USE CASE

Time Synchronization in the Vault

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

Summary

Challenge

Need for time synchronization in the vault while minimizing risk to the vault's air-gapped architecture

Solution

Owl Talon™ MK100 - Owl's one-way data diode cybersecurity solution that securely relays a source of time to the vault from the production network

Benefits

Vault operators can securely create a source of time in the vault for scenarios where time is critical to further reporting and analysis

Cybersecurity Challenge

Time is critical in a data vault. You may need to perform a recovery and collect historical data from a certain time period. Or in the event of an attack, you will need to analyze logs to identify and eradicate that attack, making time synchronization in the vault critical to those scenarios. The challenge is creating a source of time in the vault while minimizing new threat vectors to the air-gapped architecture of the vault.

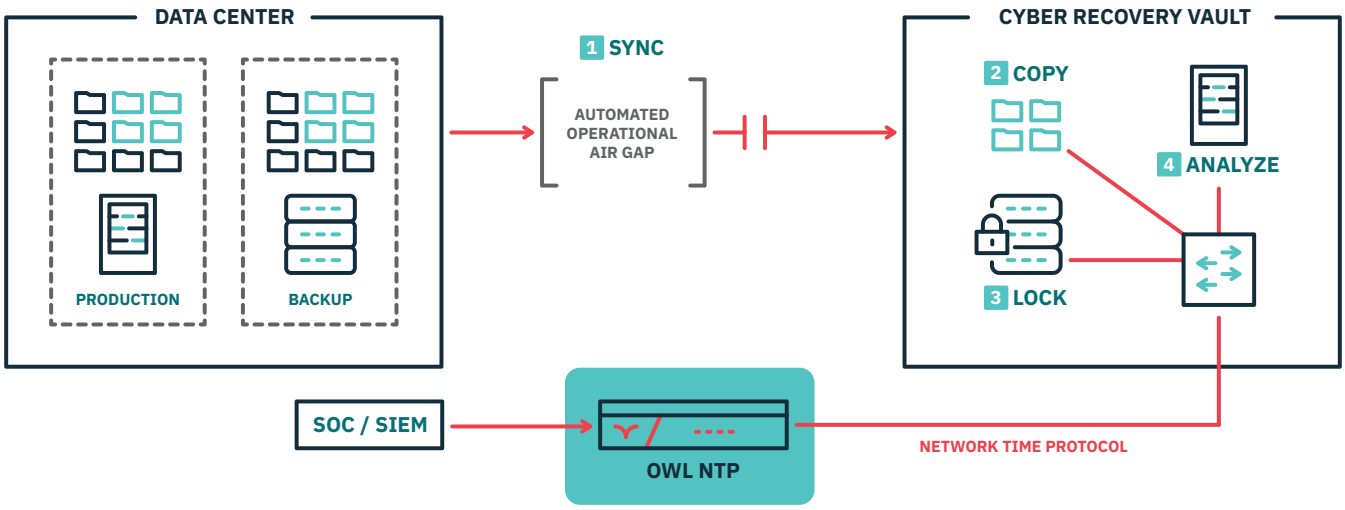
Secure Network Time Protocol (NTP) Solution

Dell has partnered with Owl Cyber Defense to provide organizations with a secure way to create a source of time in a data vault. Owl's Network Time Protocol (NTP) solution is a hardware-enforced data diode that points one-way into the vault. The Owl Talon™ MK100 data diode provides time synchronization in the vault by taking a trusted source of time from the production network (SOC, GPS device), and relaying that time to a node sitting on the vault side. That node inside of the vault then becomes the NTP server and can be used as a source of time within the vault.

Key Features

- → 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



Technical Specifications

Case

19” 1U Rackmount Chassis with 4-wire PWM

Processor

1 x Intel Xeon

Memory (RAM)

1 x 8GB DDR5 UDIMM

Primary Storage

1x 128GB SATA SSD

Power Supply

1 x 300W Flex-ATX Power Supply—US Power Cord

Input: 100~240 VAC

Estimated Normal operating usage: 120 Watts

Mounting

Rackmount ears + half-depth rackmount Sliding Rail Kit

Operating Conditions

10 - 35 C, 20% ~ 90% non operation humidity (non condensing)

Approvals/Certifications

Pending regulatory certification

Interfaces

Front: 2 USB (3.0)

Rear: 1 DB15 (VGA) 2 RJ45 (1GbE), 1 dedicated IPMI 2 Type A (USB3.2 Gen1) 1 UID button, 1 UID LED

OTO Data Diode Card: 2 RJ45 (1GbE)

Dimensions

Chassis Size:

With Mounting Ears: 482.6mm W x 257.1mm D x 44.4mm H

Without Mounting Ears: 431.8mm W x 257.1mm D x 44.4mm H

Unit Weight: 4.35 kg / 9.59 lbs.

OWL Cyber Defense™

Owl Cyber Defense Solutions, LLC, headquartered in Columbia, MD, leads the industry in data diode and cross-domain network cybersecurity solutions for faster, safer and smarter decision making. We create solutions tailored for high-risk sectors including the military, government and critical infrastructure. Our advanced technologies enable secure, near-instantaneous collaboration, bridging network barriers to protect critical missions. With a focus on scalability and interoperability, Owl ensures that organizations can maintain secure, reliable, and compliant communication channels against evolving cyber threats.

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

203-894-9342 | owlcyberdefense.com