White paper
June 2009

Securing a dynamic infrastructure

Contents

Introduction

A dynamic infrastructure is one that is designed to enable today's instrumented, interconnected, and intelligent world, helping clients integrate the components of their business with a flexible, secure and seamlessly managed IT infrastructure. With this infrastructure, organizations can deliver superior business and IT services with agility and speed, while addressing the day-to-day operational needs to improve service, reduce cost and manage risk. A dynamic infrastructure enables an organization to realize value through service management, asset management, virtualization, energy efficiency, business resiliency, information infrastructure, and security—which is the focus of this white paper.

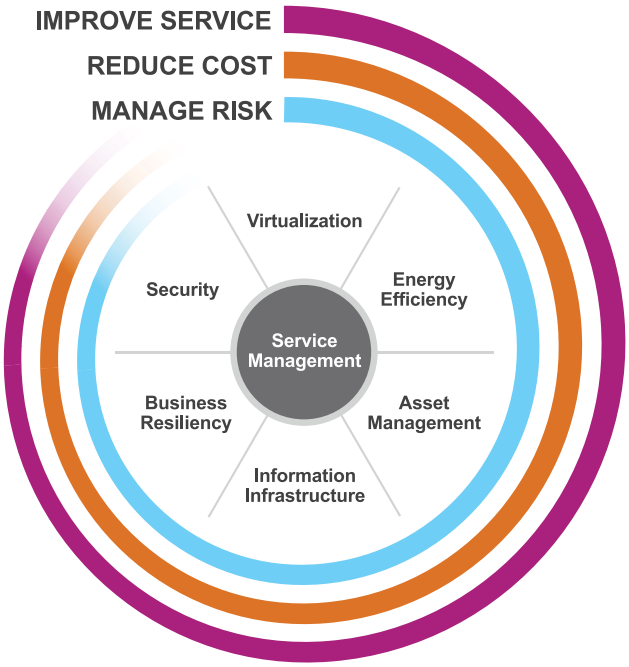

Figure 1: A dynamic infrastructure enables an organization to realize value—improving service, reducing cost, and managing risk through service management, asset management, virtualization, energy efficiency, business resiliency, information infrastructure, and security initiatives.

In order to successfully develop a dynamic infrastructure, organizations must take a new approach to security—transcending traditional security approaches to achieve a highly flexible and adaptive security strategy that can enable a more dynamic organization. The very instrumentation, interconnectivity, and intelligence that powers the new enterprise requires a comprehensive and sustainable security foundation in order to succeed—as well as to protect the organization from today's new security risks.

> *"Our security systems are vitally important. By working with IBM we're developing a state-of-the-art solution with built-in intelligence, which is agile enough to stand the test of time"*
>
> — Chief Executive at The All England Lawn Tennis and Croquet Club

Security and the dynamic infrastructure

The dynamic enterprise and new models of business computing—many designed to reduce organizational complexity and enable organizational agility—have introduced a wide range of new security concerns, including:

- *New technology—Virtualization and cloud computing adoption intended to reduce IT complexity and cost can reduce visibility into the overall risk posture, creating a more complex security challenge. For example, new development technologies such as Web 2.0 and service-oriented architecture (SOA) are becoming increasingly widespread and can introduce new threats such as SQL and iFrame injections and cross-site scripting due to coding errors that otherwise might not occur.*
- *Ubiquitous wireless access—Widespread use of mobile platforms and applications is forcing new means of user identification and information access but can have gaps in security capabilities.*
- *Increased demands on supply chains—A supply chain is only as strong as the weakest link, meaning that all partners must be operationally strong and shoulder their share of responsibility for risk and compliance.*
- *Client expectations of privacy—Data protection must be integrated into the infrastructure, processes, and applications in order to maintain privacy and compliance.*

Highlights

Given the operational complexity and the shared nature of dynamic infrastructure, it is critical that the security design fits the intended use.

The ability of an organization to thrive in today's world requires an organization to understand and embrace factors such as these in order to innovate and grow. However, without considering the security implications of these issues, business activity can come to a halt due to gaps in security that cause business disruption or regulatory non-compliance. And certainly, if security measures are implemented as an afterthought, the risk of this happening is increased significantly. Security that is built into an organization's infrastructure from the very beginning can help mitigate risks, while the lack of these security measures can impact business activity, agility, and business transformation. For that reason, leading organizations are building security into the foundation and processes of their dynamic infrastructures.

Additionally, given the operational complexity and the shared nature of a dynamic infrastructure, it is critical that the security design fit the intended use. The business risks for a given kind of workload may require a specific set and quality of security controls and compliance measures. If the security design for a dynamic infrastructure is not aligned with the business risks of the workload, the infrastructure cost savings gained by the flexibility of dynamic infrastructure will likely be offset by the risks and costs of major security incidents or non-compliant business operations. Effective security designed to reduce the complexity of addressing threats, compliance, and business needs allows organizations to:

- *Enable business change through a foundation of flexible security controls.*
- *Deliver improved agility and cost-effective control over their risk posture.*
- *Reduce the complexity of security controls.*
- *Proactively monitor and protect against internal and external threats.*
- *Meet operational requirements to retain and protect information and address compliance measures.*

The IBM Security Framework

In order to address the challenges and opportunities of the dynamic infrastructure, the IBM Security Framework provides security solutions across the organization in all the areas of potential risk–giving organizations the ability to assess their environment, prioritize their business needs and security requirements, and implement security solutions that allow the organization to be highly flexible and secure. The IBM Security Framework is composed of five elements that address security governance, risk management, and compliance through professional services, managed services, and hardware and software solutions.

Figure 2: The IBM Security Framework helps manage risk end-to-end.

> *"Streamlining and automating access and administration processes is driving significant savings and productivity improvements while strengthening security controls."*
>
> — Terry Escamilla, Ph.D., Distinguished Engineer, CTO IT Security, Office of the IBM CIO

People and identity

Organizations must address an array of challenges related to people and identity. For instance, businesses face growing risks related to ineffective access control when disparate, disconnected processes for identity and access management leave security gaps in the organizational infrastructure. Costly and time-consuming processes related to user management, user rights changes, and help desk operations can also pose a problem if these processes are not integrated across the organization. Furthermore, employees must be able to access information and applications on demand in order to do their work, so issues with access necessarily degrade employee productivity. Finally, due to the growing demand for regulatory compliance and reporting, companies are required to meet an increasing number of compliance initiatives without limiting the resources available for essential activities.

Implementing solutions to address these issues can benefit organizations in numerous ways. First, they can help organizations reduce cost, increase efficiency, and enable audit readiness in environments where the user lifecycle must be carefully managed. They can also decrease the risk of internal fraud, data leakage, and operational outages. They support the shift from traditional brick and mortar to the delivery of online services to users, customers, and partners across the globe. And they can improve the end-user experience and productivity while maintaining security with Web-based business applications, such as by enabling advanced features like single sign-on—a technology which allows highly flexible capabilities for users to access applications within their organization, between organizations, and on the Web.

Highlights

Web-based applications and service-oriented infrastructures can vastly improve productivity and flexibility, but they can also open companies up to risks and unintended exposures that require new levels of information security.

Data and information

Businesses face a number of issues related to data and information. Every breach has negative consequences for a business. Companies must consider the impacts of the threat that information stored on databases, removable media or backups could be lost or stolen. And they must be able to protect information to prevent damage to their reputations and profits while still enabling appropriate levels of access for the people who need it in order to perform their jobs. Because security issues are both internal and external, organizations must protect against unintentional misuse of information by employees as well as by malicious outsiders and professional hackers. Businesses must also deal with the challenges of inconsistent data policies and unstructured content, as well as managing the threat of legal, regulatory, and ethical exposures including privacy.

New technologies provide far-reaching benefits to organizations but also introduce new threats. For instance, Web-based applications and service-oriented infrastructures can vastly improve productivity and flexibility, but they can also open companies up to risks and unintended exposures that require new levels of information security, including measures for identifying application vulnerabilities, monitoring, access management, privacy, and encryption. Certainly in cloud-based computing environments, and in particular environments where shared data pools exist, the issue of data security is critical; understanding where the data is located, who can access it, workload priorities, and security requirements of that workload are essential elements of an overall plan.

In addition to increasing the ability to meet audit and compliance mandates and response to litigation, comprehensive security solutions can provide a cost-effective means of meeting retention, discovery, and legal hold requirements. They can help provide assurance that information is available

Highlights

to the right people at the right time and that it is not inadvertently or intentionally taken, leaked, edited, or damaged. This enables secure collaboration inside and outside of your organization. Finally, they can help decrease the complexity of security controls across the enterprise, while helping to ensure information integrity and reliability.

Application and process

Applications present a wide range of security issues that companies must address. Web applications are the primary target for hackers seeking to exploit vulnerabilities and as the number and complexity of Web applications grows, so do the number of vulnerabilities introduced into your Web environment. Companies must be aware that current defenses may not protect against attacks on new and existing applications. Poor security configurations and development practices can also expose clients to business loss.

Another critical issue is meeting industry and regulatory requirements. If your organization is legally bound to protect the privacy and security of personally identifiable information and hackers gain access to this sensitive information, you risk being noncompliant with a number of mandated global legislation and industry requirements. Organizations need automated solutions that can identify, validate, and report on application security vulnerabilities and document the status of their compliance. With massive information influxes, organizations must secure information that may inadvertently be exposed to contractors, outsourcers, and others with access to development and test environments. Protecting these environments can become extremely complex, and companies must be prepared to manage the costs of identifying and repairing any security defects. Best practices show that companies need to address threats holistically throughout each application's lifecycle–from development and continuing maintenance through end of life. Organizations can reduce long-term security costs by focusing on building security into application development and delivery, instead of retrofitting it after the fact.

Best practices show that companies need to address threats holistically throughout each application's lifecycle—from development and continuing maintenance through end of life.

> *"With new techniques for Web attacks continuously evolving and becoming more complex, it becomes extremely difficult for anyone to monitor applications without an automated process."*
> — NAV CANADA

Solutions designed to address these challenges can also enable organizations to assess and monitor enterprise-wide security policy compliance, which can reduce the risk of outages, defacement, and information theft associated with Web applications. Application security solutions can help provide improved compliance with industry standards and regulations such as Payment Card Industry (PCI), the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), the European Directive on Data Privacy, and the Federal Information Security Management Act (FISMA). They can also help improve an organization's ability to securely integrate business-critical applications and to automate testing and governance to reduce long-term security costs.

Network, server, and end point

Threats to businesses have grown both in sophistication and in number. Primary concerns include the mass commercialization and automation of threats for financial gain. Hacker techniques such as parasitic and stealth attacks can cause extreme damage in the event of an incident. Organizations must be equipped to manage new threats, such as phishing, with an integrated approach to threat and vulnerability management, even as IT security resources are stretched thin. And organizations seeking cost efficiencies through virtualization and data center consolidation must understand the inherent risk implications and implement security solutions that are aligned with corporate risk tolerance and that minimize impacts to business performance and agility.

Highlights

Effectively handling security issues is vital to maintaining consumer confidence, brand image, and business productivity.

The effective handling of security issues is vital to maintaining consumer confidence, brand image, and business productivity. Organizations must strengthen weak application controls, heighten skills to monitor and manage security inputs, and improve their ability to capture forensic evidence. Moreover, they must be prepared for the compounding costs of managing an ever-increasing array of security technologies, data and information sources, archives, and backups. Ongoing concerns also include being able to detect security breaches caused by privileged access misuse, and being able to minimize downtime from incidents. With the increasing volume of security incidents, operations must rely on sophisticated state-of-the art analysis and automated reporting and alerts that allow operations staff to prioritize exposures and focus on critical threats.

Effective solutions to these security issues can help businesses reduce the cost of ongoing security management, improve operational availability, and help assure performance according to service level agreements. Furthermore, they can help increase productivity and availability by decreasing the risk of virus, worm, and malware infestations, decrease the volume of incoming spam, enable drill down on specific violations to improve resolution, and readily show the status of compliance with regulations.

Physical infrastructure

Physical infrastructures continue to pose their own unique security challenges. Theft and fraud can have catastrophic effects on the bottom line. Companies are obligated to prevent crime and protect assets by implementing tools to monitor and analyze customer behavior. Additionally, businesses must tackle threats that exist inside their organizations. They need tools that can monitor

Highlights

Digital video surveillance solutions can provide automated monitoring, assessments, and video data. They can also provide alerts for unusual activities and tripwires around key physical assets.

employees to help prevent fraud and theft, and tools that can help improve employee training. For example, digital video surveillance solutions can provide automated monitoring, assessments, and video data. They can also provide alerts for unusual activities and tripwires around key physical assets.

By responding proactively to these challenges to the physical infrastructure with effective security solutions, organizations can prevent information loss, fraud, and theft; meet statutory requirements; improve inventory management; safeguard their reputations; and improve employee and customer safety. Some organizations will integrate their physical security and logical security systems, for instance using employee smart cards, for additional operational efficiencies in the future.

Dynamic infrastructure in action—the IBM advantage

IBM offers dynamic infrastructure solutions that are flexible, scalable and secure—bringing all of the elements of securing the enterprise together through products and services. With the IBM Security Framework, organizations gain the advantage of having end-to-end security coverage regardless of organization size, location or industry segment. Through comprehensive security assessments, design, security lifecycle methodologies, and security solutions—all backed by industry-leading security research, development, and expertise—organizations are able to manage the risks and compliance mandates associated with technology and a range of business workloads. IBM security can help ensure that the dynamic infrastructure is ready to securely support organizational innovation and growth.

For more information

To learn more about the comprehensive suite of IT security solutions offered by IBM, contact your IBM sales representative or IBM Business Partner, or visit **ibm.com**/security

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

Produced in the United States of America
June 2009

Recyclable, please recycle

GMW14022-USEN-00