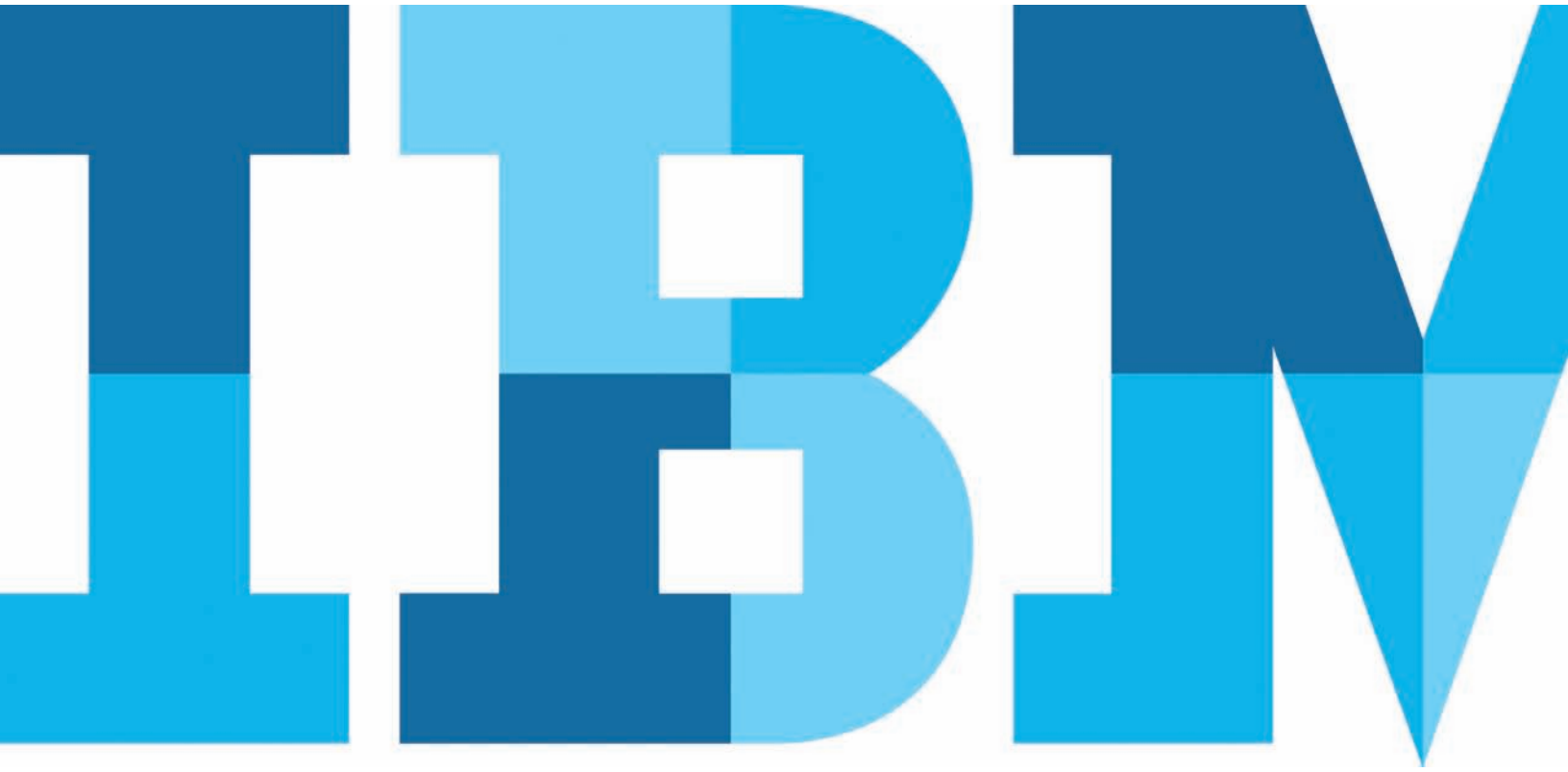
IBM Software
Thought Leadership White Paper

June 2013

Creating the ultimate security platform

IBM System z delivers proactive protection for data, web, cloud, mobile and enterprise environments



Contents

Introduction

It may sound counterintuitive, but business security challenges aren't always only about security. Sure, keeping the bad guys out is the ultimate goal. But the challenges an organization faces every day are just as likely to be about the cost of providing security or the administrative hassles of ensuring regulatory compliance. What about that database a former employee created years ago and everyone else has forgotten existed? Before you can secure it—or remove it—you have to find it. Even if it's on your mainframe, you need the right security and management tools for the job.

With those tools, you can achieve stunning results. Using software solutions from IBM, one large healthcare provider was able to decrease its compliance auditing costs by 80 percent. And a leading telecommunications company reduced the time required for audit reporting by 60 percent. All while maintaining the ultimate security of an IBM mainframe. Because even when attention turns to related security challenges, the mainframe remains the linchpin of enterprise security, the trusted home for critical data, applications, web services, cloud and mobile computing—in other words, for today's essential enterprise business operations.

This white paper will examine the nature of attacks and vulnerabilities that create the shifting landscape of enterprise security, the capabilities that must be put into place to ensure secure operations, and the IBM hardware- and software-based solutions designed to meet those challenges. It is written for any organization that either has or is planning to add a mainframe in its computing environment and that is looking for insight into how to secure data and applications as it consolidates workloads, tackles big data or moves operations to the cloud. The paper includes real-life examples of companies that have used mainframe computing to achieve the ultimate security platform.

Mainframe security challenges are changing

When mainframes were introduced in the early 1960s, system networks were small and well-defined. Users were few and known within the organization. To gain access, a person needed to be on the premises, usually during regular hours. Physical data may have been susceptible to removal or theft, but if an unauthorized user did get into the system, the information stored there was typically limited to transactions and batch processing.

Today, mainframes are connected to a network—the Internet—that spans the globe. Virtually anyone anywhere has 24x7 access via PCs and mobile devices to mainframe-based web servers. Organizations store their intellectual property and sensitive business data on mainframes. Customers freely upload personal details. And attackers aggressively seek information for financial gain.

The good news is that because mainframes contain built-in security capabilities, they are the target of relatively few successful attacks—less than one percent, according to one recent study.[1]

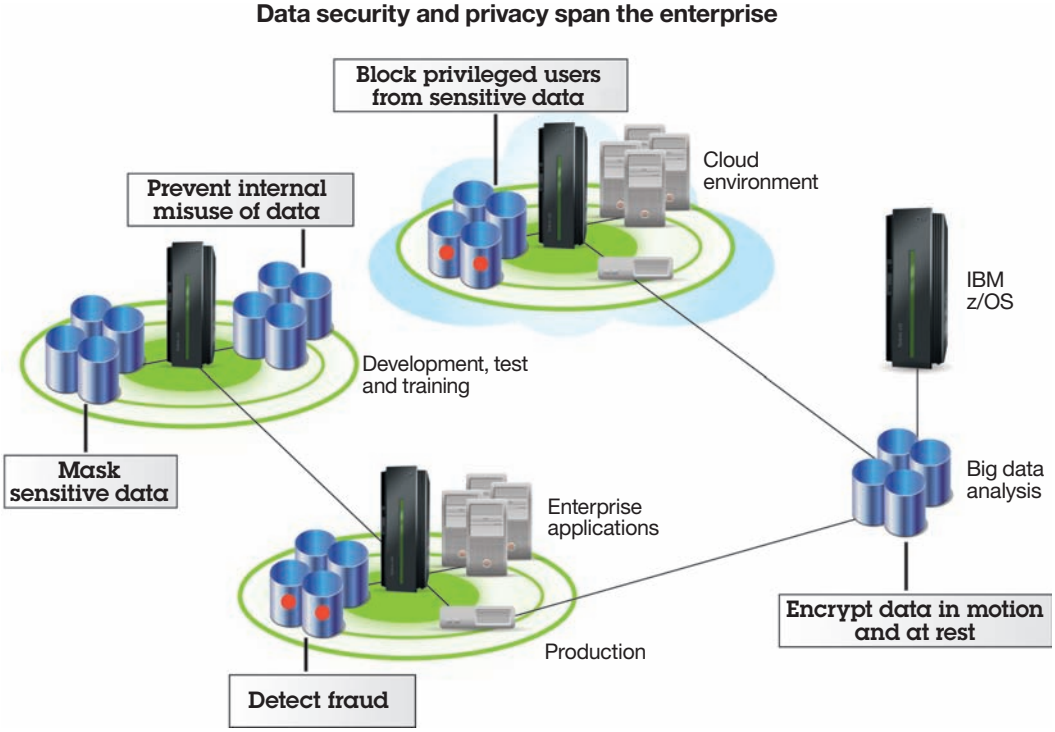
The challenge is for organizations to recognize the changing nature of security threats and to make sure their mainframe protection is up to the task. For as the number and severity of threats have increased, many organizations have diverted their energies to protecting more vulnerable platforms, mistakenly believing that the mainframe that was secure in years past is still secure today.

In reality, the growing complexity of the environments in which mainframes operate means systems can be harder to manage and more vulnerable to attack. A poorly configured or down-level system can become a target for a hacker, even if it is a mainframe. At the same time, access continues to grow.

Increasing numbers of remote workers mean less control over internal access. And expanded access for external mobile users, intended to extend more services to more customers, also opens opportunities for exposures.

Of critical importance is the need to assess and optimize the state of security monitoring processes in mainframe operations, and to ensure that the processes are sufficient to determine that a security breach exists or has occurred. Software often has the capability, but it may not have been effectively configured, or events may not have been continuously monitored. So the question becomes: Would you even know if your mainframe system were compromised?

Data security and privacy span the enterprise



Access to a system, in fact, can come from multiple sources via multiple paths. Suppliers can access data at rest via web applications to access distributed servers. Hackers can access data in motion via mobile applications to access a mainframe.

Many attacks today occur over long time periods. A systems administrator may inadvertently fall victim to a phishing attack that can extract sensitive data, such as credit card numbers, from the business database and send it directly to a malicious entity. A recent study found, in fact, that while the period from initial attack to initial compromise typically takes only seconds or minutes—and the period from initial compromise to data extraction typically takes minutes to hours—the period from compromise to discovery in 98 percent of cases takes weeks or even several months.[2]

Data vulnerabilities can remain challenging to prevent

The need to protect critical business data and operations from advanced threats—coupled with the need to comply with growing numbers of regulations and protect the brand reputation—leads many organizations to mainframes as the platform of choice for their data, web, cloud and business operations. Mainframes not only give them the ability to secure operations for business functions such as cloud computing and big data analytics, they also enable consolidated security intelligence for improved proactive risk management.

This doesn't mean that mainframe security has not presented challenges. If not handled properly, security alerts can arrive after a problem has occurred, if at all. Costs can be high, with menial administration tasks conducted manually by highly skilled professionals, who are in short supply, diverting them from higher-value security management activities. Visibility can be limited, with mainframe processes, procedures and reports often siloed from the rest of the organization. Complexity can be high, with the large scope and size of business services making identification and analysis of threats difficult. And assuring security in support of regulatory compliance can also be difficult, as verification often remains a manual task.

Even accepted practices can fall short. Security management tools have not always been scalable or flexible enough to meet the evolving requirements of complex environments—and homegrown security approaches can become out of date and obsolete. Processes have been inconsistently and ineffectively applied, with separation of duties not enforced, privileged users not adequately monitored, and policies and procedures neither followed nor structured so they can be repeated.

It is the need to manage the full range of security requirements, then—from the operations that enable security, to the legal requirement to protect data, to the business imperative to support competitive advantage and business profitability—that is at the heart of today's emerging security focus. This is in contrast to the traditional security focus, which grew from the mainframe's back-end role in support of databases and production to provide security based on governance and compliance with internal and external policies. Instead, data security and compliance look to the larger scale of security needs and to expanding its timeliness and effectiveness to meet current and potential mainframe roles, reaching beyond production to support the new business opportunities that are strategic to enterprises today.

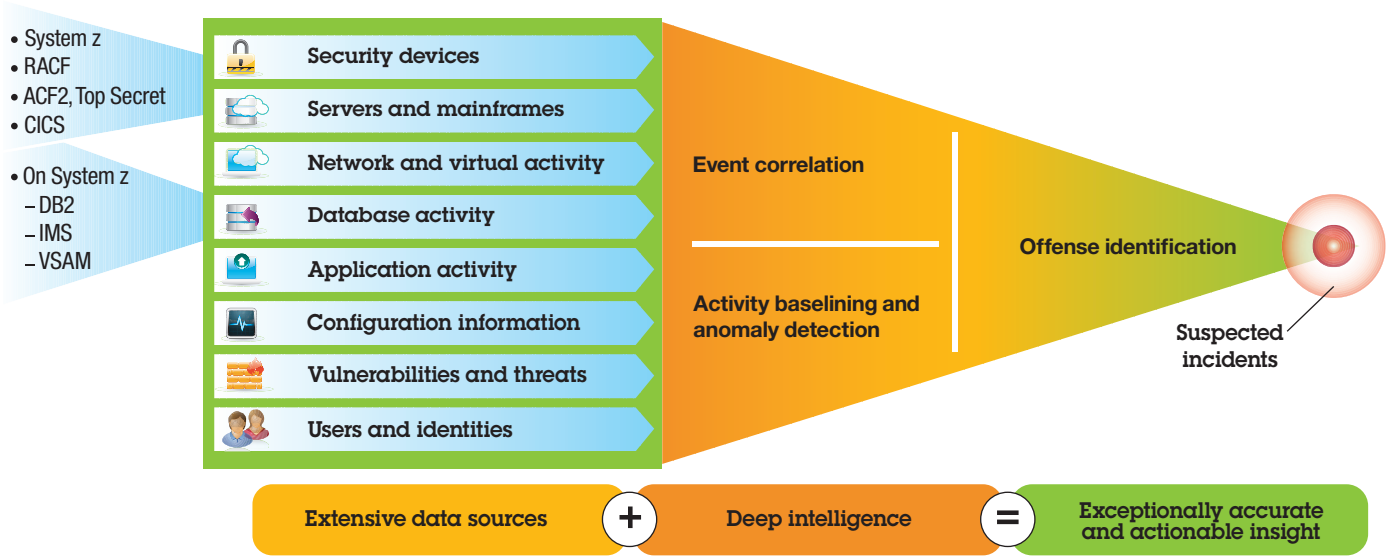
So while traditional security techniques enabled organizations to react to a breach after it had occurred, emerging techniques provide continual real-time monitoring and alerting to help detect vulnerabilities and repair them before a breach occurs. While traditional techniques enabled organizations to react within days, weeks or months, emerging techniques empower them to react in real time. While traditional techniques monitored thousands of events, emerging techniques monitor millions of events. And while traditional techniques relied on a

multitude of point security products, emerging techniques employ integrated, automated solutions that are more effective and easier to manage.

New business and IT trends require greater attention to security

In a recent study conducted for IBM, Forrester Research concluded that "information security is the new imperative." Some 94 percent of study respondents agreed that security is an essential requirement for safe delivery of their core offerings, and 97 percent stated that security is critical to their ability to compete in the marketplace. In meeting this imperative, some 86 percent said they house their most important data on mainframes, and 87 percent consider the mainframe to be their most available, scalable and secure platform.[3]

IBM solutions help improve mainframe security intelligence



This emphasis on security is central not only to meeting general goals for protecting and managing data, applications and systems, and ensuring business continuity and integrity, but also for getting the most out of key technology trends and initiatives that drive business today. These include:

- **Big data:** Mainframe environments have always handled huge amounts of data, but the phenomenon known as big data draws information from so many structured and unstructured sources and stores data so massively that it demands new levels of attention. Big data comes from everywhere—sensors gathering climate information, posts to social media sites, digital pictures and videos, purchase transaction records and more—and much of it ends up residing on mainframes. Understanding and analyzing big data gives organizations the opportunity to gain insight on customers, competitors, products or services and to make their business more agile and responsive. Big data is about managing high volume, variety and velocity of data—but in a rush to achieve new insight, some organizations are neglecting data security.
- **Security intelligence:** Designed to enable a consistent, normalized analysis of disparate data to recognize and block attacks, security intelligence solutions integrate capabilities ranging from network intrusion prevention to endpoint management to create a complete picture of the infrastructure and the attacks and vulnerabilities that threaten it. The result is the ability to respond to complex threats missed by point security solutions. And, while the mainframe itself can save up to 70 percent in audit overhead,[6] security intelligence can increase the depth of insight and real-time anomaly detection, improving the integrity of systems and protecting your mission-critical workloads.
- **Compliance and regulation:** In a world where government and industry regulations are on the increase, documenting security measures and responding to security audits can be as important as providing security itself—because audit failures can result in fines and penalties even if no security breach has occurred. Organizations need ways to collapse data silos for easier compliance reporting and improved security intelligence. They need best-practices management approaches and automated resource monitoring to quickly and reliably detect anomalies. To reduce the time and effort involved in compliance audit and validation, they need automated solutions for repetitive reporting activities. And they need insight to ensure that compliance and security goals align.

Replacing high maintenance with greater efficiency

The Brazilian bank, Itaú Unibanco, needed a substitute for its existing security management and auditing tools, which provided little flexibility and required high maintenance. Deploying solutions from IBM® Security zSecure™ suite met a variety of management, auditing, compliance and monitoring security needs for its IBM z/OS® system.

The zSecure solutions improved efficiency and productivity for security management requirements, while enabling the bank to respond quickly to security incidents and generate detailed reports for auditing and compliance.

- **Cloud computing:** The benefits of cloud computing—from rapid provisioning to more efficient use of assets and increased cost savings—are well accepted. But in a recent IBM study, 77 percent of respondents stated that adopting cloud computing also makes protecting privacy more difficult.[4] Such a widely held concern suggests the importance not only of improving cloud security, but also of streamlining and simplifying processes for keeping the cloud safe. To create a cloud that both organizations and end users will feel safe using requires security that is firmly based in the cloud's foundation of virtualized resources.
- **Web applications:** The Internet can be a risky place. According to one study, as many as 47 percent of all enterprise vulnerabilities reside in web applications.[5] And in another, 92 percent of respondents said social media increases the risk of security breaches.[3] Detecting vulnerabilities during application development is one way to contain potential problems. Care in integrating downloadable applications into the enterprise back end is another. But even after deployment, tools can provide scanning across the application lifecycle, results can be correlated with intrusion protection systems, and policies can be created to help protect against the risk of threat.
- **Mobility:** With mobile computing now the connectivity platform of choice in on-the-go business environments, organizations face persistent worries that careless user behavior or the chance of loss or theft does not compromise business data. In fact, 91 percent of respondents in the same survey that noted increased vulnerabilities in web applications also voiced concern that mobile devices increase the risk of information loss.[3] From configuring mobile devices for compliance to de-provisioning them by remotely wiping corporate information, organizations need consistent, policy-based ways to ensure security and control. They need to manage mobile devices as part of a unified infrastructure.
- **Cost reduction:** In mainframe environments, users need integrated solutions that reduce complexity and cost. They need out-of-the box integration to simplify everything from new application development to regulatory compliance. They also need automated solutions that are easy to deploy and that streamline and simplify management, reducing the security administrator workload and increasing efficiency to reduce the cost of staffing.

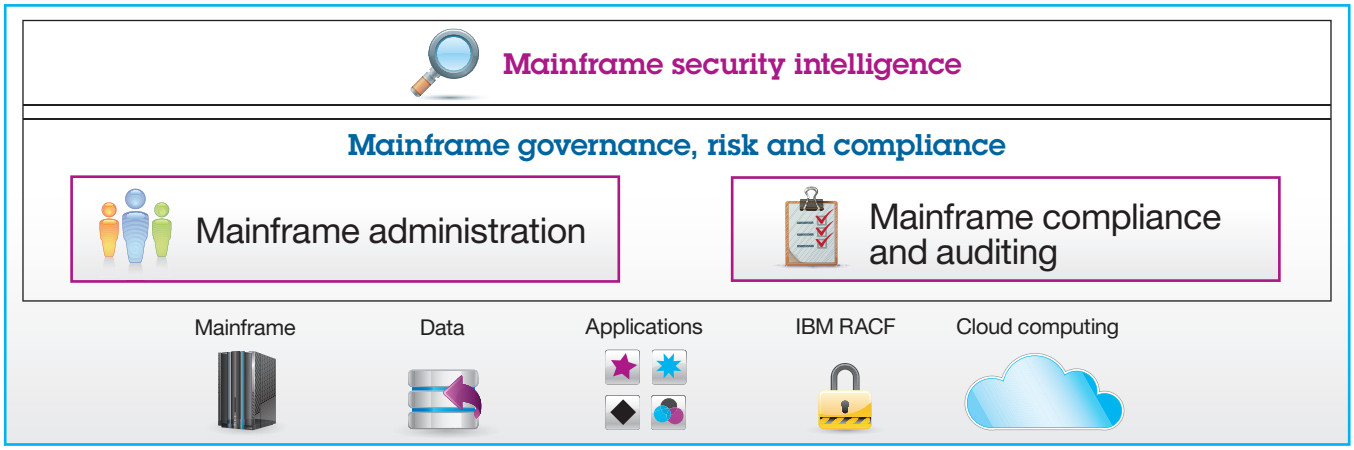
Security calls for scalable and dynamic policies, not bolted-on capabilities

Organizations know they need security to succeed in today's often risky environments. Respondents to the Forrester-IBM survey ranked security capabilities high, with 95 percent citing data protection and encryption, 94 percent citing network security, and 93 percent citing identity and access management as either very important or essential.[3]

And the consequences of security lapses are clear. The average cost of a data breach now has reached USD5.4 million.[7] In the United States and Germany, where the rate of breaches are highest, the cost per compromised record is USD289 and USD199 respectively.[7] And the cost of non-compliance—considering disruption to the business, loss of business, fees, penalties, legal costs and more—averages USD9.4 million.[8]

But how does the organization attain a secure state? How does IT know whether the mainframe security is configured properly? Or that only authorized users are given user accounts? How do they prove for auditors that all critical data is backed up and recoverable? Or that private customer data is encrypted with key management? How can an organization ensure a valid need to know sensitive data? Can it de-identify data dynamically based on established security policies? Can it provide an audit trail for all mainframe data access?

IBM mainframe security management vision



The answer: In today's fast-moving, high-risk business and IT environments, organizations need comprehensive and integrated security solutions that are built in, not bolted onto their mainframe platform. Security vigilance starts with the fundamental design—it cannot be an afterthought. Because in today's risky world, a reactive response is not good enough. And in a complex world, where human error accounts for two thirds of data breaches,[7] manual, one-off approaches cannot keep up. Effective security requires a proactive approach that anticipates the worst—and that provides multi-layered defenses to today's multifaceted attacks.

An effective approach leverages a comprehensive vision that begins with hardware, users, data and applications—and includes native security capabilities that are built into the mainframe. It simplifies user and resource management for improved and streamlined mainframe administration. It automates monitoring, analysis and auditing to enforce best practices for mainframe compliance and auditing. And it integrates all components with real-time events correlation to provide security intelligence that not only supports the mainframe, but also spans the enterprise. A variety of data protection capabilities can secure information at rest, in use and in motion.

IBM solutions offer comprehensive, integrated data protection

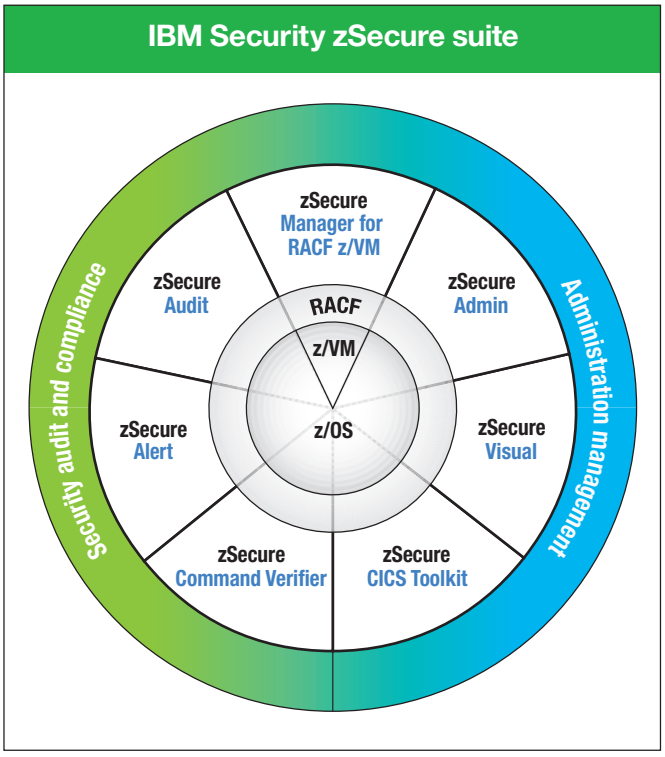
Even the world's most secure computing platforms need both protection from threats and breaches and the ability to quickly demonstrate compliance with industry and government regulations. Because they typically store some of an organization's most sensitive data, high-security mainframe platforms such as IBM System z® remain targets for hackers and insider breaches. To combat these threats, the System z platform is designed to deliver proactive protection for enterprise infrastructure and information.

System z with its z/OS operating system brings to the enterprise a rich heritage in providing the ultimate security platform. Widely considered the most secure commercial operating system available today, System z has undergone rigorous certifications spanning both traditional z/OS environments and virtualized environments. System z has received the highest mainframe evaluation of EAL5+ from The Common Criteria for Information Technology Security Evaluation. It has also received a high Federal Information Processing Standard (FIPS) 140 rating from the National Institute of Standards and Technology (NIST).

System z was the first to integrate encryption hardware into the mainframe, and it continues to build security into every level of its structure, including the processor, hypervisor, operating system, middleware, communications, storage and applications. Security features are designed specifically to help users comply with security-related regulatory requirements, including identity and access management, hardware and software encryption, data masking, communication security, and monitoring and reporting of security events.

System z creates an optimized infrastructure that is further designed to integrate with a comprehensive set of security capabilities for delivering cloud computing, reducing operational risk, offering customizable compliance monitoring and reporting, and providing deep and broad security intelligence.

And System z helps save money. When both security expenses and storage expenditures are considered, System z can reduce the total cost of information over other offerings by as much as 63.4 percent.[9] With System z, staff savings can be as much as 74 percent.[9]



IBM Security zSecure

The zSecure suite of solutions is designed to help users administer mainframe security, monitor for threats, audit usage and configurations, and enforce policy compliance. By improving the efficiency and manageability of the mainframe security environment, zSecure solutions can significantly reduce administration overhead to reduce costs, improve productivity, enable decentralized administration, and speed administrative response time to better support the business.

The ability to automate auditing, monitoring and compliance processes can help organizations pass audits more easily, save time and expense through improved security and incident handling, and increase operational effectiveness to reduce costs and risk. The comprehensive capabilities of the zSecure suite range across the complete data protection spectrum, from detecting/preventing intrusions and identifying misconfigurations through real-time mainframe threat monitoring, to data analytics that help detect concealed and complex risks, to out-of-the-box alerts and customizable reporting.

IBM InfoSphere Guardium

IBM InfoSphere® Guardium® solutions are designed to discover and classify sensitive data, detect vulnerabilities, and ensure the privacy and integrity of enterprise data. With policy-based, real-time monitoring of database activities—including actions by privileged users—along with database infrastructure scanning for missing patches, misconfigured privileges and other vulnerabilities, InfoSphere Guardium provides a robust solution for protecting data and automating the compliance auditing process across a wide range of database vendors and computing platforms.

Centralized and standardized controls support a holistic approach to data protection that can help ensure compliance and reduce costs. Using InfoSphere Guardium solutions, organizations can ensure comprehensive data protection for cloud, virtual and physical infrastructures; identify and audit structured and unstructured data; simplify compliance with preconfigured reports and automated oversight workflows; and build security into big data environments to prevent breaches and ensure data integrity.

IBM InfoSphere Guardium Data Encryption for DB2 and IMS databases

IBM InfoSphere Guardium Data Encryption for DB2® and IMS™ databases is a single tool that provides encryption across both DB2 for z/OS and IMS. It offers row-level and column-level encryption for DB2 as well as encryption at the segment level for IMS. It leverages the z/OS Integrated Cryptographic Service Facility (ICSF), which exploits the crypto hardware for data encryption and decryption.

IBM Security QRadar solutions

IBM Security QRadar® solutions collect and monitor data not only from the mainframe, but also from sources such as security devices, network devices, firewalls, operating systems and applications to provide a unified view of security and compliance risks. The ability to analyze events, network flows, vulnerabilities, user identities and threat intelligence in a unified way enables an exceptional level of context and insight.

QRadar solutions provide a control center for integrating real-time security intelligence data from more than 400 different sources—and automatically alerting security teams to unpatched applications that are vulnerable to attack. QRadar solutions can determine if malicious traffic could lead to a potential exploit and report the activity as a high-risk incident to the network administrator.

IBM RACF

As the software foundation for integrated security intelligence capabilities and access control decisions in z/OS, IBM Resource Access Control Facility (RACF®) helps organizations administer and define authorized users according to policies, make access control decisions and create security log records. In protecting resources, RACF retains information about users, resources

and access authorities, and uses that information to identify and authenticate users, authorize users to access protected resources, and log and report attempts at unauthorized access. RACF establishes separate privileged user roles for security administration and auditing, and can limit scope by groups for least possible privilege.

IBM Security Key Lifecycle Manager for z/OS

IBM Security Key Lifecycle Manager for z/OS centralizes and automates the management of encryption keys to protect and maintain the availability of data at rest on System z mainframes—minimizing the risk of loss or breach of sensitive information without reducing system performance. Robust capabilities across the encryption lifecycle enhance data security by dramatically reducing the number of encryption keys to be managed. Integration with mainframe encryption management and hardware storage encryption devices simplifies transparent data protection.

IBM Enterprise Key Management Foundation

IBM Enterprise Key Management Foundation allows for the management of Data Encryption Standard (DES), Triple DES (TDES), Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) keys while leveraging the IBM cryptographic hardware complying with IBM Common Cryptographic Architecture (CCA) as well as keys for non-IBM hardware security modules. Enterprise Key Management Foundation is a flexible and highly secure key management system for enterprises where operations that require human interaction are conducted from a secure workstation. It provides centralized key management and highly secure operations via two-factor authentication, dual control, FIPS140-2 Level 4 certified hardware and extensive audit logging.

IBM InfoSphere Optim Data Privacy

IBM InfoSphere Optim™ Data Privacy enables organizations to support data privacy and compliance requirements by masking data across platforms and data sources using a standard and repeatable process—without impacting the stability of applications. Application-aware masking, for example, helps ensure that masked data, such as names and street addresses, resembles the look and feel of the original information—and context-aware data masking routines make it easy to de-identify elements such as payment card numbers, Social Security numbers and email addresses. Persistent masking capabilities enable propagating masked replacement values consistently across applications, databases, operating systems and hardware platforms, including big data environments.

Reducing costs with improved access management

The Italian consumer credit company Findomestic Banca wanted to replace the legacy system it was using to manage user access across its complex mainframe environment with a solution that would reduce its management costs. Deploying solutions from the zSecure suite helped the company manage multiple environments with only three employees, create and manage alerts, and gather access approvals based on internal policies.

The zSecure solutions enabled the company to create a full mainframe security management solution to administer its access management software, enabling it to keep the entire mainframe security environment under control with an online alerting system and back-office auditing system.

Conclusion

On today's smarter planet, where huge volumes of data from instrumented, interconnected and intelligent devices are more important than ever to business success, IBM mainframes can provide the ultimate platform for integrating the protection of data, web, cloud, application, and enterprise hardware and software resources. For more than 50 years, IBM mainframes have been leaders in providing comprehensive, integrated security solutions across the entire security platform—people, data, applications, infrastructure and compliance. With the industry's highest evaluated platform at EAL5+ and with integrated hardware and software, IBM mainframes can help you achieve the protection you need for your most critical data, web, cloud, mobile and enterprise business operations.

For more information

To learn more about IBM security solutions for mainframe environments, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/security

[1] Verizon, "2011 Data Breach Investigations Report." http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf

[2] Verizon, "2012 Data Breach Investigations Report." http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf

[3] Forrester Research, "Secure The Enterprise With Confidence Using a Mainframe Infrastructure," March 2013.

[4] Paul Saxton, IBM Institute for Business Value, "The 2010 IBM Global IT Risk Study: The evolving role of IT managers and CIOs," *IBM Corp.*, September 2010.

[5] IBM X-Force research and development team, "IBM X-Force 2012 Mid-year Trend and Risk Report," *IBM Corp.*, September 2012. http://public.dhe.ibm.com/common/ssi/ecm/en/wgl03014usen/WGL03014USEN.PDF

[6] Based on IBM customer experience.

[7] Ponemon Institute, "2013 Cost of Data Breach Study: Global Analysis," May, 2013. https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf

[8] Ellen Messmer, "Cost of regulatory security compliance? On average, $3.5M," *NetworkWorld*, January 31, 2011. http://www.networkworld.com/news/2011/013111-cost-regulatory-security-compliance.html

[9] "Tracked, Hacked and Attacked," *Solitaire Interglobal, Ltd.*, 2013. http://public.dhe.ibm.com/common/ssi/ecm/en/zsl03232usen/ZSL03232USEN.PDF

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
June 2013

WGW03031-USEN-00