

System z: Making great security even better

If your enterprise uses System z already, it's a safe bet that you're already aware of its legendary security. Being the only commercially available server with an EAL 5 rating is just one reason why so many of the world's top banks, retailers and other businesses that conduct high volumes of critical business transactions use System z. With features such as cryptographic co-processors and integrated Public Key Infrastructure (PKI) support, System z has arguably the best foundation in the world for building secure information systems.

However, strong fundamentals can lull even the most diligent and security-minded among us into a false sense of security. The ever-increasing complexity and reach of the information systems built upon System z's secure foundation, combined with the increasing number and complexity of the security threats we face, compels us to both take more comprehensive approaches, and implement more of them, as layers of defense-in-depth move from being a best practice to a minimum requirement.

Adopting an information protection approach, instead of focusing primarily on system security, enables your enterprise to be confident that the critical data processed and/or stored in the system is authentic, secure and available; not just inside your system, but everywhere that data ever resides, from test environments to backup storage facilities.



While regulatory compliance and the auditing capabilities that enable it are indispensable, the increasing frequency and high cost of data breaches reminds us that “compliant” doesn’t necessarily mean “secure.” Proactive solutions to information protection on System z minimize the risk that you will ever need to use your audit trails to analyze anything but a simulated breach. Read on and we’ll explain how.

Related Resources



[Audit and Protection on the IBM System z Platform](#)

Protect the data, not just the systems

IBM's approach to information governance in its InfoSphere® solutions provides an integrated data security and privacy approach delivered through these three guiding principles:

1. Understand and Define
2. Secure and Protect
3. Monitor and Audit

Without a comprehensive, global view of all the data your information systems handle, it's nearly impossible to effectively prioritize and direct your security efforts. InfoSphere® Discovery will identify and document what data you have, where it is located, its interdependencies, and how it's linked across systems. It automates the identification and definition of data relationships across complex, heterogeneous environments. InfoSphere® Discovery then generates comprehensive documentation for you to guide and inform your efforts to Secure & Protect, and then Monitor & Audit.

InfoSphere® Guardium Database Activity Monitor and Vulnerability Assessment complements InfoSphere® Discovery by crawling the network to find databases and identify sensitive information; it also address these last two principles by implementing continuous monitoring of databases, data warehouses, file shares and big data feeds such as Hadoop. It does this without the database/data source knowing (and so does not adversely impact the

performance of your systems) by using S-TAPs, which are light-weight, host-based probes that are able to monitor data traffic, including local and remote access by privileged users.

This real-time solution helps prevent unauthorized activities by insiders (whether regular or privileged users) or hackers, while monitoring end-users to identify potential fraud, all without any changes to the data infrastructure and applications, and without impacting performance. InfoSphere® Guardium DAM for System z comes with S-TAPs for DB2 for z/OS, IMS and VSAM, covering the most popular traditional databases used on System z and many other platforms. With its support for enterprise applications like SAP, Hadoop, and a Universal Feed feature that lets you monitor any custom system, InfoSphere® Guardium can protect an entire distributed enterprise at any scale, including big-data/cloud architectures.

Related Resources



[Three principles to Improve Data Security and Compliance](#)



[Understanding Holistic Database Security: 8 Steps to Successfully Securing Enterprise Data Sources](#)



[IBM InfoSphere Guardium](#)



Monitoring is not enough

With the cost of even modest-sized data breaches routinely amounting to millions of dollars, the ounce-of-prevention to pound-of-cure ratio was long ago surpassed. It's no longer acceptable merely to detect breaches and respond quickly; they must be prevented in real-time.

InfoSphere® Guardium probes (S-TAPs) monitor all database transactions, including those of privileged users, at the operating system kernel level without relying on database audit logs. The probes feed database transaction activity to hardened Collector appliances on the network, where they are compared to previously defined policies to detect violations. The system can respond with a variety of policy-based actions, and behavior patterns, including generating alerts and blocking suspicious transactions in real time.





InfoSphere Guardium can feed these deeper data activity insights to IT Security Information and Event Management (SIEM) tools, such as Tivoli® Security Operations Manager, for more accurate and effective security intelligence, allowing you to improve your security policies and posture over time as your enterprise's threat profile evolves. InfoSphere® Guardium also continually monitors and assesses database vulnerabilities, including the impact of configuration changes.

IBM's InfoSphere Optim Data Masking® solution enables proactive security in System z further, by protecting data privacy throughout the data lifecycle, from requirement through retirement. Able to

mask sensitive data in test and development environments, as well as on-demand from production databases, data warehouses and big data environments, Optim ensures that critical fields like credit card numbers are replaced with realistic looking substitutes in all use cases and contexts while maintaining the behavioral characteristics of the data such as built-in checksums.

Additionally, the InfoSphere Optim Test Data Management® solution can help reduce unnecessary exposure of data in test and development by automating the creation of right-sized test data sets while maintaining data relationships and referential integrity. Used in conjunction with the Data Masking solution it allows for reliable testing while ensuring confidential production data is not put at risk in development and test environments.

Related Resources

-  [InfoSphere Guardium solution for System z Demo: A Proactive Preventative Approach to Security Compliance and Audit](#)
-  [InfoSphere Optim Data Masking and Test Data Management solutions for System z](#)
-  [Solution Brief: IBM InfoSphere Optim Data Masking solution](#)
-  [Data management strategies to improve application testing in the z/OS environment](#)

Auditing needs automation



The list of compliance mandates from government (i.e. SOX & HIPAA), and commercial organizations (i.e. PCI-DSS) grows longer every year, but the resources to respond to them never seem to keep pace. Automation of audit trail generation and reporting, therefore, is no longer a luxury, but a necessity.

InfoSphere® Guardium Database Activity Monitor automates the generation of audit data with its ability to capture and examine data traffic (from virtually every enterprise source), including local and remote access by privileged users, in a secure, tamper-proof audit trail that supports separation of duties. The latter is particularly important to prevent scenarios such as privileged operators and accounts, for instance, from modifying native logs and audit reports.

Thus, InfoSphere® Guardium creates a single, centralized audit repository for enterprise-wide compliance reporting, performance optimization, investigations and forensics.

InfoSphere® Guardium's compliance workflow automation capabilities streamlines the entire compliance workflow process, helping to automate audit report generation, including distribution to key stakeholders, electronic sign-off and escalations. Workflow processes are completely user customizable; specific audit items can be individually routed and tracked through sign-off. The reporting features in InfoSphere Guardium even include pre-configured reports for SOX, PCI-DSS and data privacy.

Related Resources

 [IBM Security zSecure Products at Allied Irish Bank](#)

[Learn More](#)

Making it happen

InfoSphere® Discovery discovers what data you have and its interdependencies while automating the creation of a comprehensive global map of your enterprise data, from big picture down to individual fields. This map helps identify the scope of your implementation.

InfoSphere® Guardium's ability to easily scale from safeguarding a single data source to protecting thousands of data sources in data centers around the world has an additional advantage beyond the obvious benefit of protecting your entire enterprise regardless of size. This flexibility allows you to roll out improved System z security at a pace and scale that meets your needs, without the need for wholesale changes across the enterprise at once. Its proactive and preventative approach helps reduce risk by acting on a potential threat before it happens.

InfoSphere® Optim extends the holistic approach beyond your production systems, ensuring data protection and privacy in your development and test environments as well.

Contact your [IBM software representative](#) today to find out how these solutions can help make your System z implementations more secure than ever.



About this eGuide

This eGuide has been prepared by CBS Interactive on behalf of IBM. IBM and Intel have specified topic, title and key themes of this guide and may have contributed to and exercised editorial control over the content. This guide may only be quoted and reproduced by IBM in its entirety.