SDS E-Business Server™: Overcoming Technical and Regulatory Hurdles to Secure Enterprise Communications

White paper

By Schlar Consulting Group

June 2014

SDS

DO MORE WITH LESS

Contents

SDS E-Business Server: Overcoming Technical and Regulatory Hurdles to Secure Enterprise Communications
White paper

By Schlar Consulting Group
June 2014

Introduction

Across virtually every economic sector, the Internet's global reach and high-speed connectivity has created tremendous business opportunities for companies around the world. Along with these favorable conditions, however, comes a new level of business risk and exposure due to record numbers of sophisticated hackers, intruders, and cyber criminals trolling the Internet in search of new companies to exploit. Furthermore, legal consequences are on the increase, as more stringent federal and international regulations come with steep fines and penalties, making the protection of sensitive information and personal records more important than ever before.

Even without direct monetary attacks such as credit card theft and wire transfer fraud, the loss of sensitive information, confidential data, and trade secrets can have a devastating effect on the bottom line and operational status of any business. One need only read recent newspaper headlines regarding cyber attacks at Target, Sony, and T.J. Maxx to know that cyber criminals are getting smarter and more brazen in their exploits. In the case of Target alone, some 40 million credit card numbers and 70 million addresses and phone numbers were stolen in 2013, racking up more than $61 million in damage-control expenses and exposing the company to more than 90 costly lawsuits.

To compound matters, a recent study by Verizon Enterprise Solutions shows that companies detect security breaches through their own monitoring only 31 percent of the time. In 2012, the FBI's top cyber cop, Shawn Henry, stated in an interview "There are two types of companies: companies that have been breached and companies that don't know they've been breached."

Most recently in 2014, U.S. Attorney General Eric Holder revealed that "members of the Chinese military

> **"There are two types of companies: companies that have been breached and companies that don't know they've been breached**

have engaged in the hacking of American businesses and entities, including U.S. Steel Corp., Westinghouse, Alcoa, Allegheny Technologies, the United Steel Workers Union and SolarWorld."

▶ CNN, May 19, 2014
http://www.cnn.com/2014/05/19/justice/china-hacking-charges/Security Concerns

Security Concerns

To respond to this fast growing threat, businesses must deploy better cyber defenses and strengthen both their internal and external data communications systems. As advocated by the Office of Cybersecurity at the U.S. Department of Homeland Security, a new "Defense-in-Depth" strategy is needed to meet this challenge.

Defense-in-Depth relies on a multi-tier information architecture and overlapping layers of security to protect critical systems and sensitive information. This multilevel approach means that if one layer in the security architecture is breached, other layers will compensate. As an example of this layered architecture, a single business application might be protected by 1) secured user access controls, 2) secured transport mechanisms (SSL and TLS, for example), and 3) encrypted data at rest (using separate keys).

> “
> **Well-protected systems are a strong deterrent to hackers; in most cases they will abandon their attack in favor of less well-defended prey**

The recent "Heartbleed" vulnerability was so damaging to web server security because that security relied on only a single layer of SSL/TLS transport security. Hackers were able to crack this security by harvesting private keys from server memory.

Had the web servers used an additional layer of data encryption using PGP, for example, the data exposure would have been reduced significantly. Well-protected systems are a strong deterrent to hackers; in most cases they will abandon their attack in favor of less well-defended and more vulnerable prey.

Other cybersecurity best practices merit mention as well.

The risk of data disclosure or loss should be minimized at all times, especially when data is sent or published to trusted third parties. In the event of data loss, the breach should be quickly and easily identified using well-maintained audit trails. Conventional and widely used file transfer protocols such as FTP (file transfer protocol) often display unwanted characteristics such as data corruption after a file transfer is completed. It is far more damaging for a recipient to receive a partial file and believe it to be a complete file than to receive no file at all. Recovery from partial file transfers often requires costly and time consuming "back-out" processes. For signed data, clear audit trail mechanisms also help to verify that data is received correctly.

There are several other criteria that should be considered when developing a security strategy and making product selections.

One strong indication of the strength of any security solution is its track record. One of the best ways to evaluate a particular solution is to look at the longevity of its use without compromise. Standards-based approaches receive greater industry and security-analyst scrutiny than their proprietary or vendor-specific counterparts. Furthermore, proprietary techniques are often shown to have flaws that are not apparent during their first year of deployment. One such example is Apple's proprietary random number generator in iOS 7, which made the mobile operating system vulnerable to brute force attacks.

▶ http://threatpost.com/weak-random-number-generator-threatens-ios-7-kernel-exploit-mitigations/104757

Although many businesses use free open source or other low cost software to move data (free FTP software is one such example) these implementations sometimes come with serious drawbacks. Support and maintenance for a lot of open source software is very weak or non-existent; users of critical production systems need assurances of reliability and support.

Low-grade encryption solutions such as ZIP or Microsoft® Office® file or message encryption can be easily defeated. Encryption and digital signatures need to be applied as close to the source as possible to minimize risk; transferring a file to a Windows® system running free PGP software, and only then encrypting the file, creates an exploitable weakness during the first phase of the transfer. Manual or non-automated data protection techniques lack reliability and are particularly susceptible to human error and operational mistakes.

“

Both data at rest and data in transit may reside within the intranet and behind the firewall, or on the extranet, outside the firewall

Lastly and most importantly, federal regulations mandate the use of well-defined encryption methods for many electronic transfers and data exchanges. Failure to adhere to these regulations can result in substantial penalties as well as costly legal action (see the “Regulatory Compliance” section later in this document).

Use Cases

Enterprise customers must consider a wide range of use cases, network topologies, and application scenarios when performing their security planning. Broadly speaking, data exists in two distinctly different states: data at rest and data in transit. Data at rest refers to all data that resides in some form of computer storage. In contrast, data in transit refers to all data moving over either trusted private networks such as LANs or untrusted public networks.

Data at rest can be stored on a wide range of devices, including physical hard drives and storage arrays, Storage Area Networks (SANs), Network Attached Storage (NAS), tape drives, optical disk, flash storage, and even off-site backup storage services or cloud storage. As hackers use increasingly sophisticated means of penetrating internal corporate networks, many businesses are turning to data encryption and multi-level password protection to protect data at rest.

Data in transit may take on many different forms, such as database updates, real-time interactive sessions, email, file sharing, documents, bulk data transfer, archives, and many more. As with data at rest, well-structured encryption policies are considered the cornerstone of any security plan for protecting data in transit.

Both data at rest and data in transit may reside either within the internal network (intranet) and behind the firewall or on the external network (extranet) and

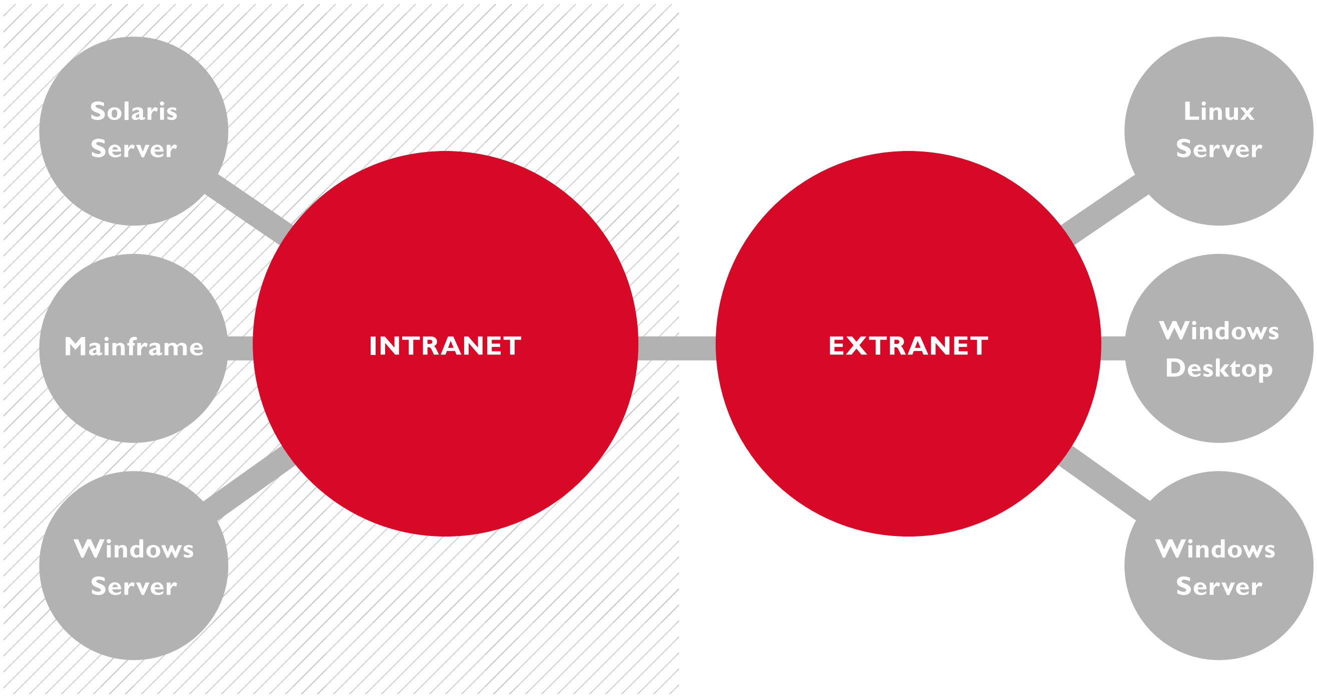

Diagram I: Intranet and Extranet Connectivity ▨ Firewall

outside of the firewall. Diagram I above illustrates a representative enterprise data communications environment with both intranet and extranet connectivity.

Every company today relies on data at rest and data in transit to communicate with customers, employees, and suppliers, and to conduct their daily business operations. As a general rule, the larger the business or corporation, the more varied the forms of data storage and data communications they regularly use.

Without careful monitoring and computer/network audits, some IT security departments may be unaware of the full breadth of data storage and communications usage in their business. Some industries are particularly data driven and rely heavily on both internal and external data communications, including:

- Small and large insurance companies
- Banks and financial institutions
- State and federal government agencies
- Manufacturers
- Fortune 1000 businesses
- Companies that work with external partners and consultants

> “
>
> **Data driven industries rely heavily on internal and external communications**

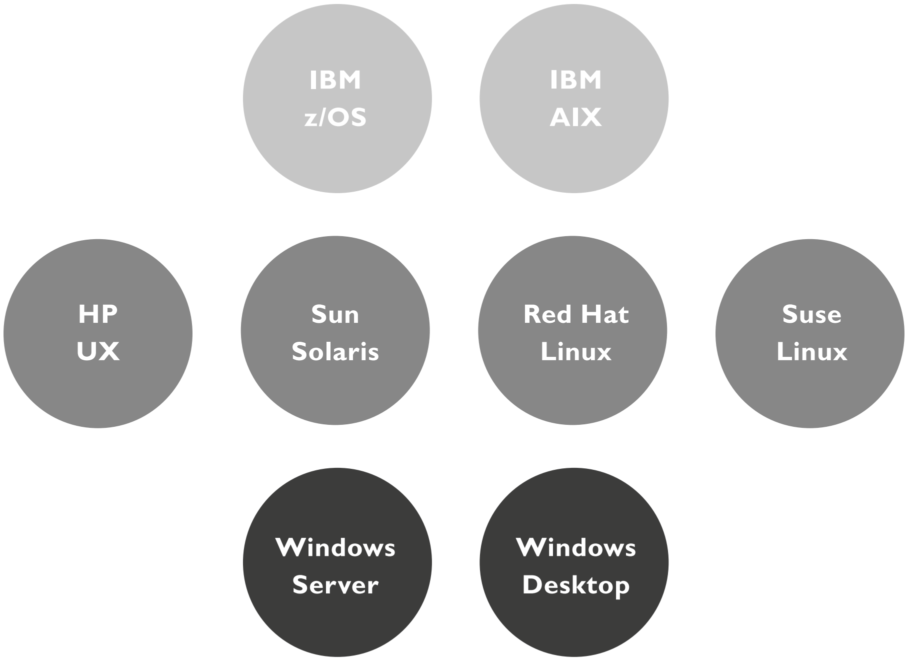

Diagram 2: E-Business Server supported operating systems

Overview of E-Business Server

Originally developed by Network Associates and in use by more than half of all Fortune 500 corporations for more than a decade, the E-Business Server from Software Diversified Services™ is a cross-platform enterprise-wide data security solution. As with any data security tool, interoperability between a diverse range of in-house and external computer systems is a key requirement for any enterprise customer.

To address this need, diagram 2 above illustrates the operating systems supported by the E-Business Server.

As part of an end-to-end secure data communications solution, the E-Business Server offers these essential functional services:

- Robust encryption and decryption based on the widely trusted OpenPGP standard, 128-bit minimum encryption.
- Key generation, exchange, and management, including key pairs and split keys.
- Digital signatures, including creation, authentication, and logging.
- Authentication – the verification that a user is who he or she claims to be.
- Character set conversion – EBCDIC-ASCII, as when transferring data from IBM to non-IBM systems.
- Data compression – significantly reduces file sizes and disk storage space, network bandwidth utilization, and file transfer times.
- APIs and scripting – Gives end-users the ability to easily embed encryption, decryption, digital signatures, and authentication into a) proprietary applications, b) third-party applications, and c) batch processes.

PGP Encryption

To maintain the highest levels of privacy and data integrity in the enterprise, a robust and well-tested cryptographic method is needed. One of the most long-standing and highly regarded commercial encryption programs is PGP, an industrial-strength encryption technology originally developed in 1991 and trusted by financial institutions and government organizations around the world.

Since its original inception, PGP has evolved to become an open standard, commonly known as RFC 4880, "OpenPGP Message Format" (Nov. 2007).

▶ http://www.rfc-editor.org/rfc/rfc4880.txt

The PGP standard is more than just an encryption algorithm; it may more accurately be described as a complete encryption/decryption application toolkit. Software developers and users may use some or all of the various software modules and components found in PGP. The features of PGP include:

Sender End

- Data compression (optional);
  reduces file sizes and speeds file transfers
- Session key generation
- Data encryption
- Session key encryption
- Digital signature
- PGP file header creation
- Text conversion (optional)

Receiver End

- Reading of PGP file header
- Session key decryption
- Data decryption
- Digital signature validation
- Data decompression (optional);

> **“ The PGP standard is more than just an encryption algorithm —it's a complete encryption/decryption application toolkit**

PGP uses both symmetric-key encryption and public-key encryption to ensure confidentiality. The former technique is used to generate a single-use session key that is coupled to the message and transmitted with it. The latter is used to encrypt the session key. The Public-Key encryption algorithm used by PGP supports key lengths up to 4,096 bits, resulting in up to 2^{4096} possible combinations.

Data encryption ensures that only the recipient can make use of the data. If the data is intercepted along its route or compromised in any other way, the risk and damage is extremely limited. Public-key encryption also offers much more robust access control than what is offered by FTP/HTTP-only solutions. Diagram 3 on the next page illustrates the basic PGP encryption-decryption process.

The digital signatures used in PGP serve a two-fold purpose: they are used to verify the authenticity of the sender, and they also validate that the data is received intact, without alteration. These two attributes of digital signatures are often referred to as authentication and data integrity. Digital signatures are also used to provide a clear audit trail for data governance that helps to ensure adherence to corporate IT and security policies.

To summarize, PGP addresses all the of major requirements needed in secure communications:

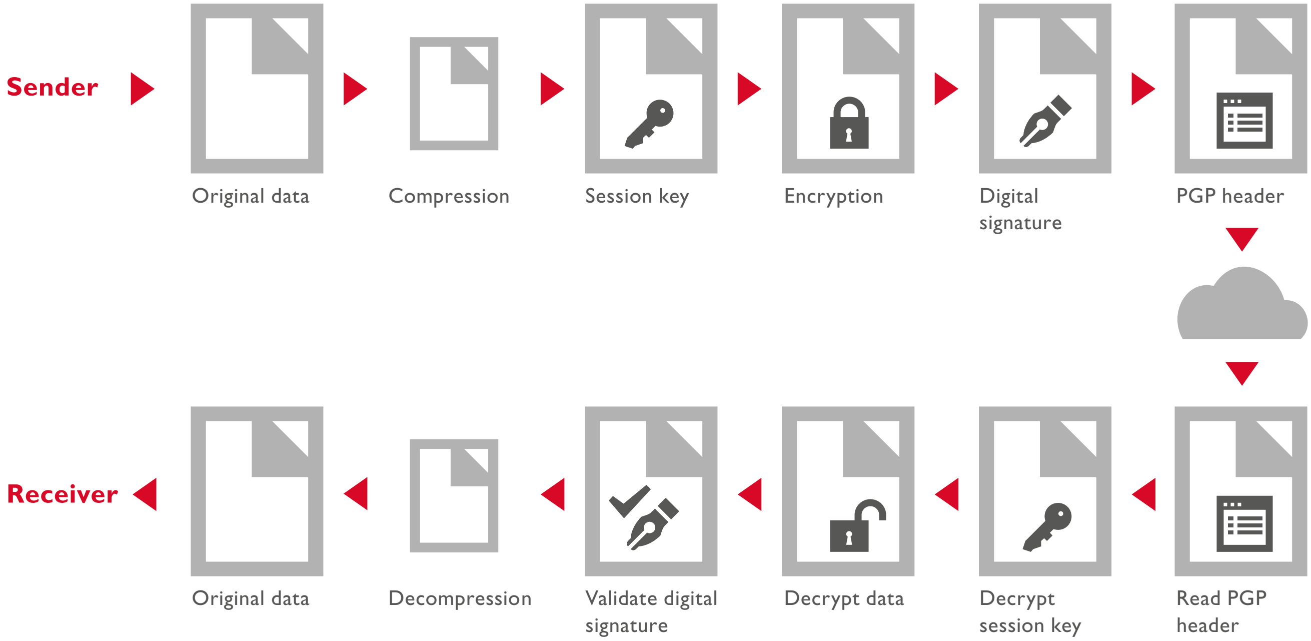

Diagram 3: PGP Encryption-Decryption process

- Data in transit is encrypted.
- Data can only be read by the recipient.
- Data can be verified as complete and unmodified with a signature.
- PGP provides a reliable, consistent tool as part of a “Defense-in-Depth” security strategy.
- PGP satisfies compliance requirements as part of a “Defense-in-Depth” security strategy.

Requirements

Regulatory Compliance

Breaches in security and compromised confidential information may carry serious legal and regulatory penalties that extend beyond commercial and economic risk. With cyber-attacks on the rise for more than a decade, the U.S. Congress and other world regulatory bodies have taken steps to protect the personal information of individuals. In addition, forty-seven states as well as the District of Columbia, Puerto Rico, and the U.S. Virgin Islands have passed laws requiring private companies to notify individuals of any security breaches affecting their personal information.

Here is a snapshot of some of the most important U.S. and international regulations governing IT security and data integrity.

The Sarbanes-Oxley Act of 2002

Although originally enacted in response to Enron’s fraudulent financial and accounting practices, the Sarbanes-Oxley Act of 2002 mandates the reporting of security events that affect company assets, including the exposure of intellectual property and trade secrets.

This law also extends to the preservation and security of financial data. Other countries like Canada, Germany, France, Holland, and Japan have passed similar laws.

The Health Insurance Portability and Accountability Act (HIPAA)

One of the tenets of the Health Insurance Portability and Accountability Act (HIPAA) passed in 1996 is the protection of individual's electronic personal health information and records. This law also specifies what safeguards must be in place to ensure that personal health information is sufficiently protected. These safeguards extend to Administrative Safeguards, Physical Safeguards, and Technical Safeguards. Included in this latter category are 1) Access Controls, 2) Audit Controls, 3) Integrity Controls, and 4) Transmission Security.

With a more comprehensive mandate than for HIPAA, Canada enacted the Personal Information Protection and Electronic Documents Act (PIPEDA) in 2000. This law specifies how private businesses and organizations may collect, use or disclose personal information in the course of their commercial activities. In addition, PIPEDA includes specifications for secure electronic signatures.

Payment Card Industry Data Security Standard (PCI DSS)

The Payment Card Industry Data Security Standard (PCI DSS) is a comprehensive set of standards created to enhance the security of payment card data and safeguard cardholder information at every step of the transaction process.

This standard specifies twelve individual requirements for compliance, including the protection of stored cardholder data and the encrypted transmission of cardholder data when it crosses open, public networks. Other control objectives of the standard include the implementation of Strong Access Control Measures and the maintenance of a Vulnerability Management Program.

Basel II

Global in geographic reach, the Basel II accords are an international set of banking laws and regulations designed to ensure that banks have adequate capital put aside to protect themselves from over exposure problems in lending and investments. An important change from the original Basel I accord is that Basel II focuses more on operational risk and includes new requirements for banks to proactively manage IT and security risk on their networks, applications, host computer systems, databases, and more. Penalties are also established for non-compliance with regulations.

Gramm-Leach-Bliley Act (GLBA)

Enacted in 1999, the Gramm-Leach-Bliley Act was created to enhance competition among financial services companies. One important provision of the bill is administered by the Federal Trade Commission (FTC) and is related to consumer privacy, whereby financial companies must develop information security programs that "protect the security, confidentiality and integrity of customer information." These safeguarding rules are designed to "Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer."

> **Security breaches carry serious legal penalties that extend beyond economic risk**

Technical Needs

Faced with the above series of laws and regulations, any enterprise IT security solution must offer a set of concrete features and capabilities that ensure both compliance and real-world operational effectiveness. With today's distributed computing systems and multi-host environments, any viable solution must offer true platform integration.

New or legacy mainframe systems must be able to securely exchange data and files with mid-range and even desktop systems across the enterprise. Interoperability across diverse operating systems is also key; mainframe OSs such as IBM's z/OS and AIX must be able to securely communicate with HP-UX and Sun Solaris systems as well as Linux servers. Given the penetration of Microsoft software in business, Windows servers and desktop systems must also be part of this communications mix.

Not to be overlooked in any IT security solution is the importance of enterprise-strength and reliability. For cost-saving reasons, many businesses have been initially drawn to low-cost or open source file transfer products, only to find the reliability of these products deficient and vendor support inadequate or non-existent.

Insecure file transfer protocols such as FTP and weakly encrypted protocols continue to be used excessively for commercial purposes, creating far too much exposure and unwarranted risk.

> **“Any enterprise IT security solution must offer features and capabilities compliant wth real-world operational effectiveness**

Using software products from leading, well-established vendors can help alleviate these problems and ensure high reliability and few operational issues. These solutions should also be designed to securely handle both intra-enterprise and inter-enterprise communications in a seamless, consistent manner. Reliable, low-cost software should be available to make it easy to communicate with external business partners in a highly secure, operationally robust manner.

Lastly, the encryption and security solution of choice should be affordable so that it may be installed on any required host or target system in the enterprise.

Virtual Private Networks (VPNs) may represent a viable secure communications approach for some businesses, but installation and implementation may be difficult and ongoing monthly service and support costs may quickly escalate.

Server-based software solutions are network agnostic and less complicated to implement, offering lower recurring monthly charges. Operations is also improved as configuration and troubleshooting can be done by in-house staff members rather than relying on outside VPN or third-party personnel.

Other Considerations

Licensing and Cost

For distributed platforms, the E-Business Server is licensed per CPU. For IBM System z mainframes, it is licensed by the number of MSUs or MIPS. License charges can vary from site to site and depend on the customer configuration.

Vendor Technical Support

Responsive, high-quality vendor support is a key element in any company's IT security strategy. Customer satisfaction is the first consideration at Software Diversified Services; we respond quickly and efficiently to any customer question or difficulty. SDS maintains a staff of skilled technicians who are on call 24/7. These technicians can escalate problems to our product developers and software engineers if needed.

SDS technical support for E-Business Server on any platform includes:

- Product upgrades and updates included as a standard part of every license.
- Alerts and remediation advice regarding new security threats as they become known.
- Support account managers to provide a single point of contact between customers and SDS.
- Phone access to technical support 24/7.
- An unlimited number of contacts with technical support.
- Direct, immediate access to technical specialists residing in the U.S.
- Support technicians with immediate access to the product development team and with comprehensive product training.
- Web and phone support with remote desktop control.

Product Enhancements

As part of its ongoing commitment to the E-Business Server platform, SDS issues periodic product enhancements.

Recent Enhancements

By default, new E-Business Servers use the new ASCII- EBCDIC translation table. With version 7.6 the translate71 option allows for decrypting data that was encrypted with the old translation table. It also allows for the sending of encrypted data from new E-Business Servers to the old ones.

Enhancements planned for 2014

The DSA 2048 algorithm – E-Business Server will soon add DSA 2048 and DSA 3072 algorithms to its digital signatures. This is in compliance with NIST requirement that all certificates expiring in 2014 should be upgraded to 2048 bit certificates.

ZLIB Compression – In the near-future, E-Business Server will support the ZLIB software library for ZLIB compressed data (RFC 1950). ZLIB supports the "DEFLATE" compressed data format (RFC 1951) used by Gzip and has become a de facto standard for data compression.

RFC 4880 – SDS plans to support this RFC requirement as part of OpenPGP.

Vendor Partnerships

SDS maintains close working partnerships with a number of leading vendors and professional organizations:

IBM

SDS is an IBM "Partner in Development," an Advanced member of IBM PartnerWorld®, and a member of the "Destination z community." SDS has developed and supported software for IT professionals in IBM mainframe environments since 1982.

NaSPA

SDS is a member of NaSPA, the Network and Systems Professionals Association. NaSPA is a not-for-profit corporation dedicated to enhancing the professional and personal lives of its members, IT technical professionals worldwide. NaSPA has thousands of members in 80 countries.

- HP

  SDS is an HP AllianceONE partner. This partnership provides SDS with the framework, tools and resources to support HP's standards-based architecture across Microsoft Windows, Linux, NonStop and HP-UX operating environments.

- SHARE

  SHARE Inc. is a non-profit, voluntary organization whose members are users of IBM information systems. SHARE's mission is to improve the effectiveness of members' information systems by providing education, promoting mutual support, and by influencing information technology strategies, products, and services.

Migration/Upgrade

As one of the most popular encryption and IT security products on the market, the SDS E-Business Server offers a simple and straightforward migration/upgrade path for current E-Business Server users. This software upgrade/move eliminates time-consuming and costly migration to a new and different encryption platform.

> **There are distinct advantages in selecting a single unifying encryption solution**

Conclusion

Given today's increasingly threatened network and application environments, the design and implementation of a comprehensive corporate network and application security architecture is more important than ever before. The selection of an enterprise-grade encryption and security platform is one of the most important factors influencing the resiliency and operational stability of this architecture.

There are distinct advantages in selecting a single unifying encryption and security solution that operates on all enterprise computer systems, versus implementing a patchwork solution built upon third-party software packages. These advantages include enhanced security strength, full intranet and extranet communications support, and multi-application support (email, file transfers, applications, and transactions).

End-users should carefully evaluate factors such as encryption strength, cross-platform interoperability, operating system support, automation/batch support, and vendor support when making this important corporate IT decision.

Note: PGP is a trademark belonging to Symantec Corporation.

About the Author

Sherman Schlar is an independent industry consultant and 30-year veteran of the IT, networking, streaming video, and video-conferencing industries.

His background includes systems engineering, quality assurance testing, DoD security validation, product certification, and product management.

During his long career, he managed one of world's largest private packet-switched networks and has worked closely with major U.S. carriers as well as leading European carriers and service providers in England, France, and Germany.

Sherman is the author of a best selling book on the X.25 protocol as well as numerous trade magazine articles, white papers, and technical bulletins. His current interests include video convergence and network security as well as the use of corporate broadband and social networks to conserve energy and enhance productivity and educational effectiveness.

He is the President of the Schlar Consulting Group (www.schlarconsulting.com) and resides in West Hartford, Connecticut.

Schlar Consulting Group

About SDS

Software Diversified Services (SDS) was founded in 1982, and now supports over 20 z/OS, MVS, VSE, and VM mainframe systems for more than 1,000 clients worldwide, as well as encryption for Windows, UNIX, Linux and AIX. PC software related to the mainframe industry is also available through SDS.

Our customers include many Global 500 companies in banking, finance, insurance, and retail, as well as local, state, and national governments.

Security, encryption, and network management are our current focus, also performance monitoring, report distribution, and client-server applications.

At SDS, technical support works hand-in-hand with development. SDS is noted for having the highest quality software, documentation, and technical support in the business. SDS technical support has been rated number 1 by the prestigious IBEX Bulletin.

Software Diversified Services
1322 81st-Ave NE
Minneapolis, MN 55432-2116
Phone: 763-571-9000
info@sdsusa.com
www.sdsusa.com

SDS
DO MORE WITH LESS