SDS E-Business Server™

Research report by
Clabby Analytics
October 2012

SDS
DO MORE WITH LESS

Contents

SDS E-Business Server
Encryption, compression, key creation and management

Research report by Clabby Analytics
October 2012

Introduction

Software Diversified Services (SDS), a well-established independent software vendor (ISV) and technical services provider, recently announced that it has acquired the rights to sell, support, and maintain McAfee's former E-Business Server environment.

> *Our initial take on this acquisition is that this is a "good strategic move" for SDS. It provides the company with an advanced, multi-vendor encryption and compression security environment that complements the company's other security and management offerings (including Net'Q & Net-Examine, its VitalSigns monitoring offerings, and VFTP-SSH) and squarely positions SDS as a leader in the PGP™ (pretty good privacy) marketplace.*

What we like most about the new SDS E-Business Server is that it offers:

- Rich Encryption – the SDS E-Business Server is a rich encryption environment that offers support of the following security algorithms: Triple-DES (3DES), CAST5, IDEA, Twofish, AES (128-, 192-, and 256-bit encryption), Blowfish, RSA v3 and v4 (up to 4096 bits), DSA, ElGamal, SHA-1, SHA-2, MD5 and RIPEMD-160;

- Excellent Compression – in some cases, up to 50% compression rates. Compression improves security by eliminating recurring patterns in the data before it is encrypted.

  Compression not only saves file space, it also lightens the load on the network (thus reducing latency) and it can lead to reduced processing time;

- Application Program Interfaces (APIs) – that allow encryption to be integrated with applications and processes using the provided APIs;

- Key Creation/Management – SDS E-Business Server can generate, disable, re-enable, and/or revoke keys – as well as change trust criteria using advanced key management;

- Multi-vendor Support – multiple platforms are supported including Windows, Linux, AIX, Solaris, HP-UX, and z/OS; and

- Non-repudiation – non-repudiation is a means of using electronic signatures so a sender cannot deny that a file was sent (this is especially useful when conducting internal security audits).

In this Research Report, Clabby Analytics takes a closer look at SDS and at the new "SDS E-Business Server" – and we ask the following critical question: "how will SDS grow the base of its new SDS E-Business Server?"

First things first: About SDS

SDS (founded in 1982) is an independent software vendor as well as technical services provider. The company's software portfolio includes over 20 mainframe security and management products – and now, a cross-platform encryption/compression product with the addition of McAfee E-Business security software.

Strategically, the company's current foci are data security and compression, performance monitoring, report distribution, and client-server applications. This includes PC software related to the mainframe industry.

The current SDS portfolio contains systems and network monitoring, security and encryption, index and search, report and backup, session and print management, file transfer and compression, and CICS utilities.

It is important to note that SDS is known for providing high-quality software, documentation, and technical support.

SDS technical support works hand-in-hand with SDS software developers and has been rated number 1 by the prestigious IBEX Bulletin.

SDS target market: The PGP marketplace

The target market for the SDS E-Business Server is the PGP marketplace – a market that needs cryptographic privacy and authentication services for data-at rest (stored data) as well as data-on-the-fly (data communicated over networks).

The way that PGP encryption works is that it uses a combination of technologies (including hashing, data compression, symmetric-key cryptography, and public-key cryptography) to safeguard data. Keys are created and bound to users – and these keys are managed using automated key management services.

The reason that IT executives use PGP services is that they are looking to protect their data from both external as well as internal threats:

External threats

- IBM recently published its mid-year 2013 X-Force security report (known simply as the "Trend and Risk Report").

  This annual report shows that Chief Information Security Officers need to increase their knowledge of the evolving vulnerability and attack landscape (including the use of mobile and social technologies) in order to more effectively combat security threats.

- This report emphasizes that known vulnerabilities (such as unpatched Web applications and endpoint software vulnerabilities) create opportunities for breaches – but also notes that attackers are improving their skills and now capitalizing on user trust coming from new approach vectors such as social media, mobile technologies and waterhole attacks.

- This report also highlighted that Distributed-Denial-of-

Service (DDoS) attacks are being used as a diversionary technique, allowing attackers to breach other systems.

To protect stored as well as networked data from these external threats it is wise to securely encrypt that data. This is why IT executives purchase PGP servers.

Internal threats

- Dishonest and disgruntled employees continue to represent a huge threat to internal information systems security (including fraud, theft of intellectual property, and sabotage).

The CERT Insider Threat Center now uses a database with over 700 insider threat cases in order to track and remediate internal threats. But some estimates show that internal threats may account for up to 80% of all security breaches.

The SDS E-Business Server uses some of the industry's most advanced algorithms to encrypt and decrypt data.

It uses a key-based approach to encrypt/decrypt data – and it uses straightforward APIs to overlay security over applications and processes. These algorithms and related key-based approaches help protect data on-the-fly or at-rest.

As for internal threats, the SDS E-Business Server uses unbreakable signature creation and authentication that provides non-repudiation services using electronic signatures (so a sender cannot deny that a file was sent).

This feature is particularly useful when doing internal security audits.

A close look: The SDS E-Business Server product offering

SDS E-Business Server is a multi-platform software tool that encrypts, authenticates and compresses data. Further, it can create and verify digital signatures in order to prove the origin of data and ensure message integrity. The way that security works within the SDS E-Business Server environment is that it generates, disables, re-enables, and revokes encryption keys – and allows changes in trust criteria. These keys can work across various platforms including Windows, AIX, HP-UX, Linux (both SUSE and RedHat), Solaris, and IBM z/OS – thus enabling multiplatform support. The SDS E-Business Server also provides key-management services, allowing users to create, find and store keys. The SDS E-Business Server also generates X.509 certificates that allow enterprises to create in-house certificate authorities.

From an implementation perspective, security services are built into applications and processes using application program interfaces (interface instructions) that allow IT administrators and developers to embed encryption, digital signing and authentication into application and batch processes.

As for application/process integration, the SDS E-Business Server is a command-line application that can easily be integrated with existing processes and scripts including z/OS JCL, batch processes, the TSO environment, and REXX (SYSREXX) during system startup and in system operator commands. Further, SDS E-Business Server security can be easily integrated into C and Java applications, and into scripts on Linux, Unix, Solaris, and z/OS USS.

Particularly noteworthy are the encryption algorithms that are available on the SDS E-Business Server. These algorithms include symmetric Triple-DES (3DES), CAST5,

IDEA, Twofish, AES (128-, 192-, and 256-bit encryption) and Blowfish support. Asymmetric algorithm support includes RSA v3 and v4 (up to 4096 bits), DSA and ElGamal (Diffie Hellman). Hash support includes SHA-1, SHA-2, MD5 and RIPEMD-160.

Notice that these are core to McAfee's security business – and that SDS E-Business Server benefits from algorithms implemented by one of the strongest security software makers in the industry.

It is also important to note that SDS E-Business Server compression is very strong. It can reduce file sizes (sometimes up to an impressive 50%). And file size reduction can lead to decreases in consumption of bandwidth, processing time, and disk space.

The SDS E-Business Server can also encrypt/decrypt files of 4GB and larger. Further, EBCDIC-ASCII conversions can be handled on the fly.

Also, the SDS E-Business Server offers unbreakable signature creation and authentication that provides non-repudiation services using electronic signatures. We think that this feature is particularly important for enterprises that wish to conduct internal audits.

The big question: How will SDS grow its SDS E-Business Server base?

SDS is an independent software vendor that has a strong focus on security and management software development. The company makes its money by developing security and management software – as well as by providing technical services related to its software offerings.

To understand how SDS will grow its E-Business Server base it is necessary to look more closely at the company's sales, support and development situation.

Figure 1: SDS worldwide sales and support coverage
Source: Software Diversified Services, September 2013

Sales and support

From a sales and support perspective, the company already has a worldwide network of distributors in North and South America, Europe, Africa, the Near and Far East, as well as in Australia and New Zealand (see Figure 1). With this broad expanse of sales and support coverage, SDS already has the resources that it needs in place to support the existing installed base while driving new sales in various geographies.

A more important question is: "How will SDS make its SDS E-Business Server a more compelling offering such that the company can grow the E-Business Server base?" The answer to this question can be found in the following subsection (Research and Development).

Research and development

From a research and development perspective it is important to note that SDS already has a wealth of security developers who currently build, support and enhance several other SDS security products.

These resources can also be used to help support and enhance the new SDS E-Business Server environment

(and other resources can be added as needed to support the expected growth of the platform).

What is involved in supporting and enhancing the SDS E-Business Server over the long run? As SDS sees it, much of the support and enhancement activity for its E-Business Server centers on keeping current with the numerous algorithms involved in encrypting and decrypting data.

Standards organizations control these algorithms – so it is important for SDS to monitor each standard's RFC (request for comment) activities in order to stay current with planned changes to the standard algorithms. SDS has added development staff to support ongoing development of E-Business Server. If the need arises, SDS will promptly employ additional E-Business developers.

As for product enhancements, SDS is very customer-centric when it comes to enhancing its software portfolio. The company is confident that it can port or write the necessary code to address customer change requests.

Remember, SDS is a 30-year-old vendor with a stellar reputation for keeping its offerings current and thriving – so there is historical precedent that shows that SDS knows how to keep its products up-to-date from a features/function perspective as well as from an enhancements perspective.

Should we stay or should we go?

Given that customers originally purchased their E-Business Servers from McAfee, a logical question from the installed base should be "should we stay or should we go?" From our perspective, existing customers of McAfee's E-Business Server need to weigh the benefits of continuing to use the E-Business Server under the auspices of SDS, versus moving to another PGP offering.

The key arguments for staying with an installed E-Business Server environment are:

1. Moving costs can include design and test migration, data backup, the actual migration and retest – and then application recertification (where auditors approve the PGP product and related processes). SDS E-Business Server can save customers from a migration process of indefinite length and expense, and uncertain outcome.

2. Removing an installed environment can be difficult because E-Business encryption and decryption services have been integrated into customers' batch and online environments. Pulling and replacing that encryption can be cumbersome.

3. Remember, existing customers have already invested in process integration, personnel training, and supporting infrastructure. Moving to another platform means re-investing in training and infrastructure – potentially for little or no gain.

4. SDS plans to actively invest in the development of new SDS E-Business Server features and functions. Staying current or leap-frogging ahead of competitors is core to the SDS strategy for its E-Business Server. So, again, moving to another platform buys little in terms of new features and functions.

Another important consideration for existing customers who are considering a migration to another PGP offering has to do with compliance. The Payment Card Industry (PCI) Standards Council has announced that systems no longer supported by their vendors will fail PCI compliance. This shows that the PCI Standards Council

understands that systems without regular maintenance cycles are at increased risk for compromise and attack, thus risking credit card compromise.

SDS plans to regularly update and maintain its E-Business Server, thus ensuring that it will remain a viable security platform in the eyes of security auditors and standards organizations.

From our perspective: given the cost of migration (including new licensing, new training, replacing the currently integrated processes with new ones, and more) – and given SDS' intent to continually add new enhancements to its SDS E-Business Server – it makes little sense for installed-base users to move to another PGP environment.

Why most existing customers will stay with SDS E-Business Server

On October 4th, 2013, Adobe Systems Inc. reported that up to 2.9 million of its customers may have been affected by a data breach.

After sophisticated attacks on its network Adobe found that its source code had been accessed – and that customer information such as names, encrypted credit card or debit card information, and "other information related to customer orders" may have also been accessed. The key word in the previous sentence is "encrypted."

SDS E-Business Server users know that they have to do their utmost to protect corporate and customer data – which is why they invest in PGP products.

But some of the reasons that they have chosen the SDS E-Business Server include:

Small insurance company
"E-Business just runs and we don't really have to worry about it. But having SDS take over the support, maintenance and more importantly enhancements, makes the product even more foundational for us."

Large bank
"We've been using E-Business for about ten years and it's tightly integrated within our applications. We're glad SDS will be looking at enhancing the product and listening to our future requirements."

Large insurance company
"It just runs and you almost don't know it's there. We're happy with the function."

State government
"I wish all software vendors had support like SDS provides; you're always responsive and you know your stuff!"

Manufacturer
"I would like to say how much I appreciated the expert support I received during our SFTP project. I could not have completed it without the SDS support and technical services team."

Insurance
"When I call SDS, I always know I'll get a live person who answers my questions the first time, every time."

The necessity for encryption services, plus ease of deployment and operation, plus outstanding service and support all ensure that the likelihood that existing customers will stay with the SDS E-Business Server is very high.

Summary observations

McAfee positions the acquisition of its E-Business Server product as a "strategic partnership" with SDS – a way to better serve the McAfee customer base through a third-party relationship. We, however, see this acquisition differently.

With the acquisition of McAfee's E-Business Server environment, SDS is expanding its existing security software portfolio, adding new encryption/decryption, key management and non-repudiation functions to its suite of security products.

This is a good strategic move by SDS because it expands the company's security portfolio and positions the company to offer broader security services to its customers.

As is the case during many acquisitions, IT buyers should be asking: "Should we stay with the new vendor or move to another platform?" The place to look for the answer to this question is at the new vendor's sales/support/development organization.

From a sales and support perspective SDS has a broad, worldwide distribution network that is prepared to aggressively market and support its new SDS E-Business Server. We believe that SDS is strategically committed to growing its E-Business Server base – and, accordingly, we expect that field sales organizations will be chartered with aggressively driving sales of this new product. Flat sales were the reason why McAfee chose to pass over the reins of its E-Business Server to SDS. We think that SDS will be far more aggressive in promoting this product.

As for the SDS development organization, it is important to note that SDS already offers several other security products – so it knows how to build and support products that encrypt/decrypt and compress data. It is also important to note that SDS development sees the task of keeping the product current as an exercise in keeping up with encryption standards (so it should be straightforward to keep-up with algorithmic changes in the industry).

As for enhancements, we have noticed several SDS customer testimonials that laud the company for great support and for its responsiveness. This shows us that the company is very customer-centric. And we expect that it will be this customer-centric focus that will drive future enhancements of SDS E-Business Server.

After evaluating both the E-Business Server and SDS, we conclude that given the company's broad, worldwide distribution network, its strong reputation for service and support, and its deep security developmental expertise, SDS has the resources needed to support existing customers while opening new opportunities for its SDS E-Business Server.

We recommend that existing customers stay with SDS for encryption/decryption/compression and non-repudiation services – and we recommend that new prospects consider SDS' new E-Business Server to protect data-in-flight as well as data-at-rest.

Note: PGP is a trademark belonging to Symantec Corporation.

About Clabby Analytics

Clabby Analytics is an independent technology research and analysis organization. Unlike many other research firms, we advocate certain positions — and encourage our readers to find counter opinions —then balance both points-of-view in order to decide on a course of action. Other research and analysis conducted by Clabby Analytics can be found at: www.ClabbyAnalytics.com.

Clabby Analytics
www.clabbyanalytics.com
Phone: 001 (207) 846-6662

October, 2013

About SDS

Founded in 1982, Software Diversified Services (SDS) supports over 20 z/OS, MVS, VSE, and VM mainframe systems products for more than 1,000 enterprises worldwide. SDS was rated number one in technical support by the prestigious IBEX Bulletin, is an HP Alliance ONE partner, an IBM Partner in Development, an Advanced member of IBM Partner World®, and a member of the Destination z community.

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