USE CASE

Secure Software Updates

Dell's PowerProtect Cyber Recovery Data Vault Paired with Owl Data Diodes

Use Case Summary

CHALLENGE

Need to securely perform software updates on a data vault while minimizing risk to the vault network

SOLUTION

SSUS – Owl's secure software update solution that leverages data diode technology to securely transfer approved files into the vault to make updates

BENEFITS

Vault operators do not need to physically access the vault to perform software updates and only approved files will enter the secure vault

Cybersecurity Challenge

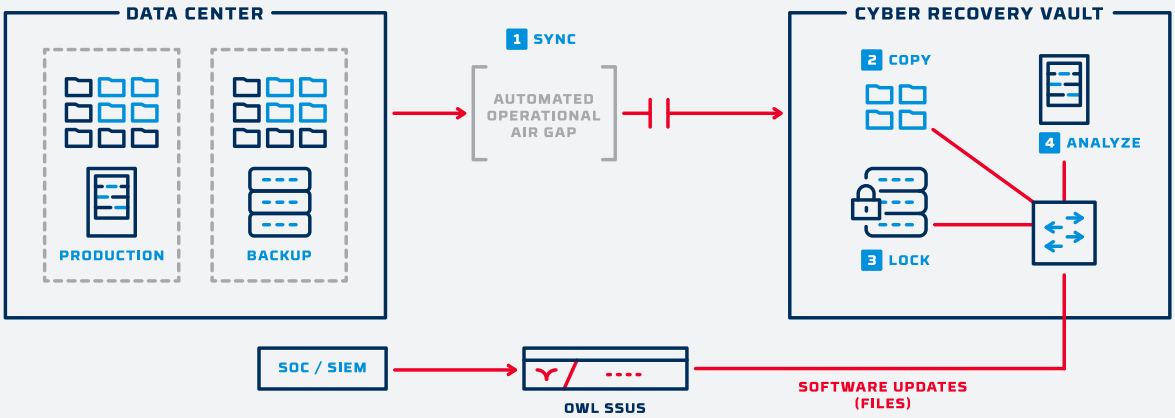
Just like any other network, a secure data vault contains computers, servers, control systems, databases, etc. that require software updates on a recurring basis. In order to update these devices, software updates may be typically downloaded from the vendor's website to a local server, copied onto a portable media device (USB drive) and hand-carried into the secure network for installation. According to the DHS, FBI, and NSA, this method is not a good choice. In the process of downloading, saving, copying to portable media, and uploading on the secure vault network, the source file could be intentionally attacked or the portable media device itself could be compromised with malware lurking. Alternatively, files may be brought into the vault network via other electronic means that do not provide network isolation and/or proof of authenticity.

Secure Software Update Solution

Dell has partnered with Owl Cyber Defense to provide organizations with a secure, hardware-enforced cybersecurity solution that enables organizations to securely make software updates inside the vault. For organizations that need a reliable and secure method to verify and transfer software patches into the vault, Owl's SSUS solution provides hardware-enforced one-way transfers for files. SSUS uses Owl's data diode technology to transfer the file(s) across the security boundary into the Cyber Recovery vault. SSUS eliminates the security risk resulting from "Walk-Netting" a file across the security boundary using portable media devices like flash drives. An administrator maintaining the vault creates a manifest file including hash codes from software providers. When a file is copied onto the SSUS solution for transfer, SSUS calculates the hash of the file, compares it to the hash in the manifest, and if it matches, transfers the file to the vault through the hardware-enforced SSUS data diode.

Key Benefits

- One-way only architecture – only files that match the hash code are allowed into the vault
- Vault operators do not need to physically enter the vault to perform software updates
- SSUS supports several checks including a file extension check, ASCII scan check, malware scanning, and validating the file against a manifest (or list) consisting of pre-configured hash numbers
- Non-routable protocol break - strips all source IP and MAC routing information to prevent unauthorized communications



Solution Architecture

To securely update software in the data vault, a vault operator will request a hash code from the software vendors that will be independently entered into a manifest on SSUS. When a file is copied onto SSUS for transfer, SSUS calculates the hash code of the file, compares it to the hash code in the manifest and if there is a match, it is transferred to the secure vault, otherwise it is quarantined. For additional security and information assurance, SSUS provides enhanced controls to enable content inspection, file type/extension checks, antivirus, and ASCII scanning. SSUS also permits implementation of two-person authentication approval and release process. These comprehensive security features allow organizations to establish a security policy which explicitly prohibits the use of portable media devices to transfer data between security levels and only allows low-to-high and peer to peer transfers.

Technical Specifications

OPERATING CONDITIONS:
- 32°F to +110°F / 0°C to 43.33°C
- 5% to 90% humidity non-condensing

POWER SUPPLY:
- Input: 75-230 VAC
- Estimated Normal operating Usage 10-16 W/side
- Max. 20W per side

STORAGE:
- -40°F to 158°F / -40°C to 70°C
- 5% to 90% humidity non-condensing

VIBRATION:
- Vibration: (IEC 60255-21-1)
- Vibration 1g(10-500Hz) (Operational)
- Vibration 2g(10-500Hz) (Operational and Non-Operational)

CHASSIS SIZE:
- 16.5” W x 1.75” H x 13” D
- 41.91 cm x 4.5 cm x 33 cm

UNIT WEIGHT:
- 7.92 lbs./3.6 kg.

MEAN TIME BETWEEN FAILURE (MTBF):
- 11+ years

OWL Cyber Defense

Owl Cyber Defense Solutions, LLC leads the world in data diode and cross domain network cybersecurity. With a constant focus on customers in the military, government, critical infrastructure, and commercial communities, Owl develops market-first, one-way data transfer products to meet a variety of operational needs, from entry level to enterprise.

For more information on Owl, or to schedule a demo, visit www.owlcyberdefense.com