IBM Software
Thought Leadership White Paper

September 2010

Consolidating security across platforms with IBM System z

Protect your business-critical information by leveraging the mainframe as a security hub

Contents

Executive summary

Organizations today are facing formidable IT security challenges, and the increasingly complex infrastructures and diverse platforms found in today's computer centers aren't making things any easier. These unprecedented security challenges stem from the need to protect critical assets in distributed, collaborative, multiplatform environments. These heterogeneous environments are the inevitable product of unbridled data and application growth—not just in the number of workloads and assets that need to be secured, but also in the varieties of workloads and assets that are involved. Add to this the fact that 73 percent of CFOs want to drive integration of information across the enterprise—integration that presents security challenges of its own.[1]

More and more organizations have already discovered the advantages of centralizing security on the mainframe to meet these challenges, because resilience and security have long been hallmarks of mainframe computing. But how can they extend the security that is enabled by the mainframe to so many different software and hardware platforms?

IBM is responding with both hardware and software solutions to address the need for security that spans the entire IT infrastructure. IBM System z® mainframes have long supported a multitude of operating system platforms. Today, System z takes multiplatform support above and beyond expectations with the IBM zEnterprise™ System, the first truly integrated hardware platform for heterogeneous computing. IBM Tivoli® and IBM Information Management solutions for security combine with System z hardware and software to provide comprehensive, centralized security capabilities for organizations with distributed, multiplatform IT environments.

Managing security in multiplatform environments

Highly distributed computing, extensive online collaboration (both internal and external), explosive data growth and heterogeneous IT environments have combined to make information security more critical and more complex than ever for organizations today. Security threats have intensified and become more difficult to manage as a result of more open and diverse IT infrastructures. The imperative now is to find effective ways to meet today's security requirements and comply with security-driven regulatory demands—while staying focused on core business activities and keeping costs under control.

Organizations that rely on mainframes to run critical applications should seriously consider using the mainframe as an enterprise security hub. The same characteristics that make the mainframe ideal for running critical applications—robust hardware, reliable operating systems and dependable security—can be used to enable it as an enterprise security hub. Mainframes can be used to centralize more operations with shared data. This facilitates more secure collaboration and also makes it much easier and more efficient to manage security on multiple disparate platforms across the IT infrastructure.

System z mainframes in particular feature a security-rich design that can help reduce the risk of data breaches in today's distributed, collaborative, multiplatform environments.

Security is built into every level of the System z structure, including the processor, operating system, communications, storage and applications. It contains security features that can specifically help organizations comply with security-related regulatory requirements including:

- Identity and access management provided by Resource Access Control Facility (RACF®).
- Hardware and software encryption along with key lifecycle management.
- Data storage protection, at rest or in motion.
- Communication security capabilities.
- Secure virtualization facilities.
- Extensive logging of security-relevant events.

In addition to delivering an exceptionally strong security foundation, System z mainframes benefit from the IBM Security Solutions "Secure by Design" initiative for building security into the IT infrastructure from the ground up. This initiative helps organizations incorporate security into the fabric of the services they deliver, making security intrinsic to business processes and daily operations. A significant example of the native System z "Secure by Design" attribute is the system integrity statement that covers the mainframe operating system.[2]

IBM zEnterprise System offers the first truly integrated hardware platform for heterogeneous computing.

IBM Tivoli and IBM Information Management security offerings for System z support the thinking behind "Secure by Design" by providing organizations with solutions for user administration and management, resource protection, and audit and compliance reporting. Organizations that deploy System z as a hub for enterprise security—and combine it with Tivoli and Information Management offerings—can benefit from strong, centralized security in distributed, multiplatform environments.

System z today: Spanning multiple platforms

System z is a natural choice for organizations of all kinds that look to mainframe solutions for performance, reliability and security to support their critical applications. But while many organizations may seek the same qualities in system platforms, they all have different functional requirements. For this reason, System z supports a multitude of platforms that address these varied and specific requirements.

- IBM z/OS® is a highly secure, scalable, high-performance enterprise operating system for organizations seeking a platform on which to build and deploy Internet and Java™-enabled applications requiring secure centralized data.
- IBM z/OS UNIX® System Services is a tightly integrated element of z/OS that brings together UNIX and z/OS environments.
- Linux® on System z is ideal for organizations that want to combine the performance, reliability and security advantages of IBM mainframe hardware with the flexibility, application portfolio and open standards of Linux operating systems.
- IBM z/VM® is a hypervisor that helps organizations that use virtualization extend the business value of mainframe technology across the enterprise. It allows them to run hundreds to thousands of Linux servers on a single mainframe.
- IBM z/TPF is a high-performance operating system specifically designed to provide high availability for organizations with high-demand, high-volume, real-time transaction processing needs.

Just as organizations may choose a platform other than z/OS to meet specific requirements, they may also choose to deploy other hardware—such as distributed servers—in addition to mainframes to meet particular workload needs. The result is a heterogeneous environment in which business processes span multiple software and hardware platforms, creating significant management and security challenges. To address this issue, IBM zEnterprise System provides a truly integrated hardware platform for heterogeneous computing. It brings together multiple platforms such as IBM POWER® and IBM x86 blades—under a single consolidated hardware view, centralizing management and security across mainframe and distributed systems. zEnterprise simply enables workloads to be deployed on the technologies that are best suited for them—without requiring those workloads and technologies to be managed separately.

Establishing System z as a hub for enterprise security

Whether an organization is running multiple platforms through logical partitions on System z, or consolidating multiple platforms on zEnterprise, IBM Tivoli and IBM Information Management solutions can be used in concert with System z to allow the mainframe to serve as an enterprise security hub. These solutions provide organizations with a centralized point for security operations across multiple platforms, providing the visibility into and control over organization-wide security that is necessary for minimizing risk in heterogeneous environments. These solutions address the following capabilities, which we will further explore in this paper:

- User administration and management
- Resource protection
- Audit and compliance reporting

Making System z the enterprise security hub also enables organizations to take advantage of mainframe extensibility and scalability by consolidating disparate systems to improve efficiencies, standardize operations (especially after a merger or acquisition) and streamline security management across all computing resources.

Using System z as an enterprise security hub for securing resources and business services across the enterprise allows organizations to:

- Improve service by leveraging the most secure platform in the enterprise.
- Reduce costs and complexity through systems consolidation and automated compliance tasks.
- Manage risk by facilitating compliance with industry regulations and internal security policies.
- Avoid the significant costs associated with a security breach due to business loss, damaged image and consumer reparations.

This paper describes specific Tivoli and Information Management security solutions on System z to address user administration and management, resource protection, and audit and compliance reporting, and shows how these solutions can help organizations realize the benefits described above.

Addressing user administration and management

User administration and management are especially challenging in multiplatform IT infrastructures. Users are accessing information in a multitude of environments, including applications, mainframes, service oriented architectures and the web. User identity information is contained in different repositories across platforms. Successfully meeting the challenge requires solutions that are designed from the ground up to deliver security-rich, policy-based user administration and access management capabilities across the IT infrastructure.

IBM Tivoli Identity Manager for z/OS

By using roles and self-service requests to automate user administration, IBM Tivoli Identity Manager simplifies administration of user access to resources, reduces the cost of administration, and lessens the risk of error and policy deviation inherent in manual processes. The solution combines role management and user provisioning to deliver access rights to users based on the roles assigned to them. In addition, a hierarchical role structure streamlines administration and provides complete visibility into user access to resources across the IT infrastructure. Web self-service for managing roles, accounts and passwords further simplifies administration and reduces administrative costs by enabling users to perform these tasks themselves. Self-service requests can be configured to define which attributes are allowed for self-service and which require approval. This is ideal for a high-volume, large-scale web client environment where the exact identity of the user is not known.

IBM Tivoli Federated Identity Manager for z/OS

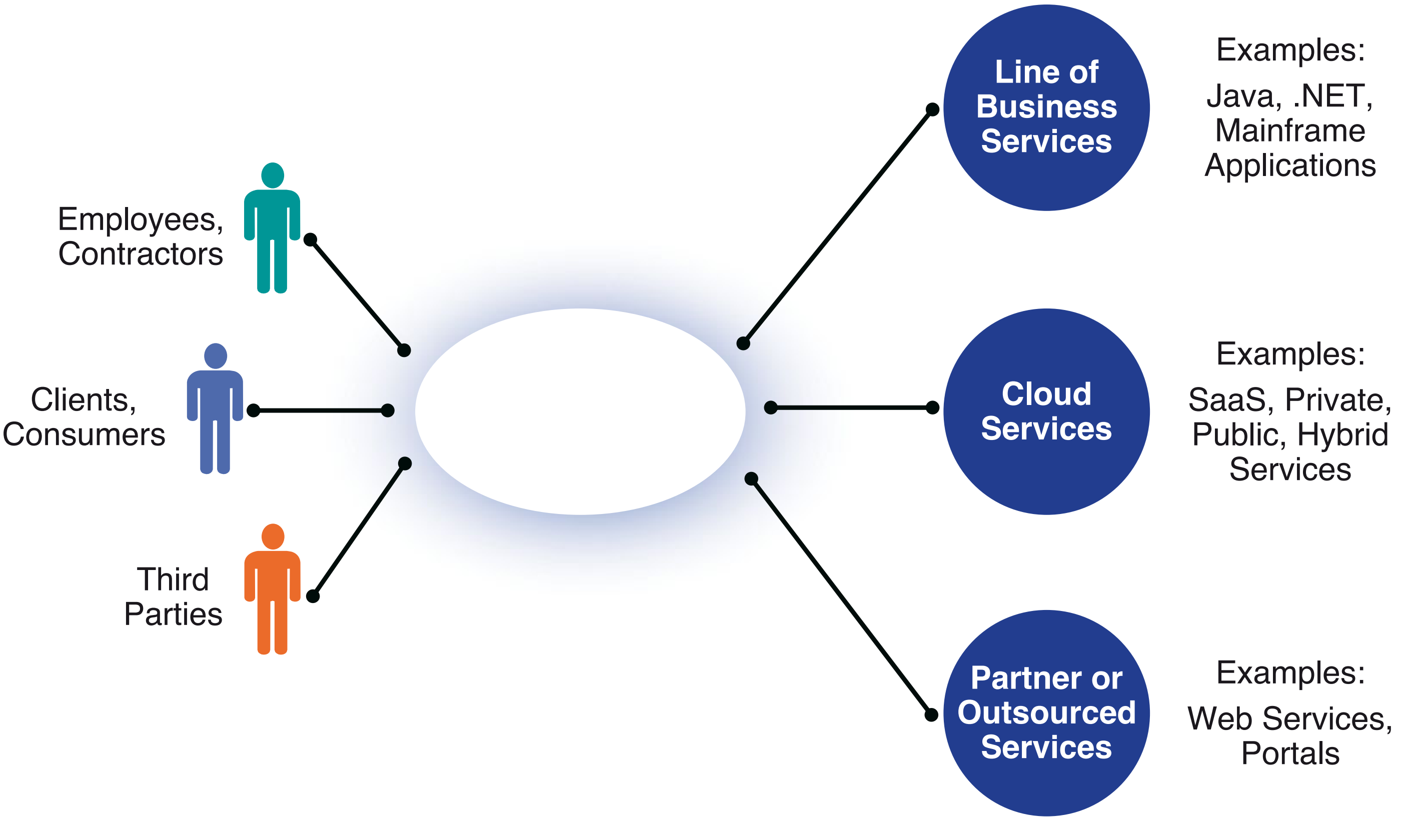
When the exchange of information and collaboration across organizational boundaries are essential, the task of managing user identities becomes even more challenging. End users must be able to access resources beyond their own organizations, and the identity information required for that is contained in repositories in different security domains. Tivoli Federated Identity Manager provides the federated single sign-on (SSO) and user access management techniques that are necessary for integration across organizational boundaries. The solution provides an identity trust management framework that enables an organization to know who is connecting to resources and what credentials they are using—without having to manage each user individually. This is ideal for protecting assets where users are connected to critical resources from access points over the Internet or a less trusted environment.

IBM Security zSecure suite

IBM Resource Access Control Facility (RACF) is the security standard for mainframes running IBM z/OS, and IBM Security zSecure Admin is designed to simplify RACF administration. The solution automates mainframe user security administration tasks such as defining and granting access to users and user groups, adding user IDs and groups, and setting and resetting passwords. Controls can limit special-user capabilities to prevent violations associated with privileged-user abuse. IBM Security zSecure suite also includes a variety of products to help ensure that everyday administration capabilities are available across a variety of operating platforms and environments. These solutions include:

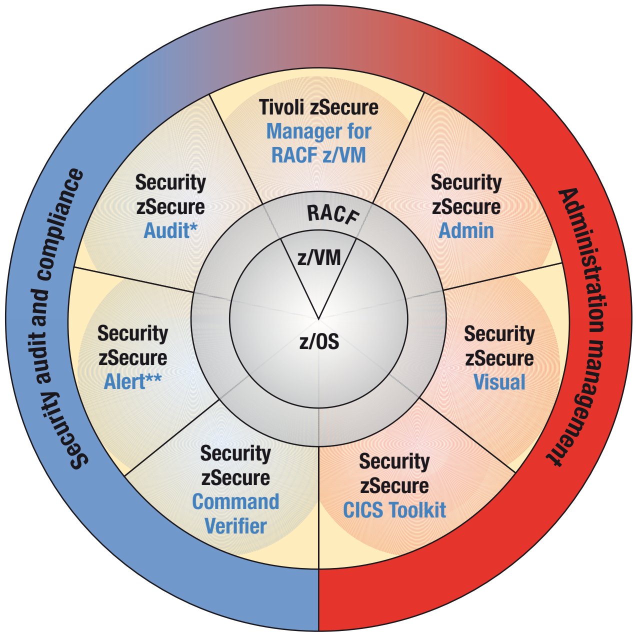
- IBM Security zSecure CICS® Toolkit, for environments where business information must be accessed from the IBM Customer Information Control System.
- IBM Tivoli zSecure Manager for RACF z/VM, which extends administration capabilities to mainframes running as guests on IBM z/VM.

To further enhance RACF administration, IBM Security zSecure Visual provides a direct, easy-to-use, point-and-click graphical interface that enables less skilled administrators to perform many administrative functions without the need for extensive RACF and TSO knowledge.



IBM Tivoli Federated Identity Manager for z/OS enables organizations to expand and simplify collaboration securely.

IBM Security zSecure suite


Security audit and compliance
Administration management
Tivoli zSecure Manager for RACF z/VM
Security zSecure Audit*
Security zSecure Admin
Security zSecure Alert**
Security zSecure Visual
Security zSecure Command Verifier
Security zSecure CICS Toolkit
RACF
z/VM
z/OS

*Also available for ACF2™ and Top Secret®

**Also available for ACF2

IBM Security zSecure solutions help ensure that everyday administration capabilities are available across a variety of operating platforms and environments.

IBM Tivoli Directory solutions

IBM Tivoli Directory Server and IBM Tivoli Directory Integrator work together to provide a powerful directory infrastructure for security initiatives in heterogeneous environments.

- Tivoli Directory Server provides the identity data foundation for integrated identity management and plays a key role in building the identity data infrastructure for identity management services.
- Tivoli Directory Integrator synchronizes data across multiple repositories to enable consistent data for organizations working with more than one identity data resource. This capability is ideal for environments where identity may be defined differently across multiple platforms.

Case in point: Casas Bahia

The largest retail chain in Latin America, Casas Bahia recently expanded its reach further across Brazil by implementing a new online store based on IBM System z. The company has used System z for years for its retail operations, enabling them to launch the new online store without the need for new hardware—and to take advantage of the multiplatform security capabilities of System z. A destination for more than 250,000 visitors a day and a major new revenue stream for Casas Bahia, the online store is based on IBM System z10® Enterprise Class servers in a dynamic infrastructure running two operating system platforms: z/OS and Linux on z/VM.

The company credits the IBM System z platform for giving it a clear technological advantage in the marketplace, which translates into a better shopping experience for customers.

Addressing resource protection

Protecting access to applications and other resources is doubly challenging when those resources are associated with a multitude of web and non-web platforms. Access management in multiplatform environments requires solutions that enable control over access from a centralized point and that make it easy to address access issues in an integrated fashion.

IBM Tivoli Access Manager family

As organizations externalize applications and other resources as services, protecting access to those resources becomes increasingly difficult. The IBM Tivoli Access Manager family of solutions enables controls for centralized security management in increasingly distributed, multiplatform environments. Tivoli Access Manager family includes Tivoli Federated Identity Manager as well as:

- IBM Tivoli Access Manager for e-business, which enables robust security for web and other applications by providing centralized authentication and authorization of user access.
- IBM Tivoli Security Policy Manager, which allows organizations to centralize security policy management to enforce access control across applications, databases, portals and business services.

IBM Security zSecure Admin and IBM Security zSecure Audit

IBM Security zSecure Admin plays an important role in helping organizations to quickly identify security problems in RACF, so that they can be addressed before they become significant threats. IBM Security zSecure Admin provides capabilities to protect resources such as datasets, databases, tapes, minidisks, and more. The solution's extensive monitoring capabilities also help minimize vulnerabilities associated with privileged users.

IBM Security zSecure Admin integrates seamlessly with IBM Security zSecure Audit, which allows organizations using RACF, CA ACF2 and CA Top Secret Security to measure and verify the effectiveness of their mainframe security and security policies. Unlike offerings that only report on a copy of a database, IBM Security zSecure Audit provides access to live security data on mainframes. It also helps improve overall service by generating reports to help identify RACF configuration problems.

IBM Tivoli Key Lifecycle Manager

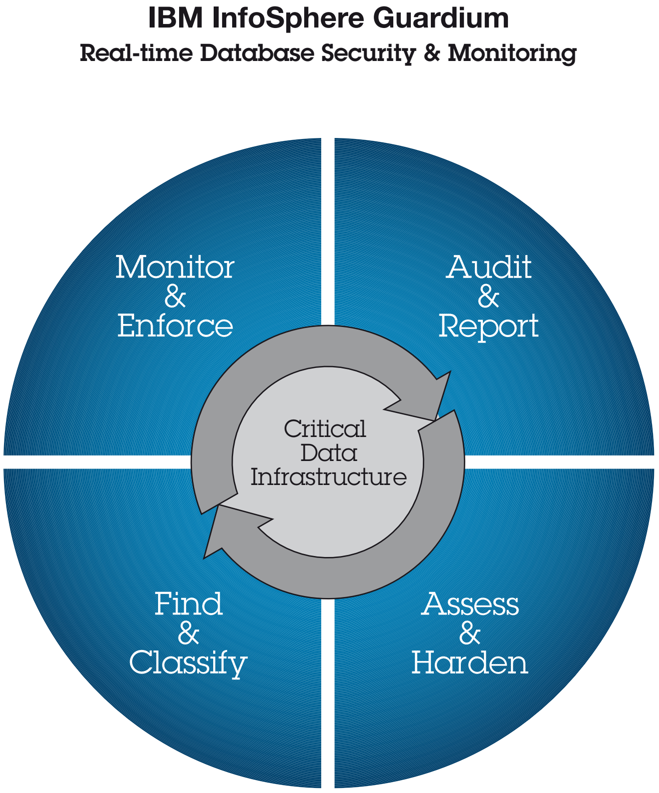
Another Tivoli solution that addresses mainframe security in multiplatform environments is IBM Tivoli Key Lifecycle Manager, which centralizes and strengthens encryption key management, simplifying key management while enhancing data security. Tivoli Key Lifecycle Manager works with the native z/OS encryption services and key stores, as well as with tape and disk storage encryption hardware, providing audit logs for security event compliance monitoring. With support for Key Management Interoperability Protocol (KMIP), it extends encryption key management to both IBM and non-IBM devices.

IBM InfoSphere Guardium

IBM InfoSphere™ Guardium is a real-time database security and compliance solution that monitors all access to sensitive data across all major database platforms and applications, without impacting performance or requiring changes to databases or applications. The solution prevents unauthorized or suspicious activities by privileged insiders, potential hackers and end users of enterprise applications such as SAP, Oracle EBS and PeopleSoft. At the same time, it reduces costs by automating the entire compliance auditing process in heterogeneous environments. The solution can be used independently for the mainframe environment only, or integrated with other InfoSphere Guardium components across the enterprise to provide a secure, centralized audit repository and management point.

IBM InfoSphere Optim Data Masking Solution with InfoSphere Discovery

InfoSphere Optim™ Data Masking Solution addresses data security in non-production environments—i.e., testing, development and training environments. Because these environments often incorporate data from live production systems, including confidential data, they are among the most vulnerable areas of the IT infrastructure. Data masking is a



IBM InfoSphere Guardium simplifies the process of guarding sensitive information across multiple platforms, managing the entire database security and compliance lifecycle enterprise-wide through a single solution.

best practice for protecting sensitive data in non-production settings, but it can be tough to discover sensitive data and to execute data masking in heterogeneous IT environments that contain multiple applications, databases and platforms. IBM InfoSphere Discovery provides comprehensive capabilities for discovering sensitive data across a multitude of data stores in non-production environments. IBM InfoSphere Optim Data Masking Solution can then de-identify this sensitive data with realistic but fictional values while retaining referential integrity throughout. This makes it possible to identify sensitive data and protect privacy while still providing the data required for development, testing and training.

Case in point: Large retailer

One of the US's largest retailers, with physical stores from coast to coast along with online shopping, recently implemented a suite of IBM InfoSphere Optim solutions to protect sensitive customer information and financial data in its application testing environment. The challenge was to implement data masking in the three different databases that the company uses to support different business applications—CA Datacom, IBM DB2® for z/OS and Microsoft® SQL Server. The company's IT team implemented InfoSphere Optim Data Masking Solution to mask data from all three sources, protecting privacy in the application testing environment, supporting industry regulations, and enabling the company to avoid the risk of a data breach.

Addressing audit and compliance reporting

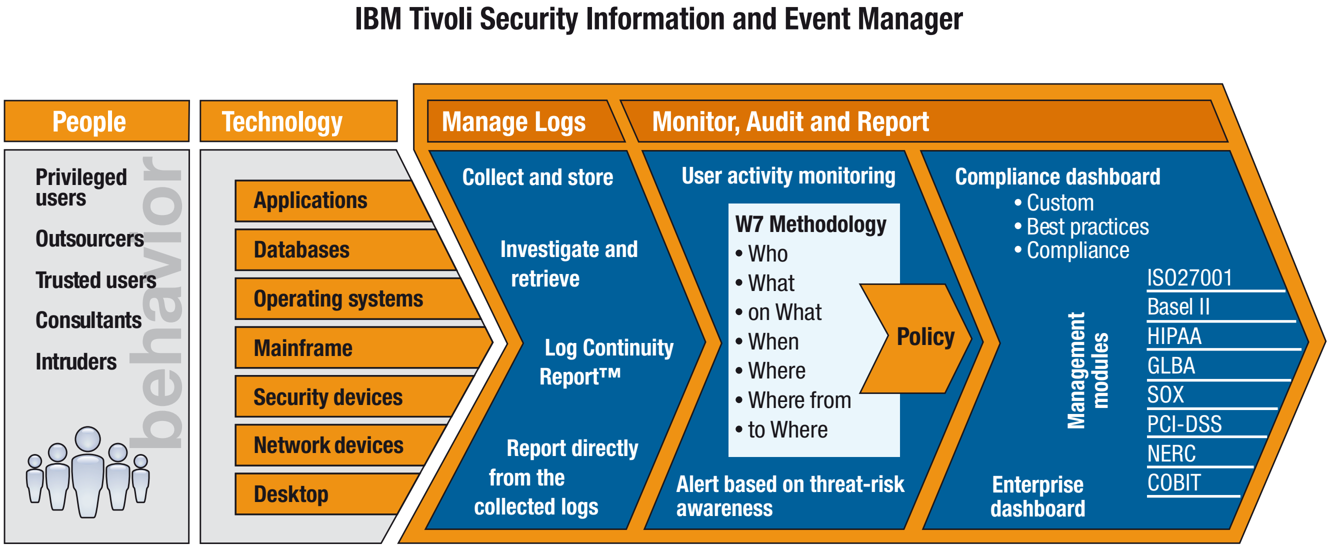
As regulations grow in number and complexity, and IT environments become increasingly heterogeneous, proving compliance can seem a nearly insurmountable challenge. Providing all the required information to show compliance with internal policies and external regulations demands audit and compliance reporting solutions that can effectively detect and extract relevant information from a multitude of sources.

IBM Security zSecure suite

The IBM Security zSecure suite of products provides a wide range of audit and compliance capabilities. For example, the compliance components of IBM Security zSecure Audit provide capabilities for extended monitoring of status changes in z/OS and RACF as well as reporting on security events for other software products such as IBM WebSphere® Application Server, IBM DFSMSrmm (Removable Media Manger), IBM Tivoli OMEGAMON®, IBM CICS, and Tivoli Key Lifecycle Manager.

Other IBM Security zSecure solutions with audit and compliance reporting capabilities include:

- IBM Security zSecure Command Verifier, which protects against unauthorized mainframe security changes that can threaten compliance or increase security vulnerability.
- IBM Security zSecure Alert, which monitors data for misuse, detects configuration mistakes that could threaten security, and issues critical alerts to audit and compliance solutions.
- IBM Tivoli zSecure Manager for RACF z/VM, which automates z/VM security management tasks, creates comprehensive audit trails and generates customized audit reports.



Tivoli Security Information and Event Manager provides centralized, comprehensive capabilities to quickly detect and report on security incidents throughout the IT infrastructure.

IBM Tivoli Security Information and Event Manager

Tivoli Security Information and Event Manager provides centralized, comprehensive capabilities to quickly detect and report on security incidents throughout the IT infrastructure—including mainframe incidents—minimizing their potential effect on secure operations. In addition, it helps organizations address the challenge of demonstrating regulatory compliance by efficiently capturing, storing, retrieving and reporting from native logs to fully support event investigation. It also offers regulation-specific Compliance Management Modules, available as add-on tools that help organizations address a multitude of regulations and standards including Sarbanes-Oxley, ISO, PCI DSS, COBIT and industry-specific regulations such as GLBA, HIPAA, FISMA, BASEL II, and NERC-CIP.

Tivoli Security Information and Event Manager can help customers demonstrate to auditors their overall level of compliance across the enterprise. In addition to integration with z/OS RACF, Top Secret and ACF2, the solution also collects data and reports on compliance across network and security devices, server operating systems, applications and databases. Tivoli Security Information and Event Manager integrates with nearly 300 different IT infrastructure devices, applications, servers and databases.

Case in point: Allied Irish Banks (AIB)

Like other banking organizations around the world, Dublin-based AIB—Ireland's largest bank—has seen competition and regulation increase dramatically in the last several years. To survive and thrive in these circumstances, the organization embarked on a complete transformation of its retail banking system, implementing the new system on the IBM System z platform. Part of the transformation involved replacing its existing mainframe security system with an IBM Service Management solution incorporating IBM RACF and IBM Security zSecure software. AIB now relies on IBM Security zSecure to meet the demands of security, audit and regulatory requirements—which eases the burden of audits on security administrators, freeing them to focus their time on improving security quality.

Summary

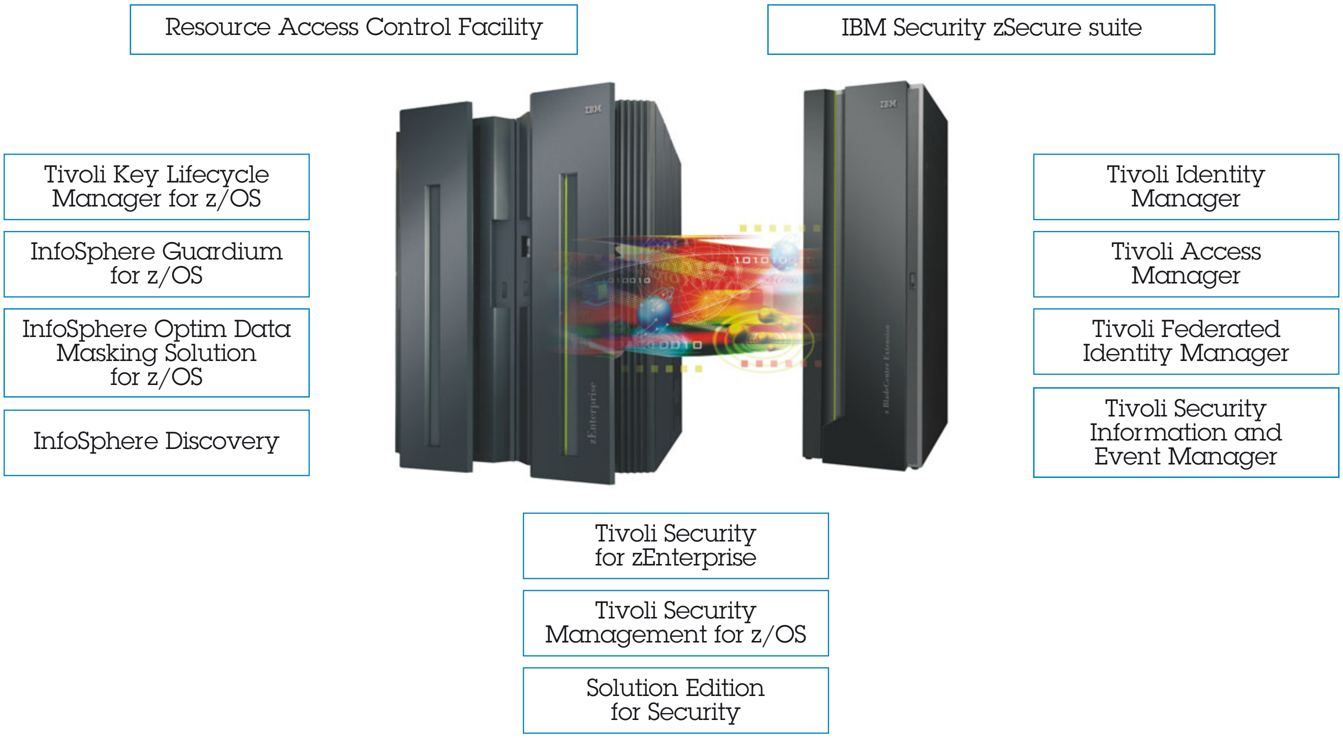
Many organizations today rely on System z mainframe technology for the performance, reliability and security they need to support critical applications, even when they rely on distributed computing for other workloads. Those same qualities make System z the ideal technology on which to centralize security management. Using IBM Tivoli and IBM Information Management solutions, they can leverage System z as an enterprise security hub. This makes it possible to extend consistent security, with secure data sharing across disparate hardware and software platforms throughout the entire IT infrastructure, gaining the benefits of:

- Minimized complexity due to simplified security administration.
- Reduced costs due to security automation, improved productivity and threat mitigation.
- Enhanced compliance with integrated audit reporting and compliance management.

For more information

To learn how IBM Tivoli and IBM Information Management solutions can help you fully realize the potential for managing security across multiple platforms on System z, contact your IBM sales representative or visit: **ibm.com**/security

Leverage the Mainframe as the Enterprise Security Hub



Resource Access Control Facility

IBM Security zSecure suite

Tivoli Key Lifecycle Manager for z/OS

InfoSphere Guardium for z/OS

InfoSphere Optim Data Masking Solution for z/OS

InfoSphere Discovery

Tivoli Identity Manager

Tivoli Access Manager

Tivoli Federated Identity Manager

Tivoli Security Information and Event Manager

Tivoli Security for zEnterprise

Tivoli Security Management for z/OS

Solution Edition for Security

With IBM Tivoli and IBM Information Management software solutions, System z is the ideal technology for your enterprise security hub.

About Tivoli software from IBM

Tivoli software from IBM helps organizations efficiently and effectively manage IT resources, tasks and processes to meet ever-shifting business requirements and deliver flexible and responsive IT service management, while helping to reduce cost. The Tivoli portfolio spans software for security, compliance, storage, performance, availability, configuration, operations and IT lifecycle management, and is backed by world-class IBM services, support and research. For more information on Tivoli software from IBM, visit: **ibm.com**/tivoli

Additionally, financing solutions from IBM Global Financing can enable effective cash management, protection from technology obsolescence, improved total cost of ownership and return on investment. Also, our Global Asset Recovery Services help address environmental concerns with new, more energy-efficient solutions. For more information on IBM Global Financing, visit: **ibm.com**/financing

The information provided in this document is distributed "as is" without any warranty, either express or implied. IBM expressly disclaims any warranties of merchantability, fitness for a particular purpose or non-infringement. IBM products are warranted according to the terms and conditions of the agreements (e.g. IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided.

The customer is responsible for ensuring compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law or regulation.

[1] "The New Value Integrator: Insights from the Global Chief Financial Officer Study," IBM Institute for Business Value, March 2010. **ibm.com**/services/us/cfo/cfostudy2010

[2] IBM z/OS Statement of Integrity. **ibm.com**/systems/z/os/zos/features/racf/zos_integrity_statement.html

© Copyright IBM Corporation 2010

IBM Corporation Software Group
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
September 2010
All Rights Reserved

IBM, the IBM logo, ibm.com, System z, Tivoli and zEnterprise are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at **ibm.com**/legal/copytrade.shtml

Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft is a trademark of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product and service names may be trademarks or service marks of others.

References in this publication to IBM products and services do not imply that IBM intends to make them available in all countries in which IBM operates.

No part of this document may be reproduced or transmitted in any form without written permission from IBM Corporation.

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

♻ Please Recycle