How to Improve Your PCI Compliance

Presented by

Linoma Software

GO ANYWHERE™
Managed File Transfer

GoAnywhere.com

Agenda

- About Linoma Software
- Introduction of Speakers
- Understanding PCI Compliance
- Best Practice Guidelines for a Successful Audit
- Q&A
- Brief Presentation of GoAnywhere MFT
- Close

Linoma Software Background

"I would definitely recommend your product to anyone, not just because it is a great product, but also because you can count on having the support when you need it!"

Linda Humbert
American Management Corporation

- Founded in 1994 – based in Nebraska

Linoma Software ranks
- ★ #17 in Nebraska
- ★ Only MFT Company Listed

- Active R&D with focus on Data Automation and Security
- Responsive technical support – Phone, Web, Email
- Over 3,000 customers around the world
- Nearly 99% renew their maintenance each year

Linoma Partnerships

- Partnered with all major OS vendors including IBM, Microsoft, VMware, Oracle, Red Hat

- Member of the PCI Security Standards Council

Introductions

Guest Speakers

Alan Sabatka, CISA, PCI QSA

Consultant, Continuum Security Solutions

Bob Huerter

Regional Sales Mgr., Continuum Security Solutions

CONTINUUM SECURITY SOLUTIONS℠

PCI Requirements

Bob Huerter & Alan Sabatka, CISA, PCI QSA

April 2016

Roles

- Payment Card Industry – Security Standards Council (PCI – SSC)
- Qualified Security Assessor (QSA)
- Approved Scanning Vendor (ASV)

PCI-Security Standards Council

- The security council formed by the member card brands ultimately responsible for creation, management, and education of the PCI DSS and related entities
- Not responsible for enforcement of standards
  - Card brands are responsible for levying of fines and removal of card payment capabilities
- Visa, MasterCard, Amex, Discover, JCB

Qualified Security Assessors

- A company approved by the PCI SSC to conduct PCI DSS on-site security assessments
- Representatives of QSA companies, certified to perform PCI DSS on-site security assessments
- ‘The Auditor’ – makes compliance determinations, validates controls and writes the ROC

Approved Scanning Vendor

- A data security firm qualified and trained by the PCI SSC to use a vulnerability scanning solution to determine compliance of their customers with the external vulnerability scanning requirements of PCI DSS Requirements 11.2

Definitions

Cardholder Data – Cardholder Data plus Sensitive Authentication Data, as follows:

Cardholder Data includes:	*Sensitive Authentication Data includes:*
• Primary Account Number (PAN) • Cardholder Name • Expiration Date • Service Code	• Full magnetic stripe data or equivalent data on a chip • CAV2/CVC2/CVV2/CID • PINs/PIN blocks

Definitions (continued)

- **Cardholder Data Environment** – any information system (person, process, technology) that store, process or transmit cardholder data
- **PCI Assessment Scope** – any network component, server or application that is included in; connected to; or could impact the security of the cardholder data environment, including virtualization components

PCI Merchant/Service Provider Levels

- Defined by the payment brand
  - Up to 4 levels for each payment brand
- Determined by the acquirer based on transaction volume
  - Based on the number of transactions from a Doing Business As (DBA) or a chain of stores (not of a corporation that has several chains)

PCI Merchant/Service Provider Requirements

- Reporting requirements based on Level
- Payment brands have different reporting requirements for each level (although they're all similar)
- Reporting elements include, ROC and/or SAQ, AOC, ASV scans, Action Plan for Non-Compliance
- Refer to SAQ Instructions to determine your reporting requirements

SAQ Description

- **A** Card-not-present merchants (e-commerce or mail/telephone-order) that have fully outsourced all cardholder data functions to PCI DSS validated third-party service providers, with no electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises.
  Not applicable to face-to-face channels.
- **A-EP*** E-commerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have a website(s) that doesn't directly receive cardholder data but that can impact the security of the payment transaction. No electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises.
  Applicable only to e-commerce channels.
- **B** Merchants using only:
  • Imprint machines with no electronic cardholder data storage; and/or
  • Standalone, dial-out terminals with no electronic cardholder data storage.
  Not applicable to e-commerce channels.
- **B-IP*** Merchants using only standalone, PTS-approved payment terminals with an IP connection to the payment processor, with no electronic cardholder data storage.

SAQ Description (Cont.)

- **C-VT** Merchants who manually enter a single transaction at a time via a keyboard into an Internet-based virtual terminal solution that is provided and hosted by a PCI DSS validated third-party service provider. No electronic cardholder data storage.

  Not applicable to e-commerce channels.
- **C** Merchants with payment application systems connected to the Internet, no electronic cardholder data storage.

  Not applicable to e-commerce channels.
- **P2PE-HW** Merchants using only hardware payment terminals that are included in and managed via a validated, PCI SSC-listed P2PE solution, with no electronic cardholder data storage.

  Not applicable to e-commerce channels.
- **D** ***SAQ D for Merchants:*** All merchants not included in descriptions for the above SAQ types.
- ***SAQ D for Service Providers:*** All service providers defined by a payment brand as eligible to complete a SAQ.

Scoping the Environment

- Maintain an inventory of all systems and facilities
- Maintain current network diagrams
- Maintain current data flow diagrams
- Identify all connected networks
- Validate controls used for segregation of networks
- Identify all information systems that store, process or transmit cardholder data

Scoping Challenges

- “Unknown” data and potential data leaks (logs, shared drives, hard copies, flash drives, email etc.)
- Valid forms of network segmentation
- Long-term storage of cardholder data (legacy)
- Databases, flat files, log files, debug files
- Third party access to cardholder data
- Encrypted data is in-scope if it can be decrypted

6 Goals & 12 Requirements

PCI's 6 Main Goals:

- Build & Maintain a Secure Network
- Protect Cardholder Data
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor & Test Networks
- Maintain an Information Security Policy

Build and Maintain a Secure Network

- Requirement 1: Install and maintain a firewall configuration to protect cardholder data
- Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

- Requirement 3: Protect stored cardholder data
- Requirement 4: Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

- Requirement 5: Use and regularly update anti-virus software or programs
- Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures

- Requirement 7: Restrict access to cardholder data by business need-to-know
- Requirement 8: Assign a unique ID to each person with computer access
- Requirement 9: Restrict physical access to cardholder data

Regularly Monitor and Test Networks

- Requirement 10: Track and monitor all access to network resources and cardholder data
- Requirement 11: Regularly test security systems and processes

Maintain an Information Security Policy

- Requirement 12: Maintain a policy that addresses information security for all personnel

Useful Documents

- PCI DSS – Requirements and Security Assessment Procedures v3.1
- Prioritized Approach for PCI DSS v3.1
- Glossary v3.1
- Information Supplements

PCI Resources

- Your QSA, ASV
- PCI Security Council site
  - https://www.pcisecuritystandards.org/
  - Document libraries
    - PCI standards, addendums, glossary, etc.
  - Lists of approved QSAs, ASVs, applications, POS units, etc.

Contact Info

Bob Huerter

402-215-1759

bob.huerter@cwcsecurity.com

CONTINUUM SECURITY SOLUTIONS℠

CWCSECURITY.COM

PCI and Managed File Transfer

Linoma Software

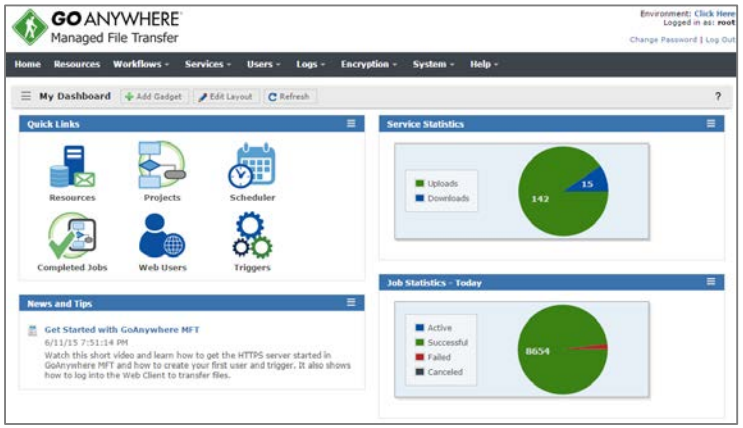
Bob Luebbe, CISSP

Chief Architect, Linoma Software

GoAnywhere MFT

Enterprise-level Features (1 of 2)

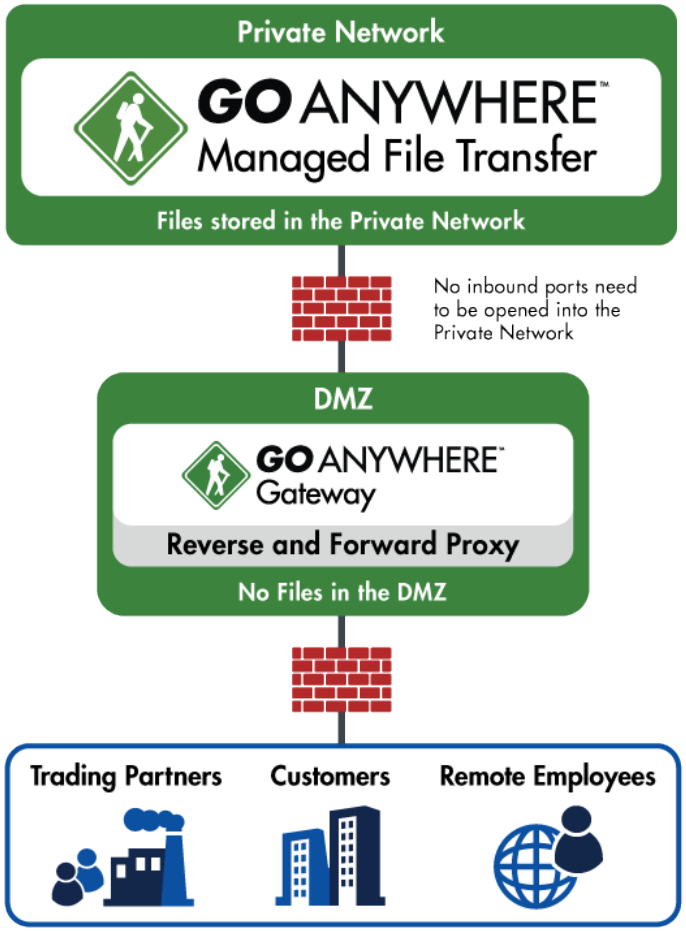
- Supports multiple platforms including Windows, Linux, UNIX and IBM i
- Includes a browser-based interface for all administration
- No programming or scripting is required
- Supports all popular file transfer protocols
- Large files can be transferred with support for auto-resume and integrity checks
- Provides file transfer acceleration over UDP
- Integrates with backend systems (SQL, APIs, Web Services, Java, .NET)



GO ANYWHERE Managed File Transfer

Enterprise-level Features (2 of 2)

- Keeps files in the Internal Network with a DMZ Reverse Proxy (Gateway)
- Protects files “in-motion” and “at rest” with FIPS 140-2 validated AES-256 encryption
- Controls administrator user access with role-based permissions and domains
- Allows jobs to be prioritized and segmented with job queues and run priorities
- Provides High Availability and Load Balancing with Clustering
- Logs all file transfer activity with centralized auditing and reporting



Security Features

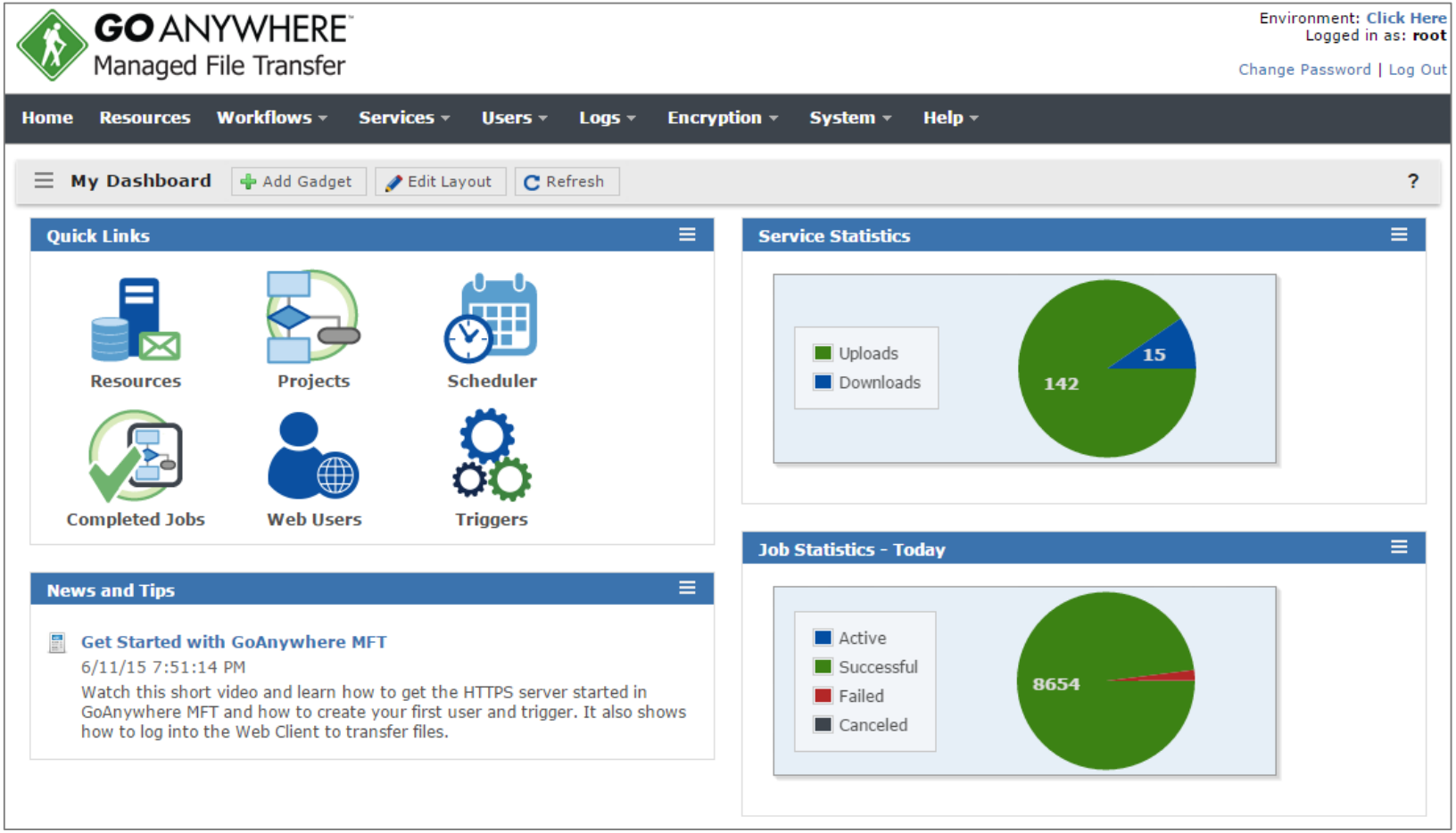
- Helps meet compliance for PCI-DSS, HIPAA, FIPS 140-2, Sarbanes Oxley, GLBA and State Privacy Laws
- Secure Protocols
  - SFTP – FTP over SSH
  - FTPS – FTP over SSL/TLS
  - SCP – Secure Copy
  - HTTPS – HTTP over SSL
  - Open PGP / GPG
  - ZIP with password protection
  - Encrypted email (SMIME)
  - AS2

- AES encryption (key lengths of 128, 192, 256) – NIST standard

- Two-factor Authentication
  - SAML
  - RADIUS (RSA SecurID)
  - SSH Keys
  - X.509 Certificates
- Key Management tools for Open PGP Keys, SSL X.509 certificates and SSH Keys
- SSL protected console

GoAnywhere Administrator

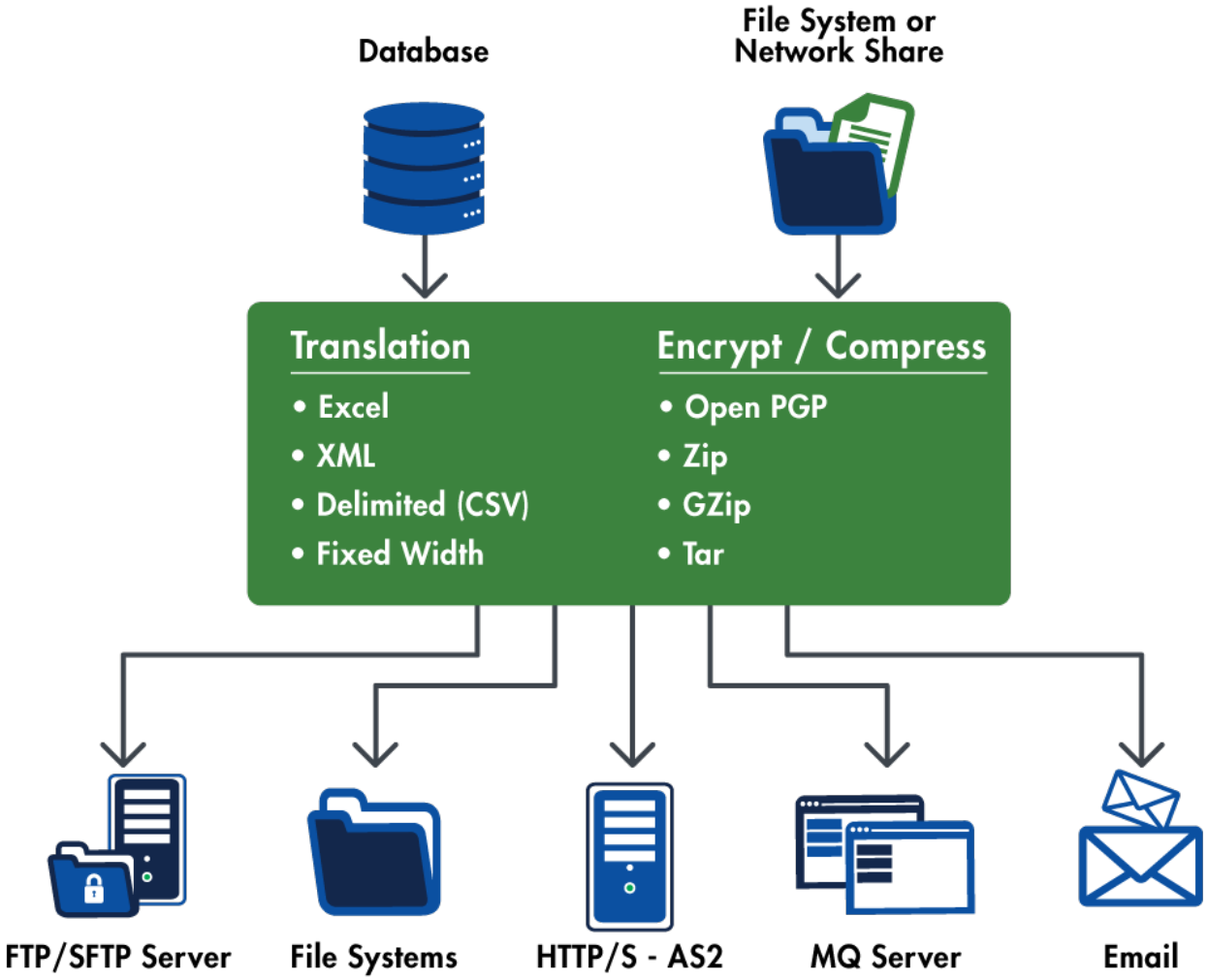
- Browser-based Dashboard
- Intelligent Gadgets
- Drag-n-Drop
- Latest HTML5 Technology



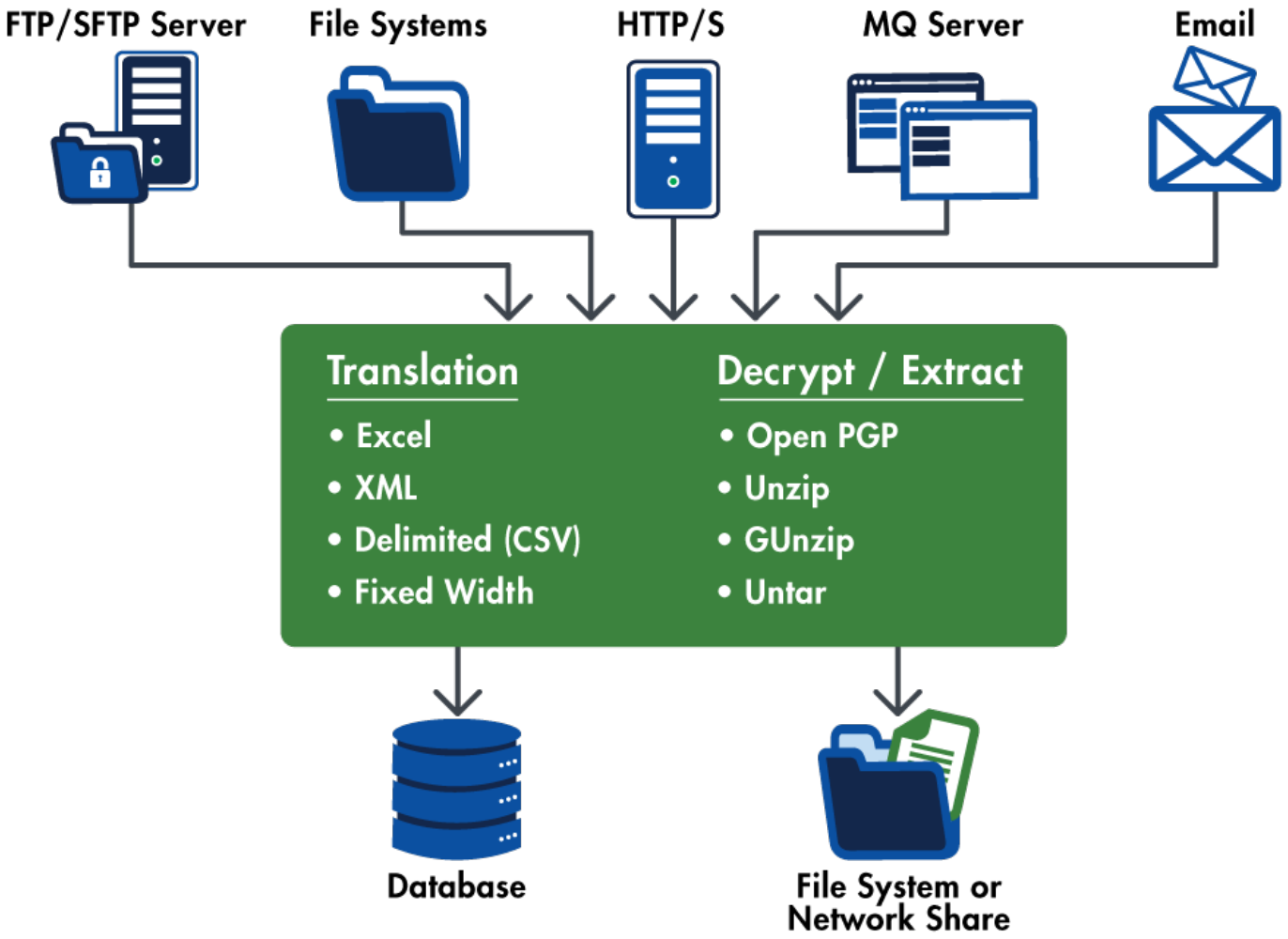
Server Connectivity

- **File Systems**
  - Network Shares (SMB/CIFS)
  - Local File System
  - WebDAV
  - Amazon S3
- **Database**
  - DB2
  - Oracle
  - Microsoft SQL Server
  - Sybase
  - MySQL
  - PostgreSQL
  - Informix
- **Enterprise Messaging (JMS)**
  - Websphere MQ
  - SonicMQ
  - ActiveMQ
  - SwiftMQ
- **FTP**
  - Standard FTP
  - SFTP (FTP over SSH)
  - FTPS (FTP over SSL)
  - SCP (Secure Copy)
- **File Acceleration**
  - GoFast
- **Web Sites**
  - HTTP
  - HTTPS (HTTP over SSL)
  - Web Services
  - AS2
- **Email**
  - POP3
  - IMAP
  - SMTP

Automated Workflow Examples - Outgoing

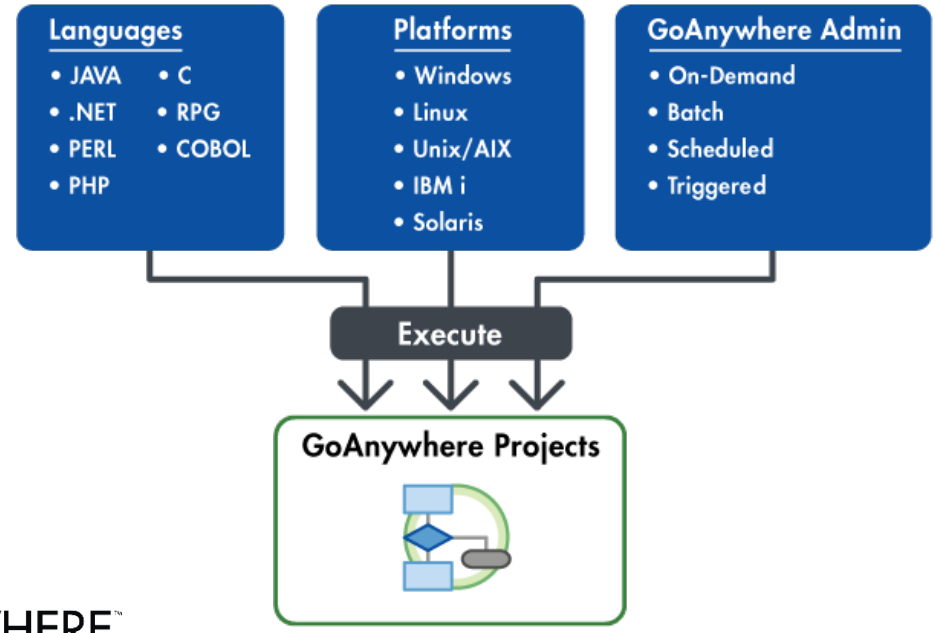


Automated Workflow Examples - Incoming



Executing Projects (Workflows)

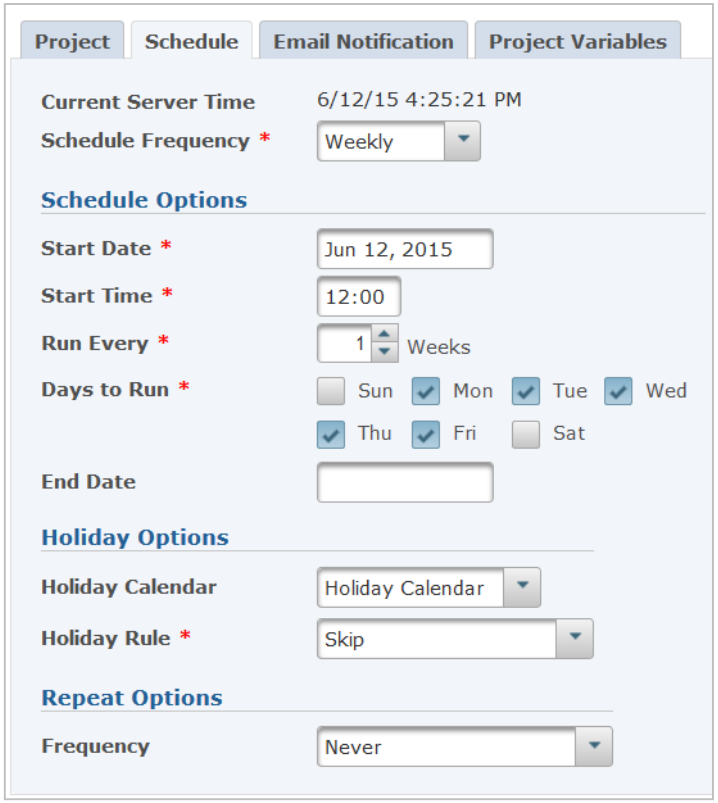
- Execute immediately or in Batch
- Run from browser-based Administrator
- Run from GoAnywhere Scheduler
- Use existing Scheduler
- Execute from OS command line or from within your applications



Integrated Scheduler

- Flexible scheduling:
  - One Time
  - Minutely
  - Hourly
  - Daily
  - Weekly
  - Monthly

- Set job priorities, job queue, etc.
- Custom holiday calendars – Skip holidays or run the business day before or after
- Auto-retry on failures
- Email notifications for success and failures
- Pass in variables to Projects



Optionally, use your own scheduler

Command Line Examples to Run a Project

Windows Example:

```
gacmd.exe –server http://192.168.1.20:8000/goanywhere/
          -user projectManager -password ********
          -command runProject
          -Project /Payroll/SendDirectDeposit
          -variables fileName “deposit.csv” folderPath “/inbound/deposit”
```

Linux Example:

```
sh gacmd -server http://192.168.1.20:8000/goanywhere/
         -user projectManager -password ********
         -command runProject
         -Project /Orders/SendPurchaseOrders
         -variables VendorNumber “423231” Status “Open”
```

APIs are also provided for Java and .NET

Examples to Run a Project from CL

```
0001.00   PGM
0002.00   DCL &MESSAGE *CHAR 80
0003.00
0004.00   /* Run the Transfer */
0005.00   RUNPROJECT PROJECT('/Payroll/SendDirectDeposit') +
0006.00              USER(SFIELD) PASSWORD(******) +
0007.00              VARIABLE((StateCode NE)) PRIORITY(5)
0008.00
0009.00   /* Project failed or could not connect */
0010.00   MONMSG MSGID(GAE1002 GAE1003) EXEC(DO)
0011.00
0012.00     /* Get the error message from the program
0013.00        message queue */
0014.00     RCVMSG RMV(*NO) MSG(&MESSAGE)
0015.00
0016.00     /* Send the error to QSYSOPR  */
0017.00     SNDMSG MSG(&MESSAGE) TOMSGQ(QSYSOPR)
0018.00   ENDDO
```

- Monitor for message IDs
- Any errors are placed in Job Log
- Retrieve any errors with RCVMSG command

RPG procedures are also available to run a Project

Security Audit Report

- Analyze your GoAnywhere product's security settings and determine if they comply with the Payment Card Industry Data Security Standards (PCI-DSS).
- For each security setting, the report will indicate if the setting meets the PCI-DSS standard using one of the following statuses:
  - **Pass** - The setting meets the PCI-DSS requirement
  - **Fail** - The setting does not meet the PCI-DSS requirement.
  - **Warning** - Further research is required to ensure your system meets the specified requirement.

Security Audit Report Example

Security Settings Audit

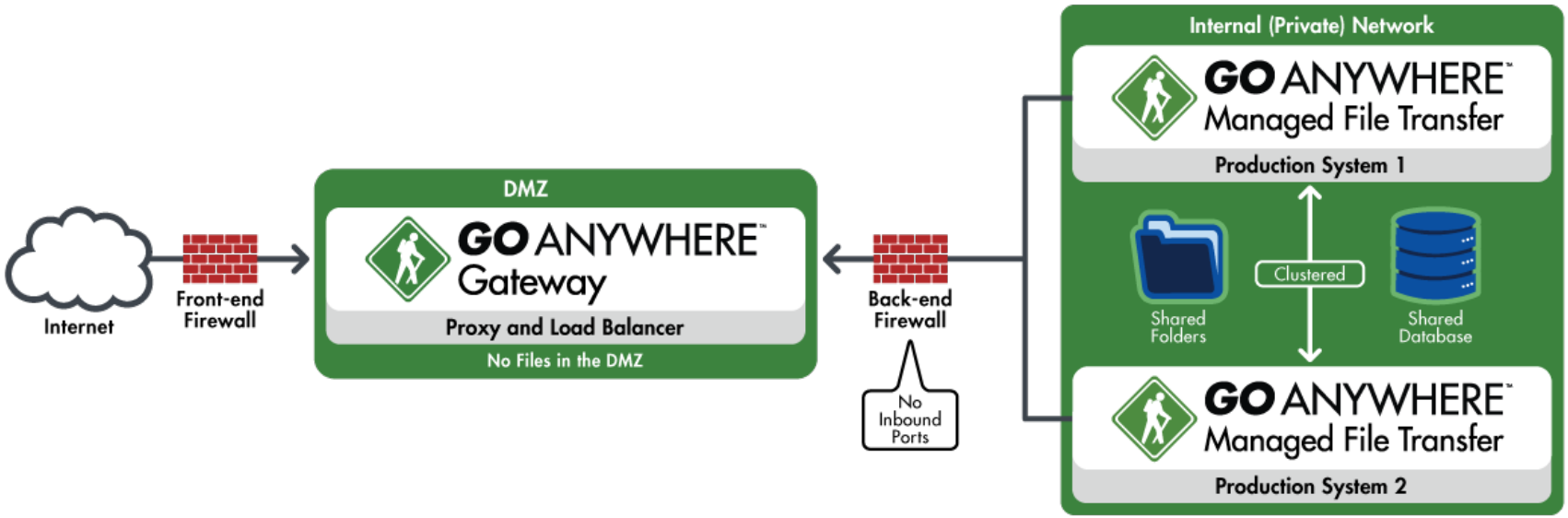
GO ANYWHERE Managed File Transfer

Generated On	6/22/15 9:41:34 AM
Organization	Linoma Software - All
Passed	30
Warning	2
Failed	32
Fatal	1
Not Applicable	0

Security Check	Status	Recommendation	PCI DSS Section
GoAnywhere Gateway is enabled to provide a reverse proxy service for inbound connections.	Failed	Install GoAnywhere Gateway in the DMZ, which will allow ports to be closed into the private network and keep sensitive files out of the DMZ. Ensure that GoAnywhere MFT is installed in the private (internal) network.	1.2.1, 1.3.3, 1.3.7
The default Admin User 'administrator' is disabled or is not using the default password.	Failed	Disable the default 'administrator' Admin User account or change its password to a different value than the default.	2.1
The default Admin User 'root' is disabled or is not using the default password.	Failed	Disable the default 'root' Admin User account or change its password to a different value than the default.	2.1
The default SSL certificate is not used by the HTTPS admin server.	Fatal		2.1
The default SSL certificate is not used by the HTTPS/AS2 service.	Failed	The following HTTPS/AS2 service listeners are using the default certificate: 'default' Create or import your own SSL certificate into the Key Store and configure the HTTPS/AS2 service to use this certificate within the Service Manager.	2.1

Gateway Overview (1 of 2)

- No incoming ports are opened into the private (internal) network
- No sensitive files are stored in the DMZ
- User credentials are maintained/stored in the private network



Installation Requirements

Linux (32-bit and 64-bit):

- Distributions	Red Hat, SUSE, Ubuntu, CentOS (not inclusive)
- Disk space	375 MB per product (not including user data)
- Memory	512 MB minimum per product

Windows (32-bit and 64-bit):

- Operating System	Windows 2000, 2003, 2008 R2, 2012 R2, XP, Vista, 7, 10
- Disk space	375 MB per product (not including user data)
- Memory	512 MB minimum per product

Virtualized Environments:

IBM i (iSeries):

- Operating System	V6R1 or higher
- Disk space requirements	275 MB per product (not including user data)
- Memory requirements	512 MB minimum per product
- JRE	1.6 or later

UNIX / AIX / Solaris / HP-UX:

- Disk space requirements	250 MB per product (not including user data)
- Memory requirements	512 MB minimum per product
- JRE	1.6 or later

Thank You

Have a great day!

GO ANYWHERE™
Managed File Transfer