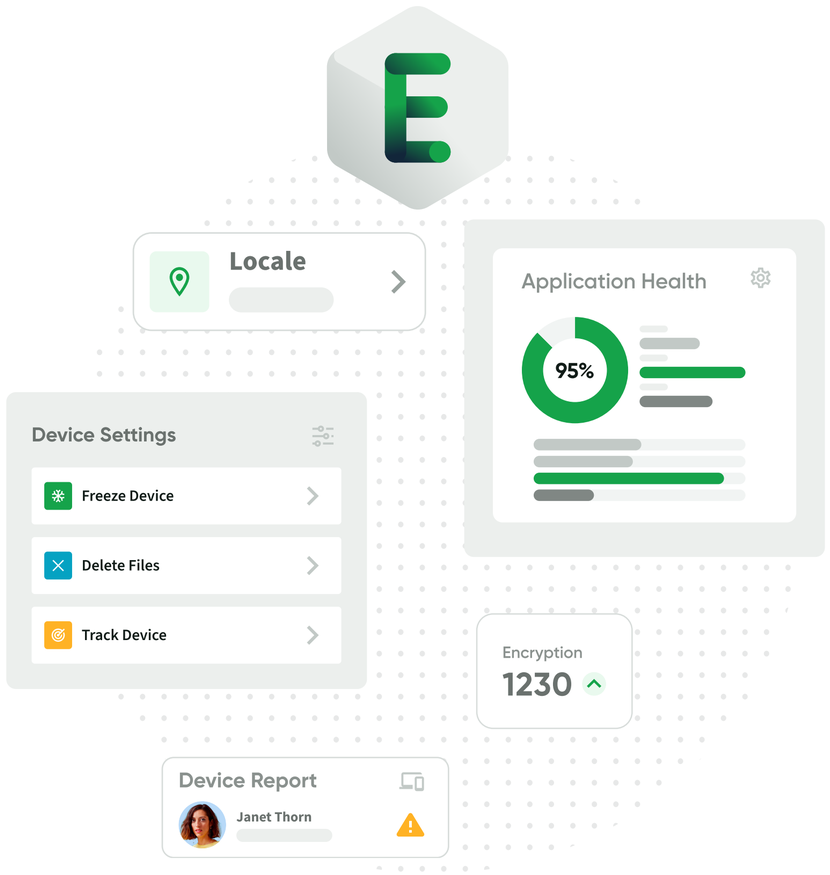
DATA SHEET

Absolute Secure Endpoint

Reliable, resilient endpoints for the anywhere workforce

Most IT teams rely on specialized software to manage and secure the endpoint, which serves as the primary work utensil for today's anywhere workforce. Endpoint management remains a foundational component of any IT team's enterprise infrastructure strategy. The rapid pivot to a work-from-anywhere workforce however threw a curve ball to organizations which were employing more traditional approaches that were relying on a connection to the business' network.



When establishing visibility and security controls across endpoints, IT and security practitioners need to establish a defense in-depth approach. Solely focusing on network security isn't enough, especially if the endpoint connecting to it, is potentially insecure due to decay in its security controls. Thus, making each endpoint resilient is paramount to implementing a successful defense strategy.

At the same time, users expect consistent and good quality experiences no matter where they are. Ultimately, users want their technology to work, and they don't care what happens in the backend if they can reliably and consistently access the resources they need. This means IT needs a higher level of visibility when users work from anywhere, to ensure a consistent experience regardless of location.

Harvest the Power of Persistence

That's where Absolute® comes into play. All major PC manufacturers — including Dell, HP, Microsoft, and Lenovo — embed **Absolute Persistence®** technology in the firmware before devices leave the factory. Absolute Persistence automatically heals and reinstalls the Absolute Agent on every boot sequence, even if the device is re-imaged, the hard drive is replaced, or the firmware is updated. Once Absolute is activated, it provides the resilience you need through an always-on digital tether, so you're always able to see and control your devices and address security gaps — no matter what happens.

The Absolute Secure Endpoint™ product portfolio leverages the always-on connection provided by Absolute Persistence to enable IT and security personnel to monitor and address laptop computers' problems and enables the laptops and their mission-critical applications to self-heal. This helps with IT management, strengthening a company's security posture, and maintaining compliance.

Empower Your IT and Security Teams

Based on its “Swiss Army® Knife-like” versatility, you can leverage the Absolute Secure Endpoint product portfolio for a multitude of use cases across different stakeholders within your organization – all from a single vendor, helping you to conserve budget and allowing for easier vendor management.

Even if you’ve already implemented endpoint management and endpoint security solutions, those tools have limitations and blind spots, are often disabled by end users or compete for device resources, and inadvertently end up not functioning as intended.

As a result, your endpoints become difficult to see, control, and secure. This leads to inaccuracies, operational inefficiencies, and security gaps, which compromises your ability to reliably detect problems and confidently respond to threats. The inescapable result: uncertain audits, resource waste, data breaches, and compliance violations.

Remove all Doubt that Your Endpoints are Secure

Today’s distributed organizations require a permanent digital connection that intelligently and dynamically applies visibility, control, and self-healing capabilities to endpoints and applications - helping them to strengthen their cyber resilience. To keep pace with a distributed workforce and achieve cyber resilience, IT and security teams rely on the powerful fusion of asset intelligence, resilient endpoint security, and confident risk response. They rely on Absolute Secure Endpoint.

Absolute Secure Endpoint Use Case Examples

GOAL

Improve Operational Efficiency & Productivity

- **Optimize Hardware Inventory Management** Keep hardware inventory always accurate, streamline hardware audits, avoid multi-platform fragmentation, and optimize lease management
- **Streamline Software Inventory and Control** Keep software inventory always accurate, streamline software audits, optimize end user productivity, detect and eradicate shadow IT
- **Understand Usage** Identify and eliminate hardware waste, identify and eliminate software waste, validate expected user behavior, analyze usage patterns and prove ROI
- **Enable Remote Device Lifecycle Management** Enable remote device provisioning, ensure remote device configuration, enforce device returns and secure reallocations, and streamline remote device decommissioning
- **Improve Helpdesk Effectiveness** Anticipate device issues, enrich helpdesk tools, solve problems efficiently and at scale, and improve time-to-resolution

GOAL

Mitigate Risk & Strengthen Compliance Posture

- **Assess Security Posture** Detect failing security apps, detect configuration deviations, detect vulnerable OS or apps, report on compliance with regulations or industry standards
- **Enforce Security Standards** make security apps self-healing, enforce standard configurations, remediate vulnerable OS or apps, enable firmware protection remotely (Lenovo only)
- **Detect Security Incidents** Detect suspicious device use or movement, identify missing devices, detect device tampering (even on way from factory), detect sensitive data at-risk
- **Respond to Endpoint Risks** Remotely protect sensitive data files, investigate stolen or suspicious devices, remediate compromised devices, respond to zero-day attacks
- **Successfully Recover from Incidents** Check strategic ransomware readiness, avoid breach notifications after incidents, find root cause to prevent future similar incidents, aid and expedite recovery efforts (e.g., ransomware)

Choose According to Your Business Needs

Within the Absolute Secure Endpoint product portfolio, we offer a variety of products.

See Related Resources ↗

Absolute Visibility

Source of truth for device and application health.

What's Included

- ✓ Device Health
- ✓ Security Posture
- ✓ Application Health
- ✓ Device Usage
- ✓ Geolocation
- ✓ Web Application Usage
- ✓ Endpoint Data Discovery

Absolute Control

Lifeline to protect at-risk devices and data.

All Visibility capabilities, plus

- ✓ Geofencing
- ✓ Device Freeze
- ✓ File Delete
- ✓ Device Wipe
- ✓ End User Messaging
- ✓ Remote Firmware Protection

MOST POWERFUL

Absolute Resilience

Delivers application self-healing and confident risk response.

All Control capabilities, plus

- ✓ Application Resilience
- ✓ Remediation Script Library
- ✓ Investigations and Recovery of Lost/ Stolen Devices

Absolute Ransomware Response

Ransomware preparedness and expedited recovery

What's Included

- ✓ Strategic Ransomware Readiness Check
- ✓ Cyber Hygiene Baseline Across Endpoints
- ✓ Recovery Task Acceleration
- ✓ Remote Assistance

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