

The Halcyon Anti-Ransomware Platform

The First Solution Dedicated to Defeating Ransomware

Ransomware groups continue to succeed despite organizations' best efforts to implement security controls. Even with investments in endpoint security and backup solutions, attackers are able to exploit gaps in your defenses. They bypass EDRs, disable security tools, and target backups for destruction. This is because other security tools are made for general threats.

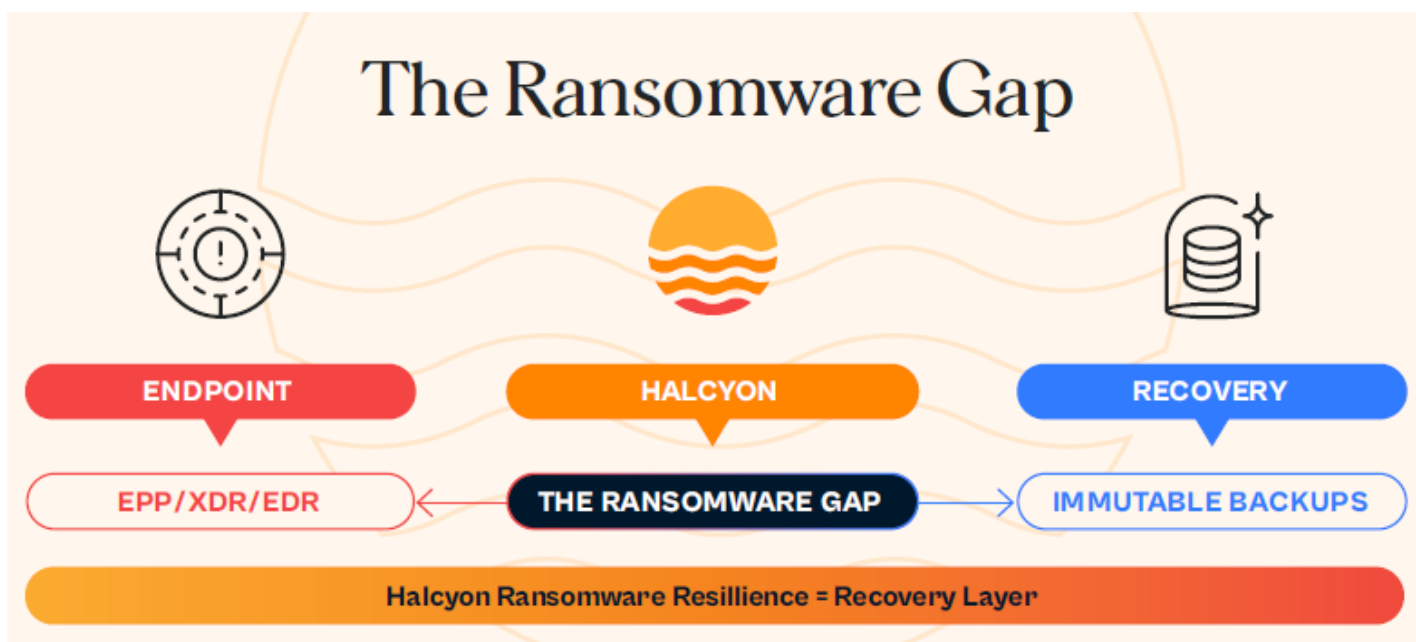
Halcyon is different. Halcyon is designed from the ground up to defeat ransomware and stop data extortion attacks. Our dedicated anti-ransomware solution takes an end-to-end approach to proactively disrupt threats at every stage of the attack lifecycle, while our 24/7 team of experts does the heavy lifting to ensure no ransom is paid and no downtime is tolerated.



Key capabilities:

- End-to-end ransomware protection across the entire attack chain
- Block and contain ransomware that other security products miss
- Stop data exfiltration and double extortion (Data Exfiltration Prevention)
- Recover encrypted data in hours (Encryption Detection & Key Capture)
- 24/7 expert monitoring & recovery (Ransomware Operations Center)

Together, Dell and Halcyon deliver the first and only commercial PCs equipped for ransomware resilience.²



The Halcyon Advantage: End-to-End Protection

Ransomware attacks aren't just another type of malware. They are multi-stage, human-led campaigns designed to inflict maximum damage. Pain points include:

- Data encryption / key encryption
- Data exfiltration / data theft
- Antivirus and Endpoint Detection and Response (EDR) limitations
- Backup tampering
- Ransom payments

This is why Halcyon doesn't just focus on one stage of ransomware; we protect across the entire attack lifecycle — from pre-execution to data exfiltration and encryption. Wherever ransomware goes, we're waiting.

Because Halcyon is focused exclusively on ransomware, we are able to detect it early in the attack chain using highly tuned AI and behavioral models. EDR tampering and privilege escalation detections uncover attempts to disable or bypass your existing endpoint security tools, while Data Exfiltration Protection (DXP) identifies signals that data is being stolen before it is encrypted. And if attackers are still able to encrypt files, Halcyon intercepts encryption keys during an attack, enabling rapid decryption and recovery without relying on backups.

With Halcyon, customers achieve the following benefits:

- Eliminate ransom payments
- Ensure operational continuity
- Maintain data integrity & availability
- Minimize downtime

24/7 Expert Monitoring and Recovery

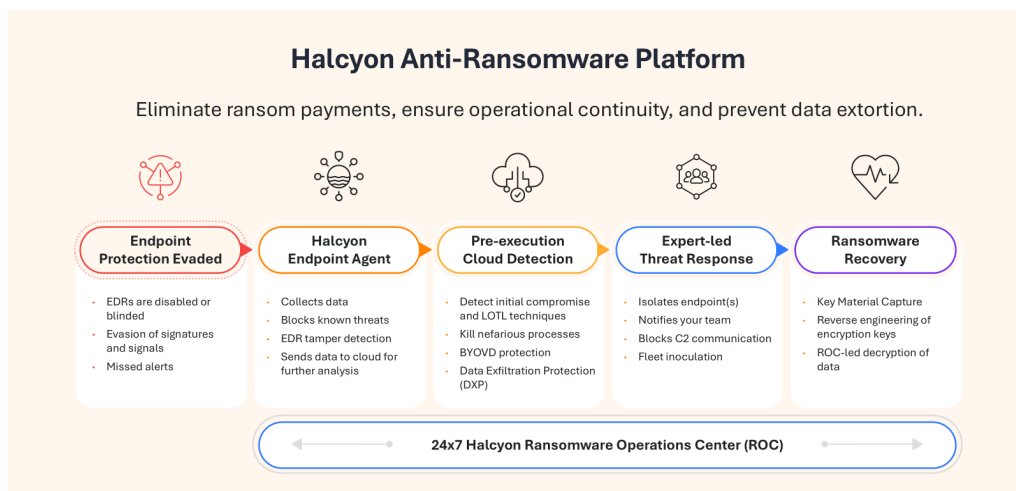
Security teams already handle a huge amount of responsibility. The last thing they need is another tool that increases their workload or causes a bunch of false alarms. That's why Halcyon includes our 24/7 [Ransomware Operations Center](#) as part of our Anti-Ransomware Platform. Every Halcyon deployment includes 24/7/365 managed ransomware protection from our team of experts. They do all the heavy lifting on your behalf – investigating alerts, responding to threats, and leading recovery efforts. This managed approach means you can rest easy knowing you are protected from ransomware around the clock, without having to hire any additional staff.

Ransomware Facts³

104% increase in successful ransomware attacks in the past 2 years

69% of ransomware victims felt they were prepared before the attack

21 days is the average recovery time from a ransomware attack



Ransomware Warranty

Ransomware doesn't just demand payment—it halts operations. Halcyon includes a comprehensive Ransomware Warranty designed to get you back on track as soon as possible after an attack. Our expert-led incident response and recovery team comes at no additional cost, eliminating the need for a ransomware-specific IR retainer. Learn more: <https://www.halcyon.ai/warranty>.

Product Availability: Exclusive On-the-Box Offer

Halcyon is available for all Dell commercial PCs globally. Licenses are available on the box (OTB) at point of Dell PC purchase. Volume licensing is available after PC purchase.

Dell is the first and only PC manufacturer to offer Halcyon's ransomware resilience solution as an out-of-the-box option for commercial PCs.⁴ *Note: Halcyon software must be purchased in conjunction with a Dell PC and activated per the [Terms & Conditions](#) to enable commercial PCs equipped for ransomware resilience.*

Part of the Dell Trusted Workspace Portfolio

Multiple Layers of Defense

Built-on Software Security	Strengthen the security of any fleet with advanced protection via an ecosystem of best-of-breed partners curated by Dell. <i>CrowdStrike • Absolute • Halcyon</i>
Built-in Hardware & Firmware Security	Prevent and detect foundational attacks with deep defenses at the BIOS, firmware and hardware levels. <i>SafeBIOS • SafeID</i>
Built-with Supply Chain Security	Trust hardware is tamper-free on delivery with optional paid add-ons for extra supply chain assurance. <i>SafeSupply Chain</i>

Dell Technologies

Additional Resources

To learn more about Halcyon and the built-on security of Dell Trusted Workspace, download:

- [Dell.com Blog: A New Era of Ransomware Defense](#)
- [Halcyon Press Release](#)
- [Dell Trusted Workspace Brochure](#)

1 Based on Dell internal analysis, October 2025 (Intel) and March 2026 (AMD). Applicable to PCs on Intel and AMD processors. Not all features available with all PCs. Additional purchase required for some features. Intel-based PCs validated by [Principled Technologies](#), July 2025.

2 Based on internal analysis of worldwide PC market, February 2026. Applicable to PCs on Intel and AMD processors. Not all features available with all PCs. Additional purchase required for some PC features. Halcyon software must be purchased in conjunction with a Dell PC and activated per the [Terms & Conditions](#) to enable commercial PCs equipped for ransomware resilience. Backed by partner validation, February 2026.

3 Source: Office of the Director of National Intelligence: https://www.dni.gov/files/CTIIC/documents/products/Worldwide_Ransomware_2024.pdf | Source: From Risk to Resilience: 2025 Ransomware Trends and Proactive Strategies: <https://www.veeam.com/blog/ransomware-trends.html> | Source: Gartner, <https://www.gartner.com/en/conferences/apac/security-risk-management-australia/featured-topics/ransomware-resilience>

4 Based on partner validation, February 2026.

About Dell Endpoint Security

Secure anywhere-work with Dell Trusted Workspace. Reduce the attack surface and improve long-term cyber resilience with multiple layers of defense.

Visit our page dell.com/endpoint-security

Contact an expert global.security.sales@dell.com

Read our blogs [Endpoint Security Blogs](#)

Follow us [LinkedIn](#) | [X](#)

The information in this publication is provided "as is." Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

This document may contain certain words that are not consistent with Dell's current language guidelines. Dell plans to update the document over subsequent future releases to revise these words accordingly.

This document may contain language from third party content that is not under Dell's control and is not consistent with Dell's current guidelines for Dell's own content. When such third-party content is updated by the relevant third parties, this document will be revised accordingly.

Copyright © 2026 Dell Inc. or its subsidiaries. All Rights Reserved. Dell Technologies, Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.