White paper
September 2009

Tivoli® software

Realizing business value with mainframe security management

Contents

Executive summary

With a globally integrated market and highly complex, dynamic environments, crimes such as credit card fraud, data breaches, and privacy violations make security a top concern. Organizations need to stay competitive by protecting themselves against security threats while staying focused on their core business activities. IBM Tivoli® Security Management for z/OS® can help organizations secure their environments by leveraging their mainframe as the enterprise security hub. This IBM solution can help drive return on investment through:

- *Simplified security administration for increased productivity.*
- *Command verification for increased administration quality, accuracy, and policy enforcement.*
- *Automated audit reporting for increased speed and efficiency.*
- *Consistent compliance management across your financial and privacy-sensitive applications and data.*

Meeting today's security challenges

Organizations face a wide range of challenges to the security of their systems and confidentiality of their data. To take advantage of opportunities and mitigate risk in the global marketplace, organizations must more efficiently manage operational cost and complexity and deliver continuous, high-quality service. They must address internal and external security threats that have intensified as a result of innovation, emerging technologies, and exponential data growth. Additionally, organizations must enforce policies and demonstrate compliance with a growing number of regulations.

Highlights

Effective security must be applied within a business context and fused into the fabric of the business rather than added on as problems occur.

The increasing frequency and sophistication of computer crime, amplified by the accessibility and anonymity afforded by the Internet, make security a high priority for all entities. Advances in technology have enabled business innovation but have equally enabled cyber crime, leading to an array of new security threats and accelerating the need for even more sophisticated security. However, effective security must be applied within a business context and fused into the fabric of the business rather than added on as problems occur.

Meeting today's security challenges means that organizations must enable the secure delivery of service while cost-effectively managing threats and compliance. Organizations must be able to trust the identities of the people using their systems, including employees, customers and business partners. They must efficiently manage access according to organizational roles, and they must secure application services such as payroll, online banking, loan applications, retail sales, and inventories. In addition, organizations must protect data throughout their environments whether at rest or in transit. They must also expand and intensify monitoring solutions and activities to be able to detect threats and vulnerabilities and to prevent confidential data disclosure and system outages.

Addressing risks in the mainframe environment

Mainframe environments have a reputation for resilience, availability, and effective security due to their robust hardware, reliable operating systems, secure storage, and dependable security components. For this reason, many organizations choose to run critical applications on mainframes. The same characteristics can be used to enable the mainframe as an enterprise security hub.

Highlights

Mainframe security must address new risks, enable automated audit analysis and compliance reporting, significantly reduce cost and complexity, and provide a strong ROI.

Mainframes can facilitate secure collaboration by centralizing operations with shared data so that organizations can move away from decentralized, distributed security. Organizations can take advantage of mainframe extensibility and scalability by consolidating disparate systems to improve efficiencies, synthesize the operations of multiple organizations as a result of mergers and acquisitions, and standardize system management practices across all computing resources.

This use of the mainframe as a management and data hub has become increasingly common in enterprises and has proved to be an effective means of reducing power consumption as well as licensing and floor space requirements compared to distributed systems. Because mainframes are increasingly used in these new ways, mainframe security must address new risks, enable automated audit analysis and compliance reporting, significantly reduce cost and complexity, and provide a strong return on investment (ROI).

An organization's ROI is defined by tangible benefits that can translate directly to monetary gain. ROI can take the form of cost avoidance, such as through productivity improvements that extend labor capacity or reduce labor costs, or through scalability features that reduce capital expenses. ROI can be generated through higher systems availability and improved service levels, or through the ability to devote staff time to more strategic initiatives. You can also improve ROI by reducing security risks; avoiding fines, penalties and costs of security breaches and reducing the costs associated with audit and compliance efforts.

This paper shows how organizations can reduce costs and improve ROI by leveraging IBM Tivoli Security Management for z/OS and the superior security environment available on IBM System z® mainframes.

Highlights

IBM Tivoli Security Management for z/OS is a comprehensive mainframe security solution designed to enhance and accelerate security management with security administration, user management, and automated audit and compliance reporting for IBM z/OS RACF.

Comprehensive mainframe security from IBM

Due to the widespread use of mainframes as security or data hubs in addition to traditional mainframe roles, organizations of all sizes can gain competitive advantages by utilizing Tivoli Security Management for z/OS on System z mainframes. Tivoli Security Management for z/OS is a comprehensive mainframe security solution designed to enhance and accelerate security management for IBM z/OS® Resource Access Control Facility (RACF®) with:

- **Simplified security administration –** *provides an efficient, user-friendly layer to help you define and grant access to users and groups in real time.*
- **Command verification and policy enforcement –** *provides consistent policy enforcement and reduces security administration errors by intercepting and scanning security commands.*
- **Automated security auditing and reporting –** *provides comprehensive auditing that can detect and report security events and exposures on mainframes.*
- **Compliance reporting when running with RACF –** *collects and stores event records using automated log capabilities, provides dashboard summaries and enables retrieval of events for follow-up investigation.*

Driving ROI with Tivoli Security Management for z/OS

Each of the key functions within Tivoli Security Management for z/OS delivers distinct benefits that can help you reduce costs and improve ROI while managing risk and improving service on the mainframe.

Highlights

Tivoli Security Management for z/OS provides simplified security administration through a user-friendly layer that helps you define and grant access to users and groups in real time.

Tivoli Security Management for z/OS can provide significant savings by reducing administrative overhead for policy and security management tasks. It can also improve productivity by reducing wait times for users.

Achieve savings with simplified security administration

Tivoli Security Management for z/OS provides simplified security administration through a user-friendly layer that helps you define and grant access to users and groups in real time. This streamlined approach minimizes the time needed to provision new users, resulting in improved productivity for users and administrators alike. The security administration function can also help administrators determine which resources a user can access by displaying all authorizations, and by cross-referencing users and groups. Likewise, help-desk support for password resets and similar issues can be reduced by automating common functions.

Security rules from different databases can be merged efficiently to enable consolidation, and administrators can copy or move users, groups, resources, applications, or entire databases between systems. In addition, administrators can improve availability and reduce impacts to production databases by testing scenarios with offline RACF copies of production databases.

Other savings can be achieved using the simplified security administration function within Tivoli Security Management for z/OS. For example, users can view data in real time from the live RACF database to verify the effect of changes that have been made without having to wait for a refresh of the unloaded RACF database. Administrators can also compare multiple users that perform the same job functions and determine whether they have access to the same resources. This comparison enables administrators to ensure that users are given only the access they need to do their jobs.

Highlights

In addition, administrators can select any given dataset and view a list of users who have access to that data. As a result, they can quickly pinpoint mistakes before they become threats to security and compliance. The simplified security administration function also enables a highly efficient RACF database cleanup, which helps improve integrity—and therefore the value—of the data.

A university IT department gained these benefits and more from the simplified security administration function in Tivoli Security Management for z/OS. Their IT department consists of two system programmers and a help desk. The function of the help desk is to assist with password resets while the system programmers create new user IDs and define user access roles in the mainframe. The system programmers wanted to find a solution that could simplify the process of creating and maintaining student user IDs.

By implementing Tivoli Security Management for z/OS, the system programmers gained IT department labor savings with a user-friendly layer on top of RACF that enables simplified security administration. They can use it to define and grant access to users and user groups, set and reset user IDs and passwords, and display all authorizations or a cross-reference of a user ID or user group. As a result of the labor savings the IT department gained, the system programmers were able to spend more time working on more high-value objectives.

Reduce costly errors and security risks through command verification and policy enforcement

The Command Verifier within Tivoli Security Management for z/OS provides policy enforcement, protecting your system from both intentional and accidental non-compliant security actions.

The Command Verifier within Tivoli Security Management for z/OS provides policy enforcement by intercepting and scanning security commands to identify risky commands, generate alerts, create audit records, and optionally reject or modify the commands prior to execution. The Command Verifier can enforce security policies such as naming conventions, strong security defaults, installation access level standards, and controls on security administrator privileges and commands.

Highlights

The Command Verifier can limit administrative authority, prevent mistakes, and detect potential abuse of administrative privileges. As a result, it can protect your system from both intentional and accidental non-compliant security actions. It enables administrators to detect policy violations quickly so that you can correct the issues before they cause security exposures or enable abuse. Because the Command Verifier is automated, its features can provide significant compliance management savings through policy enforcement, error reduction, and minimizing rework. In addition, it offers security tool customization to meet your organization's specific needs without risky installation exit programs.

A government agency improved ROI by using the Command Verifier function in Tivoli Security Management for z/OS, mitigating risks that could have cost the agency millions of dollars.

A government agency improved ROI by using the Command Verifier function in Tivoli Security Management for z/OS. The agency needed a mainframe security solution that could facilitate compliance with security policy and regulatory audit requirements. By implementing Tivoli Security Management for z/OS, the agency gained the ability to take snapshots of the active RACF database as well as the ability to unload files to analyze the state of system security. They were also able to report on questionable system options and dangerous settings of privileged users, automate System Management Facility (SMF) analysis, detect library changes, and track changes in security settings.

Before implementing Tivoli Security Management for z/OS, the agency stated that its privileged users could cost the agency millions of dollars through unintentional configuration errors and careless security commands. Malicious users with authorized access could inflict even worse damage. By mitigating these risks, Tivoli Security Management for z/OS provided the agency with peace of mind as well as a significant return on investment.

Highlights

Tivoli Security Management for z/OS provides comprehensive auditing that can detect and report security events and exposures on mainframes, providing a comprehensive audit trail.

Reduce administrative overhead with automated security auditing and reporting

Tivoli Security Management for z/OS provides comprehensive auditing that can detect and report security events and exposures on mainframes. It works by analyzing SMF log files to create a comprehensive audit trail that includes RACF, IBM DB2®, and UNIX® (see Figure 1). As a result, administrators can simplify and automate the handling of mainframe events.

Customizable reports prioritize security concerns so that administrators can address the most important issues first. Administrators can choose to receive reports daily, only when specified events occur, or when security breaches occur. In addition, the audit components can automatically send mainframe security events to the compliance management component so that appropriate reports can be generated.

Automated policy management and intrusion management can significantly reduce administrative overhead. Automated audit analysis can save inspection time, and automated reporting and alerts can enable rapid response to help prevent threats and reduce downtime. And, because many issues can also be repaired automatically, IT administrators can spend time on higher priority projects. In addition, your organization can reduce audit preparation time thanks to automated processes that are aligned with audit requirements.

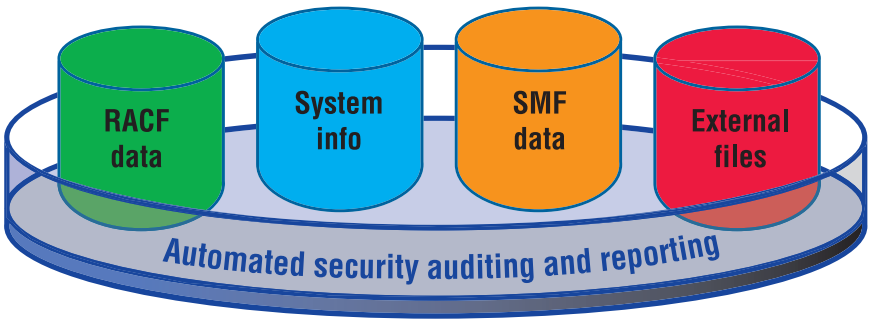

Figure 1: Tivoli Security Management for z/OS enables automated security auditing, reporting, and alerting of RACF, DB2, and UNIX.

Highlights

A large European financial services institution improved ROI by using the automated policy management and intrusion management function in Tivoli Security Management for z/OS. The organization wanted to replace its mainframe security software with a solution that would provide auditing, online alerting, and reporting while reducing the total cost of ownership for its mainframe platform. From the start, they were able to easily identify audit concerns with the added benefit of being able to fix them. The audit concerns identified are automatically prioritized, enabling effective security planning and prioritization of the required remediation work. Using the reporting language, they were able to generate a weekly management report for use by senior management and internal audit to track the number of audit concerns with a view of those numbers reducing week by week.

By implementing Tivoli Security Management for z/OS, the financial services organization was able to manage multiple RACF environments with only three specialized authority employees, despite the company's large size. With automated security auditing and reporting capabilities, the solution enabled the organization to address its security management issues as well as reduce the time and cost of managing employee access to information.

A major European-based insurance company realized dramatic administrative cost savings by implementing Tivoli Security Management for z/OS.

A major European-based insurance company has noted the following administration and auditing savings with Tivoli Security Management for z/OS:

- *Continuous automated auditing and corrective controls saves one month of administrative time per year in clean-up effort.*
- *Creating custom reports using the product's reporting language rather than using other programming languages saves one to two months of effort each year, including CPU savings.*
- *Bulk RACF command generation for administration also saves two administrative months per year.*
- *Self service, automated reporting to business units saves one month per year in report generation.*

Highlights

Tivoli Security Management for z/OS provides dashboards that display activities taking place throughout your environment.

Reduce audit time and costs with consistent compliance reporting

To help you manage security compliance efficiently, Tivoli Security Management for z/OS provides dashboards that display activities taking place throughout your environment. The compliance function within Tivoli Security Management for z/OS collects, stores, investigates, and retrieves logs using automated log capabilities from virtually any platform, enabling you to integrate mainframe logs into enterprise reports (see Figure 2).

Tivoli Security Management for z/OS, along with Tivoli Compliance Insight Manager, also features an advanced reporting engine that can create reports designed to document your level of compliance with Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry (PCI) Data Security Standards, Sarbanes-Oxley (SOX), the International Organization for Standardization (ISO), Basel II, and other regulations or standards. This cost-effective compliance monitoring and reporting function closes the security management loop (see Figure 3) and enables you to take corrective actions when you discover security exposures in your systems.

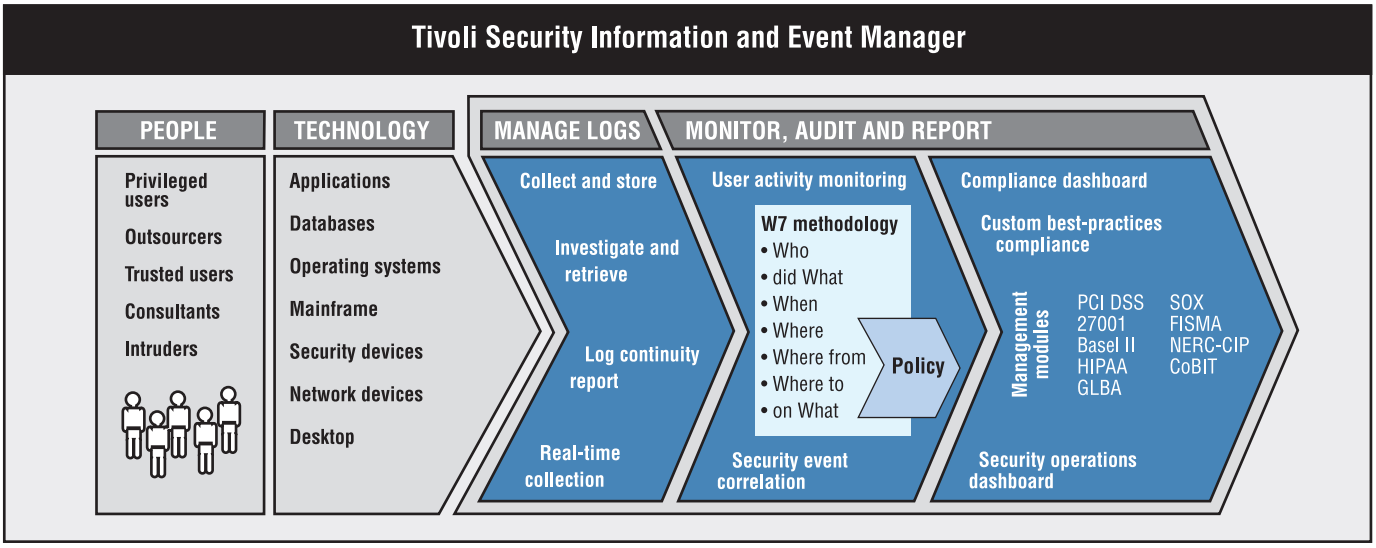

Figure 2: Tivoli Security Management for z/OS, along with Tivoli Compliance Insight Manager, provides dashboards to help you track compliance throughout your environment.

Figure 3: Tivoli Security Management for z/OS offers comprehensive compliance features to close the security loop.

The automated compliance reporting function within Tivoli Security Management for z/OS can provide significant cost avoidance by saving administration and audit overhead and reducing the time needed to provide proof of compliance. Automated log management enables universal collection, storage, and easy retrieval and investigation. Integrated forensic capabilities can help you analyze user behavior and reduce the risk of damage from internal and external threats.

Highlights

Aviva in the UK has successfully avoided significant labor costs associated with manual compliance reporting, and has reduced compliance-related errors.

Aviva was able to improve ROI by leveraging these automated compliance reporting features. A leading provider of life and pension products in Europe, the organization needed to facilitate compliance by implementing preventive, detective, and corrective controls in its IT environment. The organization implemented Tivoli security solutions to address the demands of its heterogeneous mainframe environment and facilitate compliance with tighter security policies, procedures, and regulations.

This solution supports robust auditing and compliance reporting that have improved the organization's compliance posture, enhanced efficiencies, and reduced errors. Aviva has also successfully avoided significant costs associated with the labor required for manual compliance reporting as well as the costs of noncompliance in the case of errors.

The mainframe as an enterprise security hub

With Tivoli Security Management for z/OS, IBM provides a solution that makes it possible for a mainframe to serve as an enterprise security hub for your organization. By leveraging additional components that address user provisioning, federated identity management, access management, encryption key management, audit reporting, and compliance management, Tivoli Security Management for z/OS can provide outstanding security for your entire environment (see Figure 4).

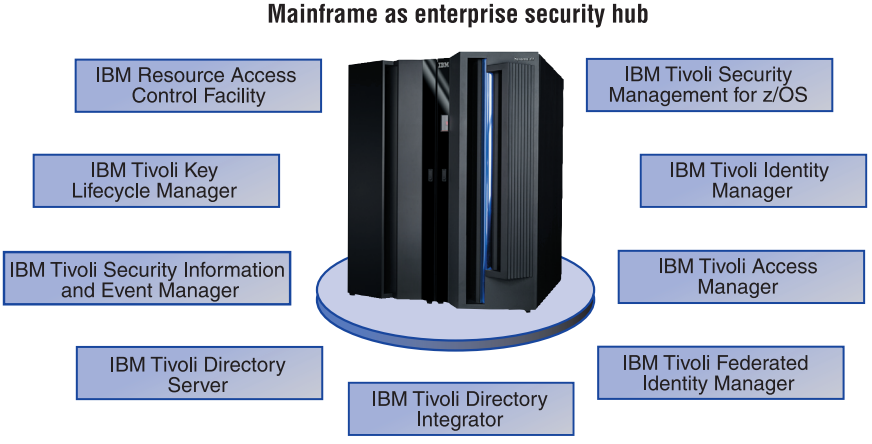

Figure 4: Tivoli Security Management for z/OS, working with other mainframe security products, enables you to use your mainframe as an enterprise security hub.

Highlights

Tivoli Security Management for z/OS offers closed-loop, integrated security information and event management with identity and access management.

IBM integrates security with service request management, which enables you to offload your service desk workload with self-service password management while still performing necessary incident tracking from the service desk.

Tivoli Security Management for z/OS also offers closed-loop, integrated security information and event management with identity and access management. As a result, you can take advantage of identity management across the information lifecycle. It also monitors users continually, along with their rights and what users have done with those rights, to quickly diagnose and remediate exposures.

By securing and auditing critical business services with Tivoli Security Management for z/OS, you can take advantage of a trusted and resilient platform. You can also:

- *Improve service by leveraging the most secure platform in the enterprise.*
- *Reduce costs through data center consolidation, embedded best practices, and automated compliance tasks.*
- *Manage risk by facilitating compliance with data disclosure and privacy regulations, as well as by improving audit preparedness.*
- *Avoid the significant and continually increasing costs associated with a security breach.*

Tivoli Security Management for z/OS in action

Allied Irish Banks replaced its mainframe security software with Tivoli security products to help the company stay ahead of security threats and to lower compliance costs.

Allied Irish Banks (AIB) was looking for ways to become more agile and cost-effective in serving its retail customers. AIB turned to IBM to replace its mainframe security system. The company needed a comprehensive security solution to help it enforce security as well as automate administration and auditing for multiple environments.

Highlights

AIB replaced its mainframe security software with IBM RACF and Tivoli security products to help it stay ahead of security threats and to lower compliance costs. AIB can now conduct proactive auditing of security configurations to detect and report on exposures and concerns. They can also monitor the AIB environment in real time for configuration errors, exposures, and intruders so that administrators can take immediate action. In addition, AIB can now access comprehensive and customizable reports to reduce audit overhead while addressing security and audit regulations such as Sarbanes-Oxley. They can automatically track changes to z/OS and RACF security to help determine if system resources are at risk.

User-friendly interfaces, interactive command generation, automated procedures, and online help enabled AIB security administrators to rapidly gain the z/OS and RACF security skills they needed. The new system has helped AIB address security concerns, enabling administrators to shift their focus from security administration to high-quality security management activities.

Building a business case for Tivoli Security Management for z/OS

IBM can provide a Business Value Assessment for your organization to rapidly assess the business value of implementing Tivoli Security Management for z/OS as your enterprise security solution.

IBM can provide a Business Value Assessment for your organization to rapidly assess the business value of implementing Tivoli Security Management for z/OS as your enterprise security solution. Through this valuable service, IBM can help you determine the strategy you need to enhance the security of your mainframe environment and provide projected improvements in ROI with the implementation of your new solution.

For more information

To learn more about Tivoli Security Management for z/OS, or to request a Business Value Assessment, contact your IBM representative or IBM Business Partner, or visit **ibm.com**/tivoli/solutions/security.

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

Produced in the United States of America
September 2009

TIW14038-USEN-00