



Our webinar will begin shortly



Quality Mainframe Software since 1982



# Security Solutions for the Mainframe

plus an **Extended Trial Offer**



## Colin van der Ross

Sr. Systems Engineer



2 SDS solutions that can help secure your mainframe

## Lori Kettles

Sales Manager



SDS introduction and extended offer details



## Quality Mainframe Software since 1982

- ▶ Expert development & technical support teams based in Minneapolis, MN.
- ▶ 25+ products for z/OS, z/VM, z/VSE, and distributed platforms.
- ▶ Hundreds of organizations worldwide rely on SDS solutions.
- ▶ Focus on mainframe security and compliance.
- ▶ Cost savings and legacy tool replacements: **DO MORE WITH LESS!**
- ▶ Long-standing global partnerships complement SDS software.
- ▶ Recognized for providing highest quality technical support.





## Shelter-in-place Plan

- ▶ Everyone works from home
- ▶ Hackers have increased their activity
- ▶ Maintaining security during this time is very important

## Our Offer

- ▶ Unlimited number of LPARs
- ▶ Limited to first 50 customers
- ▶ Accept offer by May 15, 2020
- ▶ Free to use until October 31, 2020
  - Guaranteed price after trial period
  - Cancel at no charge during trial



## SDS can help secure your mainframe

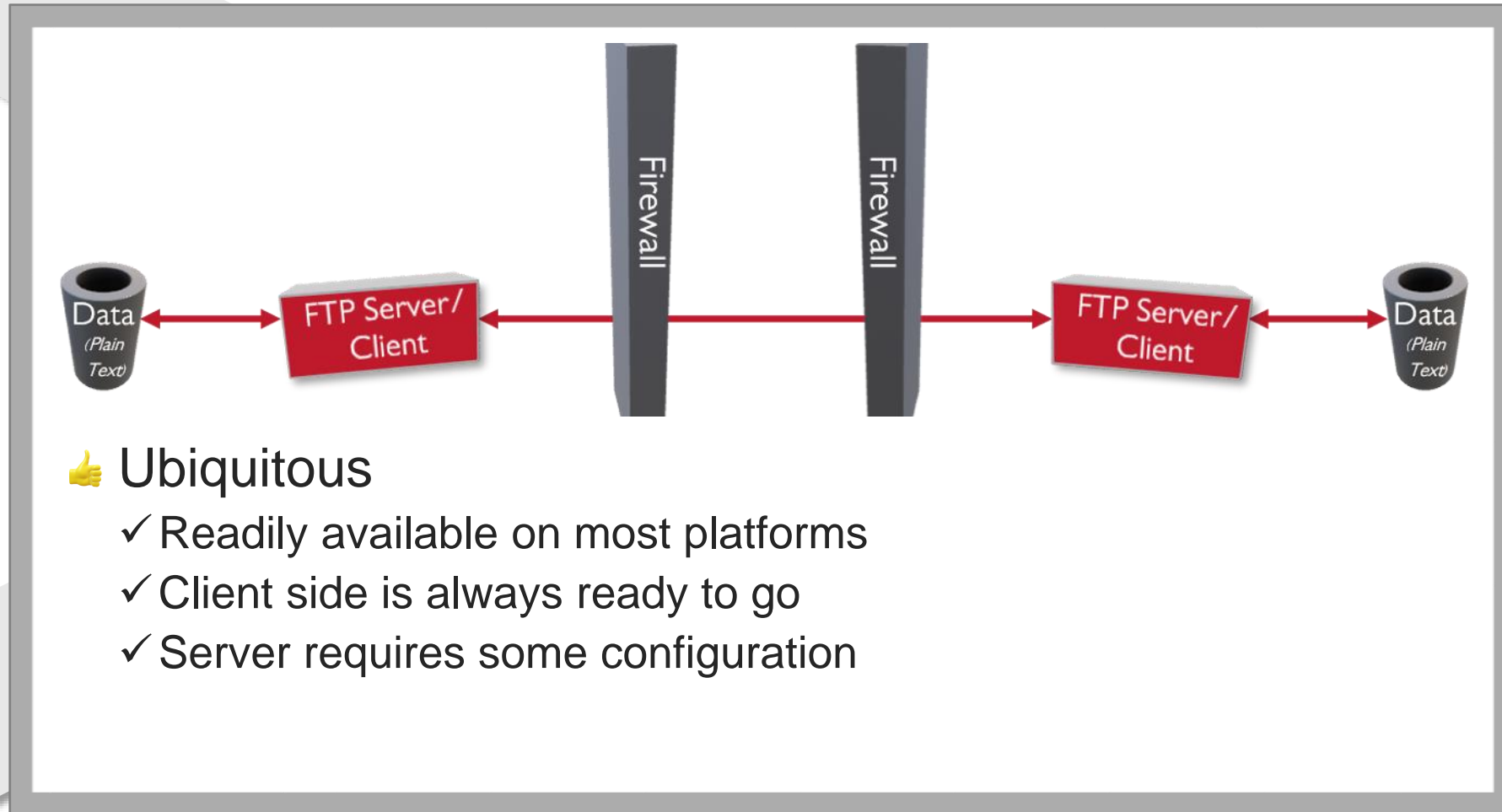
- ▶ Automate DISA STIG compliance monitoring
- ▶ Secure data at rest on z/OS and distributed platforms
- ▶ Secure 3270 terminal emulator
- ▶ Secure mainframe FTP without JCL changes
- ▶ Deliver mainframe security events to any SIEM in real time



## Agenda

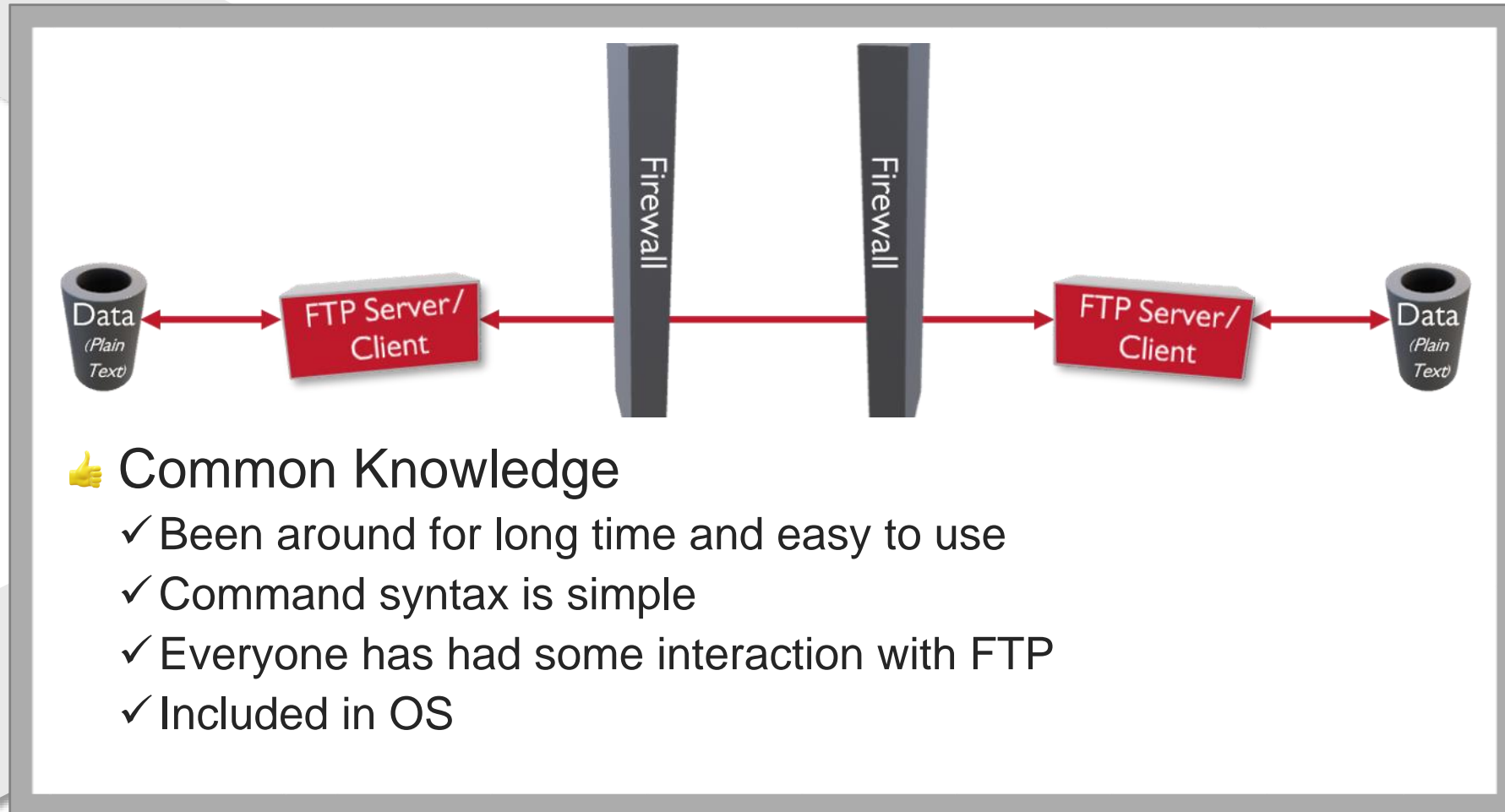
- ▶ Why is FTP so Vulnerable?
- ▶ Demo of a packet trace on FTP transfer
- ▶ Different options to Secure FTP
- ▶ Demo of Migrating FTP-to-SFTP without JCL changes

# Why is FTP so Vulnerable?

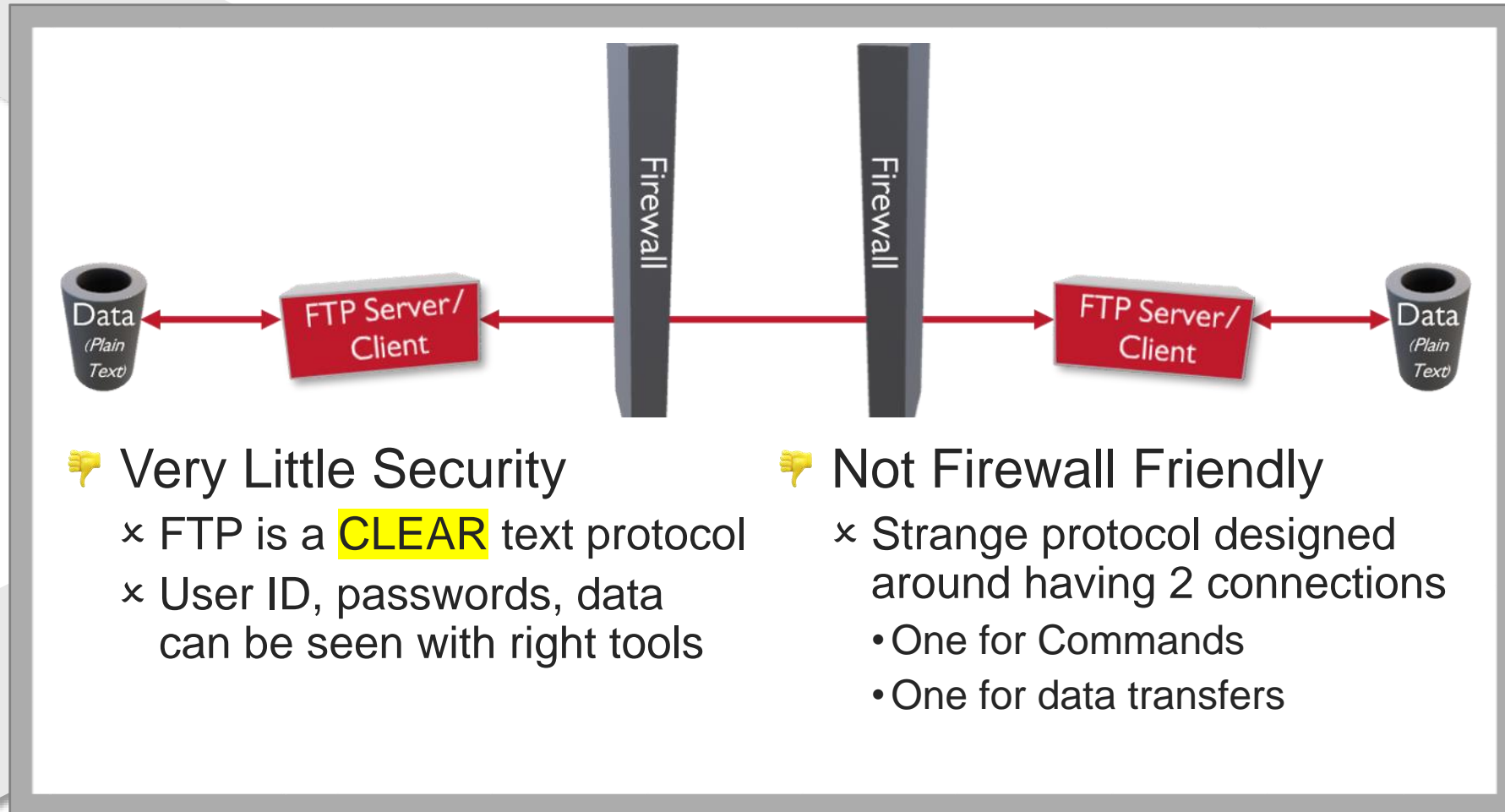




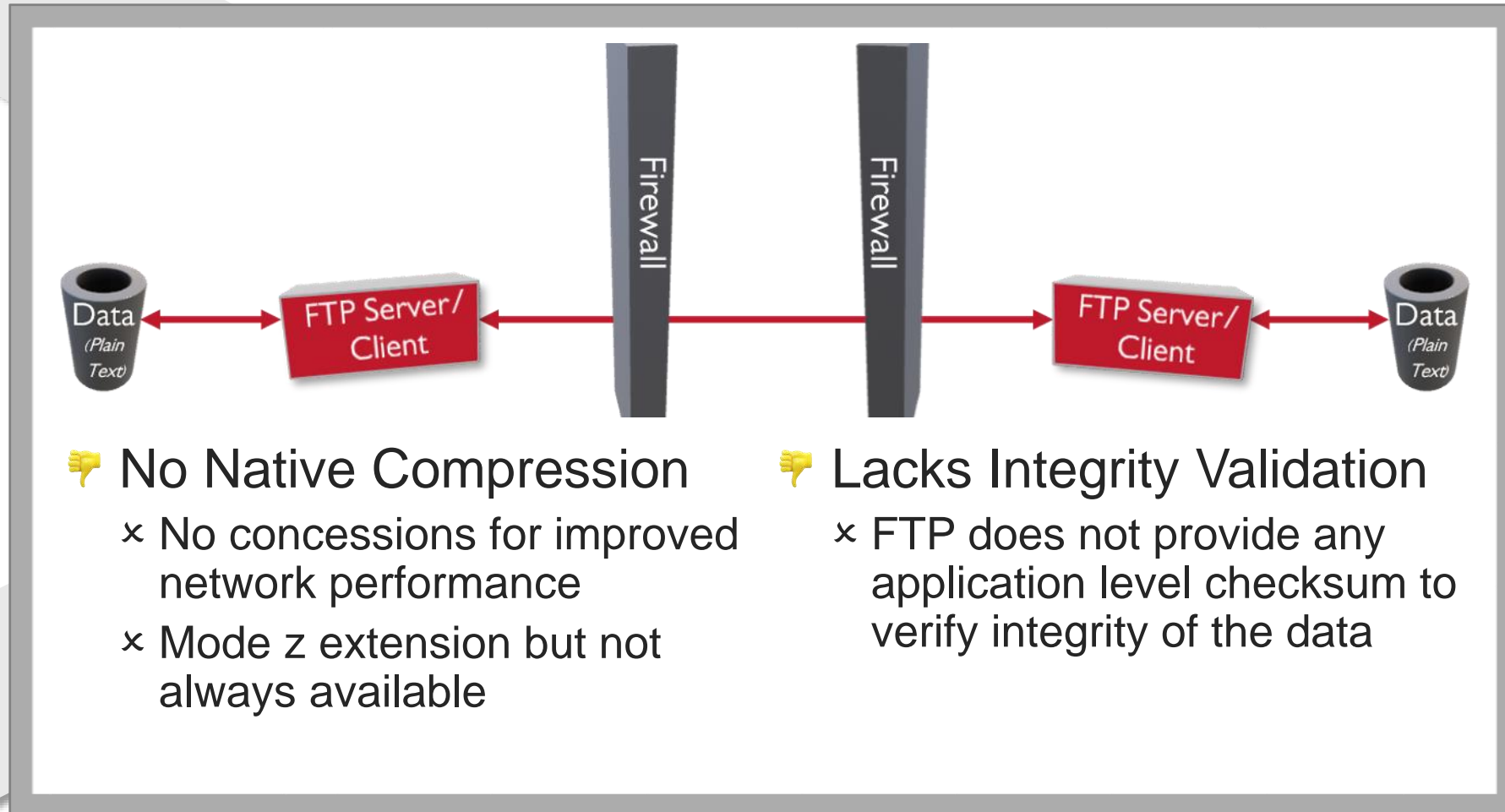
# Why is FTP so Vulnerable?

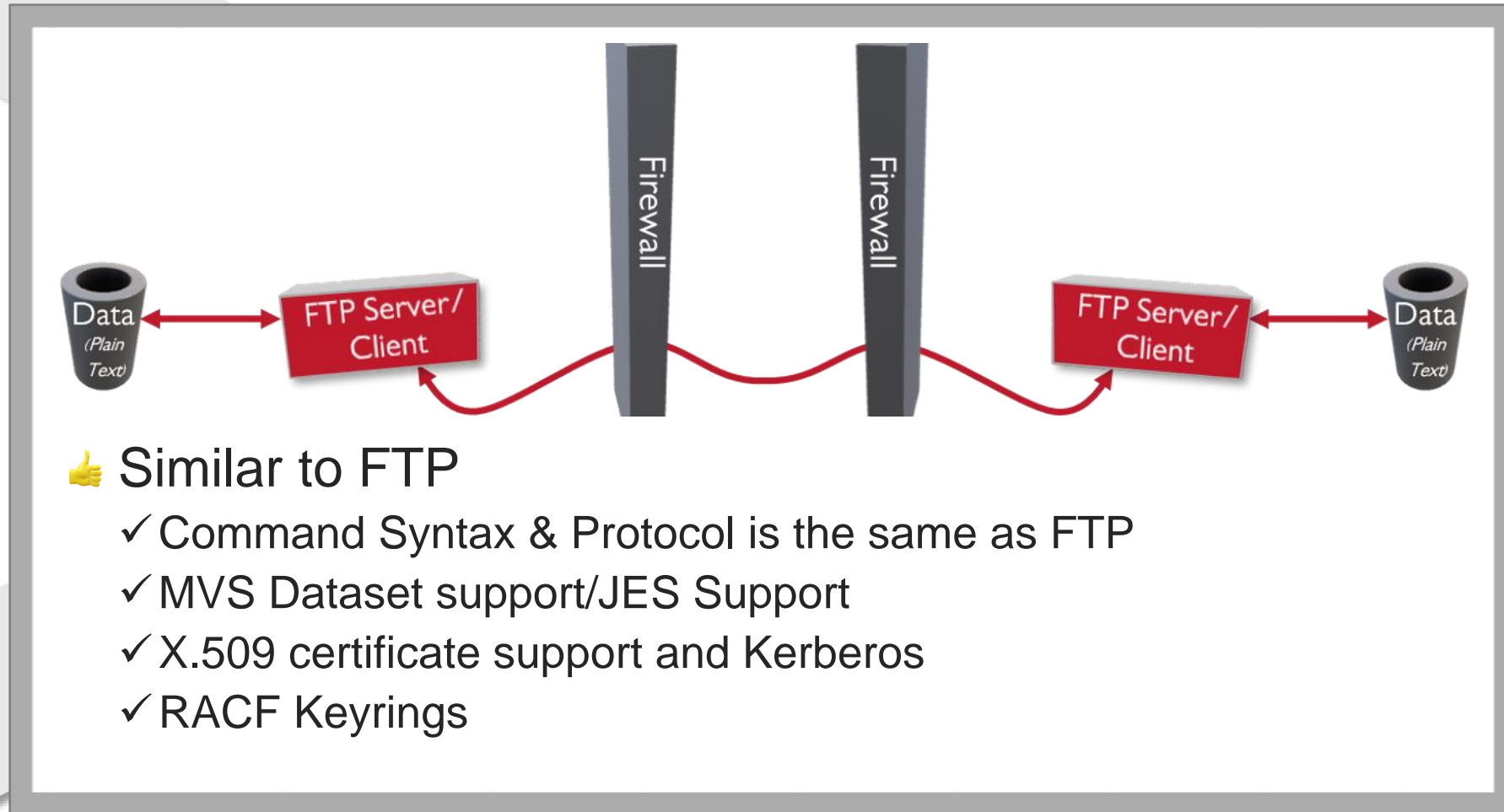


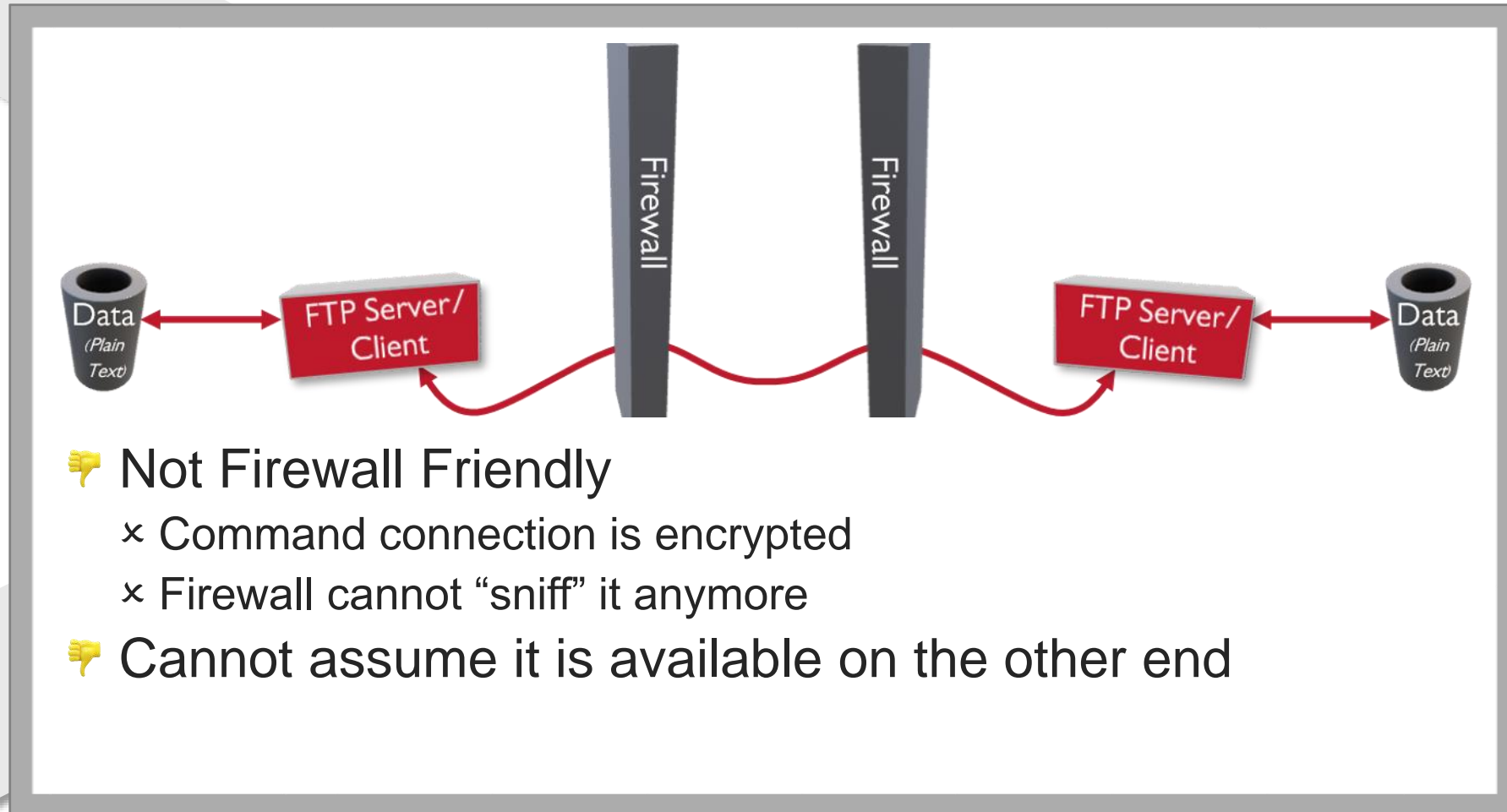
# Why is FTP so Vulnerable?

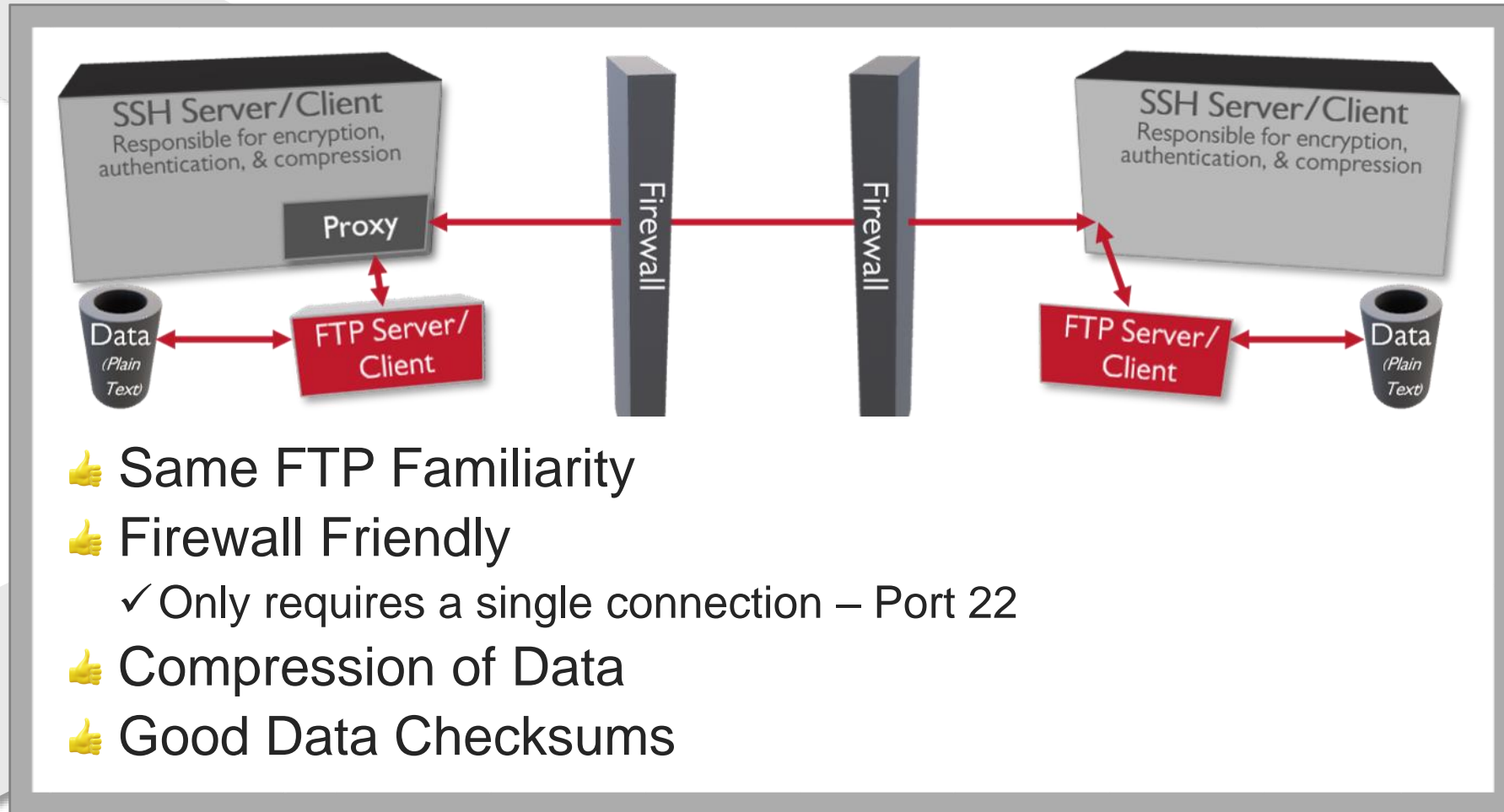


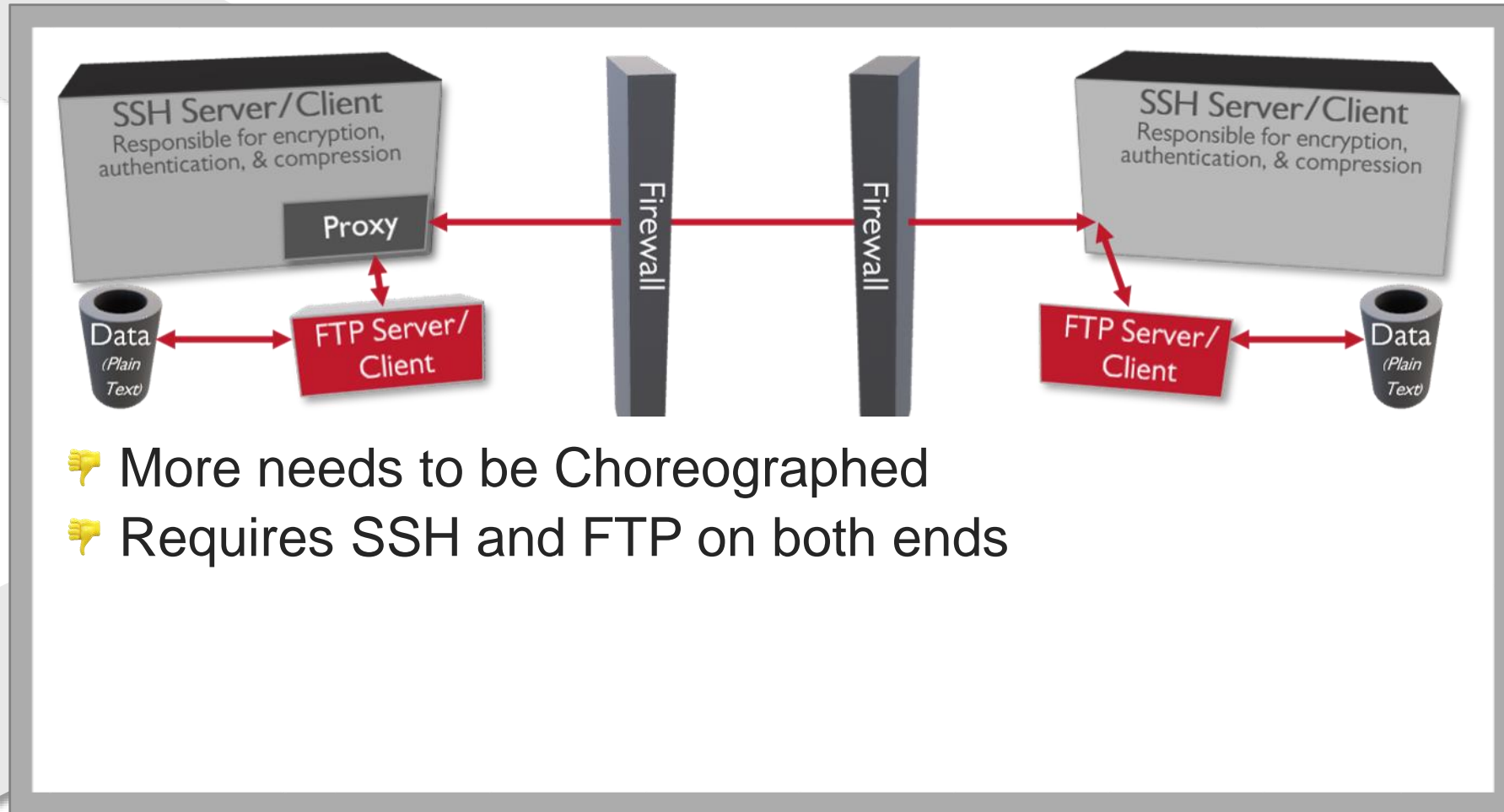
# Why is FTP so Vulnerable?

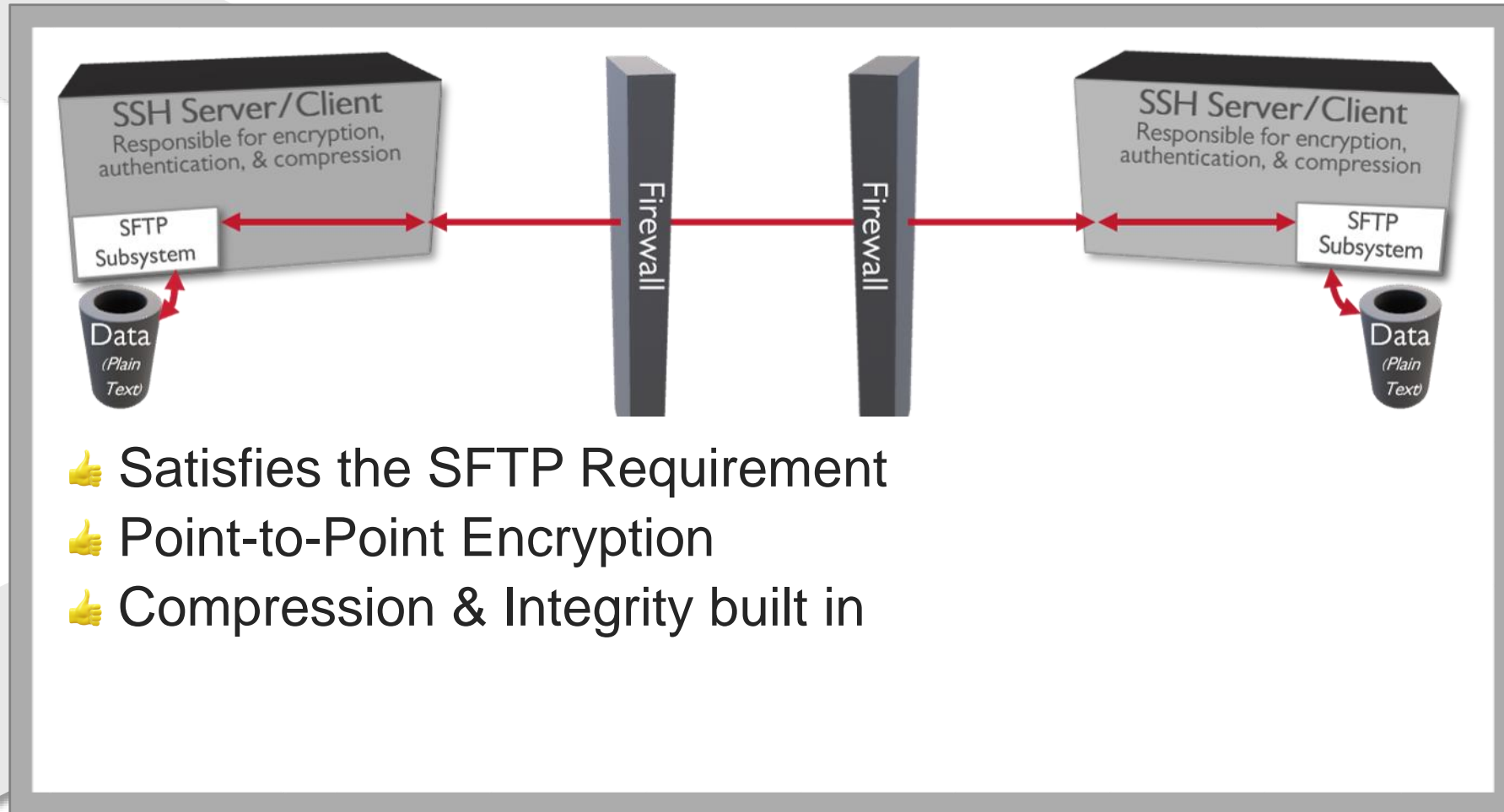






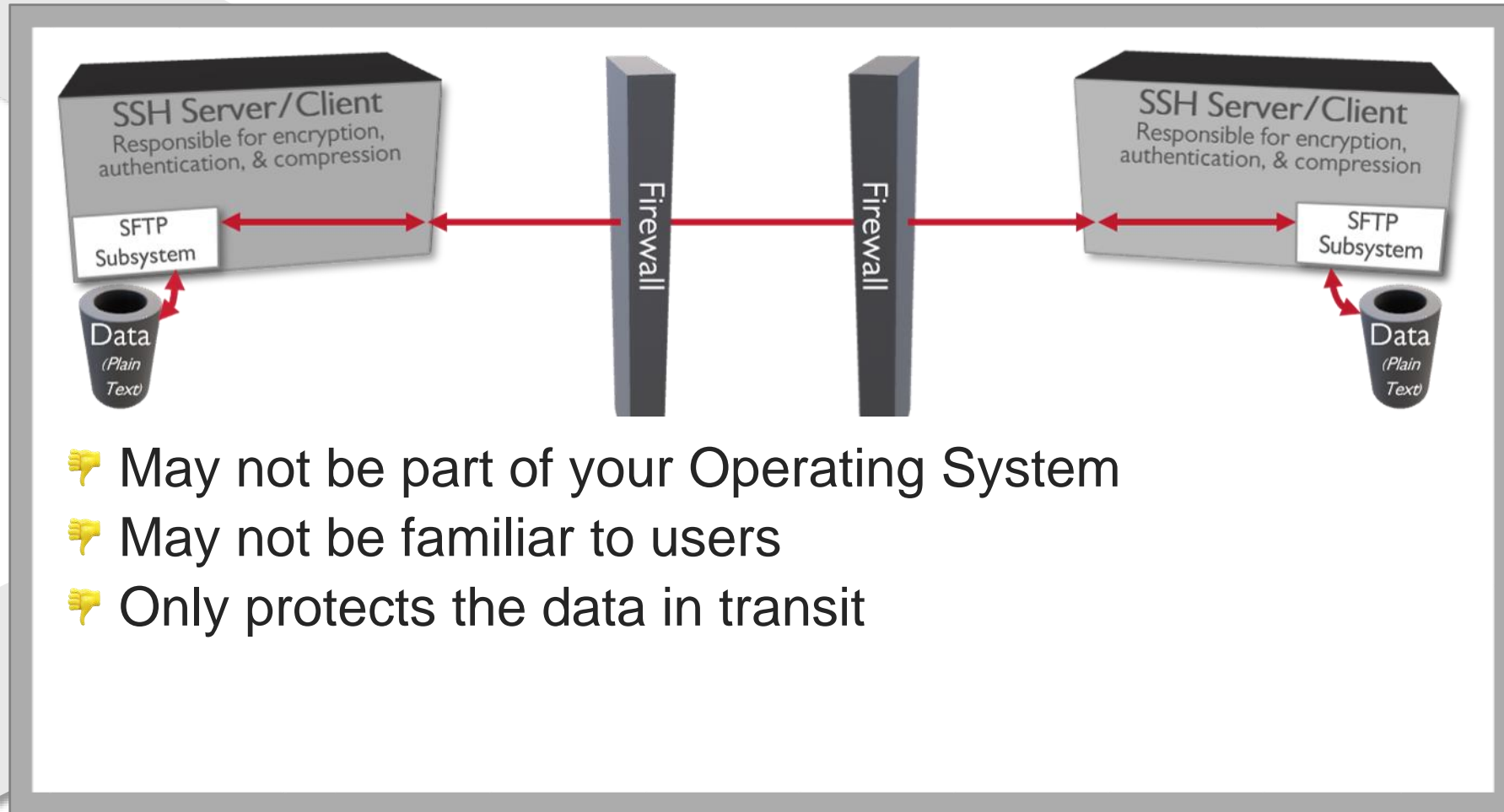




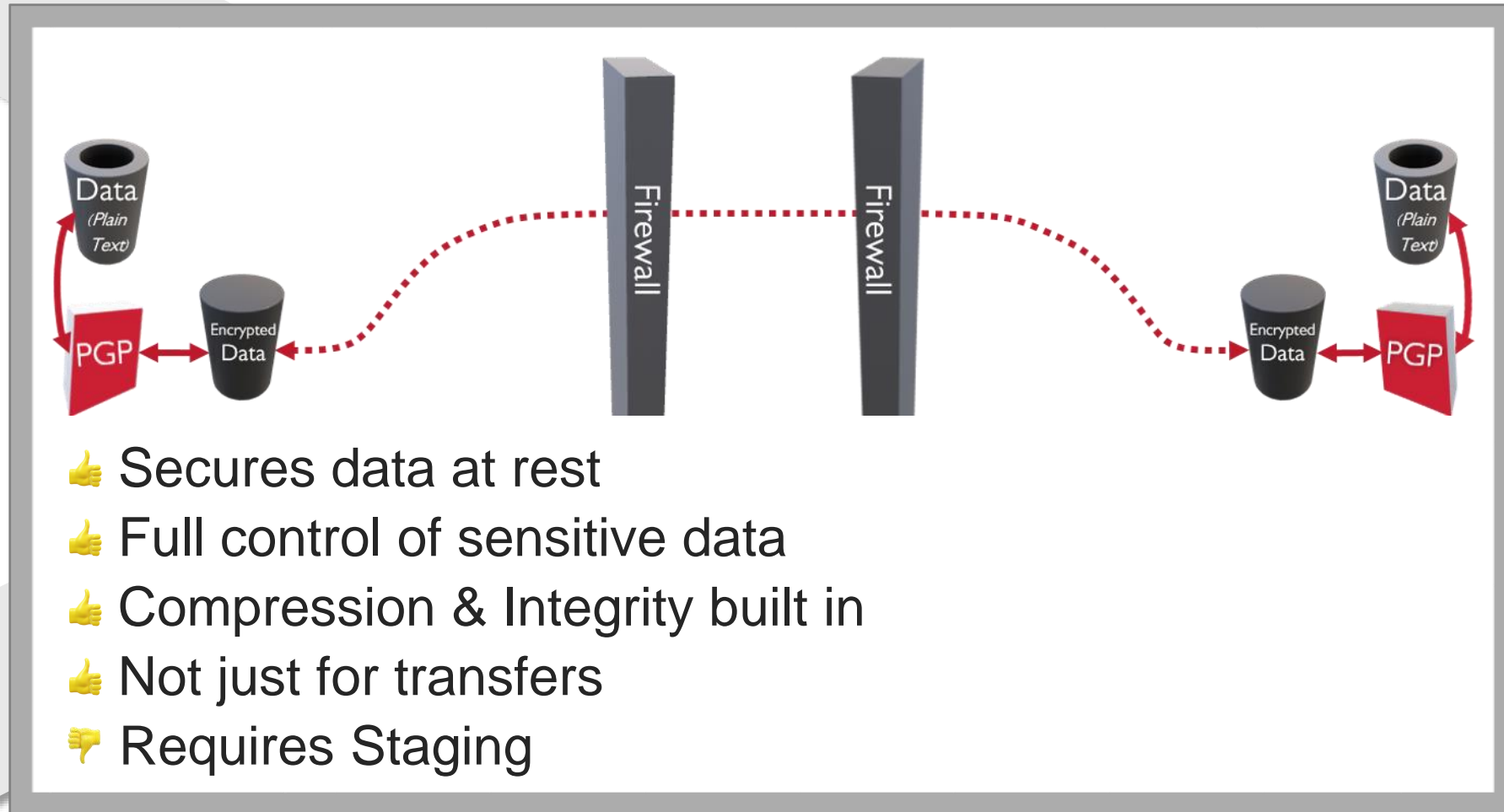


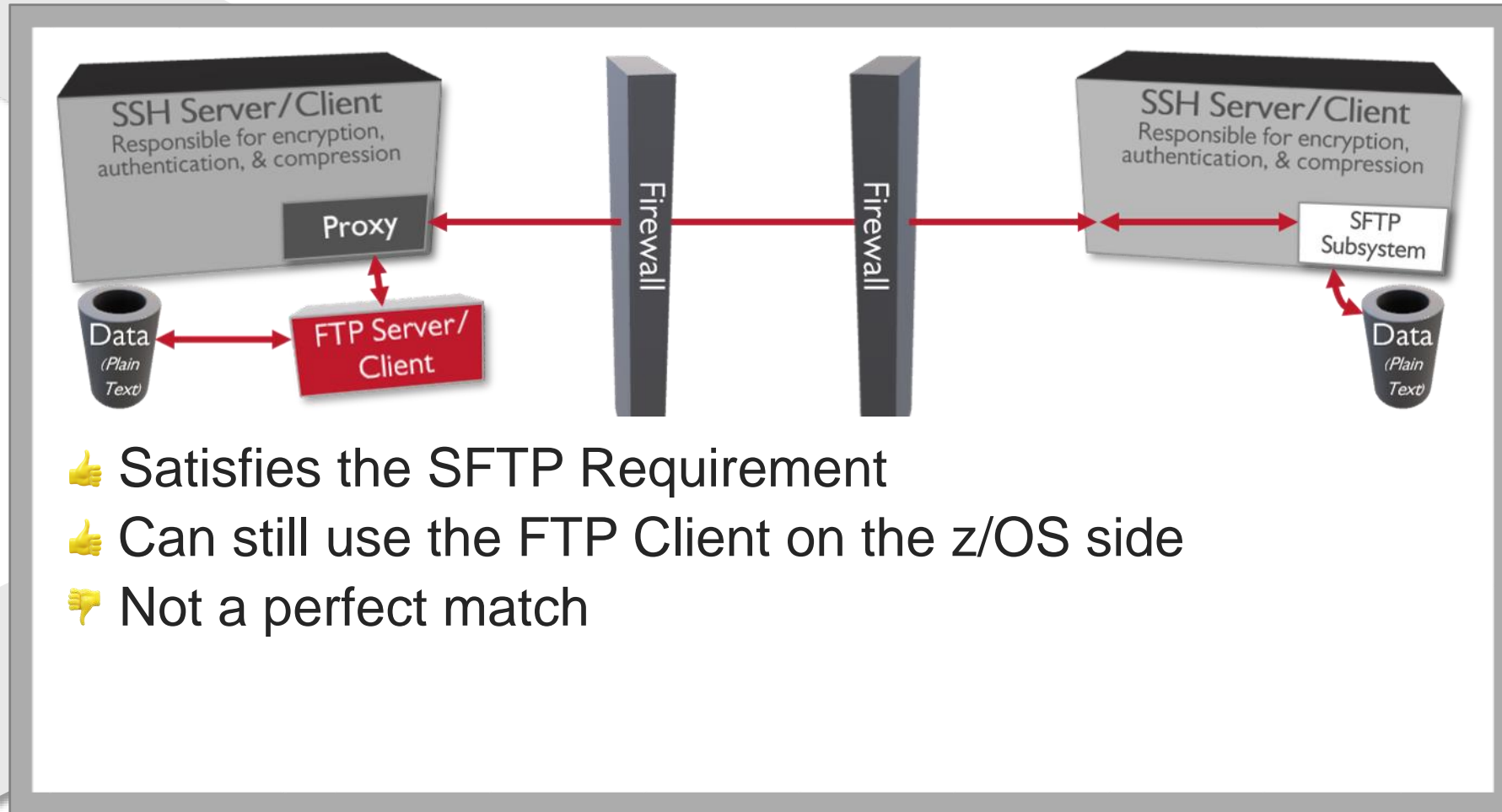
- 👍 Satisfies the SFTP Requirement
- 👍 Point-to-Point Encryption
- 👍 Compression & Integrity built in





- ⚠ May not be part of your Operating System
- ⚠ May not be familiar to users
- ⚠ Only protects the data in transit







## Product Demonstration

- ▶ Tasks completed prior to Demo
  - VFTP and SSH Tectia installed
  - Uploaded the remote servers' Public Key
  - Configured the Tectia Proxy to convert FTP to SFTP
  - Configured VFTP to job ZFTPJOB to the Proxy

**DEMO**



## Summary

- ▶ Many options to consider
- ▶ Not a “one size” fits all situation
- ▶ Could be one solution or a combination of solutions discussed here today
- ▶ What is the end goal?



## Agenda

- ▶ Short overview on “What is a SIEM?”
- ▶ Demo of sending SMF events in real time to QRadar/Splunk
- ▶ Demo of VSA Granular SMF Filtering
- ▶ Suggested SMF events to monitor



## 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





## Security Information & Event Management System

### Security Event Management (SEM)

#### Provides:

- ▶ Event Management
- ▶ Real-Time Threat Analysis
- ▶ Incident Detection & Response
- ▶ Basic Ticketing Capabilities
- ▶ Security Operations

### Security Information Management (SIM)

#### Provides:

- ▶ Centralized Log Collections
- ▶ Long-term Log Collection
- ▶ Log Search and Reporting





## Security Requirement

- ▶ SIEM is the core of a defense-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
- ▶ Your organization likely has a SIEM
  - Why not use it for your mainframe?



## SMF Types Monitored by VSA

Record Type 14 (0E)	INPUT or RDBACK Data Set Activity
Record Type 15 (0F)	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)



## SMF Types Monitored by VSA

Record Type 32 (20)	INPUT or RDBACK Data Set Activity
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



## SMF Types Monitored by VSA

Record Type 62 (3E)	VSAM OPEN
Record Type 80 (50)	RACF Security (Events 1-89; Data Types 1-438)
Record Type 81 (51)	RACF Initialization and SETOPTS
Record Type 83 (53)	RACF Security Audit Reports



## SMF Types Monitored by VSA

Record Type 90 (5A)	Changes to APF Authorized Library Lists (z/OS 2.2)
Record Type 92 (5C) Subtypes 1, 2, 4, 6, 7, 10, 11, 12, 13, 14, 15, 16, 17	Open/MVS File System activity
Record Type 102 (66)	DB2 Database Audit (Classes 1-11; Admin actions)
Record Type 109 (6D)	SyslogD



## SMF Types Monitored by VSA

Record Type 119 (76)

TCP/IP, Telnet, FTP, FTP Client, UDP Close,  
TN3270

- TCPTerm (2), FTPClient (3), StackSS (8), UPDCLOSE (A), TNSvrTerm (15)
- TSOCTerm (17), FTPServer (46), FTPLogonf (48)



## Product Demonstration

- ▶ SMF Events sent to QRadar/Splunk
- ▶ VSA Granular Filtering

**DEMO**





## SMF Type 80

- ▶ SMF Events to monitor
  - Gathered directly from SDS customers



## Summary

- ▶ Many SMF/WTORS events to monitor
- ▶ Separation of Duties
  - Discuss what events are most important to your organization
- ▶ Don't open the "flood gates"
  - Having a product that allows you to choose which events to send to the SIEM is important



## Summary

- ▶ Real-time SMF monitoring is key
- ▶ Compliance requirement
- ▶ Does your company have a SIEM?
  - If so, why not include z/OS as part of your SIEM strategy?



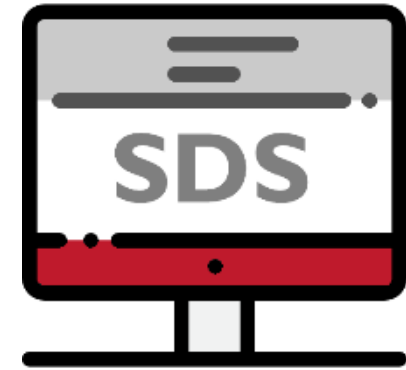
Would you like additional information?



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



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



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