halcyon

Technology Differentiation: Data Exfiltration Prevention

The Problem

Ransomware isn't just about encrypting data anymore. In 2024, up to 80% of attacks feature a "double extortion" component where an attacker first exfiltrates or removes sensitive data from a victim organization before executing their ransomware payload. Why? To increase the pain level of an incident and ensure that the victims pay an exorbitant ransom to avoid a privacy breach.

The Challenge

In today's landscape, organizations face unprecedented threats from ransomware, including data exfiltration. Traditional security measures are often inadequate in detecting and preventing the specific techniques and negative outcomes of ransomware. While DLP and Insider Threat solutions have a place, they are not purpose-built to detect the evasive methods and smash-and-grab style that ransomware attackers use in the real world when they exfiltrate data.

Additionally, the complexity, cost, and scale of DLP and Insider Threat tooling and programs are out of reach for all but the most sophisticated and well-funded defenders. **Halcyon's new Data Exfiltration Prevention (DXP) Module addresses these challenges head-on, providing a ransomware data exfiltration-focused, lightweight, and easy-to-implement solution that ensures enhanced protection and visibility.** Halcyon built DXP to address these unique issues:

"GOING DARK PROBLEM"

VPNs: Virtual Private Networks (VPNs) are increasingly used to obscure data exfiltration activities, making it difficult for traditional security measures to detect and prevent data breaches.

Cloudflared: The use of cloudflared and similar tools enables attackers to establish secure and concealed communication channels, further complicating detection efforts.

Network Encryption: The widespread use of SSL/TLS and other encryption methods to secure network traffic makes it increasingly difficult for traditional security measures to accurately detect data exfiltration from the endpoint. This encrypted traffic conceals malicious activities, allowing attackers to bypass detection and exfiltrate data without raising alarms.

DLP/INSIDER THREAT PROBLEM

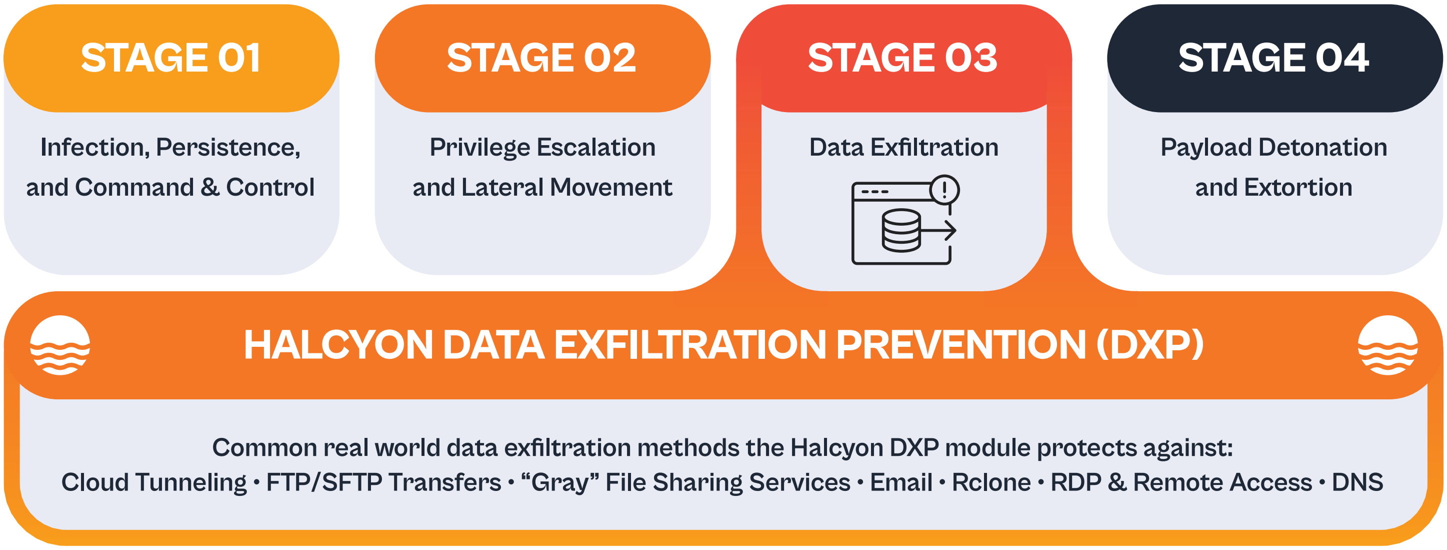
Expensive: Traditional Data Loss Prevention (DLP) solutions are costly to implement and maintain, often requiring significant investment in both technology and personnel.

Complex and Difficult to Manage: These solutions can be complex and difficult to manage, requiring specialized teams to own the tools and programs, leading to inefficiencies and potential gaps in protection.

Time to Value: DLP and Insider Threat solutions often have long deployment times and require extensive customization and tuning before they become effective, delaying their value and leaving organizations vulnerable during the implementation period.

Our Solution

Halcyon's Data Exfiltration Prevention (DXP) Module is an additional module for the Halcyon Anti-Ransomware Platform that is designed to overcome the challenges and the limitations of traditional security measures in detecting real-world ransomware-related data exfiltration events.



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 PREVENTION (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

Key Benefits and Features

- **Detects data exfiltration:** DXP identifies suspicious data movements associated with ransomware campaigns, allowing you to act before sensitive information is compromised.
- **Avoid data extortion attempts:** By detecting and preventing data exfiltration, ransomware attacks that aim to extort money via data leaks are rendered useless.
- **Early warning system:** DXP also provides an early indicator that threat actors are active in your organization, helping you to mitigate the impact on business operations and continuity.
- **Mitigate Risk of SEC 8-K Disclosures:** By identifying and blocking ransomware attempts to exfiltrate sensitive data, DXP helps prevent incidents that could trigger mandatory SEC 8-K disclosures, maintaining investor confidence and regulatory compliance.
- **No customer configuration necessary:** DXP is designed to work out-of-the-box with minimal setup, reducing the burden on your IT team and ensuring quick deployment.
- **24/7/365 Security Analyst Monitoring:** Today's security teams are overburdened with managing technologies and responding to a cascade of alerts. Halcyon supports every DXP customer with Halcyon's Threat Response team, reviewing and responding to your alerts.
- **Process-aware Platform:** DXP is designed to understand and adapt to your business processes, ensuring high signal and low noise in threat detection. This reduces false positives and allows for your security team to focus on genuine threats.
- **Easy Integration:** DXP is compatible with most modern XDRs for enhanced blocking and triage.

In Conclusion

Halcyon's DXP module is the first add-on module to the Halcyon Anti-Ransomware platform aimed at detecting and defending against data extortion attacks. It offers organizations a reliable, cost-effective, and easy-to-implement solution to the gaps left by insider threat solutions and other endpoint controls. **For more information on DXP or the Halcyon Anti-Ransomware Platform, visit halcyon.ai to get a demo!**