halcyon | Microsoft

Coming Soon! Data Sheet

Advanced Ransomware Defense for Microsoft Security Ecosystems

Purpose-Built Anti-Ransomware Protection Integrated with Microsoft Sentinel and Microsoft Defender

Ransomware moves in seconds, not days. Halcyon integrates natively with Microsoft Sentinel and Microsoft Defender for Endpoint (MDE) to deliver earlier detection, automated response, and immediate containment of ransomware threats across the Microsoft security stack.

Together, Halcyon and Microsoft provide a unified defense that transforms ransomware detection into actionable, automated protection stopping attacks before business disruption occurs.

The Challenge

Modern ransomware campaigns are fast, evasive, and human-operated:

- Threats bypass traditional EDR and security controls
- Manual response workflows delay containment
- Endpoint tampering disables security protections
- Fragmented tooling slows investigation and response

Even well-deployed Microsoft environments need purpose-built ransomware intelligence and automated containment to close these gaps.

The Solution: Halcyon Inside the Microsoft Ecosystem

Halcyon enhances Microsoft Sentinel and Microsoft Defender by injecting dedicated anti-ransomware telemetry, protection, and response automation directly into existing Microsoft workflows.

Key Capabilities

Unified Threat Visibility with Microsoft Sentinel

- Halcyon ransomware alerts mapped directly to Sentinel's schema
- Correlated visibility across Halcyon, Defender, and Microsoft telemetry
- Faster investigation using KQL, Sentinel analytics, and Security Copilot

Roadmap Preview: This integration is under development and not yet available. Details and timelines may change prior to release. This material is for informational purposes only and does not constitute a commitment to deliver any functionality.

Halcyon Features

- Always Included 24/7/365 Expert Threat Monitoring and Recovery
- Pre-execution Prevention
- Ransomware Behavior Detection
- Encryption Key Material Intercept
- Data Exfiltration Protection

About Halcyon

Halcyon is the only cybersecurity company that eliminates the business impact of ransomware. Modern enterprises rely on Halcyon to prevent ransomware attacks, eradicating cybercriminals' ability to encrypt systems, steal data, and extort companies. Backed by an industry-leading warranty, the Halcyon Anti-Ransomware Platform drastically reduces downtime, enabling organizations to quickly and easily recover from attacks without paying ransoms or relying on backups.

Where to Find Us

- Azure Marketplace
- Security Store
- Sentinel Content Hub: in app

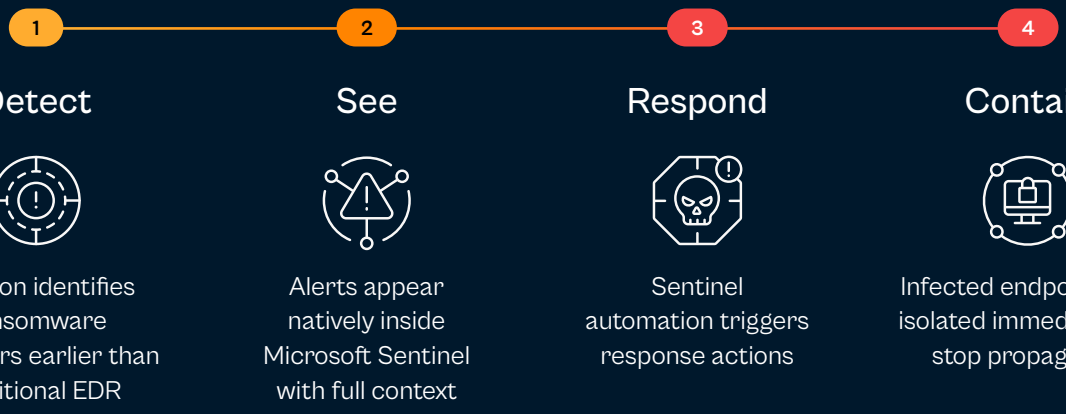
Anti-Tamper Monitoring and Enforce Response Actions in Microsoft Defender:

- Halcyon continuously monitors Microsoft Defender EDR's health and integrity.
- Detect EDR tampering, bypass attempts, and privelege escalation.
- Trigger Microsoft Defender response actions, including host isolation, on Halcyon threat detection via Microsoft Sentinel

Re-Infection and Lateral Movement Prevention:

- Continuous monitoring to detect and disrupt ransomware propagation
- Behavioral intelligence identifies malicious activity attempting to re-establish persistence or move laterally
- Ensures threats are fully contained and prevents re-compromise after isolation

Layered Ransomware Defense for Microsoft Security



Buyer Benefits

BENEFIT	IMPACT
End-to-End Ransomware Defense	Combines Microsoft visibility with Halcyon's purpose-built ransomware protection
Accelerated Response	Reduce MTTD and MTTR from minutes to seconds
Simplified Operations	Eliminate swivel-chair response with unified Sentinel workflows
Operational Resilience	Stop ransomware before encryption and business disruption
Optimized Microsoft Investment	Extend Defender and Sentinel with dedicated anti-ransomware capabilities

Roadmap Preview: This integration is under development and not yet available. Details and timelines may change prior to release. This material is for informational purposes only and does not constitute a commitment to deliver any functionality.