USE CASE

Secure Monitoring & Reporting

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

Use Case Summary

CHALLENGE

Monitoring and reporting on vault performance and system health data without introducing risk to the air-gapped network architecture

SOLUTION

OPDS-1000 - Owl's one-way data diode cybersecurity solution that securely transfers system health and performance data out of a secure vault to a SOC without introducing risk

BENEFITS

Vault operators do not need to physically enter the vault to extract system health and performance data. They can be assured that the data diode is protecting the air-gapped vault architecture, while enabling the critical data to be transferred to a SOC for monitoring and reporting

Cybersecurity Challenge

Monitoring a data vault is critical to identify suspicious activity and monitor performance and system health information. However, with an air-gapped vault architecture, reporting would typically need to be reviewed in person at the physical location of the vault for the highest level of security.

Software-based data transfer solutions can be hacked and manipulated, putting the data vault at risk. Organizations need the strongest level of security to protect the air-gapped architecture of the vault, while securely transferring data to a Security Operations Center (SOC) for monitoring and reporting on performance and system health data, as well as suspicious activity.

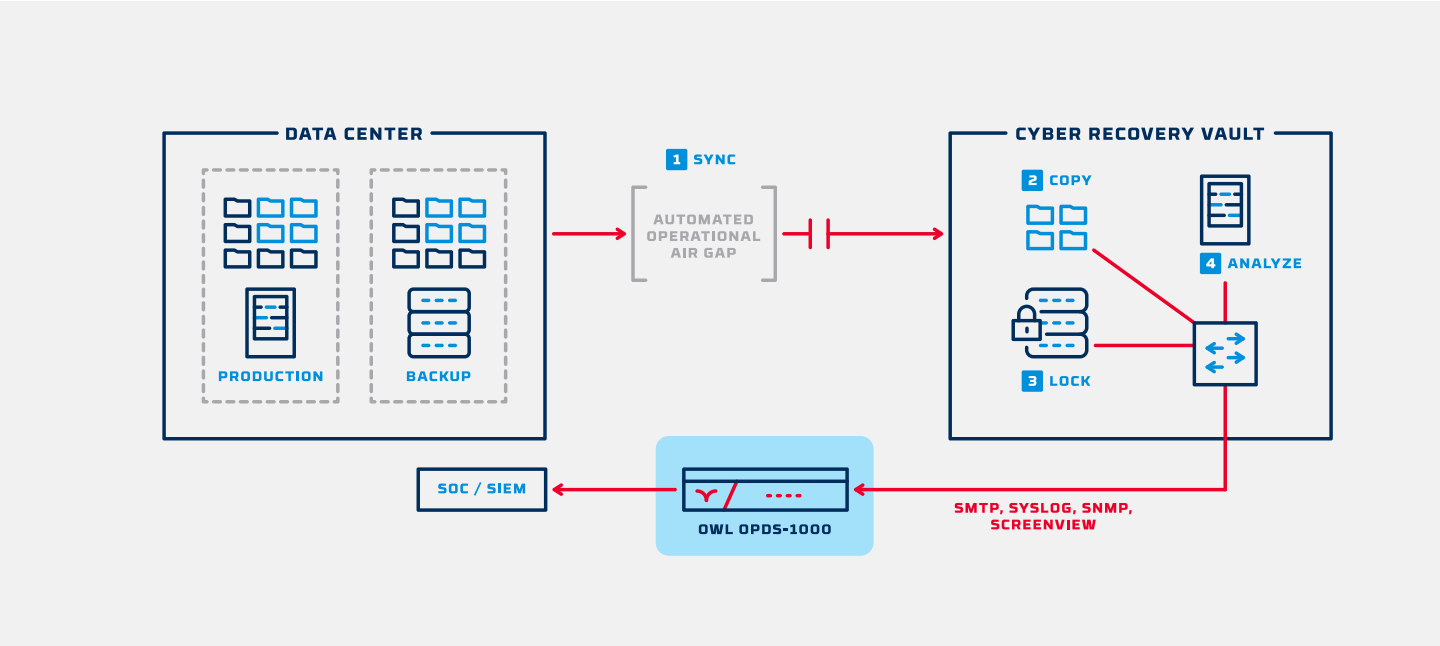
Secure Monitoring and Reporting Solution

Dell has partnered with Owl Cyber Defense to provide organizations with a secure, hardware-enforced cybersecurity solution that enables organizations to securely transfer monitoring and reporting data one-way out of a secure vault, without introducing new threat vectors to the vault.

Owl's data diode solution (OPDS-1000) maintains the air gap that is established by the Dell Cyber Recovery vault to prevent any possibility of unauthorized access to the vault. Data integrity reports can securely flow out of the Cyber Recovery vault network in real-time through a data diode to allow timely action in the production environment, so authorized operators know immediately if backups fail or threats are detected. By deploying a data diode, organizations can securely transfer system health information in real-time and allow log files and SNMP data to reach SIEM systems without delay.

Key Benefits

- One-way only architecture – hardware-enforced to prevent any threats from entering the secure vault
- Non-routable protocol break – strips all source IP and MAC routing information to maintain network isolation and prevent unauthorized access
- Vault operators do not need to physically enter the vault to extract critical information
- Data can flow out of a secure vault to a SOC in real-time
- Supports simultaneous data streams of SMTP (email), Syslog, SNMP traps, and Virtual Screenview all in one device



How It Works

By implementing a data diode in a Cyber Recovery Vault architecture, data can securely flow one-way out of the vault through a hardware-enforced data diode to a SOC for remote monitoring and reporting. Owl data diodes are comprised of two communication cards that work as a pair. The first card is the "send" card and only has electronic components that allow it to send data, with no ability to receive. The second card, the "receive" card, only has electronic components that allow it to receive data. Data can only flow in one direction and a physical barrier or "air gap" is created between the two networks.

A protocol break also occurs, which is the process of terminating a data transfer protocol, sending the data payload via a different protocol, and then re-establishing the original protocol before data travels to its destination. This makes it impossible for any external threat actor to ping, deconstruct, or otherwise obtain information about the source network. Proxies in the data diode's network interface allow two-way communication to continue seamlessly on each side of the data diode, with a one-way link in between. This allows organizations to create one-way data flows using protocols that are inherently two-way, such as TCP/IP. SMTP (email), Syslog, SNMP Traps, and Virtual Screenview. Data streams can be securely transferred over the data diode simultaneously, all in one device.

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:
- Black Anodized aluminum with Locking Top

MOUNTING SYSTEM:
- (1U) Rack Mount, tabletop

NETWORK CONNECTIVITY:
- 1000 base-T copper
- Separate Ethernet connections for network traffic and remote administration
- Physical connectors: 8P8C (RJ45)

THROUGHPUT:
- Supports three configurations: standard capacity (26 Mbps), mid capacity (155 Mbps), and high capacity (1,000 Mbps)

SHOCK:
- Shock: (IEC 60255-21-2)
- Shock 10g 11ms (Operational)
- Shock 30g 11ms (Operational and Non-Operational)

COOLING:
- Conductive cooling through enclosure side walls with High Life Expectancy/Low Noise Fans

APPROVALS:
- FCC Class A compliance
- CE Mark
- CB Certificate: DE 2-034658
- EN 62368-1:2014/AC:2015
- International Common Criteria Certification – EAL4+ Certified
- VCCI

ISO:
- Manufactured using ISO 9001:2015 certified quality program

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

LOCAL ADMINISTRATION:
- VGA connector for monitor
- USB connectors for keyboard and mouse