


NETWORK SECURITY SOLUTIONS


Mid-Market National Bank Securely Captures and Collects Forensic Data Files


Company Overview

CASE SUMMARY:

 **INDUSTRY:**
Banking

 **CHALLENGE:**
Enable transfer of forensic data files to bank's secured forensic lab network while preserving the isolation of the lab environment.

 **SOLUTION:**
OPDS-1000 data diodes deployed to capture and contain forensic evidence.

 **BENEFITS:**
One-way data flow enables file transfer to forensic lab, while ensuring the lab environment remains isolated and secure from external cyber threats.

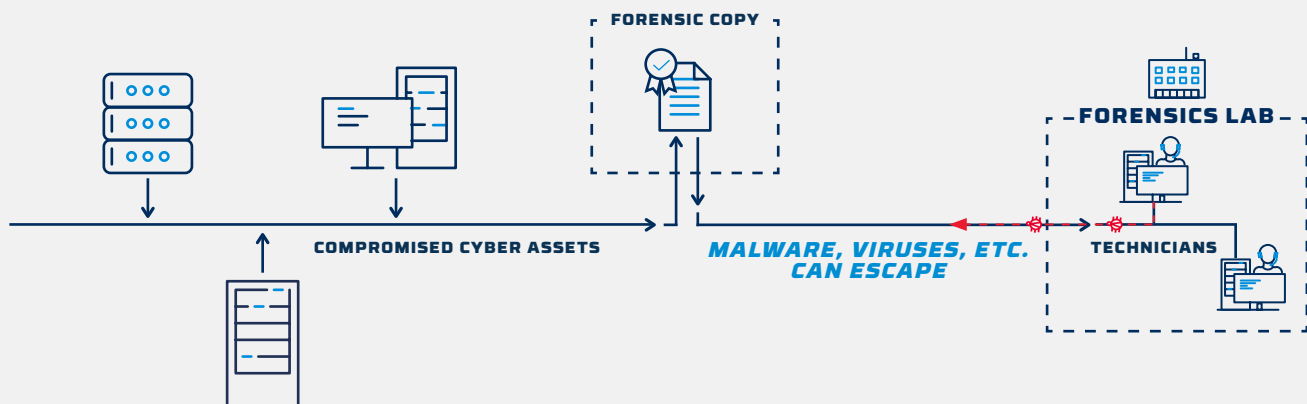
A mid-market national bank with over \$500 million in assets and capital.

Cybersecurity Challenge

Capturing and analyzing cyber asset forensic metadata related to exposure of bank cyber assets (laptops, servers, PCs, etc.) to various networks, websites, users, etc. is vital to investigating and ultimately remediating cyber threats. The bank needed a method to capture, package, and copy compromised cyber assets and their associated metadata, then securely transfer them to their forensic lab for analysis. The bank also wanted to ensure that only trusted files were allowed into the lab network, and that no potentially infected data would be allowed out.

REQUIREMENTS:

1. Compatibility with software utility which scans compromised assets and their metadata and packages them into forensic data files
2. Enable a secure method to transfer the forensic data files from the bank network to the forensic lab environment
3. Preserve "disconnected" secure architecture of forensic lab network, keeping it inaccessible from external networks



SOLUTION

OPDS-1000 was selected to transfer the forensic data files, packaged by a 3rd party software tool, to the secured lab environment. The diodes also preserved the disconnected nature of the forensic lab network, preventing access from external networks.



Deployment



OPDS-1000

Owl Perimeter Defense Solution - 1000

Self-contained 1U data diode, purpose-built for network segmentation and deterministic, one-way data transfer up to 1Gbps.

Results

- 1 Provided deterministic, one-way transfer of packaged forensic data files from bank network to secured forensic lab
- 2 Preserved disconnected architecture of lab network with secure, hardware-enforced boundary
- 3 Bank forensic lab network cannot be accessed via any external network connection and potential evidence cannot be tampered with
- 4 Potentially harmful cyber infections cannot escape the forensic lab

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



@OwlCyberDefense

203-894-9342 | Info@owlcyberdefense.com