

Centralizing security on the mainframe

Improve security and compliance by choosing the right solution



Today's IT environments are often collections of distributed, collaborative, multiplatform environments. That's both the good news, and the bad news. It's good news because those qualities have made many organizations more agile, effective and competitive—by allowing them to match resources to needs without being limited by a single IT platform. But at the same time, these qualities can make critical assets within an organization much more difficult to identify and protect.

Heterogeneous IT environments today represent the inevitable consequence of growth—not just data and application growth, but business growth. In the wake of this unbridled growth, there are more assets and workloads to be secured than ever before. And as organizations have grown in the number of customers or constituents they serve, and the number of products and services they deliver to those users, they have implemented more and more IT resources of varying kinds over time to meet changing business needs. The result: a larger, more complex, dispersed IT environment that's harder to secure because it comprises so many different technologies.

This level of complexity gives rise to numerous security problems. They include time-consuming, inefficient security administration stemming from the need to manage security across so many different resources, as well as difficulties in consistently applying access control policies and processes across the enterprise. Organizations must also comply with regulatory and audit requirements that combine growing numbers of regulations with extremely diverse operating environments, as well as demonstrate compliance by providing audit data from a multitude of sources.

To address these problems, more and more organizations are discovering the advantages of centralizing security—and using the mainframe to do it. This approach makes sense, because resilience and security are hallmarks of mainframe computing, especially when it comes to the industry-leading IBM System z® platform. The question is how to extend the security that is

enabled by the mainframe to many different hardware and software platforms. The answer is to seek mainframe security solutions that are specifically designed to both enhance and simplify security, with:

- Extensive integration of security operations across platforms.
- Widespread use of automation to reduce administrative demands on IT staff.
- Consolidated views of security and compliance activities throughout the enterprise.
- Broad, deep audit and reporting to demonstrate regulatory compliance.

Getting started with mainframe security

This buyer's guide outlines the features and capabilities of an effective mainframe security strategy, addressing the following key areas:

1. Security management
2. Identity and access management
3. Monitor, audit and alert
4. Audit and compliance reporting

For each category, this guide provides a checklist of features to help you evaluate whether or not a particular vendor's solutions address each of these functional areas effectively. You will also find tips to help you select a vendor that has the solutions, support, financial stability and other qualities to address the full range of your mainframe security requirements.

1. Security management

Managing security in multiplatform environments can be a complex and costly proposition, considering the magnitude of the task. Centralizing security operations on the mainframe is one key to getting control over it; the other is making security management more effective and efficient. This begins with ensuring that the security management tools you use are

focused on maintaining the integrity of security operations. The next step is speeding and simplifying those operations at every possible level.

To maintain security integrity, you need a security management solution that automatically takes steps to enforce policy compliance, establish security baselines, and identify and analyze threats for remediation. Look for a solution that allows you to exercise fine-grained control over security commands to prevent security errors from occurring or security intrusions from causing damage. And look for capabilities that allow the solution to readily close off avenues of attack such as unused security definitions and privileged-user and trusted-user abuses by maintaining a security system that is current.

In the interest of efficiency, you want to be sure that your security management solution is set up to handle most routine tasks automatically. This will not only reduce costs and complexity, but also improve user productivity—and allow administrators

to spend more of their valuable time on strategic work that enhances the organization's overall security posture, rather than on day-to-day security administration. It's simply a smarter way to allocate and apply skilled security resources in the IT organization.

One other issue that may arise as you transition to centralized, mainframe-based security for your organization relates to staff limitations. For example, you may not have staff with sufficient mainframe operations expertise to manage security effectively. Or you may have non-mainframe users who need to issue security commands to the mainframe from within their own application environments. The security management solution you select should be designed to accommodate such limitations. Look for a solution that allows tasks to be performed at the department level, where staff members need not have access to all security commands but might benefit from simpler departmental administration, or might benefit from ready access from their current online environment. Attention to these kinds of operational details will help ensure successful centralization of security operations on the mainframe.

Security management

Look for a solution that:	IBM	Other vendor
Automates and simplifies routine administrative tasks so that they can be performed with minimal training and little administrative effort.	✓	
Identifies and analyzes IBM Resource Access Control Facility (RACF®) problems for remediation to minimize the threat of a security breach or compliance exposure and to lower administrative costs.	✓	
Displays data from the active (live) RACF database, including recent changes by other administrators, to allow administrators to immediately verify the effect of changes.	✓	
Uses actual database usage information to analyze profiles and perform database cleanup, improving the integrity of system security (by eliminating unused or obsolete profiles and permits) and minimizing the manual effort required by compliance processes.	✓	
Reports on actual usage of profiles and authorizations and relates that information to current profiles and authorizations defined in the current RACF database, enabling a better understanding of how profiles and authorizations are used in production.	✓	

Security management

Look for a solution that:	IBM	Other vendor
Simplifies the management of multiple RACF databases, allowing you to send and execute the same commands to multiple systems, keeping security synchronized.	✓	
Creates a mirrored copy of the RACF database offline so that administrators can verify configuration changes before implementing them, reducing the risk of introducing errors into the production database.	✓	
Combines audit and administrative capabilities to provide end-to-end monitoring and remediation of security and security life cycle management for governance and compliance purposes.	✓	
Stores non-security/non-RACF information (such as custom fields like telephone numbers, accounting codes and email addresses) in the RACF database to reduce organizational costs, improve compliance reporting and consolidate user information.	✓	
Supports policy definitions to provide mandatory and default values by automating the process of ensuring that appropriate values are used, so that preventative controls can be enabled to improve security.	✓	
Prevents non-compliant administrative command execution by automatically verifying command keywords against specified policies as soon as a command is issued, reducing the risk of a security breach due to either error or malicious intent.	✓	
Stores changes to RACF database profiles to make it easy to detect profile changes without labor-intensive searches, log files investigation or guesswork.	✓	
Can be independently installed on all systems on which you want to enforce policies, eliminating the need to design, code and maintain custom-coded routines to handle parsing of keywords along with installation exit code.	✓	
Allows selective distribution of command access to grant users granular access to only the specific commands they need to do their jobs, reducing the risk of accidental or malicious breaches by privileged users.	✓	
Allows decentralization of RACF administration so that routine tasks can be performed at the department level using an intuitive easy UI, rather than at the corporate level, optimizing use of administrator time by freeing skilled security administrators to focus on higher-value activities.	✓	
Permits customization of commands so that administrators view only the commands they are allowed to perform, reducing the risk of incorrect commands, insider breaches, and abuse of privilege.	✓	
Enables decentralized administration over your standard network, eliminating the cost and effort of rolling out extra TSO/ISPF terminals.	✓	
Allows customization of screens to show only pre-selected options and fields to decentralized administrators, minimizing security exposures associated with providing too much information.	✓	

Security management

Look for a solution that:	IBM	Other vendor
Provides easy access to the active (live) RACF database so that help-desk staff can view accurate, current information about users, groups and resource profiles.	✓	
Makes it possible to add new users by simply cloning existing user templates and entering new names, reducing the risk of assigning incorrect authorizations.	✓	
Offers robust, non-intrusive capabilities to help simplify the process of managing mainframe security by reducing complex management tasks to one-step actions that can be performed without extensive RACF knowledge.	✓	
Enables RACF administration from a user-friendly interface with IBM CICS® application servers so that CICS users can issue security commands directly without having to leave the familiar CICS environment and without having to write custom CICS applications.	✓	
Provides a web-enablement CICS-RACF API so that web applications can use RACF functions for security administration, authentication and access control.	✓	
Facilitates access checks for more than 2,000 resources so that you can improve application performance by replacing internal application security with RACF security.	✓	
Centralizes (in the RACF database) security for legacy and internally developed CICS applications to enhance application security and auditability.	✓	
Enables you to empower managers to view, sort and annotate audit reports, and combine multiple reports for automatic distribution—saving time and providing focused reports.	✓	
Analyzes SMF log files (from live SMF data sets or from extracted SMF data on tape or disk) to create a comprehensive audit trail.	✓	
Supports both IBM z/OS® and IBM z/VM® operating systems.	✓	

2. Identity and access management

Successful access management is an essential aspect of mainframe security. But keeping access to resources secure is a challenge in heterogeneous environments, where resources are likely to be associated with many different web and non-web platforms. Managing access in such an environment requires the ability to control access from a centralized point and to address access issues in an integrated way. Accordingly, the identity and access management capabilities that are part of your mainframe security efforts should allow you to manage and enforce access

control policies across every application, data source, operating system and organizational boundary. They should be standards-based and should easily integrate with other systems.

An effective identity and access management solution also needs to be designed to efficiently manage users and user information throughout the entire user life cycle—so that IT staff doesn't end up spending an inordinate amount of time managing permissions and policies (not to mention user roles, identities and

access rights) on a painstaking case-by-case basis. A centralized, automated approach will enable you to manage tasks associated with user roles, identities, credentials and access permissions using consistent, standardized processes instead of slow, error-prone manual methods.

Look for an identity and access management solution that focuses on ease of use, too. For IT users, it should have an intuitive, easy-to-customize user interface; a variety of configuration wizards and templates; and out-of-the-box integration with authentication applications. For business users such as managers and auditors, it should describe access rights in business-friendly language that's easily understood by nontechnical personnel.

Identity and access management

Look for a solution that:	IBM	Other vendor
Provides integrated role-based access control (RBAC), rule/attribute-based access control (ABAC) and request-based provisioning options.	✓	
Tightly integrates user provisioning with role management, separation of duties and recertification with open interfaces for integration with continuous business controls systems.	✓	
Supports tools to build user provisioning workflows using both simple wizard-based navigation and a drag-and-drop GUI for more advanced business processes—all from a common web interface.	✓	
Reconciles accounts automatically and in an on-demand way to rapidly and reliably discover invalid “orphaned” accounts and unnecessary entitlements, and to initiate either automatic or manual remediation processes.	✓	
Offers an intuitive, customizable administration GUI with point-and-click capabilities that make it easy to create new user GUI views and to track status.	✓	
Provides a complete and integrated federation and trust management solution that includes a general-purpose security token service for common standards-based identity propagation within a web services/SOA environment.	✓	
Provides standards-based development for extension of the security token service via Eclipse-based plug-ins.	✓	
Includes robust directory and directory integration and synchronization products at no additional charge.	✓	
Provides standards-based (XACML) entitlements management (roles, rules, attributes) for data security and fine-grained access control.	✓	
Provides SOA security policy management (message protection policies support).	✓	

Identity and access management

Look for a solution that:	IBM	Other vendor
Integrates widely with identity servers, applications, middleware, operating systems and platforms including enterprise service bus.	✓	
Supports multiple standards for cross-site authentication, including Security Assurance Markup Language (SAML), Liberty Alliance, OpenID and Web Services Federation Language (WS-Federation) protocols.	✓	
Supports Java™ EE and Microsoft® .NET application and web services integration using existing application identity (e.g. LTPA, Kerberos and SAML) protocols.	✓	
Supports mainframe application and web services integration including using RACF PassTicket protocol.	✓	
Integrates with IBM WebSphere® DataPower® for secured web-services support in the demilitarized zone.	✓	
Provides business-to-consumer (B2C) self-service interfaces for user enrollments, user validation, account updates, and password resets and synchronization.	✓	
Utilizes a web authorization approach that offers high performance and scales to user implementations in the tens of millions as well as to hundreds of applications.	✓	
Offers a flexible Java web-based architecture that can protect resources using either a hardened reverse proxy, or a plug-in module to an existing web server. (In certain cases, a dedicated proxy can offer a higher level of security.)	✓	
Provides session management services that allow for the immediate termination of all active sessions for a malicious user.	✓	
Offers a post office (anti-spam) feature that aggregates like emails and user work items.	✓	
Supports B2C federation with emerging user-centric identities including OpenID and Information Card Profile using identity selectors such as Microsoft CardSpace or Higgins identity framework.	✓	
Includes an enterprise single sign-on (ESSO) solution that is distinguished in the marketplace by its advanced capabilities to work with many different kinds of applications, integration with strong authentication, flexible approach to session management, and ability to log and audit end-user activities.	✓	

Identity and access management

Look for a solution that:	IBM	Other vendor
Provides an ESSO solution that integrates with web, desktop, teletype and mainframe applications, as well as many client device platforms such as Microsoft Windows® CE and Windows XPe to accommodate the broadest possible range of applications.	✓	
Offers a wide choice of authentication factors, including user IDs and passwords, USB smart tokens, building access badges, active RFID, biometrics and an open authentication devices interface for easy integration of third-party devices.	✓	
Enables account usage auditing by tracking application logins/logouts.	✓	
Integrates with provisioning to provide automated check-out/check-in of shared and privileged identities for privileged identity management.	✓	
Allows administrators to apply a meaningful description to a fine-grained resource, categorize it for quick reference and search, assign an owner to it, define unique approval and recertification workflows, and provide detailed reports on these resources.	✓	
Allows enterprise architects to model security policies and create security policy templates for consistent use across the organization.	✓	
Allows application owners to create data entitlements using application roles and attributes without requiring knowledge of the IT operations environment.	✓	
Has a workflow that seamlessly integrates with SAP and Oracle ERP, and fine-grained separation-of-duties checking with flexible exception-handling methods.	✓	
Provides a centralized management GUI for control and making modifications, eliminating the need to manually update each individual adapter to reflect changes in authentication and authorization methodology.	✓	
Incorporates business rules into access control decisions and evaluates these rules dynamically at run time.	✓	
Sets an access policy that automatically detects and remediates both intentional and inadvertent non-compliance events in real time.	✓	
Scales to tens of millions of users for authentication and authorization; also scales to meet the needs of intranet, extranet and Internet user populations.	✓	
Enables multiple policy enforcement points in a web-services infrastructure, for DataPower, WebSphere and other web services resources.	✓	
Enables multiple policy enforcement points for application and data sources such as Microsoft SharePoint, WebSphere Portal, WebSphere Application Server, IBM FileNet®, IBM DB2®, and other application and data resources.	✓	

3. Monitor, audit and alert

To keep resources secure, you need mainframe security that continually monitors for access breaches and other security events, and then alerts the proper administrative staff of any anomalies that are detected. This is especially true in environments where resources are likely to be associated with a variety of platforms and types of users.

Real-time monitoring is essential to effective audit-and-alert capabilities. You need to be able to conduct live data analysis, for up-to-the-minute accuracy in detecting problems and alerting administrators to them. And you need this capability not just within the mainframe operating system, but in databases and other subsystems that are also affected when you are using the mainframe as a security hub. You also need audit-and-alert capabilities that are integrated to enterprise audit, compliance and monitoring solutions, to enable appropriate responses to

security events. End-to-end monitoring and remediation are essential to effectively dealing with potential exposures in centralized-security scenarios.

The solutions you choose should place a high priority on monitoring and alerts related to areas that you have designated as particularly sensitive. If your organization is a public company, for example, you want to be able to monitor critical system settings that are specifically required by SOX, for example. Or if you are at high risk for insider threats to security, the solution you choose should include features such as privileged user monitoring to help control that risk.

Finally, audit and alert capabilities should be easy to use and manage—automatically detecting system changes to minimize risk, issuing timely alerts with no special action required on the part of administrators, and providing a single view of security events to make it easier to monitor events across the organization.

Monitor, audit and alert

Look for a solution that:	IBM	Other vendor
Allows live data access and analysis for up-to-the-minute audit accuracy, including ranking and highlighting current security concerns and audit priorities.	✓	
Provides live analysis beyond z/OS and RACF to detect problems in UNIX® subsystem security definitions and to display critical activity in DB2 systems on the mainframe.	✓	
Checks for and enforces program signatures by identifying programs that are expected to have a valid signature and verifying whether the signature is present, to aid in compliance with PCI Data Security Standard.	✓	
Delivers optional custom reports daily via email when specific events occur or when there is a possible security breach.	✓	
Uses flexible and customized reporting and alert language to make it easy to create new reports (installation-specific, RACF and SMF) without the need for consulting assistance.	✓	
Includes DBCS support for audit reports, with built-in support for translating reports and menus for NLS support.	✓	
Includes NLS support for translating report titles, column headers, constants, and selection and scan values to support DBCS characters in search strings and formatted output.	✓	

Monitor, audit and alert

Look for a solution that:	IBM	Other vendor
Analyzes SMF log files to create a comprehensive audit trail in the event of incidents such as policy exceptions (for example, logging in after work hours).	✓	
Leverages external files from existing databases and corporate applications (such as a personnel database) and presents the data alongside technical data to make reports highly usable.	✓	
Uses the RACF database to analyze profiles and get fast answers to questions such as “Who has access to this data set?” Allows you to map your own events into the W7 model (who, what, when, on what, where, where from, and where to) and filter out events on the mainframe side without editing the data set.	✓	
Detects system changes (such as whether a member was added, deleted or changed) to minimize security risks.	✓	
Helps define a baseline for RACF security parameters, detects profiles and parameters that differ from the baseline, and monitors and measures baseline changes to simplify implementation of security auditing.	✓	
Includes a powerful system integrity analysis feature to detect and analyze system integrity breaches and other irregularities and rank them according to degree of exposure to help determine appropriate corrective action.	✓	
Provides integrated, end-to-end monitoring and remediation capabilities to quickly diagnose and address failures or exposures so that administrators can move quickly to remediate them.	✓	
Links seamlessly to enterprise audit and compliance solutions to include mainframe security information in company-wide reports.	✓	
Provides a threat knowledge base with parameters from active configurations to help isolate relevant attack threats and patterns, detect multiple types of attacks and configuration threats (including those external to the event log) and enable swift corrective action.	✓	
Offers multiplatform monitoring capabilities to identify resources that need protection across multiple platforms, to help maintain data integrity and stay ahead of potential security policy violations.	✓	
Automatically sends timely security alerts to enterprise audit, compliance and monitoring solutions, as well as to network and enterprise consoles, to enable rapid response to security events and to easily include mainframe data in company-wide audit and compliance reports.	✓	
Continuously monitors critical system settings per SOX and JSOX audit requirements to detect changes for which there are no event triggers.	✓	
Enables alerts to be configured to notify administrative and management personnel when changes are detected—even those for which there are no event triggers.	✓	

Monitor, audit and alert

Look for a solution that:	IBM	Other vendor
Allows support users, consultants and other authorized users to create custom alert messages by modifying existing alert messages or creating new ones based on installation-defined requirements.	✓	
Centralizes and automates log management to reduce the time and effort required to collect, organize, archive, investigate and retrieve logs for analysis.	✓	
Provides insider threat analysis and privileged user monitoring to reduce the risk of security events originating from inside the organization.	✓	
Provides a single, streamlined view of security events from thousands of network and security devices, hosts, applications and other sources to minimize the effort required to monitor events across the organization.	✓	
Provides extensive audit capabilities including the ability to audit UNIX security definitions on the mainframe, DB2 auditable security events, CICS security events, Linux® for System z events, and auditable security events from IBM Tivoli® Key Lifecycle Manager, WebSphere Application Server, and Tivoli OMEGAMON®. It also provides auditing of the communications server network configuration for TCP/IP and provides PDS(E) member-level auditing.	✓	

4. Audit and compliance reporting

The ability to produce reports that prove compliance is crucial for organizations dealing with multiple complex regulations, especially in increasingly heterogeneous environments. To effectively provide all the information required to demonstrate compliance with internal security policies and external regulations, you need reporting that can deliver on several levels.

First, you need a mainframe security solution that can quickly and effectively sort through data from multiple sources throughout the organization to detect compliance-relevant information about security events. The solution you choose must also have the flexibility to report on regulation-specific concerns, so that no matter what regulations or standards apply to your organization or industry, you have the capability to produce reports that are specific to them.

Because there are so many regulations reflecting varying degrees of complexity, you also need a solution that focuses on simplifying the process of reporting. Reporting templates covering the

major regulations are extremely helpful, as are out-of-the-box best practice reports, which can narrow down the thousands of potentially relevant individual reports that are out there to a few dozen. Templates and models like these can save significant amounts of time in report preparation.

Once reports are generated, it should be easy to get them out to the people who need them, and easy for those people to put them to use. Most of those who need audit and compliance reports are nontechnical stakeholders, including business owners, regulators, external auditors and internal audit staff. Look for the ability to translate highly technical compliance data into reports that are written in plain language that can be easily understood by these users. Make sure you have a variety of output formats available to you to easily accommodate different user preferences (such as HTML, PDF, .xls, etc.) You will also benefit from built-in capabilities for distributing reports to those who need them and for automating the report scheduling and distribution process.

Audit and compliance reporting

Look for a solution that:	IBM	Other vendor
Enables you to easily sort and browse a multitude of events and analyze them from different vectors.	✓	
Translates data into detailed, easy-to-understand reports that can be used by regulators, external and corporate auditors, and other nontechnical personnel.	✓	
Includes the user's real name as known by the directory or security system to make the report more readable.	✓	
Provides compliance management modules with regulation-specific reporting capabilities (including default templates) covering major regulations and standards including ISO 27001, SOX, PCI-DSS, HIPAA, GLBA, Basel II, FISMA, COBIT, NERC-CIP and others.	✓	
Includes out-of-the-box parameterized best-practice audit reports that reduce hundreds or thousands of individual reports to about 50 parameterized reports.	✓	
Enables distribution of reports to business owners and stakeholders for review, approval, comment and action.	✓	
Uses a patent-pending strong normalization model.	✓	
Includes a flexible custom report writer that is optimized to the normalization model, allowing you to create your own compliance and audit reports without needing to understand or write SQL.	✓	
Automates report distribution to business owners as part of the overall compliance and business process.	✓	
Offers a common system for scheduling, distributing, viewing and customizing reports.	✓	
Provides compliance-specific policy templates that represent the controls within a regulation.	✓	
Provides compliance-specific reports that allow you to monitor compliance posture against specific controls.	✓	
Provides compliance reports that are designed, created and based on standards (versus renaming operational reports).	✓	
Provides a compliance dashboard that shows the current compliance posture in the vocabulary of existing regulations or policies for easy understanding.	✓	
Provides trending information at the dashboard level to indicate the trend for compliance posture and to help ensure that goals are being achieved.	✓	
Provides drill-down from the high-level compliance dashboard through to the underlying detail events for further investigation.	✓	

Audit and compliance reporting

Look for a solution that:	IBM	Other vendor
Provides reporting at the raw log level using a simple query mechanism for forensic-type investigations.	✓	
Includes a full-featured reporting engine with scheduled reporting.	✓	
Facilitates communication of threat levels and security activities through out-of-the-box standard and customizable report templates, driven from an automated report scheduler.	✓	
Provides a wide variety of report output formats, including HTML, PDF, CSV and .xls exporting of all graphs and charts.	✓	
Offers privileged user monitoring, reporting and auditing on databases, applications, servers and mainframes.	✓	

Selecting the right vendor

The provider you choose should be able to support the full breadth of your security requirements. Ideally, you will also want a provider who can support you throughout the process of implementing your solution. Before you select a provider, make sure to ask these questions:

Is your vendor focused on true end-to-end enterprise security needs?

With a vendor who is focused too narrowly on a point solution that addresses only a particular environment, you can run into the “islands of security” problem. While this document focuses on mainframe security, that is just one key part of the challenge. Choose a vendor who can address the big picture, including:

- Mainframe security
- Application security
- Information and data security
- Threat protection
- Managed services
- Service management
- Multiple platforms and applications

Are your vendor’s products tightly integrated for seamless functionality?

The more integrated the solution, the less work you have to do to streamline functions. Make sure the vendor can respond quickly to changes in operating systems and System z infrastructure, taking immediate advantage of platform enhancements.

Does your vendor’s technology support your business goals?

Look for vendors whose solutions are designed to facilitate your business objectives. Do their solutions promote efficiencies, reduce business service deployment time, reduce costs, enhance compliance and speed time to market?

Does your vendor provide rapid time to value?

A cost-effective solution includes a number of key features designed to provide easy configuration, integration and maintenance, even in a complex enterprise environment.

What type of global presence and support does your vendor have?

If your organization has international offices, you should look for a vendor with a global presence and proven international business experience. Make sure the vendor can support your offices abroad with their own local resources.

Is the solution supported by a mature organization with the expertise and bandwidth that can be relied on when you need it?

Your vendor should offer highly responsive and highly effective customer support. Find a vendor that has a proven support organization to help you maximize the value of your software investment.

Are the vendor's solutions consistently rated highly by the analyst community?

Look for solutions that are recognized through independent analysis and examination across multiple dimensions by leading analysts.

How sure are you of your vendor's stability and staying power in today's economy?

A big issue in today's economy is vendor stability and visibility. You should consider a vendor who has a long history in the industry, a solid, forward-looking strategy and the resources to withstand adverse economic conditions.

Can your vendor deliver products that are strategically designed and technically superior?

When comparing various security solutions, look for technical superiority—well-designed functionality, an intelligent architectural design and broad support for industry standards.

Address your mainframe security needs with IBM

When you evaluate mainframe security solutions to meet your goals, you will find that IBM offers not only a best-of-breed solution, but also exceptional breadth and integration across its security solutions. As organizations look for ways to extend the security that is enabled by the mainframe to many different software and hardware platforms, IBM is responding with security that spans the entire IT infrastructure. Today, IBM Tivoli and IBM Security solutions combine with System z hardware and software to provide comprehensive, centralized security capabilities for organizations with distributed, multiplatform IT environments.

The IBM Security zSecure suite consists of a variety of modular components that are designed to help you quickly and efficiently manage mainframe RACF databases. Specific security management components of the suite include:

- IBM Security zSecure Admin to simplify RACF administration.
- IBM Security CICS Toolkit, which enables users to issue RACF commands from CICS application servers.
- IBM Security zSecure Command Verifier, which enforces RACF policies and helps reduce security risks stemming from internal errors and non-compliant commands.
- IBM Security zSecure Visual, which provides a point-and-click interface to enable less skilled administrators to perform many administrative functions without the need for extensive RACF knowledge.
- IBM Tivoli zSecure Manager for RACF z/VM, which extends administration capabilities to mainframes running as guests on IBM z/VM.

Audit and alert components of the zSecure suite include IBM Security zSecure Audit and IBM Security zSecure Alert, which combine to detect and report mainframe security events and exposures. IBM Security zSecure Audit is an audit solution that provides live analysis of critical information on mainframes, highlights security concerns and ranks audit priorities based on the relative impact of the problems it detects. IBM Security zSecure Alert offers real-time mainframe threat detection, with alerts and automated commands to counter attacks and misconfigurations. Integration between these two solutions enables end-to-end monitoring and remediation to enable administrators to quickly diagnose mainframe security failures or exposures and take appropriate steps to remediate them.

IBM Tivoli Security Information and Event Management combines with IBM Security zSecure Audit to deliver extensive audit and compliance reporting capabilities. Tivoli Security Information and Event Management provides audit and compliance reports in plain language and includes a variety of reporting capabilities specific to different regulations, so that organizations can easily target their own specific compliance needs. The solution includes capabilities for custom report writing, automated report distribution and scheduling, and support for a wide variety of report output formats. IBM Security zSecure Audit offers the option of emailing reports daily when it detects a specific event or a possible security breach, based on live analysis of critical information in the mainframe environment. It uses an

extremely flexible reporting language to make it easy to create new reports, uses built-in support for translating reports and menus, and leverages external file support to enhance report usability.

IBM Tivoli identity and access solutions provide efficient, secure and compliant access to mainframe and other resources, helping organizations ensure that the right users have access to the right information in a timely manner. Tivoli Identity Manager provides a secure, policy-based solution for managing user roles, identities and access rights. Tivoli Access Manager solutions enable controls for centralized security management in increasingly distributed, multiplatform environments; they specifically provide centralized authentication, policy management and access control services for web resources, systems and hosted applications. Tivoli Federated Identity Manager provides the federated single sign-on and user access management techniques that are required for integration across organizational boundaries. This solution provides an identity trust framework that is ideal for protecting assets when users are connected to critical resources from a variety of access points, including over the Internet.

These offerings are all part of a larger IBM mainframe security software portfolio that also includes solutions for encryption key management, database protection, application testing, network security and more. IBM Security solutions can help you to consolidate security management on the mainframe and leverage its security strengths to establish it as your enterprise security hub.

For more information

To learn more about IBM mainframe security solutions, contact your IBM representative or IBM Business Partner, or visit:

ibm.com/security



© Copyright IBM Corporation 2010

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

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

IBM, the IBM logo, ibm.com, System z and Tivoli 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 and Windows are trademarks 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.

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 noninfringement. 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.



Please Recycle