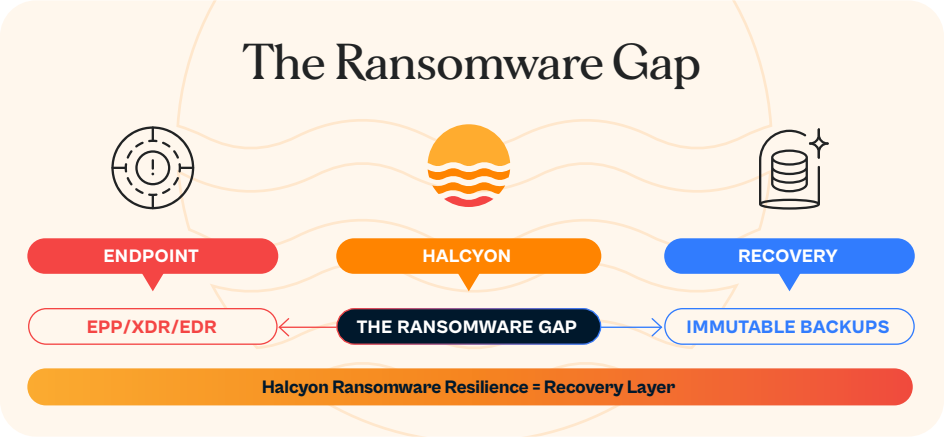
Data Sheet

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.



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. 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 to 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

Key Benefits

- Eliminate the risk of ransomware to your business
- Stop attacks that bypass your existing endpoint protection
- Add 24/7 ransomware expertise without adding headcount
- Protect against data exfiltration and extortion
- Ensure operational continuity with rapid detection and recovery
- Reduce risk with a comprehensive ransomware warranty

Ransomware Facts

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

22 Days
is the average recovery time from a ransomware attack

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

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.

Managed 24/7

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 service 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 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 services come at no additional cost, eliminating the need for a ransomware-specific IR retainer.

About Halcyon

Halcyon is the leading anti-ransomware solution provider, purpose-built to defeat ransomware attacks. Our technology takes an end-to-end approach to proactively disrupt threats at every stage of the attack lifecycle, from pre-execution to data exfiltration and encryption. With a 24/7 expert team and a robust ransomware warranty, Halcyon eliminates the need for ransom payments, ensures operational continuity, and protects businesses from data extortion. **Learn more at** halcyon.ai

To find out more about Halcyon and Cyberfort contact us at **info@cyberfortgroup.com** and one of our experts will be in touch.

Halcyon Anti-Ransomware Platform

Eliminate ransom payments, ensure operational continuity, and prevent data extortion.