halcyon

Data Sheet

Data Exfiltration Protection (DXP): Your Ransomware Early Warning Indicator

Your Data is Their Target. They Can't Get What They Can't Steal.

In the early days of ransomware attacks, the primary goal was to bypass security controls and encrypt data to demand a ransom. Today, ransomware actors use techniques conventional security tools find difficult to detect to exfiltrate your data before initiating encryption. Their assumption–that organizations are more inclined to pay a ransom if they are worried about their sensitive data being leaked–has been proven correct.

Halcyon Data Exfiltration Protection (DXP) detects potential data theft indicating an active ransomware attack. Unlike traditional Data Loss Prevention (DLP) or Insider Threat tools requiring extensive configuration, data classification, and constant human oversight, Halcyon DXP is fully automated. It detects ransomware-initiated data movement in real time without taxing your security team.

Powered by Halcyon Ransomware Detection and Recovery (RDR)

Many security vendors offer managed services centered around their products, but Halcyon is the only company providing a service specifically aimed at stopping ransomware.

Halcyon RDR:

- Performs triage, investigates thoroughly, and responds to every potential ransomware signal triggered in the Halcyon platform around the clock.
- If an active attack is detected, ransomware experts will take the necessary steps to disrupt the attack in real-time, immediately alerting the security team of the impacted assets.
- Will work to unencrypt any impacted data using the encryption key material intercept capabilities built into the Halcyon platform.

If your organization is affected by ransomware, Halcyon RDR will help restore and recover your environment at no additional cost. This is covered under the Halcyon Ransomware Warranty, which is also included with the Halcyon Platform.

How Halcyon DXP Works

Automatically monitors outbound data transfers and generates an alert if data is sent to locations known to be used by ransomware actors.

Generates an alert if data movement exceeds a preset volume threshold. This allows the Halcyon Ransomware Detection and Recovery (RDR) team to investigate whether the movement is part of a ransomware attack.

Detects ransomware exfiltration methods such as cloud tunneling, FTP/SFTP transfers, unauthorized file sharing, email, Rclone, RDP, and DNS-based remote access.

Data Exfiltration Protection During Attack Stages

STAGE 01

Infection, Persistence, and Command & Control

STAGE 02

Privilege Escalation and Lateral Movement

STAGE 03

Data Exfiltration

STAGE 04

Payload Detonation and Extortion

Halcyon Data Exfiltration Protection (DXP)

Common real world data exfiltration methods the Halcyon DXP module protects against:
Cloud Tunneling • FTP/SFTP Transfers • “Gray” File Sharing Services • Email • Rclone • RDP & Remote Access • DNS

The Benefits of Halcyon DXP:

- Respond faster to potential data exfiltration attempts that might have gone unnoticed.
- Eliminate the risk of a ransomware actor holding your data hostage to demand a higher ransom (double extortion).
- Detect data theft in real-time, reducing the potential impact of a ransomware attack.
- Get an early warning indicator that threat actors are active in your organization, helping mitigate the impact on business operations and continuity.
- Minimize incidents triggering mandatory SEC 8-K disclosures, maintaining investor confidence and regulatory compliance.
- Easily integrate Halcyon DXP alerts with most modern EPP/EDR/XDRs for enhanced blocking and triage.

Halcyon DXP detects data theft in real-time, reducing the potential impact of a ransomware attack.

See Halcyon DXP in Action

When it comes to cybersecurity, seeing is believing. With the Halcyon Anti-Ransomware Platform and Halcyon DXP working together, you can protect your business, customers, reputation, and brand from ransomware without adding resources or complexity. Visit halcyon.ai to learn more and book your personalized demo today.