RAISING THE GAME

SOPHOS

RAISING THE GAME

Updating, Management, and Reporting

- Case Study #1 - LDS
- Case Study #2 - VanOC
- Case Study #3 - Panasonic
- Case Study #4 - Teekay Shipping

LDS - Overview

- The LDS network comprises of 40,000 endpoints worldwide.
- **Majority** of Endpoints are located in some of the **most remote locations on the planet.**

LDS - Overview

LDS - Overview

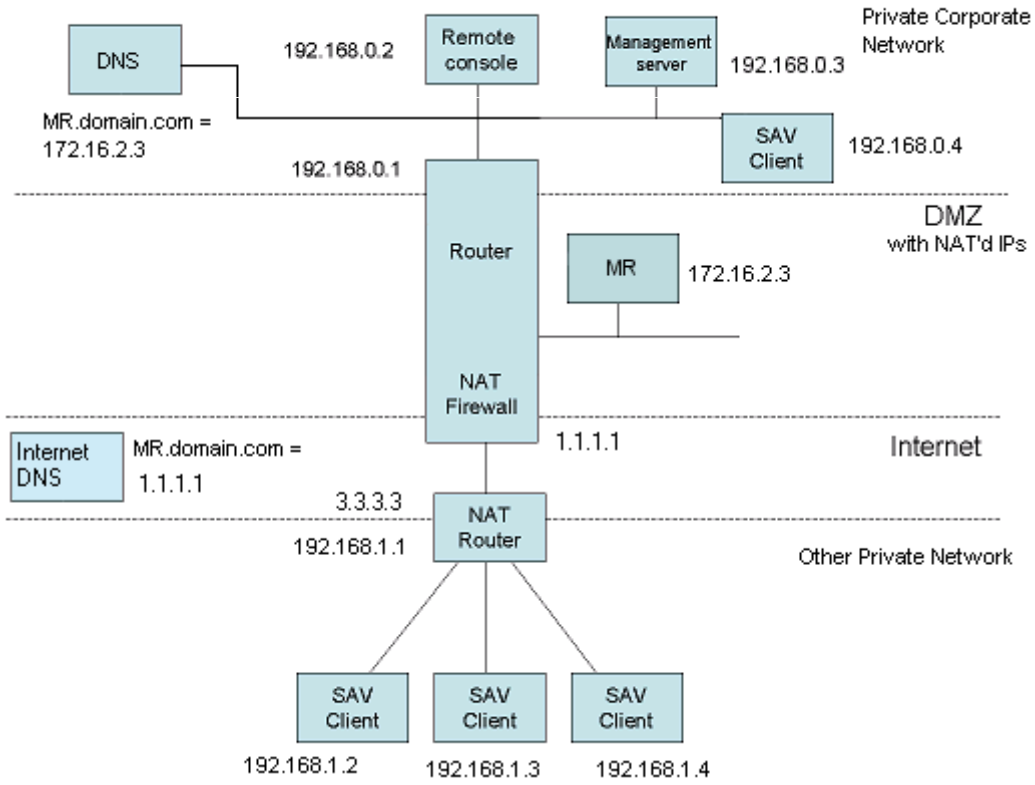
- Endpoint categories:
  - **7,000** Local network **high-speed fiber.**
  - **12,000** Remote Endpoints over **ADSL/Cable links.**
  - **20,000** Remote endpoints over **low-speed dial-up links.**

LDS – Challenges

- Dial-up endpoints only connect to the internet for 5 minutes at a time once a day and need to submit critical data during this period
- Unable to manage or update Symantec on any dial-up machines
- Large number of infections coming from dial-up environment
- No local admins in remote dial-up locations
- No visibility (difficult to track or remediate)
- Endpoints running out-dated protection not effective against latest threats

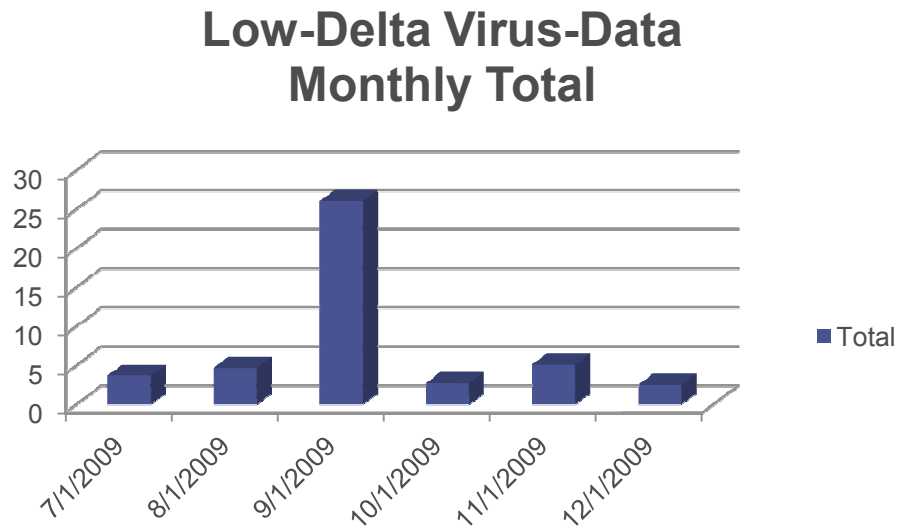
LDS - Solution

- Use Sophos Remote Management System over the internet dial-up link to provide reporting in the Enterprise Console



LDS - Solution

- Leverage the low-delta Sophos Endpoint Software to minimize amount of data transfer to dial-up Endpoints



LDS – Solution Con't

- Configure Endpoint's Remote Management System with increased heartbeat frequency and reduced certification response timeouts
- Installer created for Endpoints to configured to set RMS values post installation:
  - **CertificationIntervalTimeout** = 60 seconds (Default 900)
  - **GetterInterval** = 60 seconds (Default 900)
  - **GetterShortInterval** * = 60 seconds (Default 120)

  * Polling during certification process

LDS – Positive Business Outcomes

- Gained visibility to Endpoints they had not ever been able to report on with any other security vendor which helped **ensure compliance to security policies**
- Able to maintain latest Endpoint protection in regions of the network which were previously thought of as unmanageable **improving their protection against malware**

VanOC - Overview

- The VanOC network represented a highly-visible target during the Vancouver 2010 Winter Olympics. Security and reporting capabilities a very high priority for the network team. Need to respond quickly to new incidents.

VanOC - Challenges

- Splunk used as a mechanism for incident reporting and monitoring
- Splunk SQL connector not implemented need to retrieve data via some other mechanism like Syslog
- Data source to deliver near real-time threat details

VanOC - Challenges

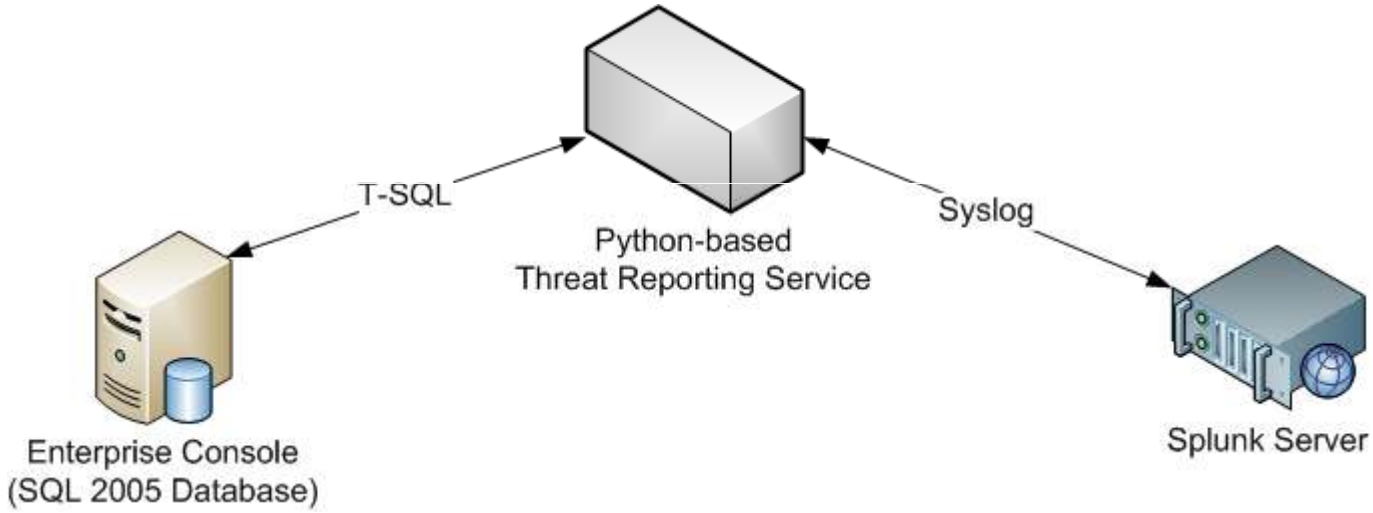
- **Syslog** is a standard for logging program for messages. It allows separation of the software that generates messages from the system that stores them and the software that reports and analyzes them. It also provides devices, which would otherwise be unable to communicate, a means to notify administrators of problems or performance.
- Sophos Enterprise Console does not support Syslog reporting protocol

VanOC - Solution

- Custom Python-based SQL to Syslog tool created
- The custom tool queries the database for any new threat incidences since last check*

  * interval is configurable - VanOC used every 60 seconds
- Threat incident details reported on:
  - **Computer Name**
  - **IP Address**
  - **Threat Type**
  - **Threat Source/Location (Web or Disk)**

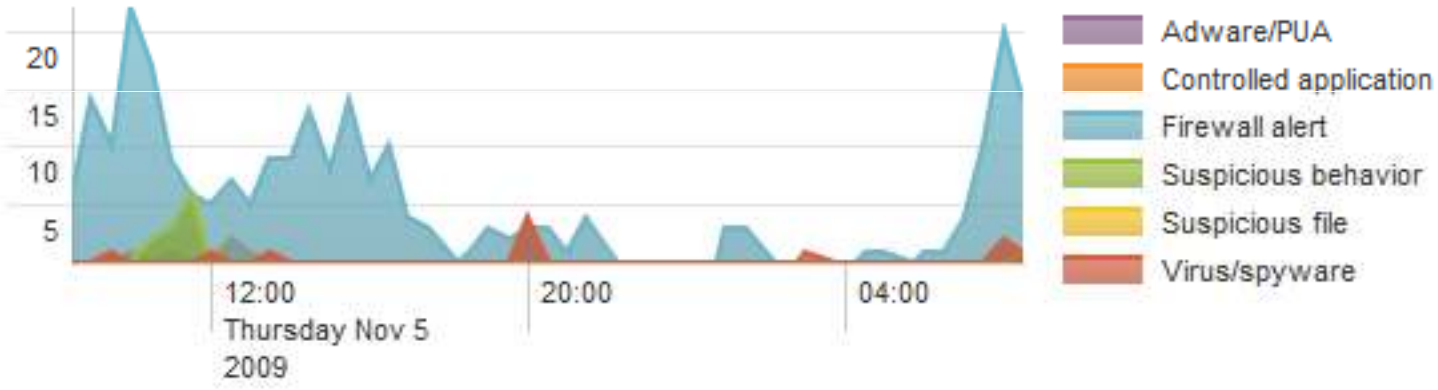
VanOC - Solution



VanOC – Solution Con't

Sophos Alerts for last 24 hours

refreshed: **today at 8:46:06 AM.**



View results

VanOC – Solution Con't

VanOC – Positive Business Outcomes

- Quickly respond to new threat incidences
- Short response times from HIPS/BHO incidents to sample submission which **improved their protection against malware**
- Reporting on internal security strategy success and weakness **improving IT efficiency**
- Minimized administrative effort required to maintain environment **keeping costs low**

Panasonic – Overview

- Panasonic Electric Works Information Systems(PEWIS) provides Network Monitoring, Security and Storage Services to their group companies (Panasonic Electric Works Group).

Panasonic ideas for life

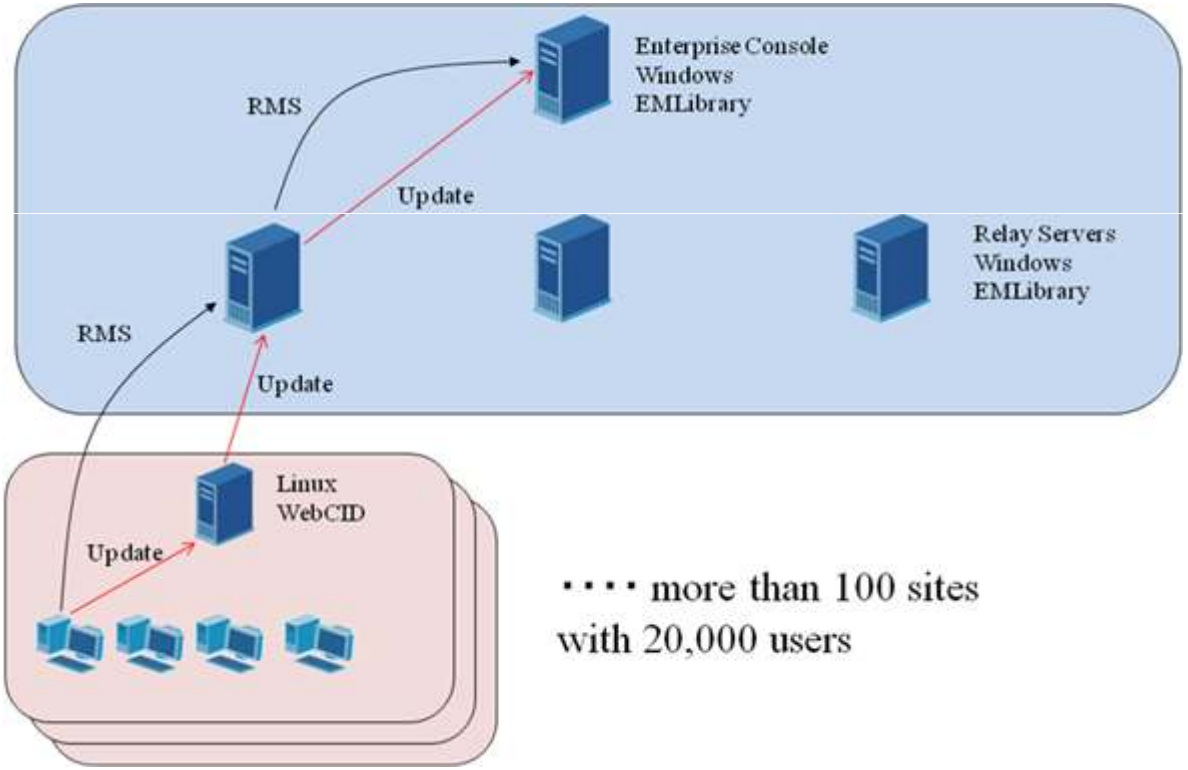
Panasonic – Challenges

- Large definition update files (50MB) cause network bandwidth issues
- Group companies do not use Active Directory strictly a peer-to-peer (Workgroup) environment.
- Many devices which have same machine name, because each group companies are independent . PEWIS cannot force the group companies to use unified naming policy.
- PEWIS does not want to use customized install packages for each group company to avoid complexity and confusion when deploying and managing their system.
- Currently no managed servers at any of the over 200 group company sites

Panasonic – Solution

- Distributed update infrastructure created using Squid on Red Hat Enterprise Linux (RHEL) servers
- Network split into two segments (approx. 100 group companies per). One Enterprise Console Server and 3 Core Update Relay Servers assigned to each segment.
- Load balanced DNS name used for updating
- Low-delta version of Sophos used to limit data transfer

Panasonic – Solution Con't



Panasonic – Solution Con't

- Linux Update Server (Physical)
  - Linux Operating System
  - P4 Processor
  - 1G RAM (512MB reserved for Squid)
  - HTTP Caching (Squid)
  - Single disk
    - Operating System/Squid (2GB reserved for Squid)

Panasonic – Positive Business Outcomes

- Low-cost Linux update servers and low-delta updates allow for
  - **Easily extendable update infrastructure**
  - **Reduction in network load**
  - **Increased update frequency**

Teekay Shipping – Overview

- Teekay's network comprises of 150 ships with 5-10 endpoints on each and each vessel connects back to the shore infrastructure via satellite. There are also 30 ships connected over higher speed links which can be managed via a persistent VPN tunnel between ship and shore. All vessels are identical in terms of network configuration. Each ship has the same server names and IP addresses.

TEEKAY CORPORATION

Teekay Shipping - Challenges

- Satellite connection very costly to transfer data across
- Symantec too expensive to update across Satellite links
- Ships updated every 6 months via a CD delivered by helicopter
- Remediation of out-breaks may require ship to dock for days as a time which is very costly to the business

Teekay Shipping - Challenges Con't

Teekay Shipping - Challenges Con't

- Endpoints running out-dated protection not effective against latest threats
- Only data transfer from shore to Satellite ships via email transfer initiated from the vessel (AMOS Connect)

STRATOS
an Inmarsat company

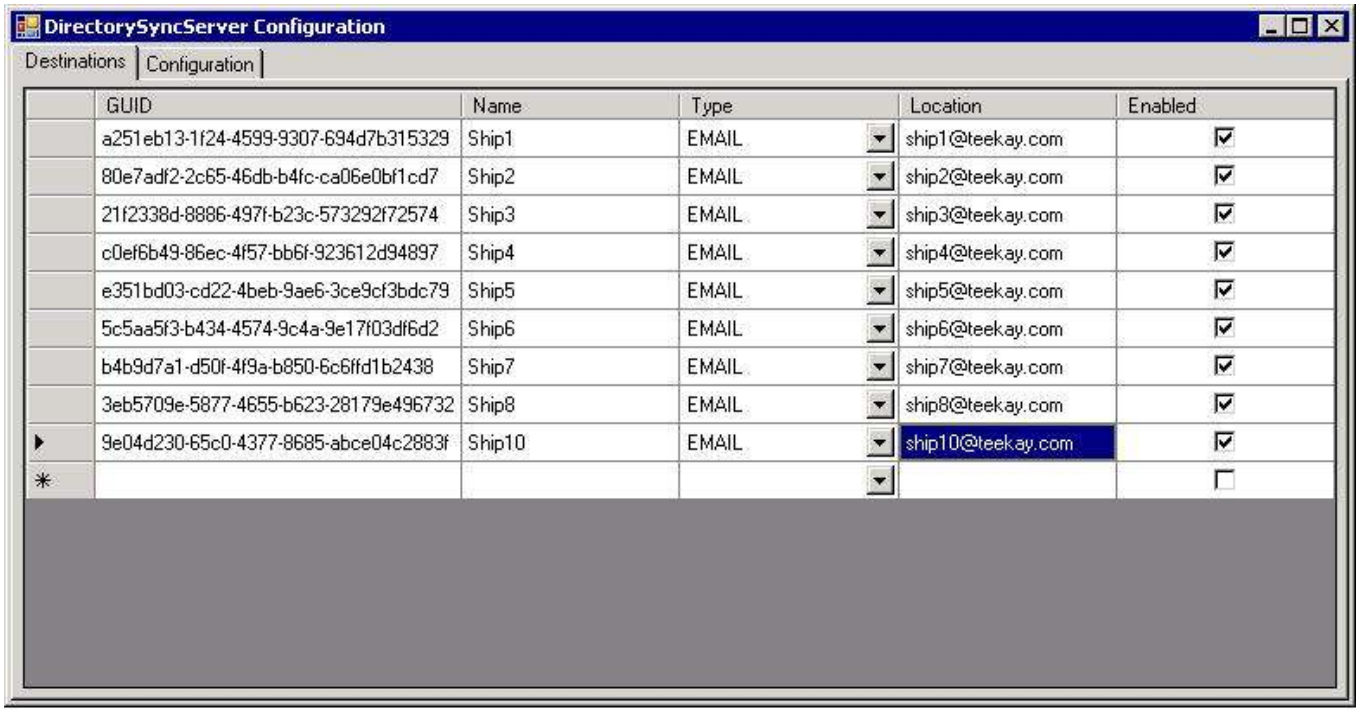
Teekay Shipping - Solution

- Template vessel configured on shore containing preconfigured policies for SAU/SAV/SUM
- RBA configured on template server which allows onboard tech some limited remediation capability without full management of the console

Teekay Shipping – Solution Con't

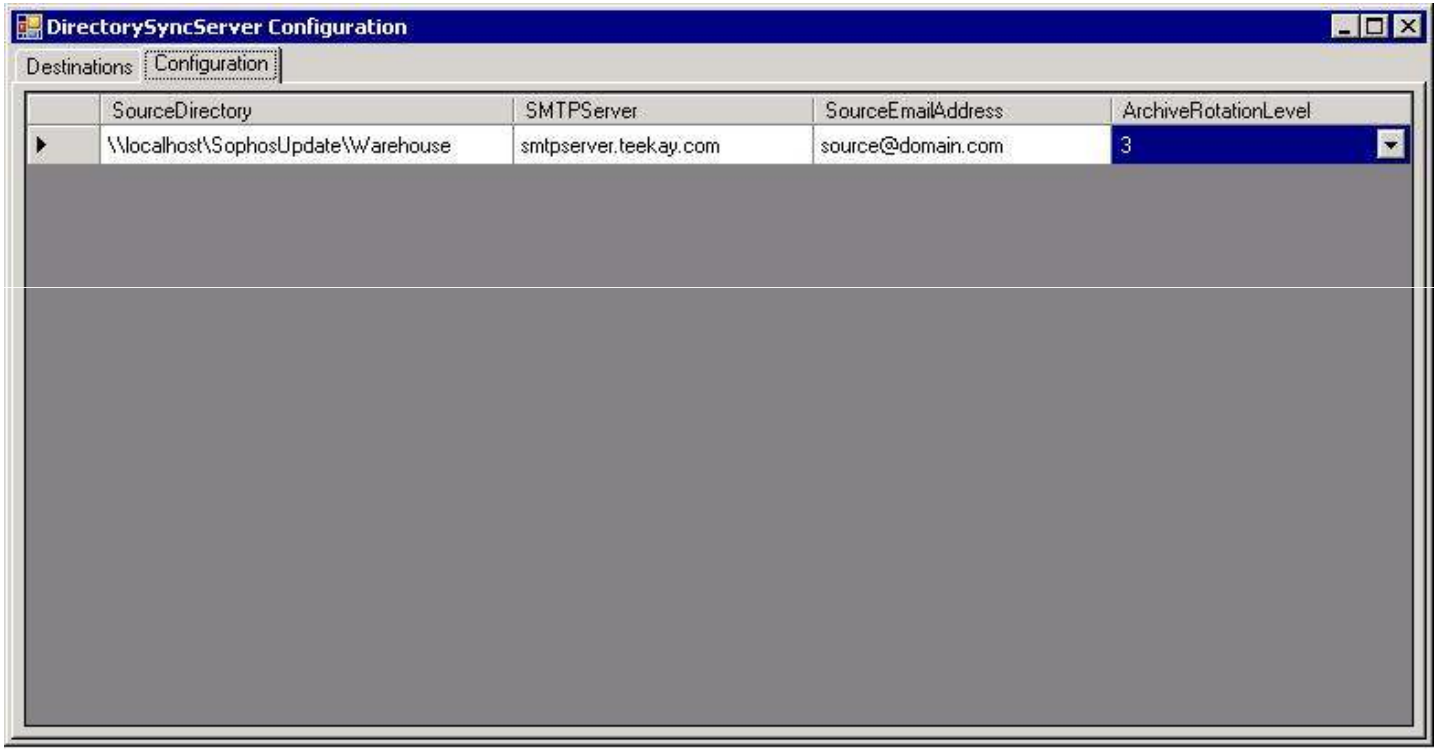
- Custom directory synchronization tool created (DirectorySync)
- Monitors shore server Warehouse directory for change
- Any new/modified files added to tbz2 archive along with a master checksum file
- Archive sent automatically to ship via Email (averages 30% compression over uncompressed data transfer)
- Master checksum file allows for the removal of any old files

Teekay Shipping – Solution Con't



GUID	Name	Type	Location	Enabled
a251eb13-1f24-4599-9307-694d7b315329	Ship1	EMAIL	ship1@teekay.com	☑
80e7adf2-2c65-46db-b4fc-ca06e0bf1cd7	Ship2	EMAIL	ship2@teekay.com	☑
21f2338d-8886-497f-b23c-573292f72574	Ship3	EMAIL	ship3@teekay.com	☑
c0ef6b49-86ec-4f57-bb6f-923612d94897	Ship4	EMAIL	ship4@teekay.com	☑
e351bd03-cd22-4beb-9ae6-3ce9cf3bdc79	Ship5	EMAIL	ship5@teekay.com	☑
5c5aa5f3-b434-4574-9c4a-9e17f03df6d2	Ship6	EMAIL	ship6@teekay.com	☑
b4b9d7a1-d50f-4f9a-b850-6c6ffd1b2438	Ship7	EMAIL	ship7@teekay.com	☑
3eb5709e-5877-4655-b623-28179e496732	Ship8	EMAIL	ship8@teekay.com	☑
9e04d230-65c0-4377-8685-abce04c2883f	Ship10	EMAIL	ship10@teekay.com	☑
				☐

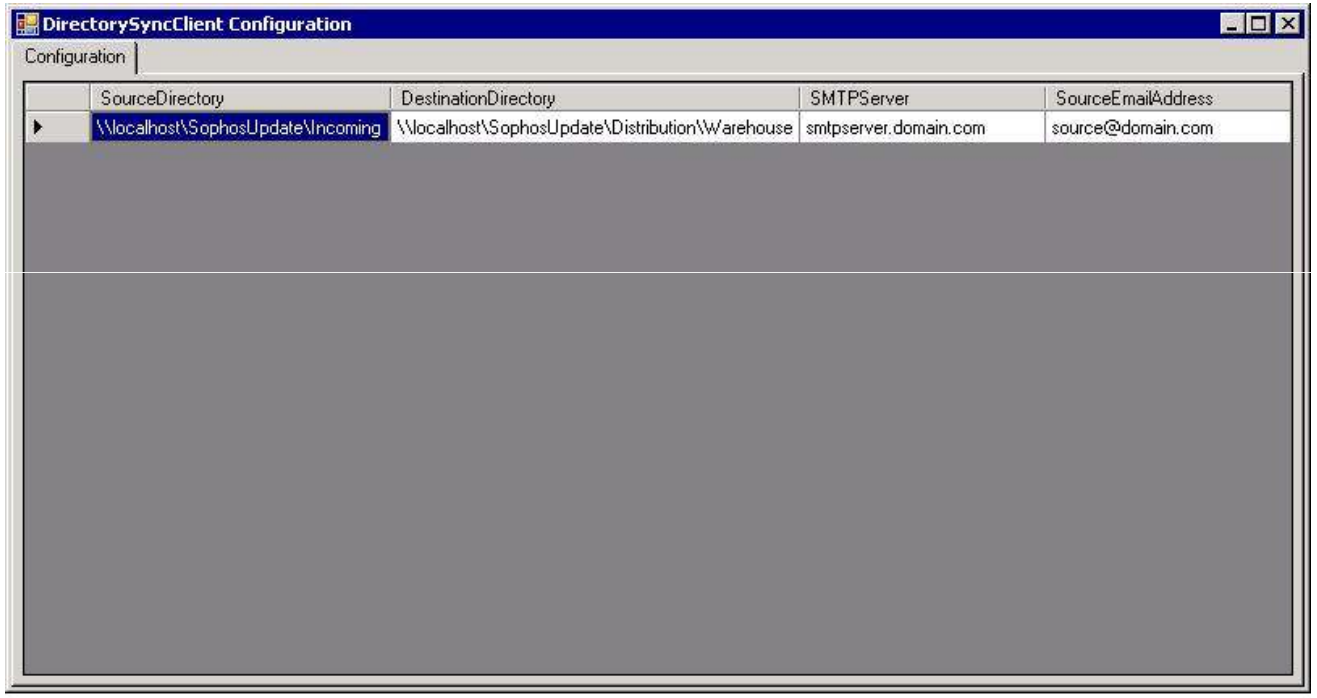
Teekay Shipping – Solution Con't



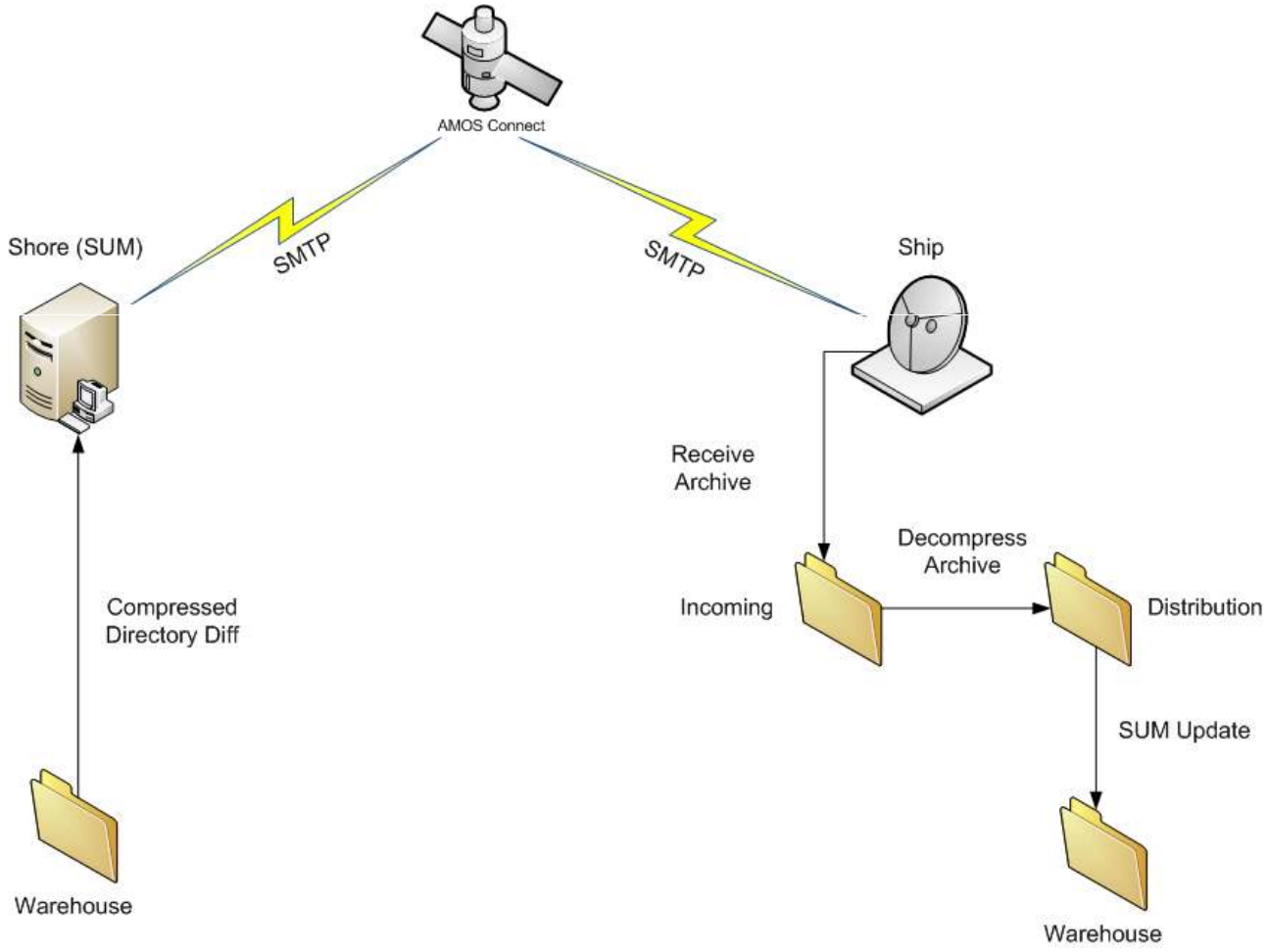
Teekay Shipping – Solution Con't

- Ship server receives Email and places archive in a local incoming directory
- Custom tool on the ship monitors incoming folder for new archive decompresses adds/removes/updates files

Teekay Shipping – Solution Con't



Teekay Shipping – Solution Con't



Teekay Shipping – Positive Business Outcomes

- Increased update frequency ensures Endpoints are running current threat protection which in-turn **limits remediation costs**
- RBA policy which allows for onboard threat remediation coupled with automated cleanup tasks allow for the **automation/completion of tasks onboard which previously cost thousands of dollars to manage/resolve**