The IBM zSecure Suite

Amplify your Z Systems security, administrative efficiency, and compliance

The IBM zSecure Suite adds layers of security assurance—auditing, alerting, administration, reporting, authentication, workshops and assessments—that enhance the security in IBM Z hardware, software, virtualization, and standard enterprise security management tools such as IBM RACF, CA ACF2, and CA Top Secret.

The zSecure Suite automates security administrative tasks to help increase efficiency and reduce errors, adds governance that can help enforce compliance management of regulations and standards, detects internal and external threats, issues real-time alerts, and monitors compliance such as pervasive encryption utilization for GDPR, HIPPA, etc.

The IBM zSecure Suite also includes basic and advanced workshops and value assessments. IBM Z Security workshops help you prioritize your mainframe security checklist. We'll determine your organization's risk factors, review your existing security approach, identify vulnerabilities, and provide recommendations.

And as your mainframe security needs evolve, our assessments help ensure you're realizing as much value as possible from your IBM zSecure or IBM Guardium for z/OS investments.

Highlights

- Automates security administrative tasks to help increase efficiency and reduce errors
- Effective identity governance can help enforce compliance management of regulations and standards
- Detect threats, issue real-time alerts, and monitory compliance such as pervasive encryption utilization for GDPR

The Suite and Related Products

IBM zSecure Audit and Alert

IBM zSecure Audit and Alert work in tandem and with enterprise security managers (ESMs) to reveal vulnerabilities in mainframe infrastructure, strengthen threat monitoring, and help ensure compliant policy.

With IBM zSecure Audit you can measure and verify the effectiveness of your mainframe policies for ESMs, IBM RACF, CA-ACF2 or CA Top Secret. As a vulnerability analysis of your mainframe infrastructure, use zSecure Audit to generate reports and quickly locate problems such as an unprotected data set. It also provides a compliance framework for testing against industry regulations.

IBM zSecure Alert helps you establish mainframe monitoring for both internal and external threats as part of your enterprise threat protection approach. zSecure Alert enables efficient incident management and streamlines audit efforts to expose improper configurations, reduce security housekeeping, enhance your system availability, and supplement access controls.

IBM Guardium for z/OS

IBM Guardium for zOS automates data discovery and classification, real-time activity monitoring, and cognitive analytics to discover unusual activity in your most sensitive z/OS databases. It protects against unauthorized data access by continuously monitoring user entrance patterns, providing real-time alerts on suspicious activities, dynamically blocking access, or quarantining user IDs to protect against internal and external threats. Feeds to security information and event management (SIEM) solutions such as IBM QRadar or Splunk for correlating threat activities help streamline and automate these compliance workflows. Plus, by tapping the power of Guardium for z/OS you can proactively assess vulnerabilities and misconfigurations in your DB2z, IMS, and Data Sets

IBM zSecure Admin Tool Set

IBM zSecure Admin enables you to automate recurring, time-consuming security administration tasks: delegate password reset authority to staff or resume a user and grant specific accesses without granting full administrative privileges. Quickly identify and analyze problems in IBM RACF such as missing or inconsistent definitions, enabling you to fix or prevent mistakes before they become a threat to security and compliance. You can also monitor privileged users to help ensure old accounts are properly deleted and products have been integrated appropriately.

zSecure Admin can administer multiple systems with a single application interface. You can compare profiles and efficiently merge security rules from different databases. You can copy or move users, groups, resources, applications, or whole databases between systems and rename IDs within the same database. When merging profiles from different databases, zSecure Admin performs extensive consistency checks and reports potential conflicts before generating commands, helping ease the burden of consolidation efforts.

IBM Z Multi-Factor Authentication

Mainframe systems are the foundation of trusted digital experiences for most of the world’s largest companies and organizations, but passwords protecting critical users, data and applications are a relatively simple point of attack for hackers to exploit because passwords rely on user education and compliance for both implementation and control. Using a variety of methods such as social engineering and phishing, criminals have exploited legitimate users to hack into even the most secure platforms.

IBM Z Multi-Factor Authentication (IBM Z MFA) raises the level of assurance of your mission-critical systems with expanded authentication capabilities and options for a comprehensive, user-centered strategy to help mitigate the risk of compromised passwords and system hacks.

Workshops and Assessments

IBM Z Security Workshops: Basic and Advanced

The mainframe has been around for decades, but they aren't used as hidden workhorses anymore. Nor can your security posture be the same for these systems. The Basic Workshop is for growing organizations whose reliance on the mainframe is maturing, organizations concerned they may not have implemented the best security framework during their rapid growth. This workshop includes the completion of a guided self-assessment tool, expert scoring, a thorough discussion of the results, and requires no fee. After completing the workshop, you should have a better understanding of your Z System framework and be aware of better ways to protect it.

The Advanced Workshop, a half-day, no fee engagement is led by an IBM Z Security SME who walks your domain experts through a discussion of six essential security controls to help you understand where your approach may be deficient. Large, complex enterprises have unique security architecture and policy needs. Most often they have implemented and nurtured a mature Z Security framework but need to understand if there are still ways to improve their overall security posture, especially given the dynamic nature of the latest breach tactics.

IBM Z Security Assessments: zSecure and Guardium for z/OS

As your mainframe security needs evolve, going through one of the IBM Z Security Value-Assessments can help ensure you are realizing as much value as possible from your investment in either the IBM zSecure or IBM Guardian for z/OS solutions.

In this three-hour (remote or on-site) engagement, our team will review your existing utilization of zSecure or Guardium. We will then deliver a report explaining how to optimize your overall security posture by: (1) Outlining our recommended mainframe security end state, including any developments or changes in strategy or environment since implementation. (2) Providing actionable, prioritized recommendations to move from current to desired state. (3) Updating your team on the evolving solution set (there can often be a few surprises here!) (4) Showing you how IBM zSecure or Guardium for z/OS can continue being enablers for your business in the future. (NOTE: final reports are usually delivered within a week from the end of the assessment.)

There is no charge for these assessments. They are delivered by our top zSecure or Guardium for z/OS technical specialists and practitioners who'll work side-by-side with your security team.

Why IBM?

IBM Security Services professionals can offer virtually unparalleled IAM expertise, broadened by their access to IBM's research and development team. Available worldwide, IBM specialists can tailor their recommendations to your region's unique circumstances. Their approach to IAM strategy and assessment examines impact at every level of your organization—from business strategy to applications to IT infrastructure — to help you implement an IAM program designed to meet your business and IT objectives.

For more information

To learn more about IBM Identity and Access Management Services for identity and access strategy and assessment, please contact your IBM representative or IBM Business Partner, or visit the following website: ibm.com/security/mainframe-security

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

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice and represent goals and objectives only.