Z security system while helping reduce administration time and effort
- Help save time and mitigate costs through improved security, efficiency and incident handling
- Help companies prepare for audits more quickly and easily
- Provide a base for virtual, cloud Linux and IBM z/OS® computing
- Integrate with RACF z/VM

For more information, visit the web page.

IBM Z Security



Click on the product names above for more information.

IBM Security zSecure Visual

Automates and simplifies IBM RACF administration through a Microsoft Windows user interface that adds security-rich features

Capabilities

- Allow your security staff to perform mainframe administrative tasks from a Microsoft Windows based graphical user interface (GUI)
- Enable you to perform common user and resource management functions in RACF without requiring security privileges to access the mainframe
- Empower business users, service desk and user provisioning teams to administer RACF and quickly identify security threats through an interface that's similar to a spreadsheet
- Allow you to view and manage data sets and general resource profiles by generating listings of profiles with similar characteristics based on search filters or selection criteria
- Enable management of multiple RACF databases through a single user interface or control point

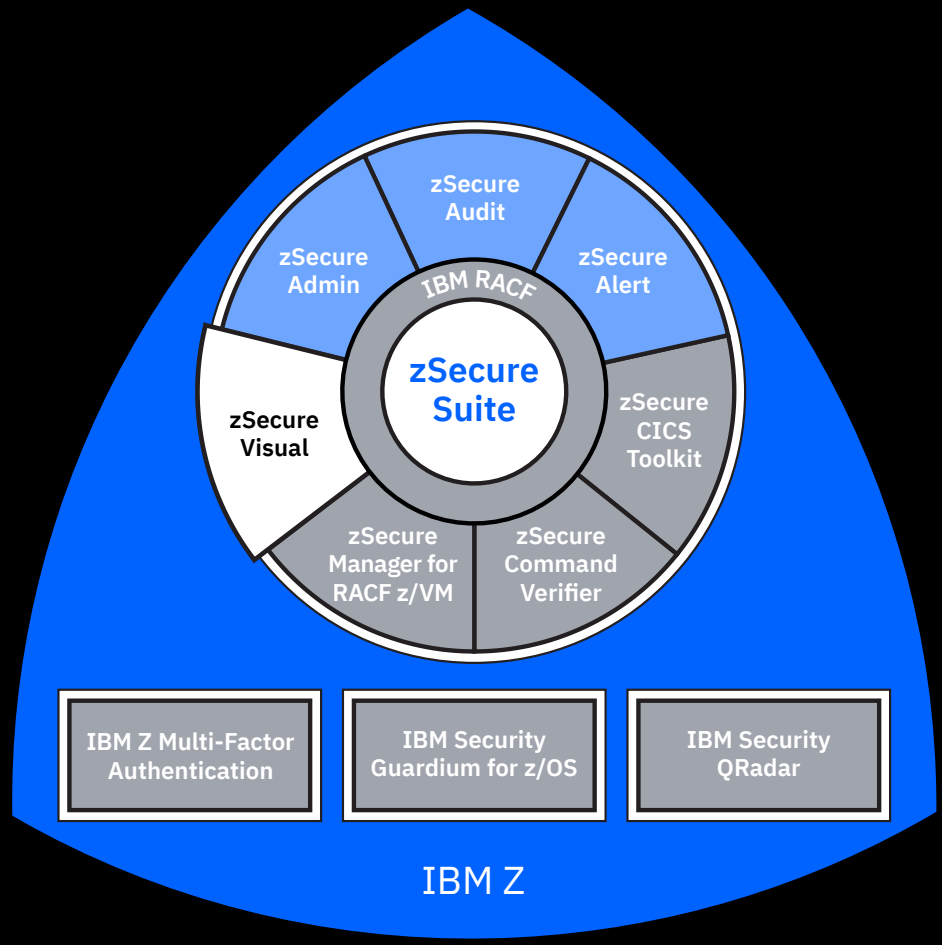
Potential benefits

- Permit changes in seconds with near real-time, online updates
- Enable business control over employees and contractors by integrating with human resource systems from PeopleSoft, SAP and other vendors
- Help manage business risk by enabling segregation of duties with roles-based administration
- Provide an alternative for the need to learn RACF, Time Sharing Option (TSO) or Interactive System Productivity Facility (ISPF) commands
- Help reduce human error and save time
- Integrates with RACF

IBM Security zSecure Visual is included in the IBM Security zSecure Administration and IBM Security zSecure Compliance and Administration solution packages

For more information, visit the web page.

IBM Z Security



Click on the product names above for more information.

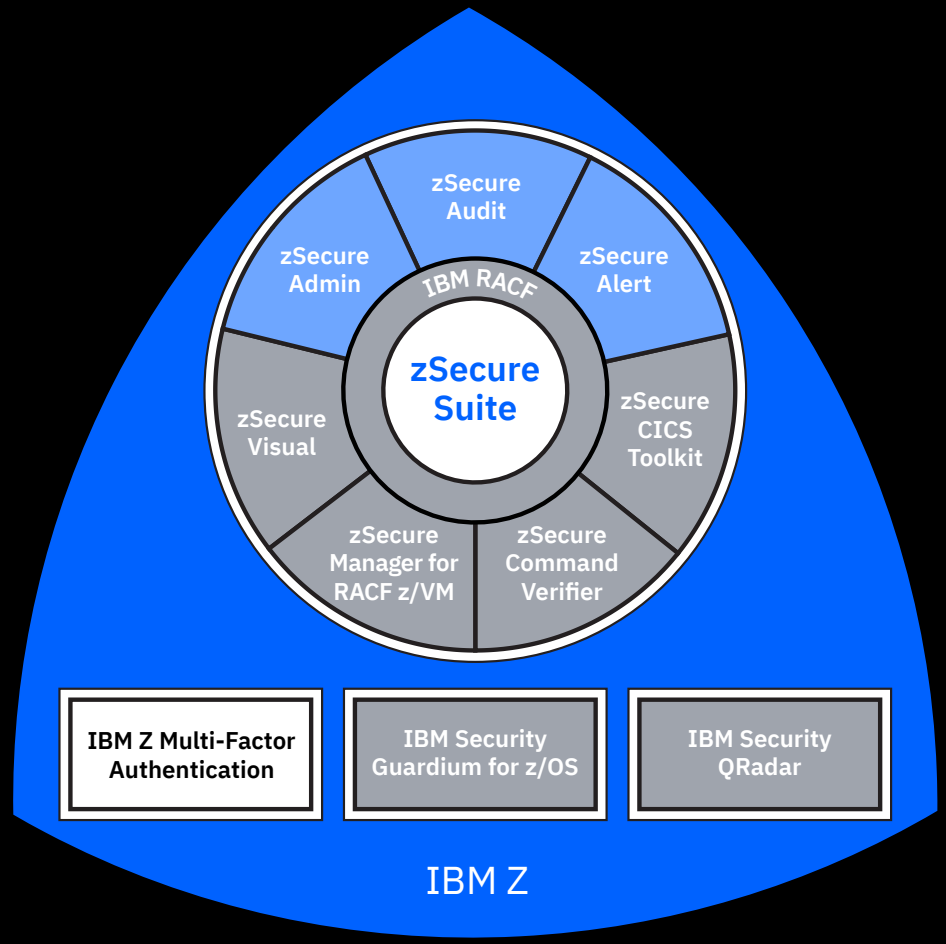
IBM Z Multi-Factor Authentication

Capabilities
- Raise the level of assurance by requiring privileged users and highly entitled users to authenticate with multiple authentication factors during the logon process
- Support extensible architecture for multiple third-party authentication systems at the same time and adds new authentication factors
- Support MFA capabilities that are easy to deploy, manage and use:
  - Generic RADIUS servers
  - Hardware and software-based RSA SecurID tokens
  - Native Yubico Yubikey one-time password (OTP)
  - Gemalto SafeNet
  - IBM TouchToken Timed-based One-time Password (TOTP) tokens
  - Personal identity verification (PIV) and Common Access Cards (CAC)
- Integrate with IBM Security Access Manager and IBM Cloud Identity Verify to create an end-to-end authentication solution
- Audit which factors are used during the authentication process for users

Potential benefits
- Offer a security-rich authentication option for users
- Address regulatory and industry requirements for strong privileged-user authentication
- Eliminate the need for exit programs to extend authentication for simple deployment
- More easily evaluate new authentication methods for different user populations on the same system
- Helps reduce business risk by enforcing strong security policies and best practices
- Integrate with IBM RACF and IBM Security zSecure with all configuration and provision data stored in the RACF database for seamless backup and recovery

For more information, visit the web page.

IBM Z Security



Click on the product names above for more information.

IBM Security Guardium

Enhance near real-time security intelligence to reduce risk and help protect the enterprise

Capabilities

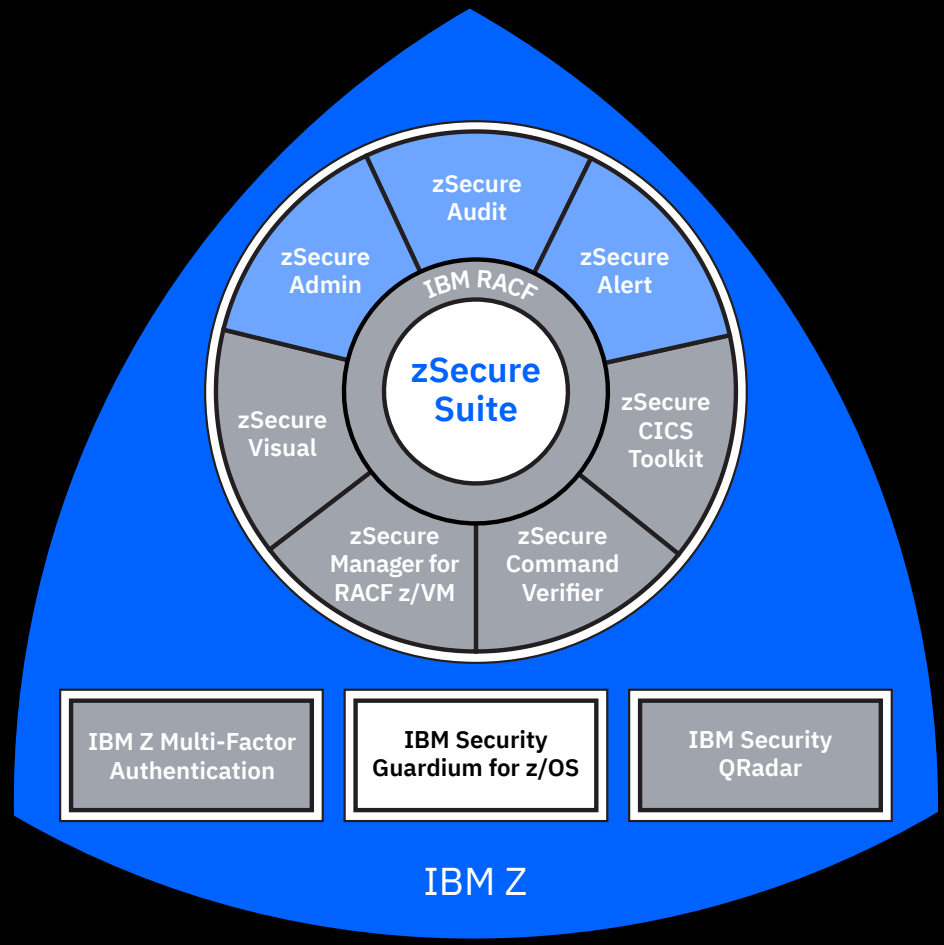
- Enable centralized, enterprise-wide collection of security event information, including information from mainframes, to eliminate mainframe isolation and enhance visibility
- Provide automated, near real-time analytics of extensive event information to detect potential threats and prioritize alerts to enable proactive response and remediation
- Monitor compliance of user defined internal security policies, best practices, external standards and industry regulations with customizable reporting
- Enable possible deep dives into specific security event information for forensic analysis, user behavior anomalies and other cognitive analysis

Potential benefits

- Support proactive, efficient, cognitive, near real-time security event analytics with capabilities including event dashboards, user behavior analysis and deep-dive forensics
- Integrate mainframe security event information with enterprise activity information to detect large-scale patterns and potential threats
- Help reduce business risk with customizable threat, audit and compliance reporting, and with prioritized, near real-time alerts for timely response and remediation
- Helps streamline detection of potential threats and prevention of breaches, outages, policy violations and financial fraud
- Enhances operational effectiveness for SOCs, risk managers, compliance managers and auditors for the investigation of relevant security event information

For more information, visit the web page.

IBM Z Security



Click on the product names above for more information.

IBM Security QRadar SIEM

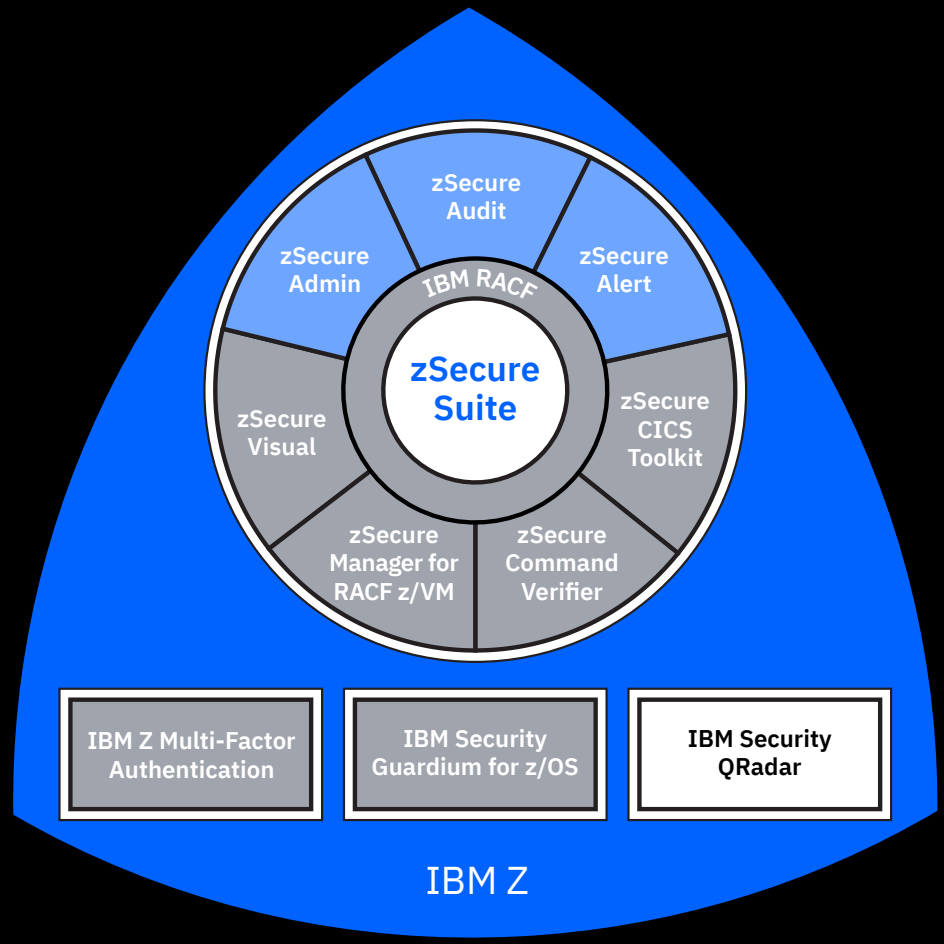
Intelligent security analytics for insight into your most critical threats

Capabilities
- Provide automated database security. including near real-time monitoring, alerting and incident detection
- Create a single, centralized audit repository for compliance reporting
- Deliver preconfigured reports for Sarbanes-Oxley Act (SOX), PCI DSS, GDPR and other data privacy requirements
- Support investigations and forensics research
- Utilize separation of duties and user administration so that sensitive data is displayed to appropriate users
- Provide an advanced workflow for signoffs, escalations and comments
- Optionally enable blocking of access to sensitive data
- Through its highly efficient infrastructure, reduce CPU million instructions per second (MIPS) consumption and utilization of IBM z Integrated Information Processors (zIIP)

Potential benefits
- Enable proactive, efficient and effective responses to audit and alert activity
- Helps reduce risk by allowing users to gain access to only the right data
- Provide insights and triggers automatic alerts when suspicious activity is detected
- Enable operational effectiveness for auditors, database administrators, and others to run reports and easily modify or create new reports and dashboards using GUI drag and drop technology
- Give flexibility for addressing future regulations and governance

For more information, visit the web page.

IBM Z Security



Click on the product names above for more information.

Additional resources

Find more information, videos, infographics and white papers at these web resources:

- IBM Security zSecure suite
- IBM Z Multi-Factor Authentication
- IBM Security Guardium family
- IBM Security QRadar SIEM
- IBM RACF
- IBM Z enterprise security, including pervasive encryption, cryptography, Secure Service Container, and cloud and mobile solutions

View blog posts, webinars and videos that cover tips and tricks, strategic insights and more:

- Security Intelligence analysis and insights
- IBM Z Security community
- IBM Systems infrastructure blog
- Enterprise Knights of IBM Z videos

Why IBM?

IBM Security zSecure suite offerings are the product of more than 25 years committed to innovation on IBM Z and to enabling you to improve and simplify mainframe security audit and administration. zSecure suite is developed in parallel with the latest innovations on IBM Z, from pervasive encryption introduced with z14™ to IBM Data Privacy Passports and hybrid cloud breakthroughs in z15.™ While some vendors have reduced their focus on mainframe security offerings, IBM Security continues to invest in research, product development and transformational services for our IBM Z clients.

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 IBM 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.