May 2003

Linux security solutions for businesses on IBM @server xSeries

Contents

List of figures

List of tables

Executive summary

The Internet and other e-business technologies have opened the door to a whole new era of business. Unfortunately they have also opened the door to security attacks on information systems. These attacks can cause considerable disruption to business, and can result in significant financial loss, loss of competitive advantage and potential criminal prosecution. Because of the high risks involved, companies are spending a considerable portion of their information technology (IT) budgets on protecting their information assets from the very real threat of security attacks.

As a consequence of the number and wide variety of threats, and exacerbated by the complexity of today's information networks, building an effective security infrastructure presents a significant challenge. It involves the selection, integration, deployment and management of several different security components from multiple vendors. That process requires expertise in a wide variety of highly specialized security disciplines and substantial resources.

Many organizations, especially small- to medium-sized businesses (SMBs), simply do not have the required security expertise and resources in-house. As a result, they need to look for a partner who can help them design, deploy and manage a strong security infrastructure, one built with best-of-breed components and integrated on a robust foundation—*all at an affordable cost*.

Today, many organizations are moving to the Linux® operating system to take advantage of the substantial advantages of an open source operating system over proprietary operating systems, not the least of which is lower cost. According to International Data Corporation (IDC), Linux is the fastest-growing operating environment.[1] Organizations that are moving to Linux are looking for a security solution to support their Linux environment.

This paper discusses the factors driving the demand for increased IT security. It examines the requirements for an effective security infrastructure. It also presents the comprehensive product and service offerings of IBM and its partners that run on IBM @server™ xSeries® systems and Linux. These products and services combine to provide a complete and cost-effective security infrastructure for the Linux environment.

The threat is real

Businesses are experiencing an alarming and growing number of security attacks and resulting financial losses. These security threats pose a variety of serious business risks, including:

- Loss of revenue
- Loss of customers
- Loss of intellectual property (including customer information)
- Loss of tangible property
- Loss of corporate communications
- Interruption of internal/external operations
- Breach of privacy for customers, partners and employees
- Legal liability
- Loss of data and source code
- Damage to brand

Businesses experienced proprietary information and intellectual property losses of between $53 billion and $59 billion from July 1, 2000 to June 30, 2001[2]. The losses are by no means limited to large organizations. According to a recent survey by *Information Security* magazine, 49% of small companies and 70% of medium-sized companies suffered loss or damage due to security issues[3]. Businesses with less than $5 billion in annual revenue reported an average dollar value per incident of proprietary information loss of $332,618[4].

The threat is coming from both outside (hackers, competitors), and inside (disgruntled employees) the walls of the organization. The Internet is a major source of security attacks, especially with the number of Web attacks doubling in 2001. But as serious as the Internet threat is, the largest of number of security breaches come from inside the organization.

Because of the high-stakes risk posed by the threat, businesses are spending a considerable portion of their IT budgets on security. Security presents a particular problem to SMBs because many of them are limited in their ability to dedicate resources to protecting information. Because of the importance of security to their success, however, SMBs, like their large corporate counterparts, are forced make considerable investments in security. In fact, SMBs are spending more per user and per system to improve their systems security environment than are large organizations.

The security issues

Because of the wide variety of threats and the complexity of today's IT networks, implementing a security solution is a major challenge and requires extensive expertise in a variety of highly specialized security disciplines. Threats include malicious code, such as viruses, worms, Trojan horses and denial of service attacks. They also include malicious access by hackers and the stealing of sensitive information by competitors. In addition, threats come from internal users, who surprisingly account for most security breaches.

The five key elements of security

There are five key elements of security, all of which must be addressed by the IT security infrastructure. This section describes the five elements. The following section discusses the requirements for a security infrastructure to address these security elements.

The five key security elements are:

Identity lifecycle management

Identity lifecycle management involves issuing, changing and deleting the variety of user IDs and passwords needed to run multiple applications across multiple platforms and servers. This user identity information provides the basis for the security system.

Access management

Access management provides a centralized mechanism to administer user authentication and the policy to enforce control of user access to resources based on user identity information. Valuable by-products of this heterogeneous access management include single sign-on and the more rapid delivery of secure in-house applications.

Threat management

Threat management identifies real security threats, protects against attacks and reduces the exposure to and the impact of threats. It includes a vulnerability assessment to ferret out weak points in the security chain. It includes intrusion detection to automatically detect and report suspicious activity such as an unauthorized user attempting to enter the system or a known user trying to access resources he or she is not authorized to access. It includes intrusion prevention, such as malicious code protection to identify and isolate malicious code before it does damage. It also includes automatic response to recover from any damage that might have been inflicted.

Privacy management
Privacy management centralizes the defining, monitoring and enforcing of privacy policies across the business to protect the confidential information of customers, employees, business partners and suppliers. It ensures the end-to-end privacy of sensitive data, protecting the data at all points along the access path.

Auditing and monitoring
Auditing and monitoring facilities provide information in the form of logs and messages that can be used by people and computer programs to track, improve and manage information security. In some industries, such as healthcare, auditing is required to comply with government privacy regulations.

Provide end-to-end protection

A security system is only as good as its weakest link. That's why it must provide strong protection end-to-end across the entire access path, all the way from user to server and back. That requires securing both external and internal points of vulnerability along the path, and it means providing protection at all system levels—server, transport, network and application.

End-to-end security begins with the server itself. The server should include security features that prevent it from becoming a weak link in the security chain. End-to-end security also requires that the server operating system should not open up security holes. If holes are discovered, they should be immediately addressed and eliminated through updates to the operating system. Transport security requires that the information be protected from unauthorized access during transit, such as by encryption. Network security requires that the telecommunications equipment not introduce vulnerabilities.

Minimize loss in the event of security breach

Currently, no security system can provide 100% protection. That's why organizations need a mechanism that minimizes loss in the event of a security breach. This requires containing the breach by limiting its sphere of influence. Furthermore, it requires fast recovery, retrieving lost data and bringing information back online quickly. This requires an environment that includes comprehensive backup and recovery software.

Non-intrusive to users

Strong security should not be intrusive to users. For example, users should not have to log in separately to multiple resources using different passwords to get what they need. In addition, the login process should not introduce long delays in gaining access.

Creating a comprehensive IT security infrastructure

Addressing the five elements of security requires implementing a comprehensive IT security infrastructure that includes the following components:

- *Firewall.* Keeps unauthorized users on the Internet from getting through to the organization's internal network while allowing authorized users to pass through. Firewalls can also isolate certain sensitive internal environments, such as research laboratories, from the rest of the company.

- *Virtual private network (VPN).* Provides secure access to sensitive resources and secures the transfer of information across public and private networks, both external and internal. Users are required to authenticate to the VPN before they are allowed to enter it. The VPN encrypts sensitive data passing through it to protect the data from unauthorized access.

- *Virus protection.* Virus protection software intercepts, isolates and where possible repairs known viruses, worms and Trojan horses before they can cause system damage.

- *Intrusion detection.* Intrusion detection systems (IDSs) provide in-depth defense for all networks by monitoring and analyzing network traffic and alerting when suspicious activity is detected.

- *Authentication and access control.* Authentication ensures that the user or application attempting access is indeed who or what he, she or it purports to be, and that the IT resource being accessed is what it purports to be. Access control ensures that users have access to only the resources that they are authorized to use, including limiting user's access to undesirable Web sites.

- *Encryption.* Encodes sensitive data—in-place data as well data in transit over the network—to prevent it from being tampered with by unauthorized people or programs.

- *Security management.* Provides a means of integrating and managing the security components. The system should provide centralized, easy-to-use tools to manage all the elements of the system as an integrated whole.

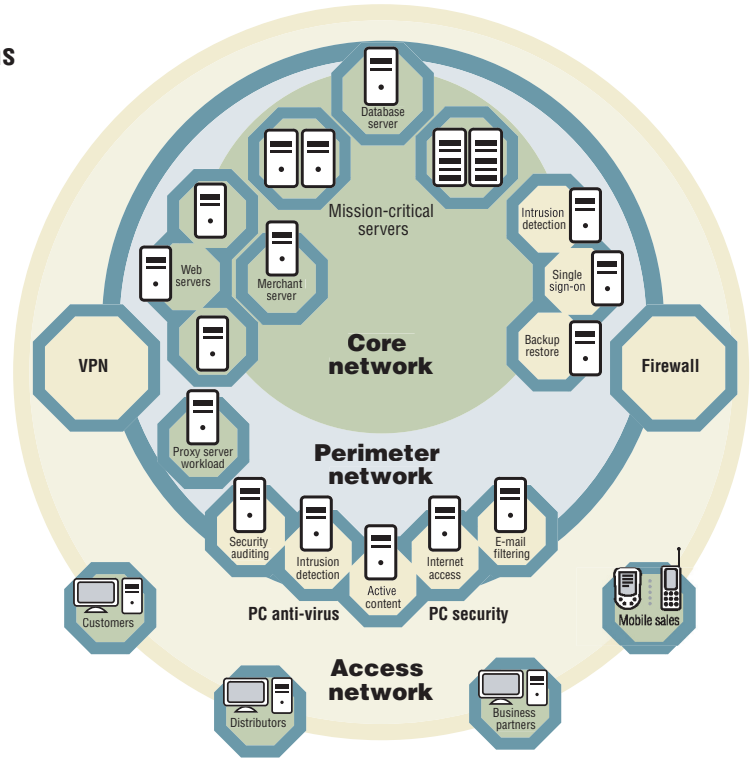


Figure 1. Representative security infrastructure

Legend

Security components:

Information network components:

Table 1. Addressing the five security elements

Security infrastructure component	Security element				
	Identity lifecycle management	**Access management**	**Threat management**	**Privacy management**	**Audit and monitor management**
Security management	•	•	•	•	•
Firewall		•	•		•
Virtual Private Network (VPN)		•		•	
Virus protection			•		•
Intrusion detection system	•	•	•	•	•
Authentication		•			
Encryption				•	

Due to the highly specialized expertise required to develop each of these infrastructure components, no single vendor has developed a security solution that provides all the necessary components. Strong security requires the integration of numerous best-of-breed security products from multiple vendors, into a unified, cohesive and manageable security infrastructure. This task is complicated by the fact that there is a wide variety of security components available, and the number is increasing as current vendors introduce new products and new vendors enter the market. That's why it is important that the security infrastructure support industry standards—such as Check Point Open Platform for Security (OPSEC™), Posix, Linux Standard Base (LSB), Secure Sockets Layer (SSL), IP Security Protocol (IPSEC), and Advanced Encryption Standard (AES)—to enable the organization to take advantage of best-of-breed solutions.

OPSEC is the industry's open, multi-vendor security framework. Currently OPSEC has over 350 partners with over 200 OPSEC Certified solutions, delivering a variety of security enforcement, management, and performance and availability applications. To be designated as "OPSEC Certified," these solutions have passed a rigorous testing process, guaranteeing interoperability.

IBM xSeries servers and Linux—A strong foundation for the IT security infrastructure

IBM xSeries servers running Linux offer an attractive foundation on which to build a comprehensive IT security infrastructure, for a number of reasons, including:

- xSeries servers include a number of security features.
- Because it is an open source operating system, Linux is supported by a huge community of software developers worldwide who are continuously testing and improving its already strong security.
- IBM and its partners offer a range of software security products to run on Linux-based xSeries servers.
- xSeries servers running Linux support popular industry standards enabling the addition of select third-party security solutions including software and appliances, to augment the offerings of IBM and its partners.
- IBM and its partners complement their product offerings with a variety of consulting and managed services to provide complete security solutions to customers.

xSeries server security features

IBM xSeries servers offer an attractive, cost-effective foundation for a security infrastructure with such security features as:

- *Self diagnostics.* Servers are designed to diagnose themselves, alerting the IT staff to potential problems so the staff can respond before detected problems result in service disruption.
- *Self healing.* Servers can detect hardware and firmware faults and contain the effects of the faults within defined boundaries. This is designed to allow the servers to recover from the negative effects of faults with minimal or no impact on the execution of operating system and user-level workloads.
- *Configuration control.* The configuration controls of IBM Director system management software are secured to help prevent an unauthorized user from making configuration changes to create a point of entry. IBM Director configuration controls are supported by xSeries hardware features.
- *Secure remote administration.* Administrators can manage the servers from virtually any place at any time over a secure link that is designed to keep out unauthorized users.
- *Secure remote monitoring.* Administrators can monitor the servers to track server activity from virtually any place at any time over a secure link that is designed to keep out unauthorized users.
- *Lights-out support.* IBM Director provides automated, policy-driven capabilities that prevent unauthorized internal users from entering the system from an unattended xSeries server console.

Linux security features

The open source community has developed a variety of open source security tools for use with Linux. But most importantly, because Linux is an open source operating system, it is supported by literally tens of thousands of developers worldwide. This huge and diverse developer community probes and tests Linux security. When holes are found, the community often sets about to develop fixes. Because of the enormous number of developers working the problems, fixes are often developed quickly, sometimes far faster even than with proprietary operating systems that are dependent upon their vendors' development teams.

In addition, because of them being open source, a company can fix their own Linux security issue instead of having to rely on their proprietary vendor to come out with a fix pack.

The fact that Linux is open source and can be accessed by many developers actually causes more vulnerabilities to be identified compared to proprietary OS. This is because vendors with proprietary systems only have limited staff available to analyze code unless customers report a problem or problems are discovered during code improvements prior to a new release or version of the OS. However, even though more vulnerabilities are identified, fixes are developed very quickly due to the large number of developers working on the problems.

Since December 2000, the National Security Agency of the U.S. Government has also contributed to Linux security and has been producing patches, reports, policies etc. for a Security-Enhanced Linux.

Linux also has already obtained Department of Defense (DoD) Defense Information Systems Agency (DISA) Common Operating Environment (COE) certification. COE is a DoD software security and interoperability specification and is broadly recognized as a critical computing standard across the U.S. Government.

Open source security tools

There is a wide variety of open source security tools available for Linux, including:

- *Intrusion detection.* Snort is an open source network intrusion detection system that has become one of the most popular and successful open source initiatives. Snort performs real-time traffic analysis and packet logging on IP networks. It performs protocol analysis, content searching/matching, and it can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and more.

- *Encryption.* Open SSL is a commercial-grade, full-featured and open source toolkit that implements the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols as well as a full-strength general purpose cryptography library.

- *Authentication.* Open source authentication tools include Open SSH, Pluggable Authentication Module (PAM), and Kerberos.

  Open SSH is a free version of the SSH protocol suite of network connectivity tools. Open SSH encrypts all traffic (including passwords) to help effectively eliminate eavesdropping, connection hijacking and other network-level attacks. Additionally, it provides a myriad of secure tunneling capabilities, as well as a variety of authentication methods.

  PAM is the new industry standard integrated login framework. It is used by system entry components to authenticate users logging into a UNIX or Linux system. It provides plugability for a variety of system-entry services. PAM's ability to stack authentication modules can be used to integrate login with different authentication mechanisms such as RSA, DCE and Kerberos, and thus unify login mechanisms. PAM can also integrate smart card authentication.

  Kerberos is a network authentication protocol that provides strong authentication for client/server applications by using secret-key cryptography. A free implementation of this protocol is available from the Massachusetts Institute of Technology. Kerberos is also available in many commercial products.

- *Recovery.* Advanced Maryland Automated Network Disk Archiver (AMANDA) provides back-up and restore functionality.

Linux distribution companies such as Red Hat and UnitedLinux offer open source security tools integrated with their Linux distributions. IBM works with these partners to integrate their Linux distributions with xSeries servers to help ensure fast and easy deployment.

Building on the foundation

IBM builds on the strong xSeries and Linux foundation to help provide an integrated security infrastructure. The infrastructure can include IBM-developed security solutions, security solutions offered by IBM Business Partners and solutions offered by other independent software developers (ISVs). In addition, IBM and its partners complement their security products with a variety of consulting services and managed services to provide complete business solutions. These services are key differentiators for IBM in helping its customers create secure Linux environments.

IBM Tivoli Security Management

IBM Tivoli® Security Management solutions offer a complete security management environment that is fully supported by IBM services. In addition to providing a number of security services, IBM Tivoli Security Management enables the integration of all security solution components, including those from IBM Linux distribution partners, IBM Business Partners and other ISVs. With IBM Tivoli Security Management, an organization can manage the security components in the infrastructure as a unified, cohesive whole. IBM Tivoli Security Management permits security management based on the organization's security policies. This not only simplifies management, but also reduces the chance for administrator errors that could result in security holes.

IBM Tivoli Security Management solutions help you quickly realize ROI by bringing users, systems and applications online fast, while effectively managing users, access rights and privacy preferences throughout the identity lifecycle. The solutions also help you actively monitor, correlate and quickly respond to IT security incidents across your e-business.

The components of IBM Tivoli Security Management are:

- *IBM Tivoli Identity Manager.* A secure, automated and policy-based user identity management solution to centrally coordinate the creation of user accounts, the workflow for automating the approval process and the provisioning of resources.
- *IBM Tivoli Access Manager.* An award-winning, policy-based access administration and enforcement solution. Access Manager provides elements that secure and provide single sign-on to e-business and enterprise applications, provide enhanced access control capabilities for WebSphere® MQ implementations, and provide enhancements to the security and auditing of Linux operating system administrators.
- *IBM Tivoli Risk Manager.* An integrated e-business risk management solution that is based on the Tivoli Framework. It enables organizations to centrally monitor attacks, threats and vulnerabilities by correlating security alerts across diverse security point product deployments.
- *IBM Directory Integrator.* Provides real-time synchronization between identity data sources enabling the enterprise to establish an authoritative, up-to-date, identity data infrastructure to serve as a platform for business-critical security applications.
- *IBM Directory Server.* Provides a powerful Lightweight Directory Access Protocol (LDAP) infrastructure to serve as a foundation for deploying comprehensive identity management applications and advanced software architectures.
- *IBM Tivoli Storage Manager.* An award-winning data back-up and recovery solution that includes extensive data protection for enterprise resource planning (ERP) data, e-mail and databases. It also provides disaster recovery planning capabilities.

IBM Business Partner security offerings

In addition to IBM Linux distribution partners, IBM Business Partners offer a variety of security solutions for the Linux operating environment. As with Linux distribution partners, IBM works closely with its Business Partners to integrate their solutions on xSeries servers to help ensure fast and easy deployment.

Check Point

Check Point Software Technologies™ is a recognized market leader in both the worldwide VPN and firewall markets. Check Point VPN-1®/FireWall-1® helps enable secure Internet connectivity and provides outstanding protection for corporate resources. Check Point solutions help secure business communications and resources for corporate networks, remote employees, branch offices and partner extranets. The solutions offer excellent price/performance through Check Point SecureXL™ technology, award-winning management with Check Point SmartCenter™, and outstanding ease of use with One-Click technologies. Extending the power of Check Point's solutions is Check Point's Open Platform for Security (OPSEC), the industry's framework and alliance for integration and interoperability with "best-of-breed" solutions from over 350 leading companies.

Rocksteady

Rocksteady Networks, Inc. provides software solutions that deliver security and premium broadband services to users at the edge of the network. With the RocksteadyNSA™ (Network Sharing Application), organizations can proactively authenticate each user before they enter the network environment and then selectively provide access to specific resources and bandwidth based on the user's relationship to the organization. RocksteadyNSA uses credentials provided by IBM Tivoli Access Manager to allocate bandwidth and to provide metering and billing information on a user-specific basis.

Sourcefire

Sourcefire, creators of the original open source Snort intrusion detection system, offers the Sourcefire Intrusion Management System that consists of two components. Sourcefire Network Sensors provides effective intrusion detection by enhancing the proven Snort technology and adding an easy-to-use interface, optimized hardware, powerful data analysis, policy management and forensic capabilities. Network Sensor can monitor all networks, even those that operate beyond Gigabit speeds. The Sourcefire Management Console provides centralized management of remote, distributed sensors and has integrated data management. It manages, correlates and analyzes events data so that the organization can make informed decisions that best protect the network. Sourcefire is an OPSEC-Certified vendor, and integrates many OPSEC innovations into their detection and sensor management capabilities.

Stonesoft

Stonesoft Corporation offers several product lines. StoneGate is a network security solution that combines clustered, high-availability firewall, VPN, load balancing and redundant Internet connections in a single, integrated package. Its powerful centralized management enables distributed policy enforcement to multiple firewall/VPN gateways or gateway clusters. StoneGate includes Stonesoft's patent-pending multi-link technology that enables VPN failover and load balancing of Internet connections. StoneBeat is a software-based high availability and load balancing solution for network security that maximizes the effectiveness and availability of critical network components such as anti-virus protection, e-mail/Web content scanning, malicious mobile code protection servers and intrusion detection network sensors.

Trend Micro

Trend Micro offers several virus protection products for Linux that protect multiple points on the network, including the mail server, file server and Internet gateway. Its ScanMail™ products provide virus protection for Linux, Lotus® Sametime/ Quickplace, and Domino™ Notes. ScanMail for IBM Lotus Notes® is a native Notes application that provides virus protection for IBM Lotus Domino R5, including multiple mailboxes.

Trend Micro also offers ServerProtect™ for Linux, which provides Linux-based servers with comprehensive protection and cleaning against computer viruses, worms and Trojan horse attacks. ServerProtect offers flexible virus scanning options including on-access, on-demand and scheduled virus scanning. The automatic update capability provides consistent and up-to-date protection with the latest pattern and scan engine updates. A Web-based management console allows remote control of the application through a feature-rich interface.

In addition, Trend Micro offers its InterScan Messaging Security Suite™, a policy-based virus protection and content security solution for the enterprise SMTP and POP3 gateway that helps protect against virus outbreaks while preserving information integrity. Customizable relay restrictions and flexible routing features provide easy deployment and integration with existing messaging environments.

Trustix

Trustix offers a comprehensive range of secure turnkey infrastructure solutions—the Trustix Linux Solutions. These solutions include a firewall with VPN combined in a single server and offered in different, highly available versions for the xSeries platform to fit small office through enterprise environments. The solutions also include: a mail server that supports SSL and provides anti-spam and anti-virus protection, a proxy server, a LAN server, a Web server and an intrusion detection solution.

Trustix Linux Solutions are turnkey software solutions comprised of a solution stack with a security-enhanced Linux OS, the infrastructure application, a management GUI and software maintenance automation. All Trustix Linux Solutions are based on open industry standards.

Complete business solutions

Many organizations, especially SMBs, do not have the expertise or resources in-house to design and implement a complete security solution. That involves:

- Security assessment
- Security architecture design
- Selection and integration of components
- Threat management

As a result, it's important that the security infrastructure vendor provide a complete business solution by complementing its security offerings with security consulting services and managed security services. That's why IBM and its partners complement their security products with a variety of consulting and managed services to provide complete business solutions.

Security consulting services

IBM offers security consulting, education, planning and implementation services including security assessment, IBM Tivoli consulting, product specific implementation, cross country and industry solutions such as Healthcare (HIPAA), and wireless security.

Managed security services

IBM customers can opt to be security self-sufficient, or they can use IBM- and IBM Partner-managed services to complement their in-house capabilities. Managed services include:

- *IBM Managed Security Services.* Through these services, IBM helps its customers evaluate current security, detect misuse and violations, respond to incidents, and implement changes to improve defenses.

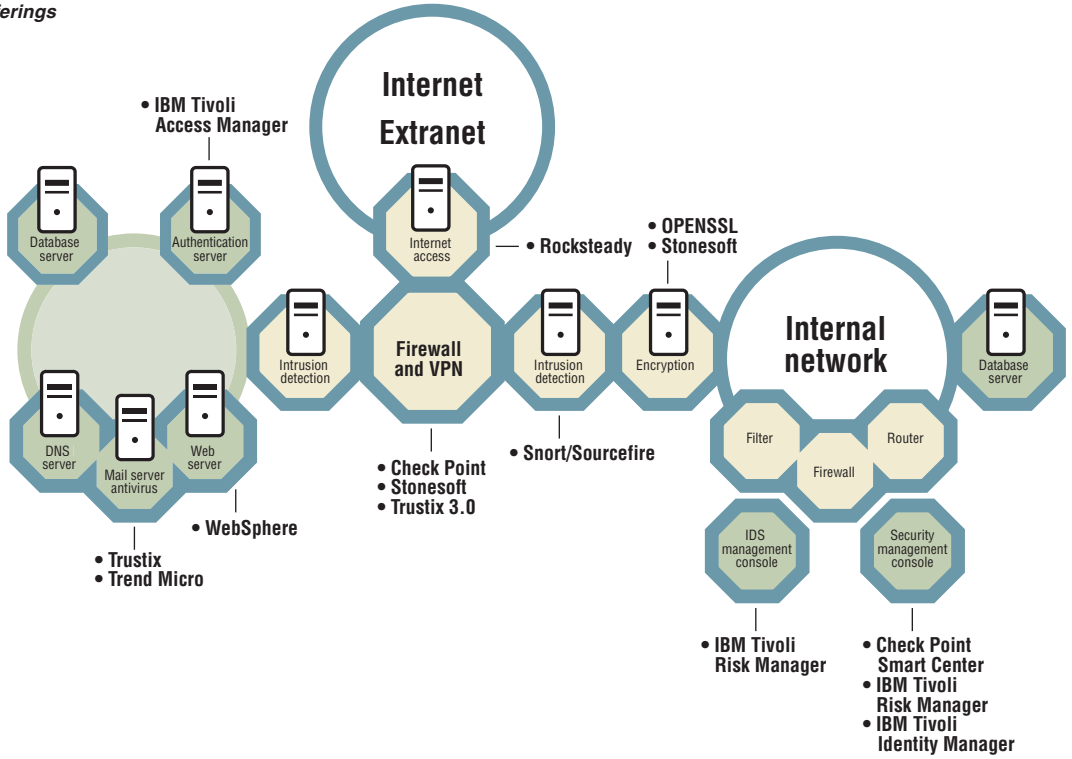
- *IBM Intrusion Detection Services.* Using state-of-the-art intrusion detection tools, IBM intrusion detection services are designed to monitor clients' networks on a 24x7x365 basis. IBM works closely with the client's security team to define and coordinate appropriate responses for accurate and efficient handling of incidents.

- *SecureWorks managed intrusion detection and prevention service.* IBM Business Partner SecureWorks offers a comprehensive managed intrusion detection and prevention service. The service includes SecureWorks iSensor, innovative enabling hardware for the SecureWorks software.

Putting it all together

Using the security components provided and integrated by IBM and its relationship with Business Partners, organizations can implement a strong security foundation that addresses all five elements of security. Figure 2 shows a representative infrastructure built with products offered by IBM and its Business Partners.

Figure 2. Security infrastructure offerings of IBM and its Business Partners



Some real-world examples

Organizations worldwide are taking advantage of the security solutions offered by IBM and its Business Partners. Following are some examples.

Ferarri UK

Ferrari UK is installing five xSeries servers with two Trustix LAN servers, a Trustix Proxy server, a Trustix Web server and a Trustix Firewall. This initial deployment replaces an existing Novell network and supplements an existing Check Point firewall with Trustix Firewall. The deployment augments Ferrari's prior deployment of a Linux-based mail server five years ago. Open source reseller LinuxIT recommended the IBM and Trustix combination to address Ferrari's keen interest in continuing to help reduce IT costs while increasing manageability through Linux-based solutions.

Chris Rooke, IS Manager at Ferrari UK commented, "The Trustix and IBM server solution will eliminate the upgrade costs associated with the Novell approach without any loss of functionality. The Trustix Firewall will supplement an existing firewall strategy and give us the ability to cost effectively and easily manage that firewall locally and remotely."

In the longer term, the company plans to develop a two-tier disaster recovery strategy based on the Trustix Linux Solution and xSeries servers. Rooke noted, "The additional protection we are planning to implement with the Trustix Linux Solution and some of the IBM hardware will provide a complete mirrored environment, which we can swap over to in the event of major disruption localized to the computer room itself."

Columbia Advanced Wireless

IBM and Rocksteady Networks are providing the infrastructure for Columbia Advanced Wireless (CAW) to offer high-speed wireless Internet access to truck drivers at more than 1,000 truck stops throughout the U.S. Rocksteady software loaded on Intel processor-based IBM servers running Linux will enable the truckers to connect to the Internet through 802.11 Wireless Local Area Networks (WLANs) deployed by CAW. CAW will deploy 802.11b or Wi-Fi hotspots at selected truck stops and offer prepaid access cards that function like prepaid calling cards. Drivers can access the Internet using wireless-enabled notebook computers.

For security and excellent performance CAW will deploy the Rocksteady NSA Network Sharing Application and xSeries servers running Linux as the platform for the new Internet access points. Rocksteady NSA selectively determines whether the truck driver is permitted to enter the network and dynamically manages the driver's Internet session based on his or her credentials. Additional capabilities, such as dynamic bandwidth shaping and metering, help provide a high level of network performance by allocating and prioritizing bandwidth usage in real time on a user-by-user basis.

William Read, CEO of CAW said, "We require virtually 100% uptime, and since we don't maintain an IT staff at the locations, we need a highly reliable solution. We tried other solutions that simply were not up to the task of performing reliably in a hostile environment. Fortunately, we have found the integration of the IBM xSeries systems and Rocksteady's Network Sharing Application meets our reliability requirements and provides us the ability to rapidly deploy and easily manage our platforms."

The Sidereus Group

The Sidereus Group develops and hosts rich media applications that tie into robust data backends. Sidereus applications include CNN/SI's *Sideline* and TNT's *Interactive Desktop*. The company also offers a variety of online applications that are available through Web services. Mobile users can access these applications from anywhere using a variety of access devices and still enjoy a consistent personalized environment that follows them around.

The Sidereus Group has installed 12 IBM @server x330s operating in a cluster to host their production environment, and is in the process of migrating all these servers to Linux. Brad Artigue, Director of Technical Services at Sidereus, said, "There are several reasons behind the migration. First is stability. In what we do, reliability is higher for Linux. The second is cost. The third reason is manageability. We find it easier to manage the Linux operating system than anything made by Microsoft."

The production servers are handling about six million hits per month. To provide security for these servers, The Sidereus Group is running the Stonegate firewall from IBM Business Partner Stonesoft Corporation. Artigue said, "The combination of the StoneGate product on Linux on the x330 has been more reliable than anything I've seen in production in years. We have operated StoneGate on the @server platform for 18 consecutive months without a single failure in either hardware or software."

Conclusion

Because of the large and growing threat of security attacks and the resulting high risks, organizations are giving a lot of attention and spending considerable sums of money on securing their IT networks. But many, because of the magnitude of the task of building a security infrastructure and the specialized expertise required, cannot go it alone.

IBM, continuing in its Linux leadership role and working together with other companies, has created a comprehensive portfolio of Linux-based security products and services to help organizations meet the security challenge. IBM has worked with these companies to integrate their security solutions with xSeries servers running Linux to build a comprehensive and cost-effective security infrastructure that can be deployed quickly.

With IBM as a partner, organizations can get to market quickly with their e-business initiatives, and they can do it with confidence, knowing they have a robust security infrastructure in place that helps protect them from the risk of security threats.

For more information on the security offerings of IBM and its Business Partners, visit: **ibm.com**/security.

IBM Systems Group
3039 Cornwallis Road
Research Triangle Park, NC 27709

Printed in the United States of America
5-03

[1] "Worldwide Client and Server Operating Environments Forecast and Analysis 2002–2006," IDC report, September 2002.

[2] "Trends in Proprietary Information Loss Survey," September 2002, ASIS International, PricewaterhouseCoopers LLP and U.S. Chamber of Commerce report.

[3] *Information Security* magazine survey, September 2002.

[4] Ibid.