



Software Diversified Services

Securing Mainframe Data

SPARTA Meeting

December 5, 2017



# Agenda



About Software Diversified Services



Options for Securing Mainframe Data



Secure FTP Using SSH



E-Business Server (PGP) Encryption



SIEM z/OS and DB2 Collector Agents

# Software Diversified Services

## Proudly Serving Enterprise Customers for Over 35 Years

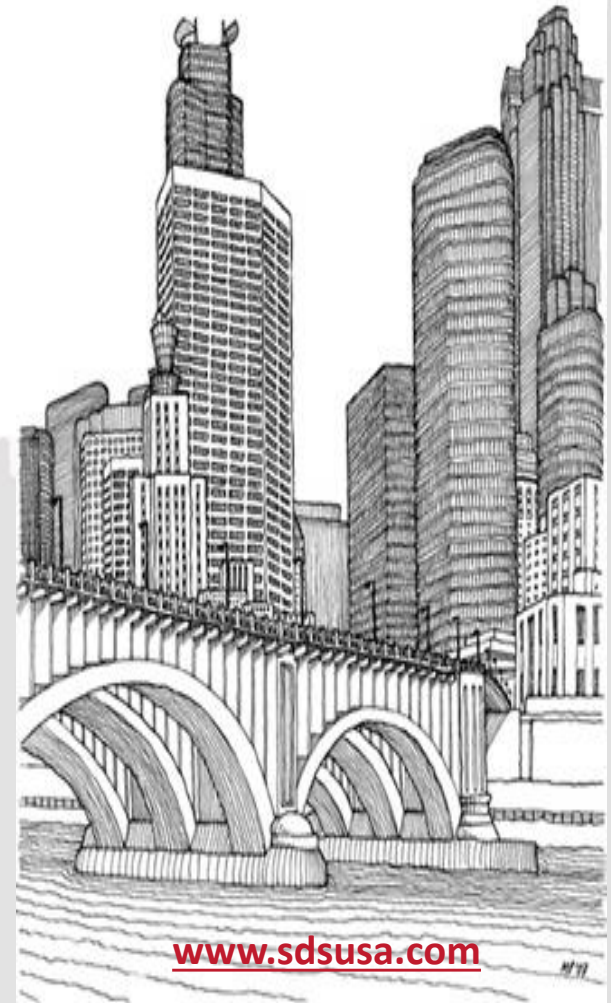
- ▶ Financially Rock Solid
- ▶ Several Hundred Satisfied Licensed Customers Worldwide
- ▶ Over 20 z/OS, z/VSE and z/VM Mainframe Systems and Distributed Products
- ▶ World Class Support 24x7
- ▶ Full Time Development / Support Staff / USA
- ▶ VitalSigns Network & Security Solutions
- ▶ Partner Solution SSH Tectia for z/OS (Secure FTP)
- ▶ Partner Solution Virtel for Thin Client 3270TE and Secure TN3270



HQ in Minneapolis  
1322 81st Ave. NE  
Spring Lake Park, MN  
55432-2116 USA



(800) 443-6183,  
(763) 571-9000



[www.sdsusa.com](http://www.sdsusa.com)

# Introductions

**Dave Ellis**

**Software Developer  
Raleigh**

**Deb Hodson**

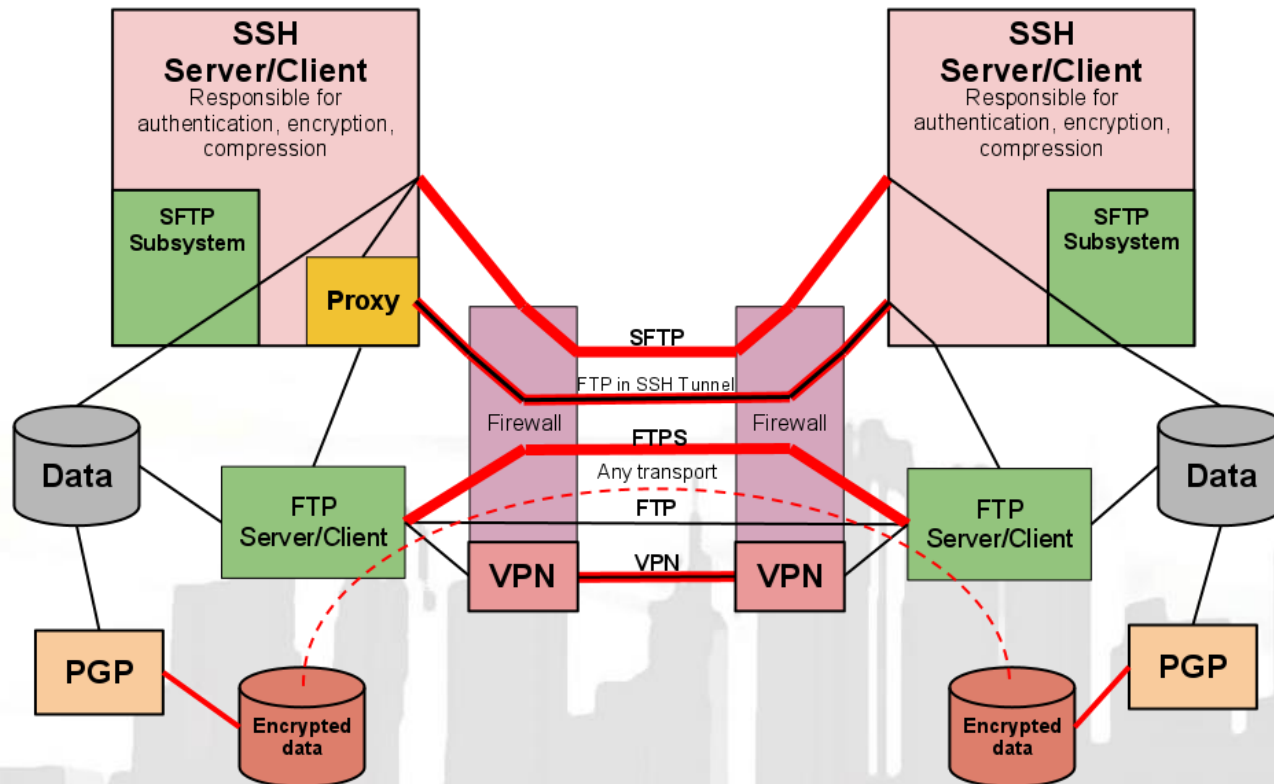
**Sales Manager  
Raleigh**

**Tim Full**

**Technical Services  
Manager  
Minneapolis**

# Securing Data at Rest and In Flight

# Securing Data in Motion and at Rest

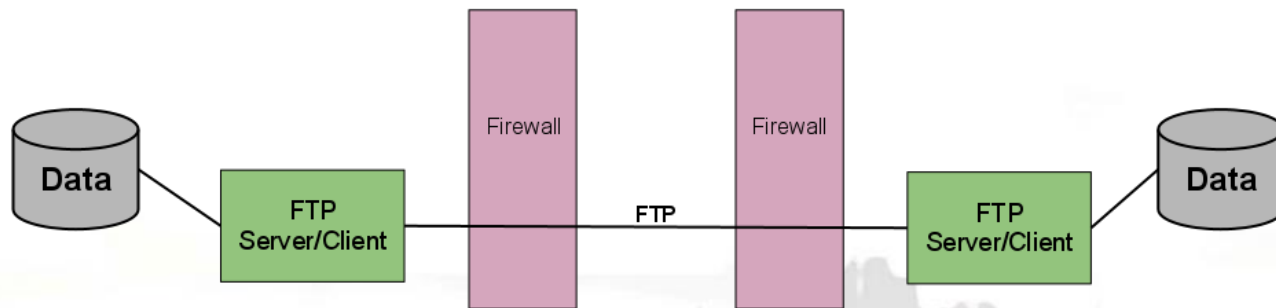


# QUESTION

How Many Of You Use  
FTP?

SFTP?

# FTP



## ■ Pros

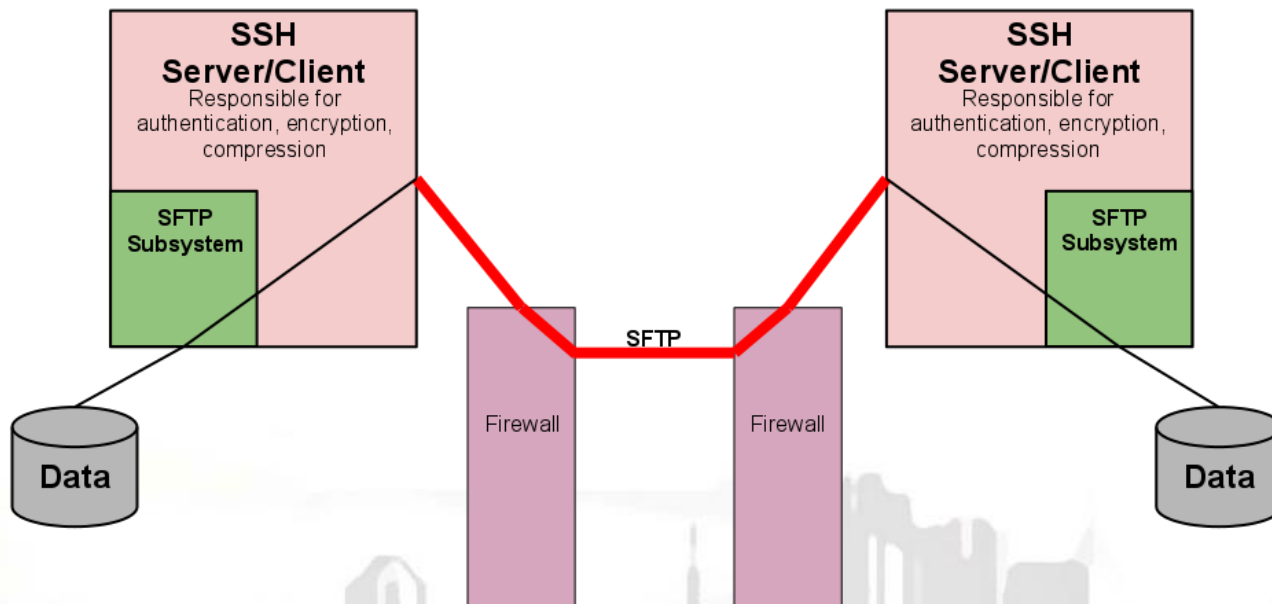
- Ubiquitous
- Common knowledge
- Included in base OS

## ■ Cons

- Very little security
- Not firewall friendly
- No native compression (Mode Z in some implementations)



# Secure FTP (SFTP)




## ■ Pros

- Point to point encryption
- Compression and Integrity built-in
- Already ready to go on Unix/Linux servers

## ■ Cons

- Not part of base on z/OS or windows
- Command Syntax different – Unfamiliar to some users



# Secure FTP

## VitalSigns for FTP

## SSH Tectia z/OS

# VitalSigns for FTP –Monitoring, Automation, Auditing, Security

## ■ Monitoring

- ✓ Complete visibility on all FTP transfers
  - ✓ Failed Sessions, Secure, Unsecure, User ID, IP address, Customized queries

## ■ Automation

- ✓ FCL scripting Language – IF, Then, DO, ELSE
- ✓ Restart Failed transfers
- ✓ Create and enforce rules



# VitalSigns for FTP –Monitoring, Automation, Auditing, Security

## ■ Auditing

- ✓ Retain all FTP transfers for user defined period
- ✓ See context of FTP transfer and technical details
- ✓ Extract information from Database into EXCEL or SAS for graphical charting
- ✓ Sample Batch reports (SMF)

## ■ Security

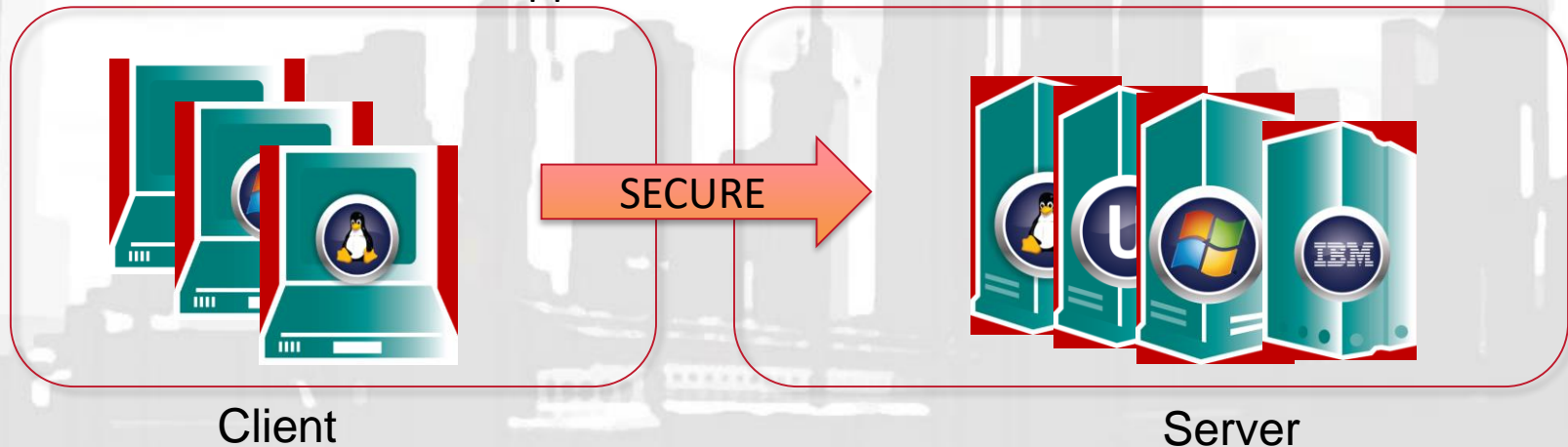
- ✓ Use VFTP Client Rules to route FTP batch job(s) to the SSH Socks Proxy (NO JCL CHANGES REQUIRED)
- ✓ Control access to FTP commands like
  - ✓ SITE, CD, Prevent users from submitting jobs through JES internal reader
- ✓ Restart Failed transfers
- ✓ Create and enforce rules



# What is SSH ?

## ► SSH (Secure Shell Protocol)

- SSH Communications Security was founded in 1995 by Tatu Ylonen, original developer of the Secure Shell Protocol (SSH)
- SSH is the de-facto standard used by millions of worldwide for secure remote login, command execution, file transfer and application tunneling
- SSH z/OS is the server application for SSH communications to and from z/OS



# SSH / Tectia Server for z/OS is .....

## Tectia Server for IBM z/OS is

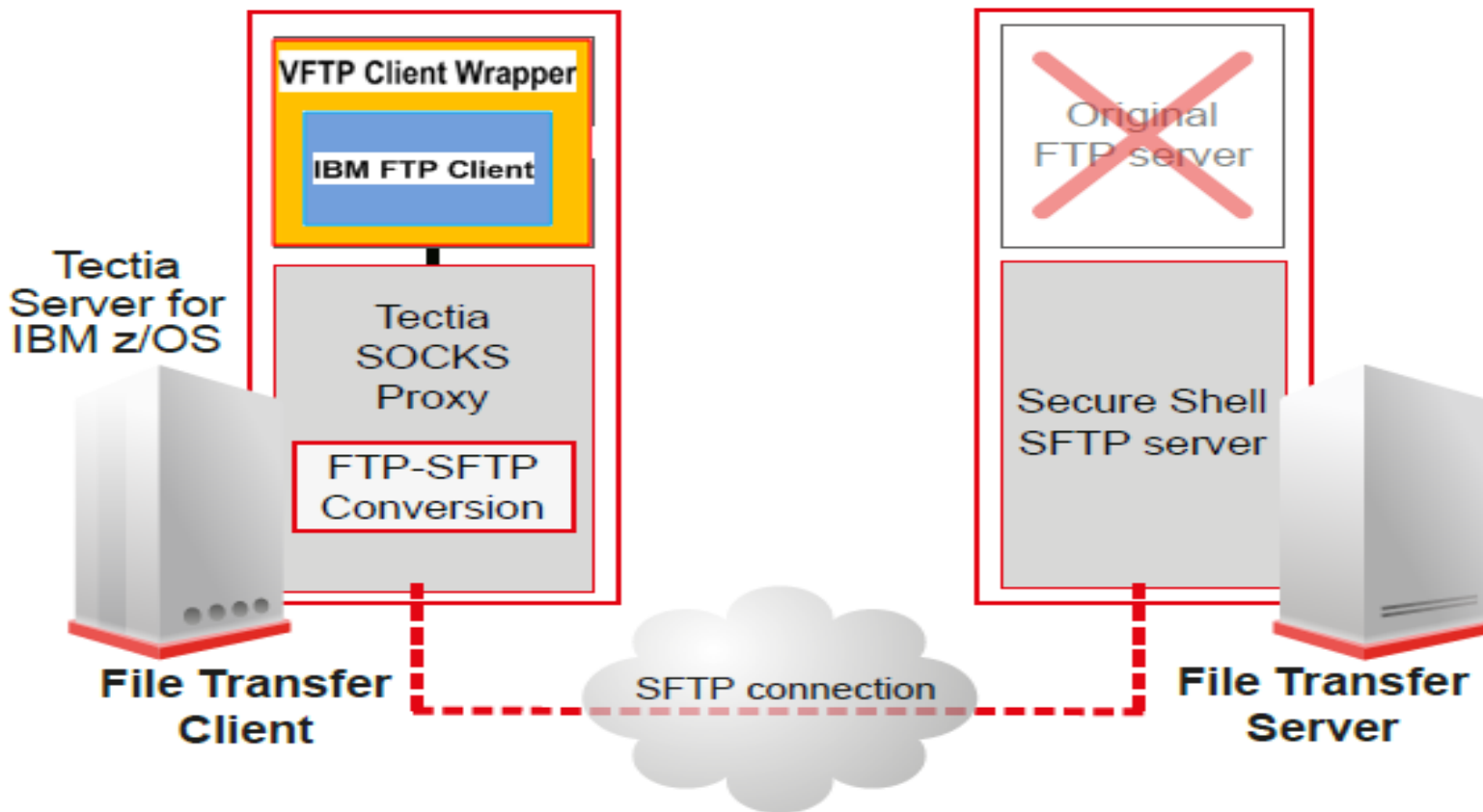
- Enterprise class security solution for IBM z/OS mainframes providing
  - Secure File Transfers
  - Secure Application Connectivity
  - Secure System Administration

## Tectia Server for IBM z/OS is

- Transparent FTP-SFTP Conversion and FTP Tunneling
- Native z/OS dataset support
- Hardware acceleration of cryptographic operations
- Configurable ASCII/EBCDIC conversion
- Integrated authentication for RACF, CA-ACF2 and CA-TSS
- SMF and syslog file transfer auditing



## SSH / Tectia and VFTP – The Complete Solution – FTP to SFTP Conversion With NO JCL CHANGES NEEDED



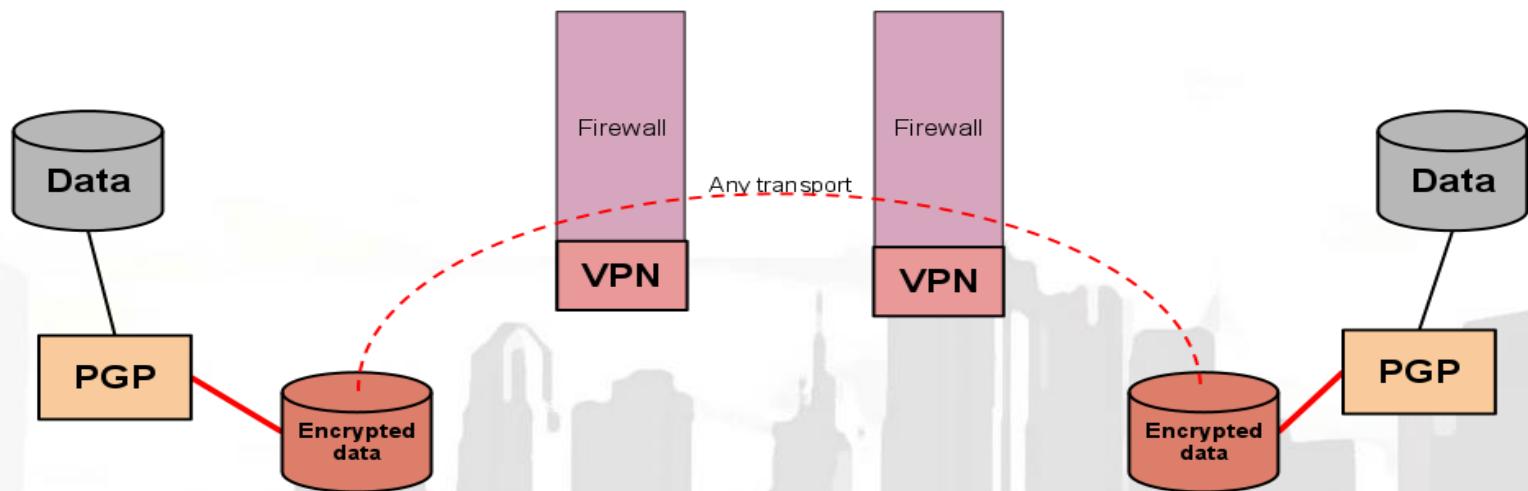
- VFTP can direct the FTP Client to transfer data through a SOCKS Proxy
- VFTP can direct z/OS clients to alternate configuration files
- VFTP Client configuration allows users to define selection criteria for batch jobs

# QUESTION

How Many of You Use  
Encryption (PGP) for  
Securing Data at Rest?



## PGP (Data at Rest)



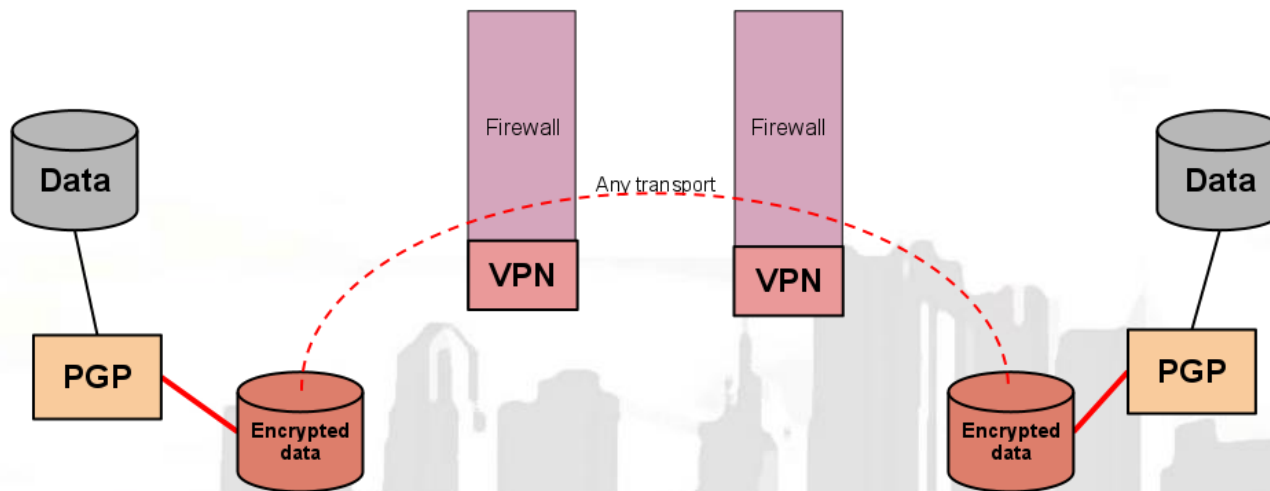
- Pros

- Full control of sensitive data
- Transport is not important
- Compression and Integrity
- Not just for transfers

- Cons

- Requires staging of data

## PGP (Data at Rest)



- Common uses
  - Sensitive data that needs protection at destination as well as in transit



# PGP Encryption

## SDS E-Business Server

# PGP Encryption At Rest

## SDS E-Business Server Overview

- ▶ Based on the Open Standard
- ▶ Use of Public Key Cryptography
- ▶ Provides Strong Encryption
- ▶ Generates keys, encrypts, decrypts, digitally signs and authenticates
- ▶ Creates Certificates (x.509)
- ▶ Provides Key Management
- ▶ Ensures File integrity
- ▶ Non repudiation of sender
- ▶ Additional Decryption Keys (ADK)
- ▶ Self Decrypting Archives (SDA)

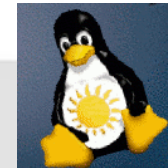


## E-Business Server Overview

- ▶ Conserves Bandwidth and improves transfer speed with built-in compression
- ▶ Secures files over 4 GB
- ▶ Automatic ASCII to EBCDIC character conversion
- ▶ Seamlessly integrates into existing E-Business process (or enables new ones)
- ▶ Provides API's for easy integration with Application and Processes

# E-Business Server Supported Platforms

- ▶ z/OS
- ▶ Windows
- ▶ Linux
- ▶ HP-UX
- ▶ AIX
- ▶ Solaris



# E-Business Server – User Interfaces

- ▶ Command – line : EBS
- ▶ APIs : C ,COM, Java (JNI), REXX
- ▶ GUI : Java administration console for key management and configuration

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\beuri>cd\
C:\>ebs --help

Help for basic operations.
Use "--help" with the following options for individual usage.

--armor          Encode a file with E-Business Server's base-64 encoding,
                  with optional compression
--decrypt        Decrypt data that was previously encrypted
--encrypt        Encryption
--help           Display help for E-Business Server
--key-edit       Specifies a keypair to be updated
--key-export     Exports a key from the keyring
--key-gen        Generate a new keypair
--key-list       Display keys on the keyring
--key-sign       Sign a key
--list-aliases   Show the active aliases
--sign           Perform a cryptographic signature on input data
--version        Displays version information about the E-Business Server
                  executable
--wipe           Performs a secure deletion of files

For help on key management operations:  ebs --help --key
For help on key editing operations:      ebs --help --key-edit
For help on keyserver operations:       ebs --help --keyserver
For help on group operations:           ebs --help --group
For help on smartcard operations:       ebs --help --smartcard
For help on X.509 operations:           ebs --help --x509
```



# QUESTION

How Many Of You Have  
Been Asked (Required?)  
to Collect Mainframe  
Data for SIEM?



# What is SIEM ? – Security Information & Event Management

- ▶ Security Management provides a holistic view of an organization's information technology security
- ▶ SIEM combines SIM (Security Information Management) and SEM (Security Event Management) functions into ONE Security Management System

## SIEM

Asset  
Discovery

Vulnerability  
Assessment

Threat  
Detection

Event  
Collection

Correlation

Event  
Management

Log Storage

# SIEM – Security Information & Event Management

Security Information & Event Management System	
Security Event Management (SEM)	Security Information Management (SIM)
Provides - <ul style="list-style-type: none"><li>▶ Event Management</li><li>▶ Real Time Threat Analysis</li><li>▶ Incident Detection &amp; Response</li><li>▶ Basic ticketing capabilities</li><li>▶ Security operations</li></ul>	Provides - <ul style="list-style-type: none"><li>▶ Centralized log collections</li><li>▶ Long term log collection</li><li>▶ Log search and reporting</li></ul>

# Why SIEM?

## Security Requirement

- ▶ SIEM is the core defense for an in-depth strategy
- ▶ Attackers leave behind a trace – Logs
- ▶ Security Events provide insight into
  - When the event occurred
  - Why it happened
  - What happened



## Why integrate z/OS into SIEM ?

- ▶ Compliance Requirement
  - ▶ PCI, SOX, HIPAA, GLBA, etc
- ▶ Mainframe contains sensitive data
  - ▶ Large corporations have 70% of data on Mainframes
- ▶ z/OS is not invulnerable
- ▶ Most companies have a SIEM; why not include your mainframe?



# SIEM – One view of your entire Enterprise

- ▶ A Enterprise SIEM collects / aggregates logs from heterogeneous sources
  - ▶ Databases
  - ▶ Routers
  - ▶ Switches
  - ▶ Other SYSLOG devices
- ▶ All in ONE central location



# SIEM – One view of your entire Enterprise

- ▶ Makes searching easy
  - ▶ Exact Time
  - ▶ Corresponding Security Event
  - ▶ Who
  - ▶ When
  - ▶ Location



# SIEM – One view of your entire Enterprise

- ▶ Configure Rules
- ▶ Kick off scripts
- ▶ Based on thresholds
- ▶ Conditions
- ▶ Violations
- ▶ Anomalies




## z/OS Filtering

- ▶ To process the vast amount of data coming from SMF and WTOs, but **NOT** filter out irrelevant events.....

Would be like trying to drink from a fire hose!





A faded, grayscale image of a city skyline, likely New York City, serves as the background for the slide. The Empire State Building is prominent on the right side. The text is centered over this background.

# SIEM for z/OS & DB2

## VitalSigns for SIEM Agent

# VitalSigns SIEM Agent

- ▶ Delivers Real-Time of alerts to be managed, filtered, routed, and searched via Enterprise SIEM software
- ▶ Gathers intelligence from z/OS SMF and the system operator interface
- ▶ Provides certified integration with HPE ArcSight and IBM QRadar
- ▶ Integrates with Splunk, LogRhythm, EMC RSA Security Analytics, McAfee Enterprise Security Manager, Dell SecureWorks, etc.
- ▶ Easy installation
- ▶ Small footprint with little CPU overhead

# VitalSigns SIEM Agent

- ▶ Collects standard SMF record types related to
  - ▶ Security
  - ▶ DB2 activity
  - ▶ Operational activity
  - ▶ Networking
- ▶ SDS provides a list and spreadsheet of recommended / suggested SMF record types to collect

## VitalSigns for FTP

### LET'S RECAP...

- ▶ VFTP helps customers identify all of their FTP traffic both inbound and outbound on z/OS
- ▶ VFTP can assist customers in their migration of unsecure FTP to Secure FTP
- ▶ It can help protect “unauthorized” FTP commands like SITE, CD etc.
- ▶ It can assist customers to automate FTP transfers using FTP Control Language (FCL)
- ▶ It can retain logs for specified time periods for audit requirements

## LET'S RECAP...

- ▶ SSH Tectia
  - ▶ Secures data in transit
  - ▶ No Staging of Data – Direct MVS dataset access
  - ▶ Solid, Secure Shell Protocol
  - ▶ Used in conjunction with VFTP, customers can migrate their batch JCL to SFTP WITHOUT making any JCL changes



# E-Business Server (PGP)

LET'S RECAP...

- ▶ E-Business Server
  - ▶ Securing Data at Rest
  - ▶ Cross Platform
  - ▶ Easy to generate and manage keys using Console Key Manager
  - ▶ Automatic conversion of ASCII / EBCDIC data
  - ▶ Low on CPU resources

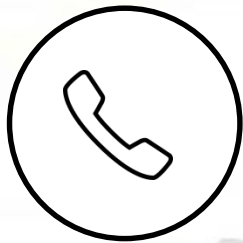


# VitalSigns SIEM Agent

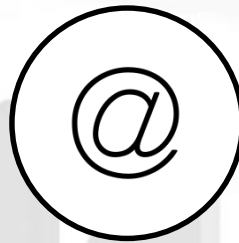
LET'S RECAP...

- ▶ VitalSigns for SIEM Agent
  - ▶ Agnostic with all Enterprise SIEMs
  - ▶ Easy Collection of SIEM events/logs/WTORs
  - ▶ z/OS and DB2
  - ▶ Low on CPU resources

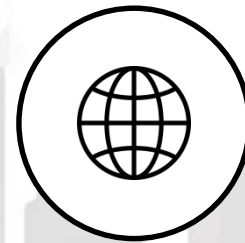




(800) 443-6183,  
(763) 571-9000



[info@sdsusa.com](mailto:info@sdsusa.com)



[www.sdsusa.com](http://www.sdsusa.com)



## Just a few of the Events

### SMF Types Monitored by VitalSigns for SIEM Agent

- ▶ Record Type 14 (OE) -- INPUT or RDBACK Data Set Activity
- ▶ Record Type 15 (OF) -- OUTPUT, UPDAT, INOUT, or OUTIN Data Set
- ▶ Record Type 17 (11) -- Scratch (delete) of Data Sets
- ▶ Record Type 18 (12) -- Rename of Data Sets
- ▶ Record Type 30 (1E) -- JOB/STEP TERMINATION (BATCH, TSO, STARTED TASK)
  - TYPE30\_1: Job Initiation
  - TYPE30\_4: Step Termination
  - TYPE30\_5: Job or Session Termination
  - TYPE30\_6: System Address Space
  - TYPE30\_D: DD Segment Detail
  - TYPE30\_V: Interval Accounting

## SMF Types Monitored by VitalSigns for SIEM Agent

- ▶ Record Type 32 (20) -- Termination of TSO Session (Often = 30)
- ▶ Record Type 42 (2A) – System Managed Storage (SMS) PDS/E activity
  - Subtype 20 – STOW initialization (delete all members)
  - Subtype 21 – Delete member
  - Subtype 24 – Add or Replace member
  - Subtype 25 – Rename member
- ▶ Record Type 62 (3E) – VSAM OPEN
- ▶ Record Type 80 (50) -- RACF Security (Events 1-89; DataTypes 1-438)
- ▶ Record Type 81 (51) – RACF Initialization and SETOPTS
- ▶ Record Type 83 (53) -- RACF Security Audit Records

## Filtering of SMF Events – Type 80

Event	Description
8	ADDSD
9	ADDGROUP
10	ADDUSER
11	ALTDSD
12	ALTGROUP
13	ALTUSER
14	CONNECT
15	DELDSD

## Filtering of SMF Events – Type 80

Event	Description
16	DELGROUP
17	DELUSER
18	Password
19	Permit
20	RALTER
21	RDEFINE
22	RDELETE
23	Remove
24	SETROPTS
25	RVARY
59	RACLINK
66	RACDCERT CERTIFICATE EVENT TYPES
87	RACMAP