

## **Keep Your IT Infrastructure and Assets Secure**



---

## Contents

---

- 2 *Executive overview*
- 4 *Monitor IT infrastructure to prevent malicious threats*
- 5 *Protect IT assets and information from unauthorized access*
- 7 *Defend infrastructure, confidential data, applications and services*
- 9 *Summary*

### Executive overview

More business transactions occur electronically every year, and mid-sized organizations are retaining a growing volume of sensitive data. This data is available to an expanding user base, including employees, trading partners, suppliers and customers. IT infrastructures are more extensive, more complex, more distributed—and more accessible. This accessibility is making organizations susceptible to attacks and intrusions from ever-increasing and evolving threats. Hybrid threats and sophisticated, profit-driven hackers are increasingly bypassing traditional security defenses like firewalls and anti-virus scanning.

When an attack compromises data, an organization faces customer service issues and lost revenue, data and productivity, some of which might be unrecoverable. In many industries, there is also the requirement to retain data to comply with government regulations and audits—losing this data to an external threat or insider attack could create severe consequences to your bottom line and reputation in the form of fines or even the closing of your business. In a recent McAfee poll of 1,400 IT professionals with at least 250 employees in their companies, one-third said that a major security breach could put them out of business.<sup>1</sup>

With so much at risk, it would be logical to assume that companies are taking great care to make sure that their data, systems and IT infrastructure are protected from malicious threats. However, this is just not so. Most companies have only basic protections in place—simple solutions such as VPNs, firewalls, anti-virus software and spyware detection. According to a recent Information Week article, most IT managers in mid-sized companies say they are ill-prepared when it comes to systems and security management and that they are not confident in their safeguards.<sup>2</sup>

There are numerous reasons why so many companies do not have adequate protection from external and internal malicious threats. For mid-sized companies, the most common reasons are a lack of expertise and tools that

*“A large proportion of security execs admitted they’re not in compliance with regulations that specifically dictate security measures their organization must undertake or risk stiff sanctions, up to and including prison time for executives.”*

—Alan Holmes, “The Global State of Information Security 2006,” CIO, September 15, 2006<sup>3</sup>

are required to address today’s security challenges adequately and the belief that hiring additional IT personnel or consulting staff is too expensive and too time-consuming for the average mid-sized company’s budget.

At the same time, companies are presented with a confusing array of solutions that are supposed to be comprehensive but in reality do not provide the protection necessary to keep not only systems, data and networks safe from attacks, but also investments and brand.

IBM understands the challenges that mid-sized companies face when they try to make their IT infrastructures more secure. IBM IT Security solutions for mid-sized businesses deliver effective, easy-to-manage and affordable security capabilities that:

- Protect business-critical information
- Make information about security available on demand
- Can readily adapt to ever-changing threats
- Can help ensure that compliance requirements are met

Our solutions help companies secure their IT infrastructure by:

- Monitoring IT infrastructure to prevent malicious threats
- Protecting IT assets and information from unauthorized access
- Defending infrastructure, confidential data, applications and services

Using these solutions and drawing on the knowledge of IBM Business Partners, you can understand where you are vulnerable and protect your networks and critical information at several levels to reduce the risk and costs associated with a security breach. These solutions are designed and priced for mid-sized companies that are seeking exceptional performance but also want applications and tools that are easy to install, use and manage—and help from experts. This paper describes these solutions and how they meet the requirements for a secure IT infrastructure.

### **Monitor IT infrastructure to prevent malicious threats**

Today's hackers are more technology savvy than ever. Even less experienced intruders are finding ways to bypass common security mechanisms—such as patches, firewalls, VPNs and anti-virus updates—to breach or damage Web sites, applications and infrastructures. They are attacking applications at multiple levels and using wireless access points to gain unauthorized entry.

In a secure IT infrastructure, virus, spy ware, spam and hacker intrusions and the risk of unauthorized access to assets and information are minimized by proactively monitoring and blocking threats to the IT environment from external and internal invasions. IBM and our Business Partners provide a set of solutions designed to help you monitor and protect your IT infrastructure.

To monitor your systems and networks effectively, you need to know where the weaknesses in your IT environment are. IBM Express Vulnerability Assessment can help you identify your weak points and define ways to reduce risks. IBM experts assess the security of your Web-based systems—and the potential business impacts of security breaches. The experts then present a final assessment report that ranks IT weaknesses as high, medium or low risk. The solution has worldwide scalability, too—our consultants can reach around the world for standardized evaluation at all sites.

Another step in safeguarding your IT environment is to address weaknesses before they can be exploited and to have comprehensive preemptive protection against unknown threats. IBM Express Managed Security Services for Web Security features anti-virus and anti-spy ware services and URL filtering. These services monitor Web traffic and block viruses or spy ware from being downloaded as part of a Web page. The IBM Proventia® Network Intrusion Prevention System automatically blocks malicious attacks while preserving network bandwidth and availability. In addition to ensuring business uptime, this solution helps businesses comply with regulatory mandates and industry standards.

Monitoring your network and systems also means watching for unauthorized users on your property that might be trying to gain access to information. IBM Consulting, Integration and Deployment Services for Surveillance and Security provides services—ranging from assessment, strategy and architecture to deployment—and integrated security applications running on a modular architecture.

The IBM solution goes beyond the obvious components for monitoring your infrastructure. To help you assess the impact of regulatory changes, establish a flexible software delivery process, plan and execute risk mitigation strategies and generate the documentation necessary to help pass audits, we offer IBM Rational® ClearQuest®. Also, IBM Secure Perspective for System i™ helps you define an understandable security policy using natural language, so that it is meaningful for all parties in your business. It then implements your system security settings, demonstrates compliance to your policy and reports on your compliance.

### **Protect IT assets and information from unauthorized access**

Access to sensitive data has expanded far beyond the walls of organizations. At any given time, employees, trading partners, suppliers and customers all might be connecting to one or more of your company's data repositories. This interconnectedness affords you many benefits, but it also introduces a great deal of risk.

To try to control access, most companies are introducing processes such as more passwords and other identity recognition tools. However, by doing this, they risk affecting user productivity. For example, employees and other users have so many passwords that they cannot always remember them, resulting in lost time and effort spent contacting the party responsible for resetting the password. There are other, potentially more serious risks. Consider what might happen if one of your employees keeps passwords in a PDA or day planner and then leaves it at a public place like a coffee shop. Access to your proprietary and sensitive information is compromised.

IBM IT security solutions for protecting assets and information from unauthorized access deliver effective, easy-to-manage and affordable tools that keep business-critical information out of the hands of the wrong people while streamlining user access. Using these solutions, organizations protect their networks and critical information at several levels to reduce the risk and costs associated with a security breach without sacrificing user productivity.

Identity management is a key component of this IBM solution. IBM Tivoli® Identity Manager Express is an automated identity management solution designed especially for mid-sized organizations, supporting up to 5000 users. It can help you manage an increasing number of users with fewer resources by establishing a central point to manage user rights. To advance your identity management, compliance and authentication initiatives, IBM Tivoli Access Manager for Enterprise Single Sign-On provides single sign-on for all your applications without a lengthy and complex implementation effort. The architecture supports your technical requirements and computing environment and integrates with Tivoli Identity Manager Express.

Controlling access also means patching and protecting system flaws that could compromise your business. Keeping your sensitive information safe requires a solution that combines vulnerability management with preemptive blocking techniques to optimize protection. With IBM Proventia Network Enterprise Scanner, you gain detailed visibility into system vulnerabilities, you can prioritize and assign ownership to risk-reducing activities, you can organize and track remediation tasks and you can generate reports that demonstrate the successful results of your work.

Unauthorized users often exploit e-mail systems to gain access to your information and documents. You need to keep malicious e-mailers out while retaining e-mail correspondence for legal purposes and compliance. IBM CommonStore is a family of e-mail archive management products used to help mid-sized companies protect their critical business assets from the access issues created by the proliferation of e-mail. IBM Content Manager goes one

*“The average fraud scheme continues for 18 months before being detected.”*

—Association of Certified Fraud Examiners, “2006 ACFE Report to the Nation on Occupational Fraud and Abuse.”<sup>4</sup>

step further, helping you use your digital information for maximum effect while ensuring that only authorized users have access to your content.

From multimedia to text, this solution supports a range of information formats and makes content from multiple applications and workgroups available only to those granted access to that content.

#### **Defend infrastructure, confidential data, applications and services**

Watching and monitoring your systems and infrastructure and managing user access to them are similar to having a lookout in a tower and a drawbridge controlled by a keeper to protect a castle. However, without a moat and several layers of walls, the castle isn't completely safe. The same can be said for your infrastructure, confidential data, applications and services. You need more than a lookout and a gatekeeper—you need strong protection that will block any attempts by unwanted intruders to attack. You also need to take it one step further, and put protection in place that can stop attacks from the inside.

The IBM IT security solutions for defending your infrastructure, confidential data, applications and services proactively block internal and external threats so that your company can keep running if there is a security incident. They also speed the detection and reaction time.

A favorite target of attack is your network. Hackers and automated network sniffers constantly scan the Internet for vulnerable systems. And insufficiently encrypted traffic can expose your confidential information. IBM Express Managed Security Services for Firewall and VPN is a managed service that helps you protect your network while reducing maintenance requirements and costs. It provides IBM hardware that can be set up easily at your location with help from the IBM Help Desk or an IBM Business Partner and professional management. IBM Lotus® Mobile Connect™ protects your wireless communications by creating a mobile VPN that encrypts data over vulnerable wireless LAN and WAN connections so that your mobile employees can access enterprise resources. For added defense, IBM Proventia Network

Multi-Function Security appliances stop all types of Internet threats before they penetrate your network and IBM Proventia Network Intrusion Prevention System delivers uncompromising protection for every layer of the network, protecting your business from both internal and external threats.

As mentioned in the previous section, another source of threats are the viruses and worms that often arrive in e-mails, leaving company assets at risk, jeopardizing compliance and diminishing worker productivity. IBM System p5™ Network E-Mail Security Express helps protect e-mail from virus, spam, phishing and fraud attacks. Powerful enough to protect business-critical e-mail and flexible enough to adapt readily to ever-changing e-mail threats, it features a network e-mail monitor, multiple spam scanning engines and multiple virus detectors to prevent threats from reaching desktops. IBM Express Managed Security Services for e-mail security can also help you mitigate the risks inherent in e-mail communications. This solution provides a comprehensive suite of services that scan and monitor your Internet e-mail before it ever reaches your network—giving you confidence that your company's e-mail is free from harmful or damaging content.

Defending your assets also includes your physical and human assets. IBM Digital Video Surveillance and Security is a comprehensive data capture, storage and retrieval solution that safeguards the privacy of digital content, while providing fast, easy access to footage for authorized personnel. It automatically archives new content and purges old footage and helps security personnel effectively collaborate with internal departments and external agencies during emergencies. It also deters violence, vandalism and other illegal behavior because it can capture and quickly retrieve high-quality images that might be admissible in court.

*“Organizations that reported that their security policies and spending are aligned with their business processes experienced fewer financial losses and less network downtime than those that did not.”*

—Alan Holmes, “The Global State of Information Security 2006.”<sup>5</sup>

### Summary

IT security offers many benefits by building a secure dynamic infrastructure. These include:

- Expansion of your business reach on a global scale
- Trusted electronic relationships with your trading partners
- Improved response to customer needs and marketplace demands
- Strong employee and partner relationships
- Reduced regulatory, financial and legal exposure
- Improved business productivity
- Risk management
- Protection of information assets
- Prevention of problems before they occur

IBM and our Business Partners have put together the IBM Express Advantage portfolio of IT Security solutions to address each type of IT security threat. These solutions are designed and priced specifically to help medium-sized businesses meet the challenges of today’s environment. In addition, several solutions in the portfolio can be hosted at IBM sites to ease your burden of acquiring and maintaining the hardware and software.

Only IBM and its vast network of Business Partners provide a range of solutions to help mid-sized companies improve the security of their IT infrastructures, as well as deep expertise in every industry, extensive local presence, and the support and backing of IBM to deliver simple, affordable, custom solutions.

<sup>1</sup> Sharon Gaudin, “Companies Say Security Breach Could Destroy Their Business.” *InformationWeek*, 24 April 2007. <http://www.informationweek.com/showArticle.jhtml?articleID=199201085>

<sup>2</sup> Sharon Gaudin, “IT Managers Fear Security Breaches Could Cost Their Jobs.” *InformationWeek*, 30 April 2007. <http://www.informationweek.com/showArticle.jhtml;jsessionid=DQIU10DOKTVHWQSNLDRCKH0CJUNN2JVN?articleID=199202582&queryText=king+research>

<sup>3, 5</sup> [http://www.cio.com/article/24979/The\\_Global\\_State\\_of\\_Information\\_Security\\_/1](http://www.cio.com/article/24979/The_Global_State_of_Information_Security_/1)

<sup>4</sup> <http://www.acfe.com/fraud/report.asp>



© 2007 IBM Corporation

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

Produced in the United States of America  
05-07  
All Rights Reserved.

IBM, the IBM logo, System x, Tivoli and WebSphere are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries or both.

Other company, product and service names may be trademarks or service marks of others.

References in this publication to IBM products or services do not imply that IBM intends to make them available in any other countries.

The IBM home page on the Internet can be found at **[ibm.com](http://ibm.com)**