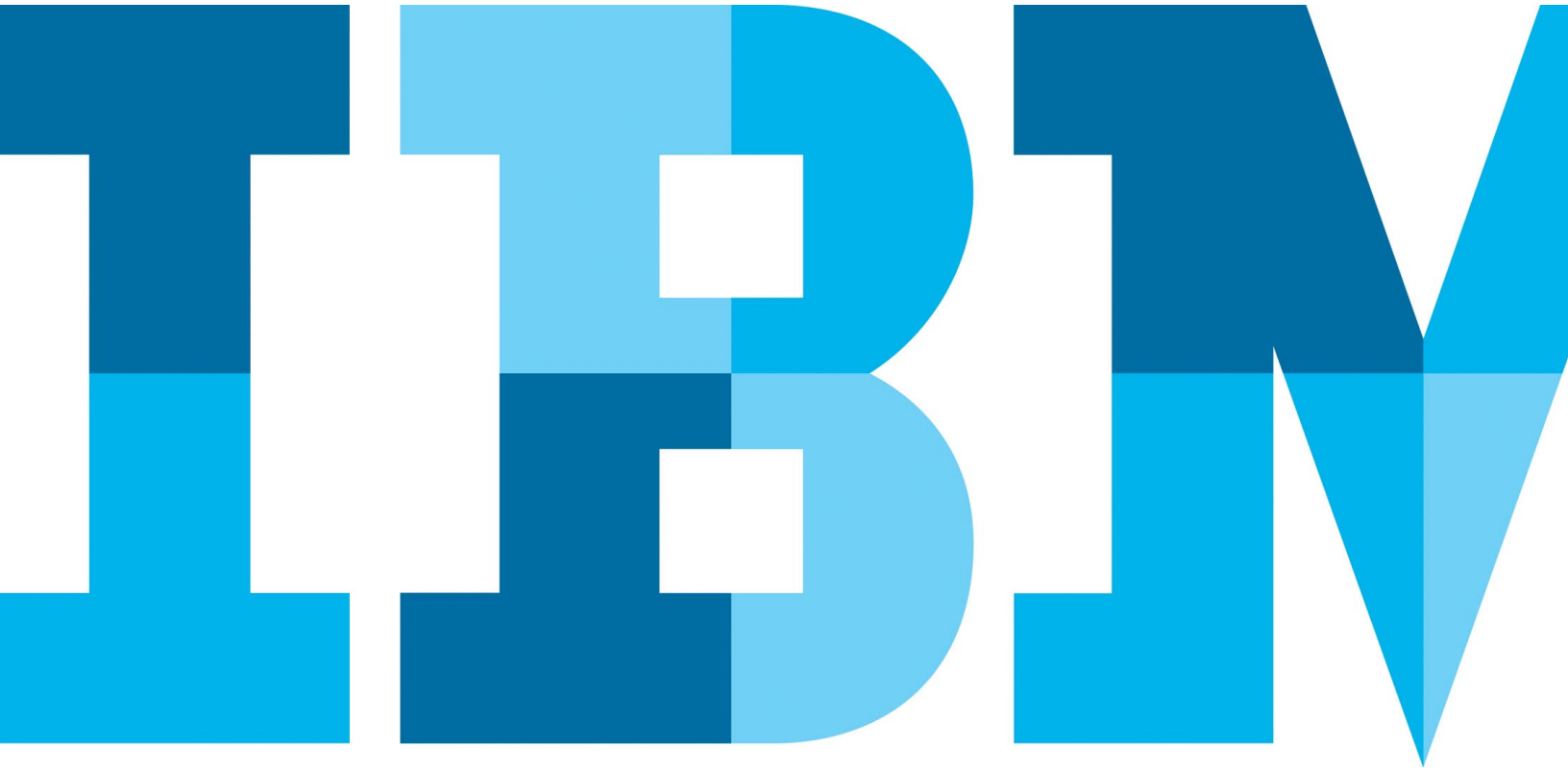
IBM Software
Thought Leadership White Paper

July 2014

Safeguard enterprise compliance and remain vigilant against threats

IBM System z mainframe and risk management software deliver the integrated capabilities infrastructures demand



IBM

Introduction

Organizations around the world—including 92 of the world's top 100 banks, 23 of the top 25 US retailers and nine of the world's 10 largest insurance organizations—trust their business to securable, scalable, self-optimizing IBM® System z® mainframes.[1] Estimates are, in fact, that despite the growth of distributed computing, mainframes still process roughly 30 billion business transactions daily, including most major credit card transactions, stock trades and money transfers.[1] Now, as threats of data breaches and attacks continue to grow, the security made possible by System z becomes more important than ever.

But enterprise security is an ongoing process requiring persistent vigilance. And in a constantly changing landscape of data theft and compromise, organizations can never rest. They must remain alert and protected with their own changing and improving defenses, taking full advantage of the security that System z makes possible and deploying the latest software solutions for eliminating management silos, detecting vulnerabilities and providing threat visibility.

This white paper will discuss challenges organizations face in changing risk and compliance environments. It will present IBM mainframe and software solutions that can help sustain security and regulatory compliance amid that change.

As threats increase, security and compliance remain a challenge

Security threats come from myriad directions. From malicious access by privileged, internal users as well as sophisticated attacks by skilled, international hackers. From careless administration that disables protection in shared cloud infrastructures. From exposed user IDs in mobile and social applications that open gateways into data repositories.

These diverse dangers, however, share damaging results. A recent report noted that when an attack does succeed, a single compromised record now costs an organization an average of USD207—and the average total cost of an enterprise data breach is now USD5.85 million.[2]

The bottom line? Safeguarding the huge—and hugely valuable—data volumes produced by today's applications means security and compliance is a key imperative.

Security and compliance can be a challenge, however, as both threats and methods of protection change. The traditional focus of security strategies, for example, was to react when breached—but today's focus is on continuous management. Reactions traditionally required days or months, but now they must happen as close to real time as possible. And while security solutions traditionally provided adequate coverage with specialized point products, organizations now need integrated capabilities for the comprehensive protection growing infrastructures demand.

Organizations must deal with changing threats, infrastructures and regulations

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

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

Regulatory requirements, such as the Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS), Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) and other regulations worldwide, must be met. Security intelligence, along with automated threat analysis and remediation, must be provided to help ensure maximum visibility into activities within the operational environment. And complexity must be reduced, with automated solutions that are simple and cost-efficient to

deploy and utilize, scalable solutions that can keep up with enterprise growth, and integrated solutions that can take the place of siloed point products.

To avoid a big breach, big data requires comprehensive protection

In the face of changing demands, organizations must sustain both a strong security posture and compliance with security requirements. The variety, volume and velocity of big data give organizations the opportunity to go deeper and faster into information to derive meaningful business insights. But vulnerabilities in the data environment can give attackers the opportunity to exploit weaknesses.

With data environments moving beyond traditional relational and hierarchical databases to encompass a huge variety of information, data security can be difficult to achieve and security compliance can be difficult to define—especially in diverse, distributed environments. Structured machine-created data, for example, is generated at tremendous velocity. That's matched by the continuous production of unstructured enterprise content such as emails, voice and video.

In the face of such complexity, security and compliance techniques must address both distributed and mainframe environments. Major shortcomings appear in the frequent reliance on manual management processes and on security alerts that arrive only after a problem has occurred. Proactive, integrated security information and event management (SIEM) solutions can meet the demands of differently structured data so information can be better utilized in business decisions.

Mainframes can help an organization stay on top of change

When change is moving fast, a mainframe can give the organization the ability to stay in control—whether the source of change is the dynamic variety of unstructured data or the organized policies and processes of an updated compliance regulation. A mainframe environment, in fact, can enable organizations to go beyond current data requirements to meet future needs.

Companies around the globe rely on IBM for security and compliance

Organizations worldwide have used IBM mainframe and software solutions to sustain and improve security and compliance.

- **Swiss Re, a leading European insurance provider, deployed the IBM Security zSecure™ suite on an IBM mainframe—significantly reducing the manual effort needed for compliance checking, reporting, and security and vulnerability scanning.**
- **Itaú Unibanco, the largest private bank in Brazil, deployed zSecure software—helping reduce IT risks and improve compliance with regulations including the Sarbanes-Oxley Act (SOX) and Basel III.**
- **Allied Irish Banks replaced its existing mainframe security system with IBM RACF® and zSecure software—helping it stay ahead of security threats and lower the cost of compliance.**

This capability can be particularly important when security needs become more demanding than compliance requirements—an all-too-common situation in which being in compliance does not necessarily mean being secure. These gaps occur when compliance regulations, which may have been written some time ago, do not incorporate current security best practices. A mainframe, however, can be extensible and flexible to keep up with best practices as they evolve. Once an organization achieves compliance, a mainframe can help sustain high levels of security by continuously meeting new levels of management and protection.

In such a case, a mainframe can help the organization take the first step—compliance—toward security. But its benefits can also work the other way around. A mainframe can help address compliance because it can help the organization proactively stay ahead of changing needs for security to defend against threats or

comply with regulations. In rapidly changing environments, a mainframe can support compliance by first helping ensure the highest levels of security.

IBM System z supports security best practices as well as compliance

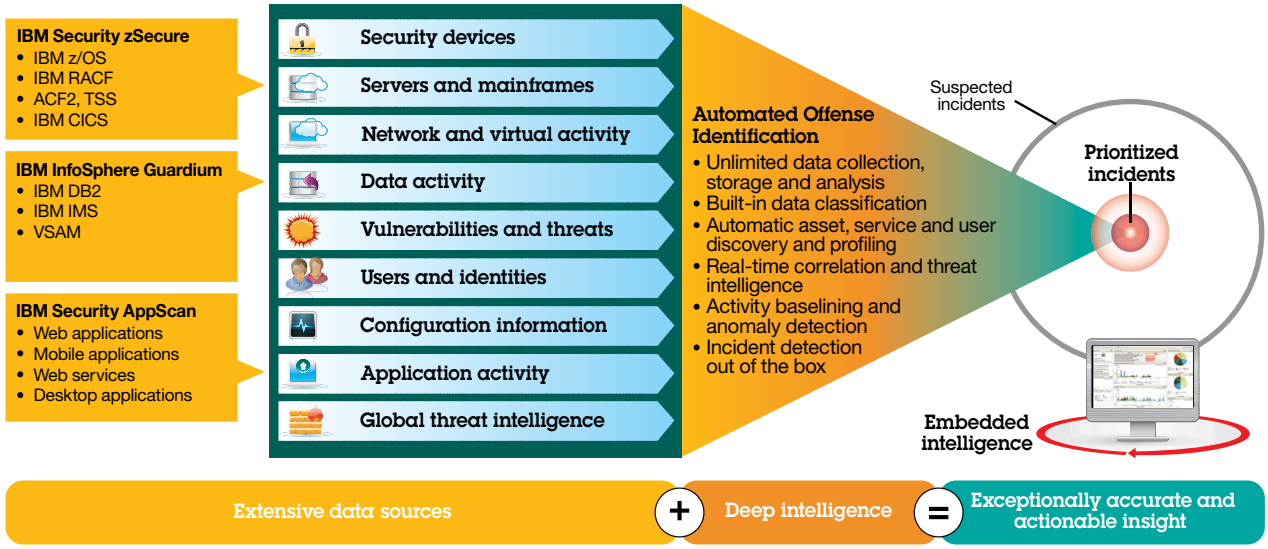
System z mainframes leverage 50 years of industry leadership with security capabilities built into the entire system stack to provide a secure base for critical business operations. Security is so integral to System z, in fact, that the operating system will not start unless the security package has been defined. The mainframe is so reliable that typical application downtime is only about five minutes a year.[3]

Central to sustaining security and compliance in changing environments, System z also supports mainframe security best practices ranging from separation of duties and management of privileged access to safe defaults for system configurations, encryption of sensitive data and the ability to identify and classify sensitive and essential data. A critical function is the ability to provide consistent and repeatable monitoring and auditing of security events to detect potential threats and provide automated analysis of user- and activity-related big data.

Establishing and maintaining safe security settings are fundamental to staying secure and compliant. Establishing a baseline snapshot of the security configuration and safe defaults, and then automatically monitoring that status for changes that could jeopardize security, provides security health checking that can prevent exposures. Additional compliance framework checklists can test specific compliance capabilities to demonstrate governance.

The result is a mainframe that both maintains its system integrity and delivers security capabilities to help provide the lowest risk of exposure to its enterprise users. IBM Security solutions for integrated security and risk management provide the enterprise-wide view of threat activities organizations need in order to sustain ongoing regulatory compliance as well as system and data security.

Integrated solutions improve security intelligence to drive deep insight

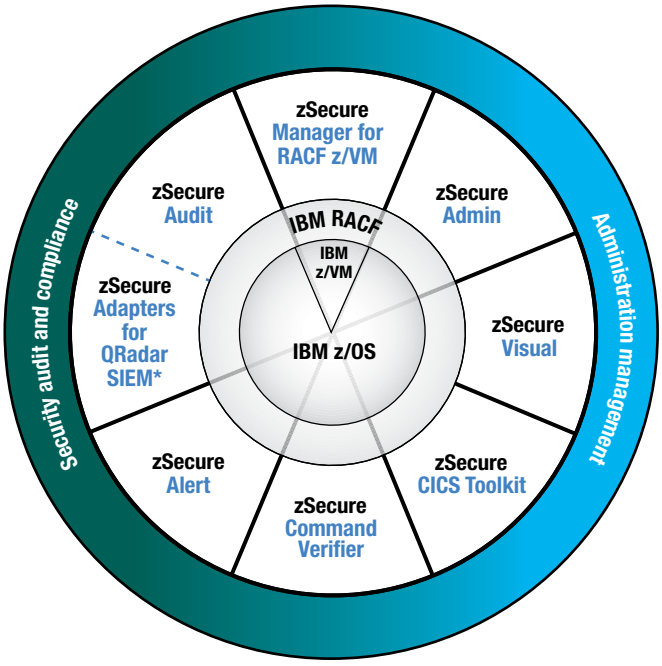


IBM software solutions enable comprehensive security capabilities

IBM helps organizations sustain mainframe security and compliance with leading software solutions:

- **The IBM Security zSecure suite** provides end-to-end security solutions to eliminate management silos by integrating with mainframe security products, System z subsystems and other IBM Security solutions. The Compliance Framework in IBM Security zSecure Audit tests compliance for security regulations, including PCI DSS, DISA STIG and privacy.
- **IBM Security zSecure Adapters for QRadar® SIEM** collects, formats and sends enriched mainframe audit records to IBM Security QRadar SIEM to be included in the enterprise-wide, integrated capabilities for SIEM, log management, anomaly detection, incident forensics, and configuration and vulnerability management.
- **IBM InfoSphere® Guardium® Data Activity Monitor** provides enterprise-wide, real-time threat detection, alerting, blocking of suspicious transactions, automated compliance workflow, audit and a library of predefined compliance processes and reports. In addition to databases, it also supports big-data sources such as Hadoop distributions, fileshares and more.
- **IBM InfoSphere Guardium Vulnerability Assessment** finds and scans database infrastructures to discover sensitive data sources and to detect exposures such as missing patches, weak passwords, unauthorized changes and misconfigured privileges.
- **IBM Security QRadar SIEM** consolidates vast amounts of log-source event data from throughout the infrastructure, surfacing suspected incidents in near real-time to support more effective threat management.
- **IBM Security Key Lifecycle Manager** centralizes, simplifies and automates the encryption key management process to help minimize risk, reduce operational costs and comply with regulations.

IBM Security zSecure suite



* Product offers a subset of the capabilities provided by zSecure Audit

Conclusion

IBM offers comprehensive, end-to-end, integrated mainframe security capabilities for enforcing industry standards and compliance regulations to prevent sophisticated attacks and breaches. Addressing the entire security platform—people, data, applications, infrastructure and compliance—across the mainframe and distributed systems environment, IBM solutions are designed to grow as security and compliance requirements change.

IBM capabilities for collecting information, automating corrective actions, continuously enforcing security policies, and monitoring, analyzing and auditing records to create compliance reports can help reduce operational risk with integrated capabilities for the comprehensive protection growing infrastructures demand.

For more information

To learn more about security solutions for IBM mainframes, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/software/os/systemz/security/

For more information on the IBM Security zSecure suite of security products, visit: **ibm.com**/software/security/products/zsecure/

[1] Janet Sun, "Don't Believe the Myth-information about the Mainframe: Part 1," *SHARE*, May 07, 2013. http://www.share.org/p/bl/et/blogid=2&blogaid=234

[2] "2014 Cost of Data Breach Study: Global Analysis," *Ponemon Institute with IBM*, May 2014. **ibm.com**/services/costofbreach

[3] According to IBM lab measurements. Five-nines is a term used to denote that a piece of equipment is functioning with 99.999 percent availability on average, which translates to roughly five minutes of downtime per year.

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
July 2014

WGW03063-USEN-00