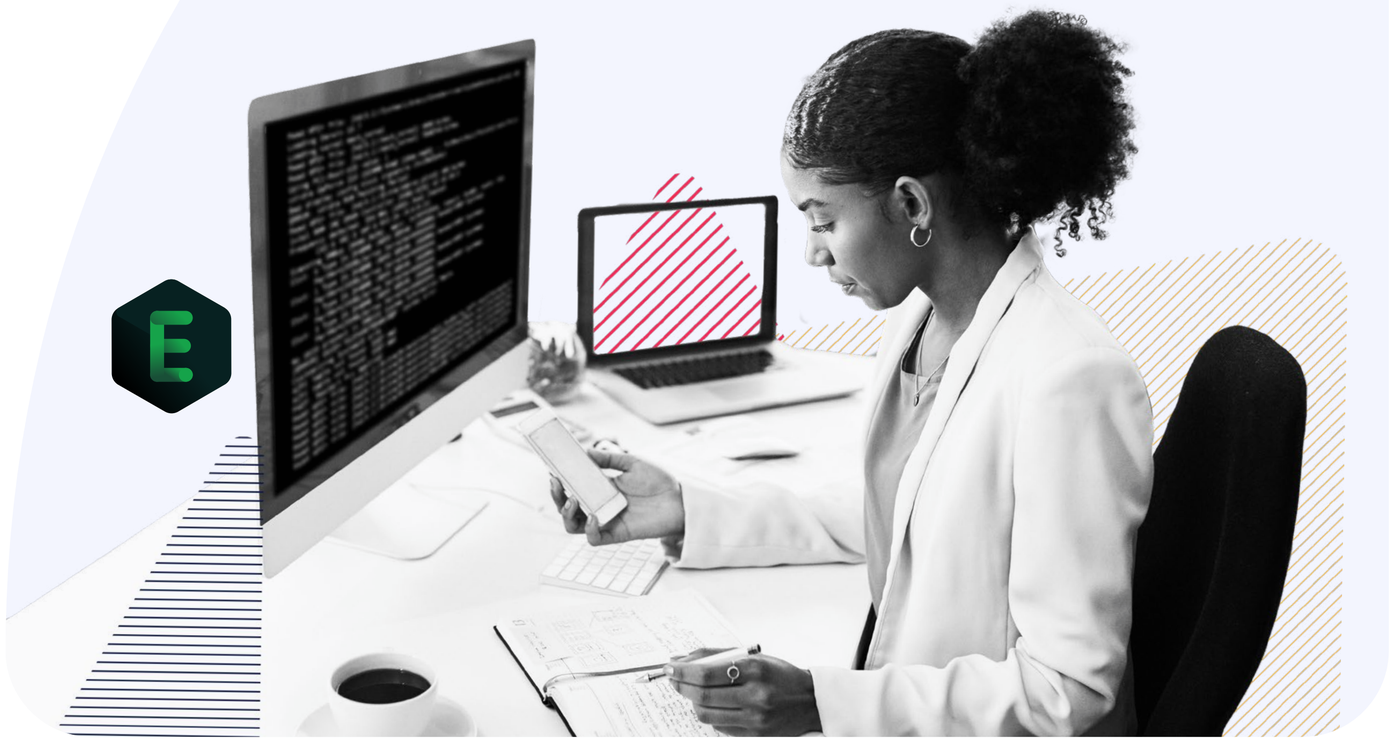
DATA SHEET

Absolute Ransomware Response

Giving you an advantage for preparedness and recovery



Ransomware is one of the most significant threats to businesses worldwide. Cybersecurity Ventures estimates that an organization suffered a ransomware attack every 11 seconds in 2021, and it is expected there will be a new attack on a business every two seconds by 2031.

A ransomware attack can cripple an organization in a matter of minutes, leaving it incapable of accessing critical data and unable to do business. But that's not all — recent years have seen threat actors move from just infesting systems with ransomware to multi-faceted extortion where they also steal data and then threaten to release it to the public or sell it.

The Need for Preparedness and Response

In turn, it is important to increase an organization's ransomware preparedness and assure that the tools needed for remediation, eradication, and recovery are not just in place but also functioning as expected. This holds especially true for the recovery of endpoints, which represent an essential tool for remote workers to conduct their assigned business tasks in today's work-from-anywhere environment. While recovery efforts for endpoints are still considered secondary considering the importance of restoring critical infrastructure (e.g., Active Directory, database servers, application servers, message servers) and business applications, the shift to an anywhere workforce puts increased demands on already hard-pressed IT and security teams when it comes to recovering employees' devices.

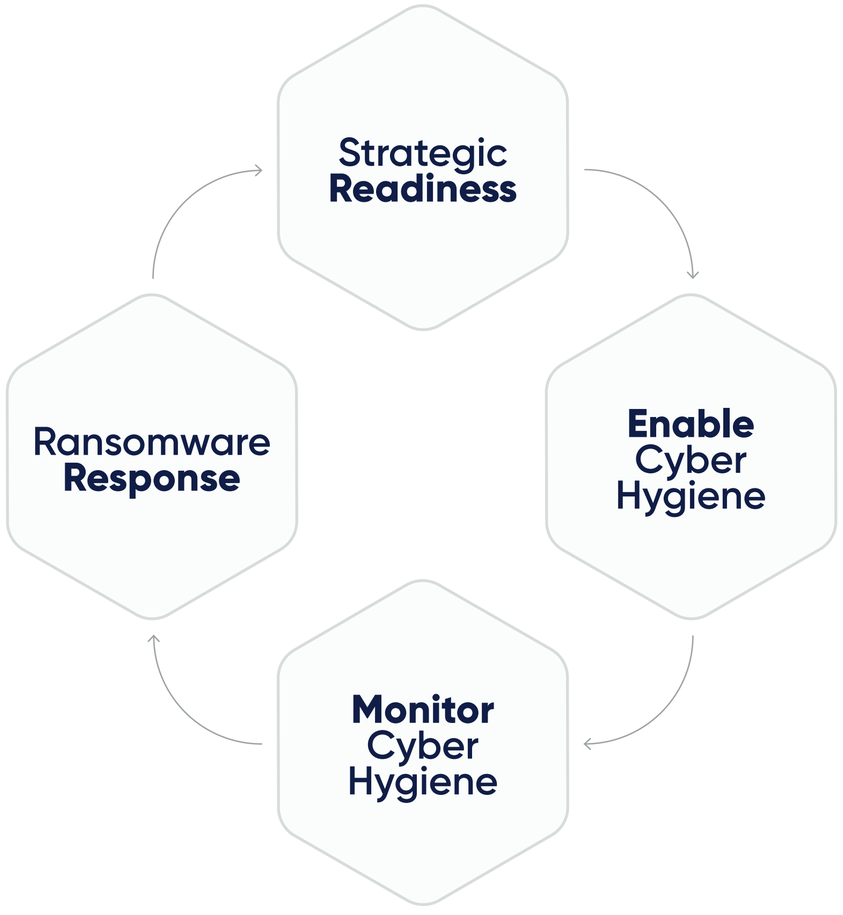
Ransomware attacks often put endpoints in a state where they're either open to reinfection or making it almost impossible to be re-imaged/recovered because the necessary tools are no longer functioning. Ultimately, this creates increased challenges for IT and security teams that by the time they are tasked to recover their employees' endpoints have already exhausted their resources.

Increasing Resilience in Ransomware Response

That's where Absolute® Ransomware Response comes into play. It was developed based on extensive experience responding to and recovering endpoints from ransomware incidents.

The product enables organizations to assess their ransomware preparedness for endpoints, monitors their endpoint cyber hygiene across their device fleet, and allows for an expedited endpoint recovery leveraging Absolute's always-on connectivity, automated restoration capabilities for key security and management tools (e.g., Microsoft® Endpoint Manager, Ivanti®, Tanium™, SentinelOne®, CrowdStrike™), and library of Absolute Reach scripts.

Ultimately, Absolute Ransomware Response improves the confidence of customers in being able to prepare and quickly recover endpoints from ransomware attacks. In the stress of incident response, Absolute provides one less thing to worry about, as we face these threats together.



How Absolute Delivers Ransomware Preparedness and Response

By utilizing Absolute Ransomware Response, organizations can enhance four core ransomware competencies

Strategic Readiness Across Endpoints[1]

- ✓ Review existing standard security controls across endpoints[2]
- ✓ Identify key controls (e.g., anti-malware) and device management tools required to minimize ransomware exposure and assure expedited recovery

Enable Cyber Hygiene Across Endpoints[1]

- ✓ Establish application resilience policies to ensure identified mission-critical security applications and device management tools are installed and functioning as intended
- ✓ Train customer personnel on how to monitor application health and apply these baseline policies to new devices as they are enrolled

Monitor Cyber Hygiene Across Endpoints

Leverage the Absolute Platform to:

- ✓ Report on hardware and software inventory
- ✓ Assess device security posture
- ✓ Discover sensitive endpoint data (e.g., PII, PHI) to identify at-risk devices and ensure for proper back-up via existing tools

Ransomware Response Across Endpoints

Leverage the Absolute Platform to:

- ✓ Deliver secure, on-device end user communications
- ✓ Freeze at-risk devices
- ✓ Expedite recovery tasks via library of script commands
- ✓ Self-heal endpoint security or device management tools[3]

Receive remote help[1] in endpoint recovery efforts for up to two incidents per year, following a pre-defined playbook and leveraging the existing Absolute product capabilities

1 Delivered by Absolute professional services consultants

2 Available on Microsoft® Windows devices only

3 Only one anti-malware and one device management application from the Absolute Application Resilience catalog

Success Story

Problem

A large retailer reached out to Absolute for help after encountering a ransomware attack. The customer was hit with the "Hard2Decrypt" ransomware and was forced off-line for the first week of the attack. The attackers explicitly rendered the customer's security and management tools inoperable prior to dropping the ransomware. This put the customer into a state where they could neither prevent the infection spread nor restore the already infected machines.

Solution

By using a combination of Absolute's Application Resilience capabilities and custom-scripting, the customer was able to break the re-infection cycle by identifying and quarantining the infected machines, reinstalled updated security tools, and kept users safely offline until the machines were restored to an operable, protected, and infection-free state.

Result

Able to begin recovery efforts much faster and confident that critical security controls will remain installed and healthy, minimizing risk exposure against future ransomware attacks.

Benefits

- Identify key controls and device management tools required to minimize ransomware exposure across device fleet and assure expedited recovery efforts
- Establish a cyber hygiene baseline across Absolute registered endpoints
- Monitor endpoint security posture and automatically heal critical controls
- Expedite recovery efforts leveraging custom workflows and task automation commands
- Receive high actionable recommendations and guidance to manage endpoint recovery efforts, putting less demands on hard-pressed IT admin and security teams.

Don't Be Held Hostage by Ransomware

Selecting Absolute Ransomware Response is one of the most critical technology investments an organization can make to assess their ransomware preparedness for endpoints, monitor their endpoint cyber hygiene across the entire device fleet, and allow for an expedited endpoint recovery.

ABSOLUTE®

Trusted by more than 18,000 customers, Absolute Software is the only provider of self-healing, intelligent security solutions. Embedded in more than 600 million devices, Absolute is the only platform offering a permanent digital connection that intelligently and dynamically applies visibility, control and self-healing capabilities to endpoints, applications, and network connections — helping customers to strengthen cyber resilience against the escalating threat of ransomware and malicious attacks.

Request a Demo

Nasdaq | ABST TSX | ABST