

# E-Business and the Internet: Meeting the Security Challenge

Safe, Cost-Effective Data Security with McAfee E-Business Server



## ABSTRACT

As companies have embraced the Internet as a business medium, they've discovered that their biggest challenge isn't establishing connectivity, it's the safe and secure transmission of sensitive information. McAfee E-Business Server products present an ideal solution, used by seventy-five of the Fortune 100 to secure and automate Internet file transfers ranging from straightforward spreadsheets to large-scale replacement of legacy EDI supplier networks. These companies choose McAfee E-Business Server because they want a cost-effective, easy-to-implement and use solution that allows them to send and receive many types of files to and from business partners. E-Business Server additionally offers ease and speed of deployment, straightforward integration with existing applications and processes, and widely used, cost-effective PGP encryption technology.

This whitepaper examines the business case for encrypted business-to-business communication, provides a detailed view of E-Business Server's benefits and operations, and makes a detailed cost comparison between E-Business Server and alternatives such as leased lines, virtual private networks, and others. Altogether, the evidence points to what demanding enterprises already know: that McAfee E-Business Server is a top choice for secure, automated transmission of sensitive information over the Internet.

## Table of Contents

<b>I. The E-Business Challenge: Increasing Security to Lower Risk</b>	<b>2</b>
Security Needs Drive the Search for Effective Solutions	2
McAfee E-Business Server: A Capable and Cost-Effective Solution	2
<b>II. McAfee E-Business Server: Meeting Stringent Security and Business Requirements</b>	<b>3</b>
An Introduction to McAfee E-Business Server	3
<b>III. McAfee E-Business Server Product and Technology Highlights</b>	<b>4</b>
How Does McAfee E-Business Server Work?	5
API Enhancements for Windows NT and UNIX platforms	7
Enhancing Productivity and Enterprise Security	7
<b>IV. Other Data Security Alternatives Fall Short</b>	<b>8</b>
Leased Lines	8
Virtual Private Network (VPN)	8
Secure FTP	9
SSL	9
Customized Solutions	9
<b>V. Cost-Comparison Scenario</b>	<b>10</b>
<b>VI. Summary</b>	<b>11</b>
Business	11
Product	11
Technology	11
About McAfee Security	12
<b>Appendix A</b>	<b>13</b>

## I. The E-Business Challenge: Increasing Security to Lower Risk

In the past several years, using the Internet to do business has evolved from a novelty to a mainstream practice. Companies of all sizes and in every industry not only buy and sell goods online; they also service customers and collaborate with business partners. By exploiting the convenience, availability, and worldwide reach of the Internet, many companies have implemented e-business strategies that able them to conduct business around the world, twenty-four hours a day.

While the Internet as a business medium offers unprecedented reach and low cost, data security remains a crucial issue. The following statistics from the 2002 CSI/FBI Computer Crime and Security Survey underscore a harsh reality:

- Ninety percent of the nearly 5,300 respondents (primarily large corporations and government agencies) detected computer security breaches during the 12-month measurement period.
- Eighty percent acknowledged financial losses due to computer security breaches.
- The 44 percent that could quantify these losses reported a total of nearly \$456 million lost as a result of computer security breaches.
- Forty percent detected system penetration from the outside.
- Seventy-four percent of respondents cited their Internet connections as a frequent point of attack.

As alarming as these statistics are, the trend is actually worse—these numbers are all significantly higher than those contained in the 2001 CSI/FBI Survey.

## Security Needs Drive the Search for Effective Solutions

As organizations suffer security breaches and data thefts are perpetrated both internally and externally, many approaches are being used in an attempt to ensure data privacy. These solutions include virtual private networks (VPNs) and similar network-layer approaches, Secure Sockets Layer (SSL) implementation (a transport-layer approach), and customized encryption solutions. While these approaches all have merit, they also have significant shortfalls, including high costs for implementation and ongoing operations, easily penetrated security holes, and inherent vulnerabilities.

## McAfee E-Business Server: A Capable and Cost-Effective Solution

To meet the growing security challenge, forward-thinking, security-savvy companies are entrusting their mission-critical data to E-Business Server™ solutions from McAfee Security, a global leader in data security. McAfee® E-Business Server products use strong PGP encryption technology to protect data stored on the server, in transit over the Internet, and during access by network users. More flexible and lower in cost than alternatives such as leased lines, virtual private networks, and Secure File Transfer Protocol (SFTP), McAfee E-Business Server assures end-to-end information confidentiality, identity authentication, and integrity—allowing e-business operations to flow smoothly, securely, and cost-effectively.

## II. McAfee E-Business Server: Meeting Stringent Security and Business Requirements

McAfee E-Business Server was designed to meet the rigorous requirements of today's competitive e-business environment, providing end-to-end information security without speed degradation or loss of flexibility. It combines superlative data security with strong business benefits, including significant return on investment (ROI), cost savings, compliance with a broad spectrum of legal and partner requirements, and the ability to leverage new technologies for maximum competitive advantage.

### An Introduction to McAfee E-Business Server

McAfee E-Business Server, a fully integrated application-layer solution for encryption, simplifies the process of ensuring end-to-end data security. It protects data by automating encryption, decryption, digital signing, and verification on Microsoft Windows, UNIX, and IBM OS/390 platforms. Encryption plays an essential role in information security, protecting data so that only authorized users or processes have access to sensitive customer and business data. After data has been encrypted by E-Business Server, it can be securely stored, transported over the Internet via FTP or other transport protocols, and processed within the company infrastructure.

Based on the Open PGP standard, McAfee E-Business Server uses trusted public key encryption technology, scrutinized by thousands of the world's leading cryptographers and used by millions. Its 128-bit encryption is regarded as the de facto standard for data protection worldwide. By securing data automatically, companies consistently protect sensitive data, reduce manpower costs and eliminate human interaction errors.

Both IT staff and end users easily utilize McAfee E-Business products. Using a simple command-line interface or natively, within applications in C/C++, Visual Basic, Java, or Perl, developers and administrators can harness E-Business Server to protect data throughout its lifecycle: from its point of origin, to data processing and storage. In deploying the McAfee E-Business solution to end users, McAfee E-Business Client provides an easy-to-use drag-and-drop user interface, allowing PC users

to encrypt and send files to an E-Business Server at another site or partner location.

*McAfee E-Business Server highlights include:*

#### A Versatile, Cost-Effective Solution

E-Business Server is protocol independent and protects data with or without other protective technologies including Secure Sockets Layer (SSL), leased lines, and VPNs (see Section IV for details). It complements current transport protection technologies such as SSL and VPN by adding a layer of security. Thus, companies with sensitive data need neither acquire nor dismantle protective technologies in order to encrypt and store data with E-Business Server.

#### Return on Investment

Inter-enterprise file transfer eliminates the costs associated with the lease and management of dedicated communication lines. McAfee E-Business Server's data compression capabilities help to conserve bandwidth and improve data throughput, speeding processing and minimizing storage space requirements. In addition, E-Business Server's encryption can significantly reduce costs when transferring data.

#### Security at All Points of Access

Not only does data need to be secure when it is transferred from point A to point B. Information needs to be stored securely as well. According to the 2002 CSI/FBI security survey, most data theft and hacker attacks come from inside the corporation; access to information needs to be carefully controlled within the company network as well. McAfee E-Business Server addresses this challenge by allowing encrypted data to be stored and decrypted on demand by appropriate recipients.

#### Protection of Intellectual Property

Theft of proprietary information causes significant financial loss and reduces competitive advantage. McAfee E-Business Server offers the industry's strongest encryption algorithms to protect key intellectual property, including Triple-DES, CAST, IDEA, and AES Cipher Algorithm. With application-level integration and end-to-end encryption of sensitive business data, the security of the overall solution is ensured. The parallel architecture of E-Business Server software can handle multiple processes simultaneously, sustaining high performance.

### Reduced Liability

Businesses that store customer information (e.g., Social Security numbers, credit card numbers, healthcare data, and similar sensitive information) will not only enhance the privacy of their critical business data by implementing McAfee E-Business Server, they will also reduce their liability in the event of a security breach. Whether a company has taken reasonable steps toward preventing security compromises is a key consideration in any security-related litigation.

### Legal, Regulatory, and Industry Compliance

Banks, insurance companies, investment firms, healthcare providers, and other industries are closely governed by a variety of regulatory bodies. For example, the Gramm-Leach-Bliley Act mandates data protection for financial institutions, and HIPAA does the same for healthcare providers. The North American Energy Standards Board (NAESB) has codified in its legislation so that all company members must use PGP technology to encrypt the transaction data they exchange among themselves.

The ability to demonstrate that appropriate steps have been taken to protect the privacy and integrity of customer data, patient records, and other sensitive data is not just good business, it is the law. McAfee E-Business products allow these requirements to be readily met.

### Compliance with Partner Requirements

It is not always practical or possible for every partner in an extended enterprise network to use the same security solution. When selecting a solution to enable secure data transfer, it is critical to choose one that supports Internet standards and protocols, as well as X.509 certificates. This assures wide interoperability with as many partners as possible without requiring extra hardware or software at the partner location.

McAfee E-Business products use trusted PGP encryption for broad interoperability with data partners, allowing information to be safely and universally shared in the extended enterprise. In addition, it maintains company control over security by eliminating exposure to partner VPN tunnels (see Section IV).

---

## Additional Benefits of McAfee E-Business Server

- *Automation ensures consistent security eliminating user intervention and reducing manpower costs*
  - *Highly scalable in both number of partners and size of data exchanges*
  - *Simplifies encryption, allowing data to be protected with fewer errors*
  - *Improves security where most required within applications, storage or transfers*
  - *Avoids e-mail file size limitations*
- 

## III. McAfee E-Business Server Product and Technology Highlights

McAfee E-Business Server products leverage the most trusted technologies available for encryption, authentication, data compression, data integrity, and digital signature. They secure data within automated and batch processes (for file transfer, remote archive, and transactions) and within standard or proprietary applications. Most importantly, McAfee E-Business server solutions protect the privacy of data in storage, during access, and in transit over the Internet, providing true end-to-end security.

McAfee E-Business Server is transfer-protocol independent, allowing companies to add encryption into current processes without changing protocols. With pass phrase-protected, self-decrypting archives, E-Business Server enables users to exchange information without requiring encryption technology on every user's desktop.

## How Does McAfee E-Business Server Work?

Developers or administrators have three choices to protect business data with encryption from E-Business Server:

- 1) Encrypt files interactively using the Windows command prompt to enter encryption commands.
- 2) Create scripts that automate encryption with simple E-Business Server commands.
- 3) Incorporate simple E-Business Server commands within C/C++, Visual Basic, Perl, or Java applications using native APIs for automated encryption (see Section III).

In the case of an FTP transfer, an E-Business Server encrypts data using a recipient's public key to render it unreadable, accessible only by the intended recipient. The data may be digitally signed to ensure its integrity. Data is reduced in size for transport and storage up to

fifty percent by on-board compression; the data is then sent to a recipient FTP server. The recipient FTP server sends the data to E-Business Server, where the data is decrypted and decompressed to make it readable. It is then verified to prove the data has not been altered or corrupted, and processed or accessed by the authorized user with the public key. E-Business Server can also add non-repudiation so a sender cannot deny that the file was sent. This may be required in financial transaction processing.

## End Users Exchange Data Securely with McAfee E-Business Client

McAfee E-Business Client, the end-user complement to E-Business Server, simplifies protecting data in transit and storage with PGP encryption by providing a pre-configurable drag-and-drop user interface. Businesses can quickly configure the McAfee E-Business Client to encrypt and send files to their E-Business Server via

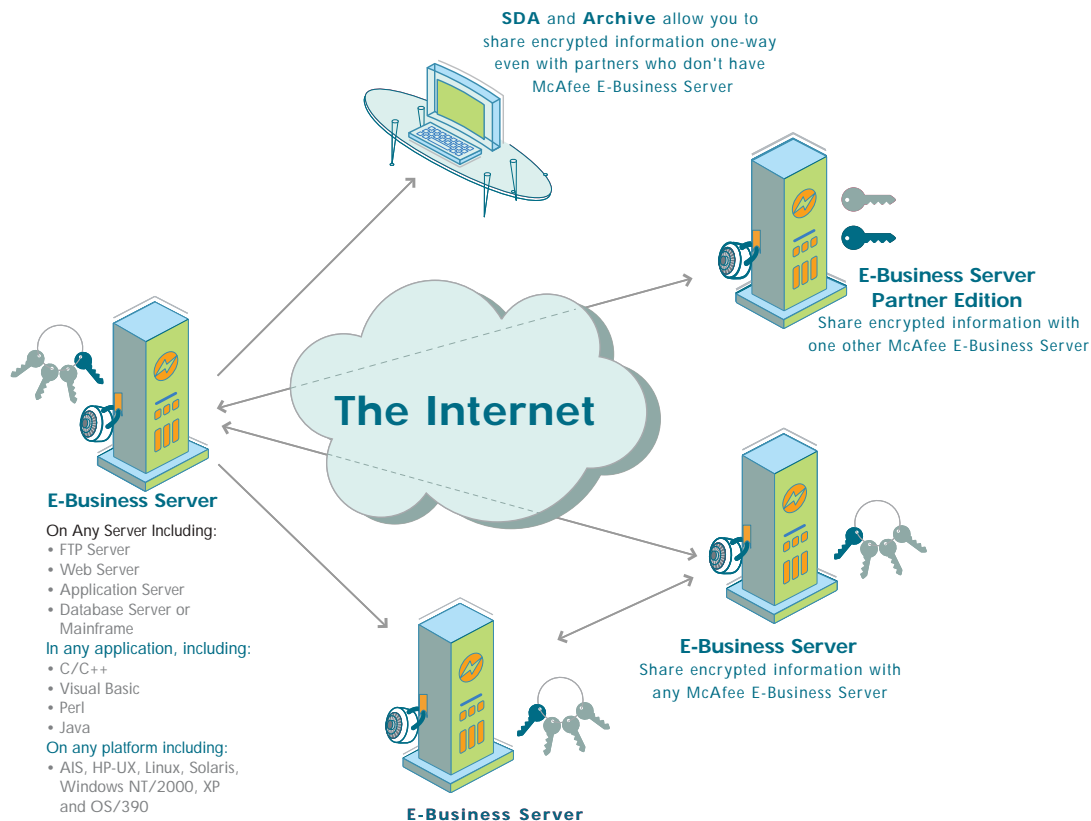


Figure 1. McAfee E-Business Server products provide a versatile, cost-effective way to safely and securely share data with trading partners outside the enterprise, as well as providing an extra measure of data security within.

Simple Mail Transfer Protocol (SMTP) or FTP. The end user receives a simple-to-install, pre-configured user interface into which they drag files to encrypt and send them, or to decrypt files that they receive from E-Business Server. Each partner can brand the user interface to foster customer loyalty and increase usability.

If an end user has multiple partners providing E-Business Clients, a self-configuring drop-down menu allows users to select the appropriate partner, making it easy to exchange encrypted data with new ones. McAfee E-Business Client makes it possible for partners to supply end users with the ability to protect data to meet government, industry, or best practices standards (such as VISA's Cardholder Information Security Program).

Users do not need to have any encryption knowledge to encrypt, sign, decrypt, and verify data. They simply drag a file onto the GUI and confirm with one mouse click. In the background, the file is encrypted and sent to the partner's McAfee E-Business Server. E-Business Client's graphical user interface can have the partner's company logo inserted to make it more intuitive for novice users. Also, the E-Business Client can have a trading network's hub's public key and transport information (FTP server IP address) pre-installed so that files will automatically be encrypted and sent to the proper place. Administrators can update the policy by re-running the administration wizard.

### **Key Technology Benefits**

In addition to strong business benefits, McAfee E-Business Server offers equally compelling benefits from an IT perspective. Highlights include:

- *Application layer encryption* allows E-Business Server to be integrated into thousands of other applications more easily than if an encryption tool kit were used. Tool kits require specialized skills and entail lengthy integrations. With E-Business Server, the tool kit is already built into an application. Applications integrate with other applications more easily than with lower level technology.
- *Multi-platform support* enables E-Business Server to run on a multitude of operating systems, making it easy to implement in heterogeneous environments. McAfee E-Business Server is available for AIX, HP-UX, Linux, Solaris, OS/390, and Windows NT/2000

platforms. Mainframe Linux support is available for SuSE Linux for S/390 and zSeries. Additionally, McAfee E-Business Client supports a wide range of Microsoft Windows operating systems.

Because data can be encrypted on one platform and decrypted on another, customers can implement E-Business Server to work with the computers that already handle data rather than set up dedicated machines with "friendly" operating systems. In a business-to-business (B2B) trading scenario it is not necessary for one party to impose an operating system on another in order to share encrypted data.

- *Fast implementation* of an encryption solution into any back-end process with minimal integration time—typically less than a day—without special programming skills. By leveraging existing FTP capabilities within the enterprise, users can implement E-Business Server software without engaging the IT security department to negotiate VPN support or firewall policy changes. Fast implementation leads to fast return on investment; for example, an automotive manufacturer achieved ROI in just one month with McAfee E-Business Server.

---

### **Defense-Related Designs Leaked**

A French defense contractor believed its designs were being leaked outside the company, despite a strict policy regulating how digital information leaves its premises. They discovered that a computer criminal, working within the company as part of the team, was embedding trade secrets inside images that were posted to the company's external Web site. An outside hacker then stole the secrets directly from the company's home page. This example demonstrates the growing problem of proprietary information theft. In fact, the American Society for Industrial Security found that Fortune 1,000 companies sustained losses of more than \$45 billion from the theft of proprietary information during a recent one-year period.

---

- *Flexibility* to use industry-leading Open PGP security technology—the de facto standard for Internet e-mail and file encryption—on the widest platform range in the industry. E-Business Server makes it possible to use a single Public Key Infrastructure (PKI) server to interface with PGP and X.509 certificates. E-Business Server solutions can additionally scale easily to meet the demands of a growing business.

### API Enhancements for Windows NT and UNIX platforms

The latest version of McAfee E-Business Server goes beyond standard C++ to support newer, more Web-friendly application environments. Native Perl API for McAfee E-Business Server, Native COM API for McAfee E-Business Server, and Native Java API for McAfee E-Business Server are add-on native application programming interfaces (APIs) that facilitate easy integration of encryption into existing applications within the developer's chosen language.

#### API Operating system support includes:

- Native Perl API: Windows NT/2K, Linux, Solaris, AIX, HP-UX
- Native Java API: Windows NT/2K, Linux, Solaris, HP-UX
- Native COM API: Windows NT/2K

The standards supported by these add-on APIs—Visual Basic, Perl, and Java—are popular programming languages among developers of Web and e-business

applications. Application developers can now use their programming language of choice to integrate E-Business Server functionality into their applications. The APIs act as the integration tool between E-Business Server and the application that will use PGP to encrypt, decrypt, digitally sign, or verify data.

### Enhancing Productivity and Enterprise Security

The Web-friendly native APIs for McAfee E-Business Server enhance productivity along with security. Now, the same developer can create the application and ensure that application data is protected without extensive infrastructure changes. The resulting programs are also easier to understand and maintain. By making encryption easier to use, E-Business Server helps eliminate common implementation errors that lead to vulnerability of company data. A poorly implemented security solution is dangerous, because companies send sensitive data believing it is secure when it is not. In addition, mission-critical data may be inaccessible if a problem occurs, and developers unfamiliar with the original code may have difficulty understanding the intent of the program.

Simple commands combined with the context of the application make it easier to discern the intent and function of encryption elements, even if the developer is unfamiliar with the original program. By using McAfee E-Business Server to improve the security of sensitive business data, companies save money, exchange secured data to any business partner, and protect data rapidly and easily.

---

### Financial Services Firm Hit

As many as eight million credit card numbers were believed stolen from a company that processes transactions in early 2003. Omaha, Neb.-based Data Processors International, which processes transactions involving Visa, MasterCard, American Express, and Discover Financial Services for merchants, said in a statement that it had "recently experienced a system intrusion by an unauthorized outside party."

---

## IV. Other Data Security Alternatives Fall Short

Since the rise of e-Business as a way to conduct business with customers, suppliers, and partners, enterprises have tried many different approaches to addressing the growing challenge of ensuring data privacy. These include virtual private network technology and similar network-layer approaches, SSL implementation (a transport-layer approach) and customized encryption solutions. While these approaches all have merit, they also have significant shortfalls.

### Leased Lines

Leased-line solutions carry a recurring cost, no matter how much (or how little) data is transferred. The bandwidth of the lines and the associated cost can vary, but in order to increase or decrease bandwidth, the customer must request it from the telecommunications vendor. As a result, leased lines are highly inflexible and cannot readily scale or dynamically adjust to changes in either numbers of partners or the amount of data exchanged. Moreover, transmitting sensitive data via leased lines does not ensure that the data is secure in an encrypted format, or that the final data that is saved and stored is secure. (See Section V and Appendix A for a detailed comparison.)

McAfee E-Business Server solutions run over the Internet, offering high levels of security and flexibility without the cost of leased lines.

### Virtual Private Network (VPN)

On paper, VPN technology looks simple and safe; however, it carries many risks and disadvantages. First and foremost, because there is much incompatibility between vendors, VPN environments take considerable time to plan, develop, implement, and manage. Securing the data transfer with VPN requires the involvement of the security team on the receiving end, or some other special process to approve, initiate, and manage the connections at that site. Customers and partners may be required to purchase and maintain dedicated VPN hardware and software to accommodate even simple data transfers, adding substantial cost to the proposed setup.

It is also important to note that VPNs can compromise the security of the transmitting party, because the open connection provides a “VPN tunnel” directly back into the enterprise. Many VPN products are not able to filter or firewall the data over a VPN connection. And perhaps most importantly, VPN encrypts the data only as it is being passed from one network to another. Once inside the corporate network—where many compromises and attacks take place—it is in readily accessible “clear text.”

Because of the overhead of VPN implementation, it is also not a solution for situations where time-to-market is critical. It is not easily scalable to include partners rapidly or with diverse security and VPN architectures.

McAfee E-Business Server eliminates the cost, long implementation time, and compatibility and security issues associated with VPNs. Implemented in just hours, it can be up and running quickly over the Internet; since encrypted data is delivered directly to

---

## Telecommunications Providers Targeted

AT&T and Verizon, two of the largest U.S. telecommunications companies, experienced security breaches that may have allowed outsiders to see confidential information on hundreds of customers. The customers found their private information—including credit card numbers, Social Security numbers, and drivers’ license numbers—publicly posted in Internet chat rooms; many also noticed strange charges on their credit cards. These customers had ordered wireless services over the Internet from the compromised firms.

The personal data was probably leaked as a result of unencrypted files used by the wireless providers, by third parties involved in the transaction, or by a malicious worker inside one of the wireless or third-party companies.

the sender from the recipient, the VPN tunnel, and its vulnerabilities, are eliminated.

### Secure FTP

Secure FTP has similar architectural problems to VPN, since the data is protected only from FTP server to FTP server and not within the enterprise network, where the greatest risk exists. As a result, secure FTP solutions provide only partial protection for data. In addition, the strength of the protection offered FTP data varies with these solutions. Partners must also implement a matching solution on the other end of the secure FTP.

McAfee E-Business Server eliminates FTP's risks by allowing encrypted data to be sent intra-enterprise, ensuring its security. It provides consistent protection and, when used for inter-enterprise communication, does not require software to be installed by partners in order for their use.

### SSL

SSL dominates the Web e-commerce environment, as it is typically integrated into standard Web browsers as a no-cost feature. SSL technology is robust for transferring data from the browser to the Web server. However, once the data reaches the Web server, it is no longer protected. In fact, any data that goes through the Web server is vulnerable.

The Web server itself is surprisingly vulnerable to malicious code attacks and hybrid viruses, such as Nimda, and hackers can use even common search engines to locate vulnerable servers. If a Web server is successfully penetrated, hackers can compromise any data to which

that server has access throughout the corporate network. SSL is therefore an incomplete approach to the challenge of ensuring end-to-end data security.

By using E-Business Server's APIs, a Web server's SSL security capabilities can be further extended into the enterprise. Data received by the Web server as it exits the SSL tunnel is immediately encrypted using E-Business Server while still in [the Web server's] memory, before it is written to disk. This ensures that if the Web server is compromised, the encrypted data is not. Encrypted data can then be passed further into the enterprise for processing by other implementations of E-Business Server.

McAfee E-Business Server provides complete security for data; it arrives on both clients and servers in an encrypted format that can be decrypted only by the intended recipient.

### Customized Solutions

Some organizations turn to proprietary tool kits to address their security challenge, writing their own cryptography applications rather than buying commercially developed solutions. This approach requires a high level of sophistication, since cryptography is a complicated domain that is extremely difficult to execute properly. A poor cryptography implementation leaves an enterprise more vulnerable than no security solution at all.

McAfee E-Business Server uses market-proven, industry standard PGP encryption technology, ensuring that enterprises large and small receive uniformly robust protection.

### V. Cost-Comparison Scenario

As noted above, McAfee E-Business Server offers significant savings over a variety of alternatives, including leased lines. Figure 2 below illustrates the significant savings that can be gained by using E-Business Server to operate a trading network. Over four years, E-Business Server delivers cumulative savings of more than \$900,000 to the “hub” organization of the trading network.

In this scenario, year one assumes five trading partners, and year two assumes ten partners; in year three the

number of partners rises to fifteen, and twenty-five in year four. The diagram illustrates the principle that leased lines entail higher initial cost and dramatically increasing marginal cost. McAfee E-Business Server infrastructure has a lower start-up cost and can seamlessly scale to serve a rising number of partners with a much flatter cost curve.

For a detailed view of the comparison, please see Appendix A.

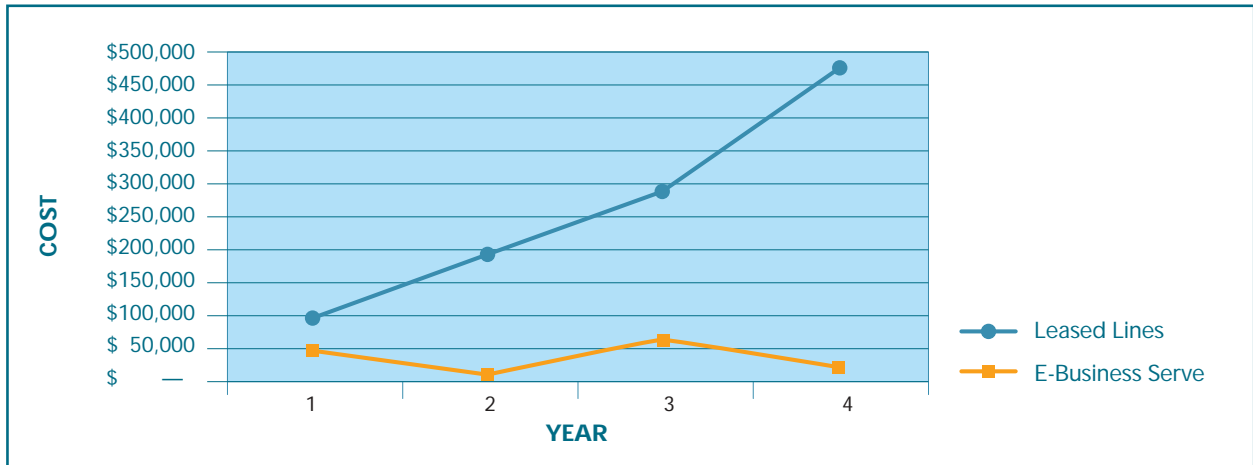


Figure 2: Over four years, using McAfee E-Business Server on a trading network with 10-25 partners can deliver savings of 54.3 percent to 95.3 percent.

## VI. Summary

McAfee E-Business Server is squarely positioned at the head of the data security value chain, providing superior, industry-leading end-to-end security. Enterprises can start by securing data in one application and expand coverage to others. They can also recommend E-Business Server to customers and business partners after experiencing its rapid implementation and cost savings, extending the E-Business Server's benefits up and down their demand and supply chains.

A broad range of industries benefit from the data protection provided by McAfee E-Business Server:

- Financial institutions processing checks, credit card transactions, and account information
- Healthcare institutions facing HIPAA compliance in patient records, payments, and insurance data
- Manufacturing companies exchanging supply chain transactions, engineering designs, and manufacturing data
- Insurance companies examining claims, payments, and customer records
- Retailers collecting local outlet and online sales and credit card transactions
- Government and federal agencies archiving confidential records and sensitive data
- Enterprise environments transferring branch employee records, benefits information, financial data, and sales information

McAfee E-Business Server products lead the industry with comprehensive data privacy protection capabilities, providing automatic file and e-mail encryption, compression, data integrity, and authentication.

Key benefits include:

### Business

- Protects the enterprise throughout the data lifecycle: in storage, in transit over the Internet, and during access, providing security at all points of access
- Reduces costs and improves flexibility by eliminating the need for leased lines and expensive developer resources
- Protects intellectual property from external theft and internal misuse

- Delivers rapid return on investment with low relative cost and fast implementation
- Reduces liability in the event of a security breach
- Enables easy compliance with legal, regulatory, industry, and partner requirements

### Product

- Scales to accommodate an unlimited number of partners
- Offers the flexibility to use industry-leading Open PGP security technology on the widest platform range in the industry
- Integrates into thousands of other applications via application layer encryption
- Implements an encryption solution into any back-end process with minimal integration time, and without special programming skills

### Technology

- Facilitates the automation of end-to-end file and e-mail encryption, compression, data integrity, digital signature, and authentication
- Facilitates the automation of the encryption and decryption of files for storage, transactions, transit, and remote archive for consistent security without user intervention
- Performs encryption on the server or mainframe where the data and applications reside, eliminating unprotected data storage and transfer
- Provides the widest available interoperability and flexibility with PGP keys, X.509 certificate compliance, and Self-Decrypting Archives
- Makes it easy to implement and integrate encryption into batch processes and applications using scripts, command-line interfaces, a choice of native APIs, or the McAfee E-Business Server software developer kit

With E-Business Server products from McAfee Security, sensitive customer data and critical enterprise information are protected from internal and external security breaches—no matter where the data are located, or where it is going.

For more information about McAfee Security's E-Business Server solutions, please visit [www.nai.com](http://www.nai.com).

## About McAfee Security

McAfee Security is a product line of Network Associates, Inc. that protects businesses from security breaches, virus attacks and blended threats. McAfee Security provides comprehensive network protection through industry leading anti-virus, encryption, desktop firewall, intrusion detection, vulnerability assessment and managed security technologies. All McAfee Security

products and services are backed by the world-leading anti-virus research organization, AVERT™ (Anti-Virus Emergency Response Team), the team responsible for providing cures for major outbreaks like LoveLetter, CodeRed and Nimda. For more information, McAfee Security can be reached at 888-VIRUS-NO, and on the Internet at <http://www.mcafeesecurity.com>.

## Appendix A: Comparison Analysis: Leased Lines vs. McAfee E-Business Server

### Assumptions

Hubs	E-Business Server	Leased Lines
# of hubs	1	1
Setup, install and testing time (man days)	1	1
Service provider line setup fees		\$ 1,000
Monthly cost per line		\$ —
Router equipment cost *		\$ —
Firewall equipment + software cost *		\$ —
Annual support for firewall + router *		\$ —
EBS Hub license - 4 CPU Server	\$ 24,600	
EBS Annual support per hub	\$ 8,200	
EBS Type of license (perpetual/subscription)	Subscription	
Hub server cost	\$ —	
Hub server annual support cost	\$ —	
<b>Partners</b>		
# of partners	5	5
Number of partners in year 2	10	10
Number of partners in year 3	15	15
Number of partners in year 4	25	25
"Template" configuration and testing (man days)	3	3
Setup, install and testing time per partner (man days)	0.1	0.2
Service provider line setup fees (per line)		\$ —
Monthly cost per line **		\$ 1,582
Router equipment cost *		\$ —
Firewall equipment + software cost *		\$ —
Annual support for firewall + router *		\$ —
EBS Partner license	\$ 2,000	
EBS Annual support per partner	\$ 150	
Partner server cost	\$ —	
Partner server annual support cost	\$ —	
<b>General</b>		
Cost per man day	\$ 416	\$ 416
% of partner cost paid by hub company	100%	100%

### Other

1. A three-year leased line contract is purchased to get the best per line monthly rate
2. It is possible to setup a standard template for both the EBS and partner firewall
3. It is not possible to re-assign equipment and licenses from a dead partner as a new one goes live
4. All EBS partner licenses are two-year subscription
5. EBS partner licenses and support purchased after initial purchase co-terminate and are then all renewed together
6. Incremental EBS partner licenses are purchased evenly throughout the year
7. Each partner line is a T1
8. Average IT employee costs (all in) \$100k per year, works five days per week

\* assumes this is already in place, if not additional costs need to be factored

\*\* based on contract between a medium/large company with an existing contract with a major telco

**Summary Comparison**

	Year 1	Year 2	Year 3	Year 4
<b># of Partners</b>	<b>5</b>	<b>10</b>	<b>15</b>	<b>25</b>
<b>Leased Lines</b>				
Hub company costs	\$ 1,416	\$ —	\$ —	\$ —
Partner costs	\$ 95,336	\$ 190,256	\$ 285,176	\$ 475,432
Total	\$ 96,752	\$ 190,256	\$ 285,176	\$ 475,432
<b>E-Business Server</b>				
Hub company costs	\$ 33,216	\$ 8,200	\$ 32,800	\$ 8,200
Partner costs	\$ 10,958	\$ 6,708	\$ 32,458	\$ 14,166
Total	\$ 44,174	\$ 14,908	\$ 65,258	\$ 22,366
<b>Total Savings</b>	<b>\$ 52,578</b>	<b>\$ 175,348</b>	<b>\$ 219,918</b>	<b>\$ 453,066</b>
<b>Analysis</b>				
<b>Leased Lines</b>				
Allocated cost for hub	\$ 98,168	\$ 190,256	\$ 285,176	\$ 475,432
Allocated cost for each partner	\$ —	\$ —	\$ —	\$ —
Cumulative allocated cost for hub	\$ 98,168	\$ 288,424	\$ 573,600	\$ 1,049,032
<b>E-Business Server</b>				
Allocated cost for hub	\$ 77,390	\$ 23,108	\$ 98,058	\$ 30,566
Allocated cost for each partner	\$ —	\$ —	\$ —	\$ —
Cumulative allocated cost for hub	\$ 77,390	\$ 100,498	\$ 198,556	\$ 229,122
<b>Total Savings</b>				
Allocated cost for hub	\$ 20,778	\$ 167,148	\$ 187,118	\$ 444,866
Allocated cost for each partner	\$ —	\$ —	\$ —	\$ —
Cumulative allocated cost for hub	\$ 20,778	\$ 187,926	\$ 375,044	\$ 819,910

All Network Associates® products are backed by our PrimeSupport® program and Network Associates Laboratories. Tailored to fit your company's needs, PrimeSupport service offers essential product knowledge and rapid, reliable technical solutions to keep you up and running. Network Associates Laboratories, a world leader in information systems and security, is your guarantee of the ongoing development and refinement of all our technologies.

