Security on System z eGuide

The top organization around the world trust their business to IBM System z mainframes

Organizations around the world—including 92 of the world's top 100 banks, 23 of the top 25 US retailers and nine of the world's 10 largest insurance organizations—trust their business to the scalable, highly available, self-optimizing - and above all - ***secure*** IBM System z mainframe.

IBM System z security provides a core set of robust services such as cryptographic hardware, system integrity, EAL5 certification and more. While it might be the perfect place to store sensitive data and perform business critical transactions and analytics it can also be a target for would-be cyber criminal and hackers that seek to breach that data.

IBM provides a comprehensive eco system of security solutions extending that protection across many data sources, applications, users and transactions helping customers to reduce the business risks and costs or a security breach.

Read on and learn how you can help your organization make data breaches a thing of the past by taking a more proactive, preventative approach to the many aspects of security.

IBM Security on System z has four strategic capabilities that help safeguard mission critical data and applications while enabling mobile cloud and analytics:

Establish identities and manage access control: Creating trustworthy user identification and authorization establishes the foundation necessary for controlling access to data, applications, and other system resources.

Protect and manage enterprise-wide information: Ensuring compliance through security and privacy controls across big data and analytics environments with real time threat prevention, without impacting critical application performance.

Automate audit reporting and compliance monitoring: Utilizing extensive audit logging, analysis and reporting helps you enforce security policy, detect privileged user abuse and pass compliance audits.

Enhance security intelligence to detect potential internal and external threats: Collecting and combining mainframe security event information with enterprise-wide security helps organizations to detect potential internal and external vulnerabilities and to react quickly to prevent breaches.

This e-guide will show you how a security strategy can protect your essential data for cloud, mobile and big data applications.

Resources

Webpage: System z Enterprise Security

White Paper: Creating the ultimate security Platform

Mainframe 50 Security video: Mainframe Security Celebrates 50 Years

Analyst White Paper: Secure the Enterprise with Confidence
Video: zSecure for Superior Mainframe Security

Analyst White Paper – Information Protection – The Impact of Big Data

Identify and authenticate users for access control to data, applications and system resources on the mainframe

Identity and access management establishes the basis for data protection, security auditing, compliance reporting and threat detection. The key capabilities include:

- **User identification**
- **User authentication**
- **Access control**
- **Special privileges, roles and groups**

A wide variety of users have access to applications and data on the mainframe, often through distributed applications. Management of these users must be from "cradle-to-grave", including user provisioning, de-provisioning, self-service for routine tasks (i.e. password resets), and automated tracking of access to critical enterprise resources and commands.

The goal of user management is to provide access and authorization control to prevent fraudulent use of applications and data. This requires automated management and risk-based enforcement of access control policies across every application, data source and operating system. User management also includes role-based identity and access management that aligns users' roles to their access capabilities, as well as separation of duties and special privileges.

IBM helps organizations establish their identity and access control foundation with System z security solutions such as IBM Resource Access Control Facility and IBM Security zSecure suite. There are additional enterprise wide security solutions which manage user information across multiple platforms to establish trust across the internet.

IBM provides the following Identity and Access management solutions to help your organization:

IBM Resource Access Control Facility (RACF) grants access only to authorized users of the protected resources. After identifying and authenticating the user, it controls the interaction between the user, system resources, communications capabilities, programs and applications. It also provides detailed audit and administrative capabilities.

IBM Security zSecure Admin automates and simplifies RACF and DB2 security and compliance administration tasks and enhances delegation capabilities. It helps you maximize IT resources, reduce errors, increase efficiency, and identify problems quickly to help minimize security risks and demonstrate compliance.

IBM Security Identity Manager enables organizations to drive effective identity management and governance across the enterprise. It automates the creation, modification, recertification and termination of user privileges and supports policy-based password management throughout the user lifecycle. It integrates with CrossIdeas for identity governance.

IBM Tivoli Federated Identity Manager provides web and federated single sign-on (SSO) to users throughout multiple applications. It uses federated SSO for security-rich information sharing for private, public and hybrid cloud deployments.

IBM Security Access Manager for Mobile provides mobile access security protection in a modular appliance package. It addresses mobile security challenges by proactively enforcing access policies for web environments and mobile collaboration channels. It can also integrate Trusteer Mobile Fraud protection information.

Resources

IBM Systems Magazine, July/August 2014: A Secure Fortress

Customer Video: IBM Security zSecure Products at Allied Irish Bank

Data sheet: IBM Security zSecure Admin

Webpage: IBM Security Identity and Access Management

Protect critical data with military strength security solutions from application to mainframe

Protect critical business data and sensitive customer information for big data analytics and mobile applications:

- **At rest on the system or storage devices**
- **In motion across trusted or untrusted network and communication lines**

Big data represents a significant business opportunity by analyzing increasing volumes and varieties of information to gain deeper insight. It can also represent a big threat if the proper security and privacy controls are not in place. The goal of information protection is to reduce the business risks and costs associated with this data by helping prevent breaches for both data at rest and in motion - whether by local or remote users, web and mobile applications. Over the last 4 years attacks have become more frequent and more sophisticated with spear phishing , watering holes, malware, XSS and more.

Many attacks occur over long time periods. A recent study found that while the period from initial attack to initial compromise typically takes only seconds or minutes, and the period from initial compromise to data extraction typically takes minutes to hours, the period from compromise to discovery in 98 percent of cases takes weeks or even several months.

Effective information protection solutions require sophisticated capabilities like real time threat monitoring and prevention. privacy of sensitive information in test, development and production environments, separation of duties, managing inactive or orphan user accounts, monitoring for inappropriate server configuration changes, ensuing regulatory compliance and control. In addition, all data must have an appropriate level of encryption and the encryption keys properly managed.

IBM's solutions provide your organization with the tools to ensure your enterprise mobile applications have the highest possible security built in from the start, not bolted-on as an afterthought:

IBM InfoSphere Guardium Database Activity Monitor and Vulnerability Assessment provides a simple, robust solution for continuously monitoring access to data sources, and automating compliance controls in heterogeneous enterprises. The solution prevents unauthorized activities by privileged insiders or hackers while monitoring end users to identify fraud, without requiring any changes to data sources, applications or impacting performance.

IBM InfoSphere Guardium Data Encryption for DB2 and IMS Databases provides row and column level encryption for DB2 for z/OS databases and segment level encryption for IMS databases.

IBM InfoSphere Optim Data Masking ensures compliance during test and development by de-identifying all data while retaining its behavioral characteristics and referential integrity to the real data sets. It is used in conjunction with IBM InfoSphere Test Data Management which produces right sized data sets without having to clone entire data sources.

IBM Enterprise Key Management Foundation (EKMF) provides centralized key management on IBM zEnterprise and distributed platforms for streamlined, efficient and secure key and certificate management operations.

IBM Security Key Lifecycle Manager (for z/OS) manages encryption keys for storage, simplifying deployment and maintaining availability to data to protect data privacy and comply with security regulations.

Resources

Demo: Information Protection Solutions with InfoSphere Guardium for System z

Demo: Protecting Data in Development and Test Environments

Whitepaper: Safeguard Enterprise Compliance and Remain Vigilant Against Threats

Analyst White Paper – Information Protection – The Impact of Big Data

Case study: South American Automotive Financing Company Prevents Unauthorized Activities and Monitors Database Changes Across Its Distributed and Mainframe Application Databases

Automate audit reporting and compliance monitoring

Today's security environment is experiencing rapid change on all fronts—in risks and dangers from advanced and sophisticated threats, technology innovations for a secure computing platform, compliance and governance strategies in response to regulations and best practices, and business needs to help ensure business continuity and prevent financial loss.

In each of these areas, the centralized big data created and collected by modern connected, intelligent infrastructures must be kept secure. So must cloud environments, which continue to grow and evolve. So must mobile applications, which have rapidly entered widespread business use.

Regulatory requirements, such as the Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS), Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) and other regulations worldwide, must be met.

Security intelligence, along with automated threat analysis and remediation, must be provided to help ensure maximum visibility into activities within the operational environment. And complexity must be reduced, with automated solutions that are simple and cost-efficient to deploy and utilize, scalable solutions that can keep up with enterprise growth, and integrated solutions that can take the place of siloed point products.

The audit and compliance solutions on System z include:

IBM Security zSecure Command Verifier enables you to compare each IBM Resource Access Control Facility (RACF) command to your security policies prior to processing. Commands are intercepted as they are entered and compared to your security policy to determine whether or not they should be run.

IBM Security zSecure Audit is a mainframe solution that measures and verifies the effectiveness of mainframe security policies for IBM DB2, IBM RACF, CA-ACF2 and CA Top Secret Security. It generates reports to quickly locate problems associated with a particular resource to provide vulnerability analysis of your mainframe infrastructure. It also provides a compliance framework for testing against industry regulations.

IBM Security zSecure Alert helps you establish mainframe monitoring as part of your enterprise threat monitoring approach. It monitors for internal and external threats and improper configurations. zSecure Alert provides responsive incident management and streamlines audit efforts to reduce security housekeeping on the mainframe, enhance system availability and supplement access controls.

IBM InfoSphere Guardium Database Activity Monitor and Vulnerability Assessment helps enforce compliance with prebuilt policies, processes, automated workflow and sign off to ensure legislation and regulation is followed, with proof of who did what, when, where and how.

Resources

White Paper: Safeguard Enterprise Compliance and Remain Vigilant Against Threats

Video: How Swiss Re Manages Mainframe Security Compliance

Enhance security intelligence to detect potential internal and external threats across your entire organization

IBM delivers Next generation security intelligence from applying advanced analytics and automation to massive amounts of data, events, incidents and network flows.

Security intelligence provides a common, intuitive view that combines deep analytics with real-time security monitoring. Security intelligence unifies existing tools to reduce complexity and lower the cost of maintaining a strong security posture.

Near real-time surveillance for threat detection and prioritization throughout the entire IT infrastructure is essential for security intelligence. Data silos are consolidated by gathering information across the enterprise, including System z and other systems, into one enterprise view.

Complex correlation is performed using rule triggers on threats, insider fraud and business risk across the enterprise computing and transmission environment. The prioritized results allow for investigation on an actionable list of suspected incidents. Threat and compliance management is established using detailed data access and user activity reports.

Resources

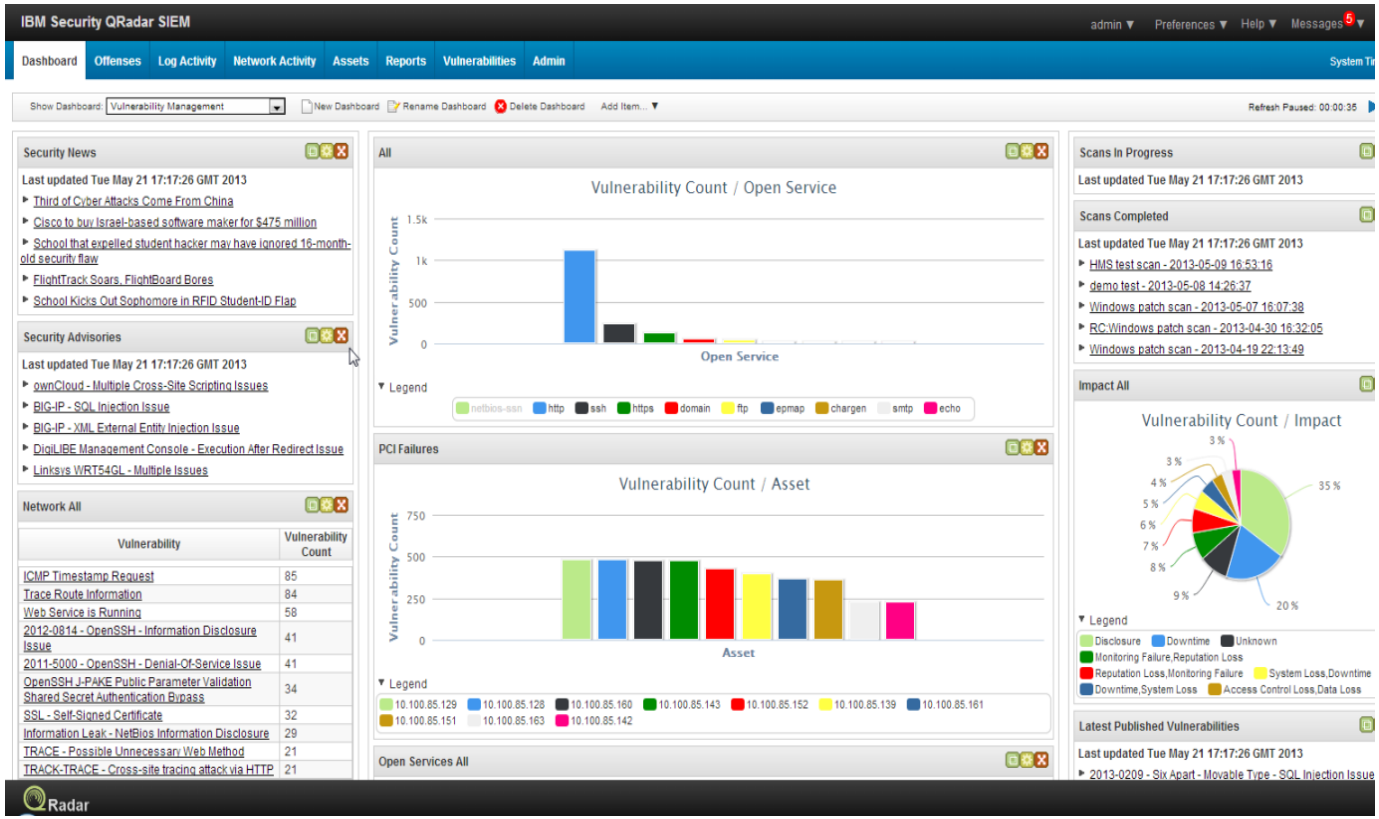
Whitepaper: Get actionable insight with security intelligence for mainframes

IBM X-Force Threat Intelligence Quarterly Report

IBM provides the following Security Intelligence solutions to help your organization obtain a combined view of both your Enterprise and Distributed Environments

IBM Security QRadar SIEM consolidates log source event data from thousands of devices including mainframes, servers, networking devices, databases, endpoints and applications distributed throughout a network. It performs immediate normalization and correlation activities on raw data to distinguish real threats from false positives. IBM Security QRadar SIEM can also correlate system vulnerabilities with event and network data, helping to prioritize security incidents.

IBM Security zSecure Adapters for QRadar SIEM collects, formats and sends enriched mainframe System Management Facility (SMF) audit records to IBM Security QRadar SIEM. As a result, IBM Security zSecure Adapters for QRadar SIEM helps you extend protection against advanced threats and integrate mainframe security with enterprise-wide security intelligence.



Explore, Learn, and Implement

IBM's comprehensive Security solutions for System z empower you to easily meet your enterprise's objectives by enabling you to:

- Rely on policy based user authentication, access control, audit and management
- Protect critical data with high-speed encryption and centralized key management
- Secure with real time-monitoring, alerting, blocking of suspicious behavior / transactions
- Mask sensitive data during test and development
- Create a secure foundation for enterprise cloud and consolidated workloads
- Strengthen compliance and audit responsiveness to evolving regulations
- Reduce operation risk with early detection of application and network vulnerabilities

Now that you have seen how the System z infrastructure is the ideal platform for securing your enterprise cloud, mobile and big data analytics plans, what's next?

To get started, please check out the additional resources provided in each section of this e-guide, and go online to see what webcasts and seminars IBM provides. As IBM solutions continue to improve and evolve, visit the System z Security website for all the latest information, including new white papers, videos, demos, etc.

Of course, the fastest course of action is to call your IBM software representative today so they can analyze your unique needs and recommend the best mix of products and services to get you up to speed the fastest.

Resources

Webpage: IBM Security Software for System z

Webpage: System z Enterprise Security

White Paper: Consolidated security management for mainframe clouds

Case Study: Nationwide: Banking on the mainframe to drive unprecedented transformation and growth

Analyst White Paper: Secure the Enterprise with Confidence

Video: zSecure for Superior Mainframe Security