IBM Security
Thought Leadership White Paper

February 2012

Consolidated security management for mainframe clouds

Leveraging the mainframe as a security hub for cloud-computing environments

IBM

Contents

Introduction

Organizations today grapple with the expansion of distributed computing, increased online collaboration, explosive data growth and heterogeneous IT environments—all issues that make information security more critical, yet more complex than ever. Moving data to a virtualized, cloud-based environment can help develop and manage a more flexible infrastructure, and reduce operational costs and total cost of ownership. In addition, a virtualized environment can help accelerate time to market through increased efficiency and automation; scale operations to meet market dynamics and business strategy; and virtually eliminate downtime. The question, therefore, is not whether to move to the cloud—it's how to do it while protecting critical data. Not surprisingly, the level of data security depends largely on which platform supports the cloud environment.

The mainframe has a strong heritage of being an extremely secure platform for virtual environments and workloads, and offers a compelling alternative to massively scaled-out environments often deployed in the cloud—particularly in the realm of security. Also, many organizations are already using a mainframe as their data hub running key applications, providing a natural jumping off point to create a security hub for the entire enterprise.

From automation to advanced virtualization technologies and open industry standards, IBM System z® mainframes help deliver a solid, secure foundation on which to build the virtual environment. They support expandable cloud environments with industry-leading security, as well as availability, performance and cost-effectiveness. These benefits are particularly valuable on today's smarter planet, where instrumented, interconnected and intelligent businesses collect, process, use and store more information than ever before.

Realizing benefits of mainframe clouds

Besides many of the traditional reasons to choose the mainframe over other hardware platforms—security, reliability and consolidated workloads among them—the following are a few real-world examples that demonstrate why organizations deploy virtualized environments on System z platforms:

- One organization already had a mainframe in their data center running customer workloads. They wanted to maintain the mainframe skill base and migrate non-mainframe workloads to Linux on System z.
- Another organization wanted to offer cloud-based software as a service to its customers. The company's calculations revealed that the cost of deploying IBM middleware on the mainframe would be lower than other platforms.
- A third organization wanted to provide customer workload hosting on a mainframe-based cloud. Already a mainframe user, they wanted to protect their workload hosting base by offering a cloud environment on System z.

Addressing security concerns in the cloud

More than ever, organizations are faced with the need to protect critical data in distributed, collaborative, multiplatform environments. Although the operational and capital benefits of cloud computing are clear, so is the need to develop proper security for cloud implementations. It's a justifiable concern. According to IBM X-FORCE® Research & Development, attacks are getting more sophisticated and more common. Halfway through 2011, X-Force reported that the number of critical vulnerabilities had already exceeded the total for all of 2010.[1]

The same characteristics that make the mainframe ideal for running critical applications—robust hardware, reliable operating systems, industrial-strength system management capabilities and dependable security—can be used to enable it as an enterprise security hub. These features extend to virtualized environments.

Security is built into every level of the System z structure, from its processor, hypervisor and operating system to its communications, storage and applications. Hosting virtual workloads and cloud environments on a System z mainframe running IBM software solutions can address each of the following security concerns, and offer far more benefits than risks:

Control

Many organizations are uncomfortable with the idea of public clouds, because their information resides on systems they do not control. However, typical mainframe cloud environments enable users to implement their own "private cloud," which provides more control. Also, these environments can offer a high degree of security transparency, which helps users have a better view across the enterprise and puts them more at ease.

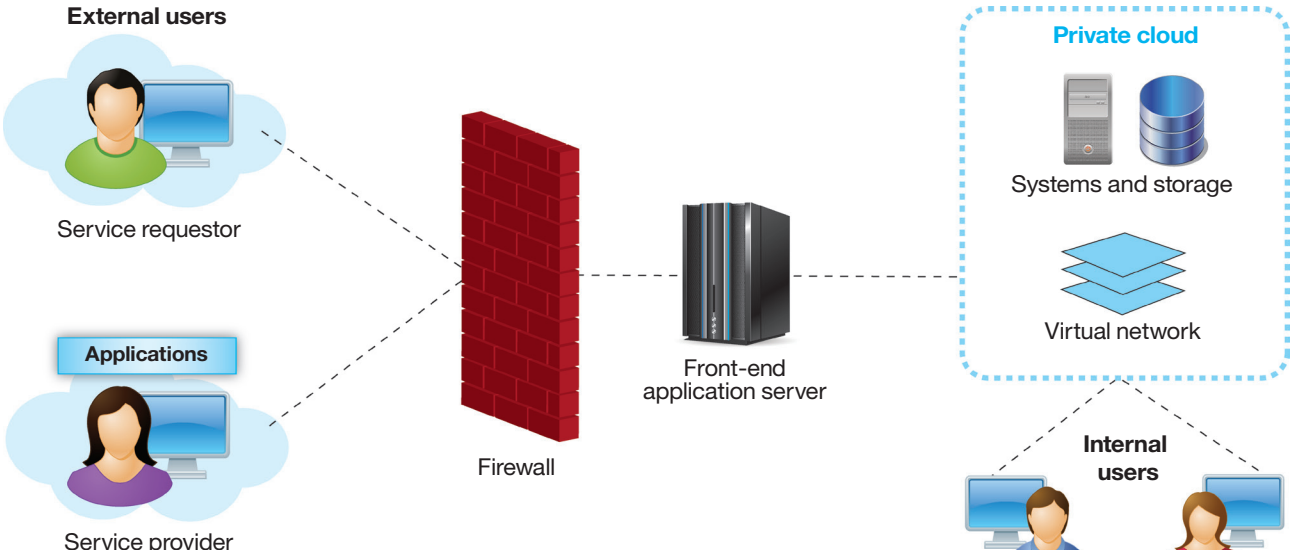

Figure 1: Cloud deployments need the same or better security than traditional deployments.

Migration

While migrating workloads to the shared network and compute infrastructure of a public cloud can increase the potential for unauthorized exposure, migrating to mainframe cloud environments can provide critical authentication and access technologies to protect data. Access and identity management are critical to cloud security, as they limit access to data and applications to only authorized and appropriate users. Limiting who can view and manipulate data helps ensure that it is not mishandled.

Reliability

High availability is understandably a major issue for IT departments, which must prevent loss or degradation of service in the event of an outage. In addition, mission-critical applications may not run in the cloud without strong availability guarantees. One of the hallmarks of mainframes is their high availability, making mainframe cloud environments extremely stable and secure platforms. This can help customers utilize the mainframe as a highly scalable and reliable hosting platform to support multiple customer workloads concurrently.

Ease of management

Mainframe cloud environments can offer easy, visual controls to manage firewall and security settings for applications and runtime environments in the cloud. This can lower IT management costs, saving money in the long run. An internal IBM study found that the overall total-cost-of-ownership (TCO) over three years for a private cloud based on IBM zEnterprise™ systems was 76 percent less than a third-party service provider's public cloud. This is due to consolidated and virtualized workloads, as well as a smaller footprint equaling less hardware and software costs.

Compliance

Complying with the Sarbanes-Oxley Act (SOX), Health Insurance Portability and Accountability Act (HIPAA) and other regulations may limit or even prohibit the use of clouds for some applications. Fortunately, mainframe cloud environments can provide comprehensive auditing capabilities to offset this risk. System z has security features designed specifically to help users comply with security-related regulatory requirements, including identity and access management; hardware and software encryption; communication security capabilities; and extensive logging and reporting of security events.

General benefits to mainframe cloud environments

Besides the security benefits, there are many other reasons to consider deploying virtual environments on larger, scale-up servers like System z.

System z provides up to 100 percent CPU utilization, as well as a "share everything" architecture that can host thousands of mixed workloads. System z can also enable a more efficient data center, since it uses less power and cooling, takes up less floor space and has fewer parts to manage.

There are compelling price advantages, as well. IBM customers have saved as much as 70 percent in audit overhead, up to 30 percent in reduced help desk calls and have had up to 52 percent lower administrative costs using System z as the platform for their cloud environment.

System z supplies all the components necessary to deliver cloud today, including:

- **Workload management—Manage cloud infrastructure capacity requirements consistent with business policies.**
- **Transaction processing—Support cloud integration with mission-critical, online transaction processing applications.**
- **Scalability—Scale vertically with IBM z/OS® and logical partitions (LPARs), and horizontally with Linux on System z and IBM z/VM® coupled with IBM Workload Manager.**
- **Availability and provisioning—Use automation to deploy virtual machines and recovery applications.**
- **Auditing and metrics—Workload-based accounting and metering supports capacity planning and chargeback to line of business.**

In addition, the mainframe supports industry security standards that help ensure interoperability, such as Public Key Infrastructure, OASIS eXtensible Access Control Markup Language, OASIS Key Management Interoperability Protocol and more.

Optimizing—and protecting—virtualized platforms

The mainframe's support for multi-architecture, virtualized environments enables customers to run a broad range of workloads. This means users can add processors, blades and more, quickly and easily, and automate hypervisor and network setups to reduce the manual time required to get a virtual server environment up and running. Once the virtual platform is optimized, it is easier to consolidate workloads due to the smaller footprint; smaller system; fewer licensing fees; and data-consolidation capabilities.

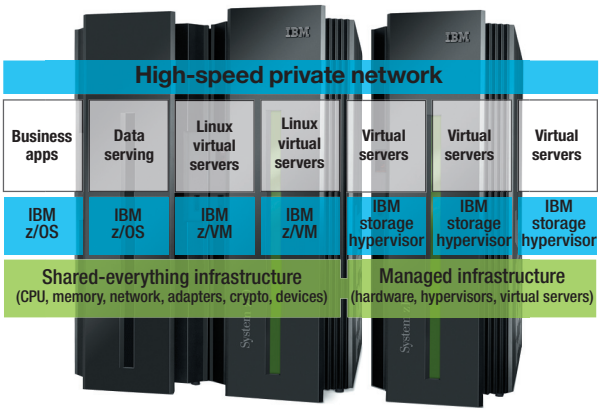

Figure 2: Leverage a mainframe environment for IT optimization, workload consolidation and cloud computing.

Choosing IBM security for mainframe cloud computing

To optimize enterprise security, there needs to be a high level of planning and assessment to identify risks across key business areas. This security framework includes people, processes, data and technology throughout one's entire business continuum. This holistic approach can facilitate a more business-driven security blueprint and strategy that can act as an effective shield of defense for the entire organization.

IBM can help. Our security solutions provide comprehensive, end-to-end, integrated security capabilities on mainframes, enabling enterprises to consolidate their security management and to leverage the mainframe as their enterprise security hub.

Figure 3: Treat security holistically using the IBM Security Framework.

IBM Resource Access Control Facility

IBM Resource Access Control Facility (RACF®) is a premier product for securing the most valuable corporate data. Working closely with the operating system, IBM's industry-leading licensed program can improve data security by protecting vital system resources and controlling what users can do on the operating system. RACF grants access only to authorized users of the protected resources. After identifying and authenticating the user, it controls the interaction between the user, system resources, communications capabilities, programs and applications. It also provides detailed audit and administrative capabilities.

IBM Security zSecure suite

IBM Security zSecure™ suite provides cost-effective security administration, improves service by detecting threats and reduces risk with automated audit and compliance reporting. The following tools, in particular, can enhance mainframe cloud environments:

- **Security zSecure Audit—**Compliance and audit solution enables users to automatically analyze and report on security events and detect security exposures
- **Security zSecure Admin—**Enables more efficient and effective RACF administration, using significantly fewer resources
- **zSecure Manager for RACF z/VM—**Provides combined audit and administration for RACF in the virtual machine (VM) environment

Tivoli Federated Identity Manager (for Linux on System z)

IBM Tivoli® Federated Identity Manager is a standards-based, access-control solution for federated single sign-on and trust management in web services and service-oriented architecture (SOA) environments. It handles all the configuration information for a federation—including the partner relationships, identity mapping, identity token management and more.

Tivoli Identity Manager (for Linux on System z)

IBM Tivoli Identity Manager is an automated and policy-based solution that manages user access across IT environments, whether in a closed enterprise environment or across a virtual or extended enterprise. Through the use of roles, accounts and access permissions, it helps automate the creation, modification and termination of user privileges throughout the entire user lifecycle.

Tivoli Access Manager for e-business (for Linux on System z)

Tivoli Access Manager for e-business software is a highly scalable user authentication, authorization and web SSO solution for enforcing security policies over a wide range of web and application resources. It centralizes user access management for online portal and business initiatives.

IBM Security Key Lifecycle Manager (for z/OS)

IBM Security Key Lifecycle Manager for z/OS manages encryption keys for storage, simplifying deployment and maintaining availability to data at rest natively in System z mainframe environments. It also simplifies key management and compliance reporting to protect data privacy and comply with security regulations.

IBM InfoSphere Guardium Database Security

IBM InfoSphere® Guardium® Database Activity Monitor provides a simple, robust solution for continuously monitoring access to databases and automating compliance controls in heterogeneous enterprises. The solution prevents unauthorized activities by privileged insiders or hackers while monitoring end users to identify fraud without any changes to databases, applications or impacting performance. Use this solution to deploy centralized and standardized controls for real-time database security and monitoring, fine-grained database auditing, automated compliance reporting, data-level access control, database vulnerability management and auto-discovery of sensitive data.

IBM Proventia Server Intrusion Prevention System (for Linux on System z)

IBM Proventia® Server Intrusion Prevention System for Linux uses host firewalling and deep network packet inspection to identify and block thousands of known and emerging threats, targeting vulnerabilities across operating systems, client applications and web applications—all while providing real-time situational awareness and intelligence to security administrators.

Conclusion

As economic issues drive focus on reducing operational costs, and as security needs rise, the opportunity to leverage the mainframe to deliver operational efficiencies, along with excellent security, is clear. This is particularly true in virtualized environments, where mainframes have proven to be strong, secure foundations on which to build cloud infrastructures.

System z can help protect key data and essential, mission-critical applications, while enabling users to virtualize and share these components in a flexible, secure environment. Take advantage of inherent System z efficiencies to deploy a usable, scalable virtualized environment that can provide enhanced availability, performance and cost-effectiveness.

For more information

To learn more about IBM System z cloud computing, contact your IBM representative or IBM Business Partner, or visit http://event.on24.com/r.htm?e=322059&s=1&k=42285CDCC0D5EA69BC2C885FB5F2C394 to access the webcast, "Consolidated Security Management for Mainframe Clouds."

About IBM Security

IBM's security portfolio provides the security intelligence to help organizations holistically protect their people, infrastructure, data and applications. IBM offers solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. IBM operates the world's broadest security research and development organization and delivery organization. This comprises nine security operations centers, nine IBM Research centers, 11 software security development labs and an Institute for Advanced Security with chapters in the United States, Europe and Asia Pacific. IBM monitors 13 billion security events per day in more than 130 countries and holds more than 3,000 security patents.

For more information on IBM security, please visit: **ibm.com**/security

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

Produced in the United States of America
February 2012

[1] IBM Security Solutions Executive Summary, "IBM X-Force 2011 Mid-year Trend and Risk Report: CIO Security Priorities." September 2011. The complete report can be accessed here: http://www.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&appname=SWGE_WG_WG_USEN&htmlfid=WGL03009USEN&attachment=WGL03009USEN.PDF

Please Recycle

TIW14125-USEN-00