SOLUTION BRIEF

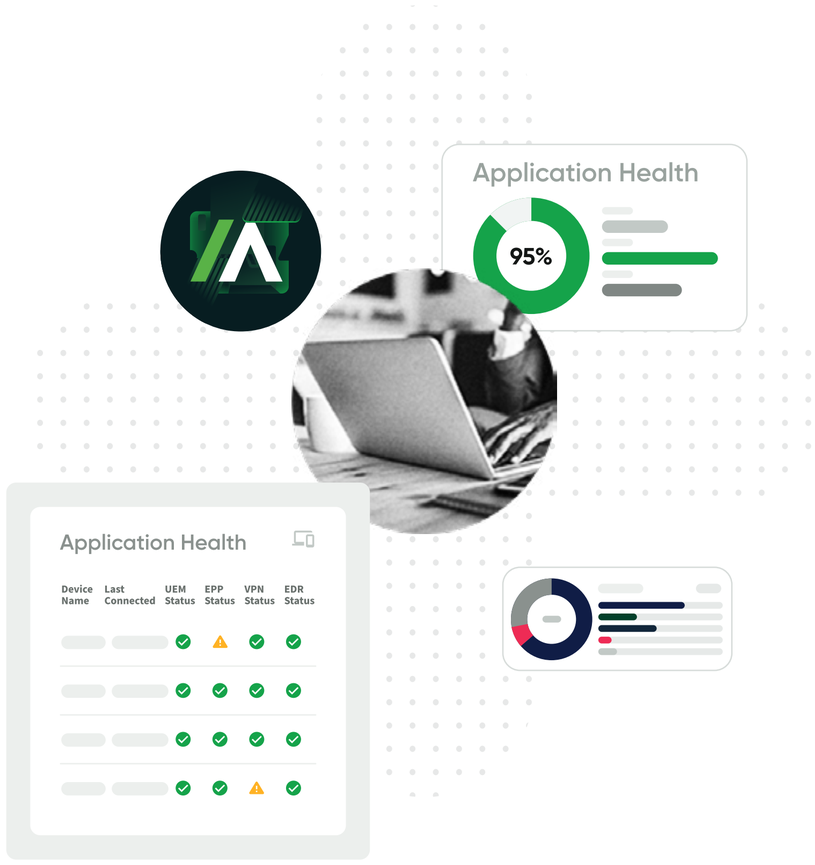
Absolute Application Resilience

Self-Heal Your Mission-Critical Applications

You've invested in the right tools to protect your organization against cyber threats. You've secured your endpoints with ironclad security apps — but how long until even one of those apps or devices becomes vulnerable?

According to our research, it's faster than you'd think. For example: at any given time, 42% of endpoints have encryption failures at any given point. The average time to failure for encryption agents? 12 days.

And it's not just encryption. Every security application eventually fails, often through no fault of its own. Careless users disable them to "speed up their machines." Other apps compete for the same resource, causing conflicts that leave devices vulnerable. In endpoint security, the only constant seems to be compliance drift.



The typical organization takes days or weeks to remediate any application vulnerability. But you've already invested so much in your security. You need a solution that can not only provide continuous visibility and protection, but can help these apps heal themselves almost instantly.

Absolute Application Resilience monitors application health and automatically repairs and/or re-installs unhealthy third-party applications covered in the Application Resilience catalog to restore them to healthy operations.

That means instant remediation of vulnerabilities. It means ironclad proof of compliance. It even means improved staff productivity, because your devices will require far fewer IT tickets to solve application errors.

Application Resilience leverages Absolute Persistence® technology embedded in the firmware of more than 600 million devices, providing a secure and always-on connection between the Absolute Platform and the endpoint.

Now you haven't just made an intelligent one-off investment — you're actively and continuously mitigating risk.

Benefits

- ✓ **Ensure and prove compliance** through self-healing encryption and standardization of your app deployments
- ✓ **Eliminate blind spots** through uninterrupted visibility of any application, no matter where it is or what network it's on
- ✓ **Find and respond to threats quickly** with always-on application intelligence and instant, zero-touch remediation
- ✓ **Maximize staff productivity** by guaranteeing VPN access and optimal operation of your business-critical applications
- ✓ **Streamline software inventory and control** with flawless reporting of usage and configuration across your fleet
- ✓ **Peace of mind and operational efficiency** relying on automatic, zero-touch, built-in resilience
- ✓ **Recover from incidents** successfully and in a fraction of the time by reasserting your security posture

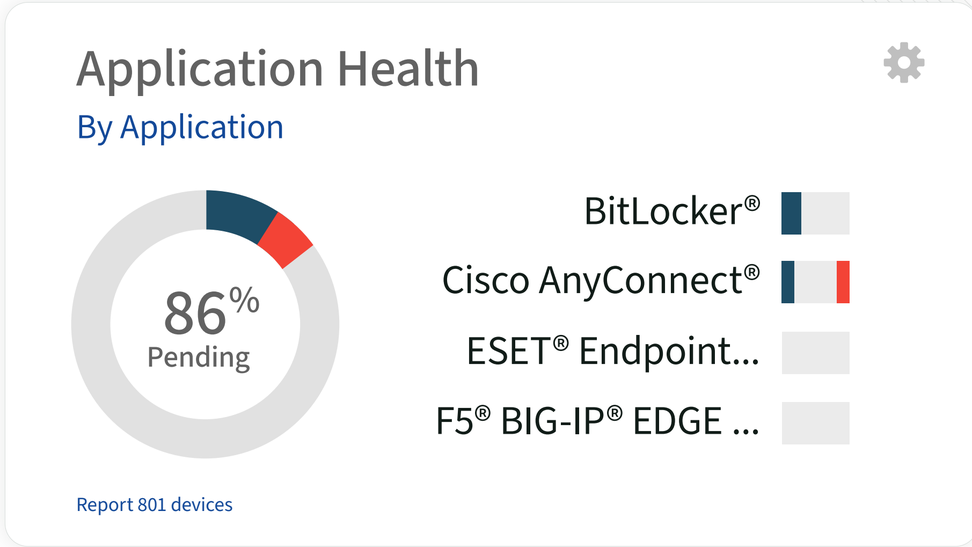
Application Resilience Ecosystem

You can activate Application Resilience policies across a variety of mission-critical applications that are covered by Absolute's ever-growing Application Resilience catalog* that includes, but is not limited to:

- **Endpoint Protection** Ensure your devices have necessary anti-malware and threat detection and response capabilities to guard against cyber threats. Examples include Crowdstrike, Carbon Black, ESET Anti-Virus, McAfee ePO, Ziften Zenith and Dell Advanced Threat Protection.
- **Device Management** Empower your IT team to manage assets and deploy corporate applications, a unified OS build, and security patches. Examples include Ivanti Endpoint Manager, Ivanti Patch, VMware Workspace ONE, and Microsoft Endpoint Manager.
- **Network Security** Let your employees access corporate resources without compromising security. Examples includes Cisco AnyConnect, F5 BIG-IP Edge Client, Pulse Connect Secure, Zscaler, Netskope, Fortinet, and Palo Alto Networks
- **Data Protection** Protect sensitive corporate and customer data at rest and in motion. Examples include WinMagic SecureDoc, Microsoft BitLocker, Dell Encryption, and Dell Data Guardian.

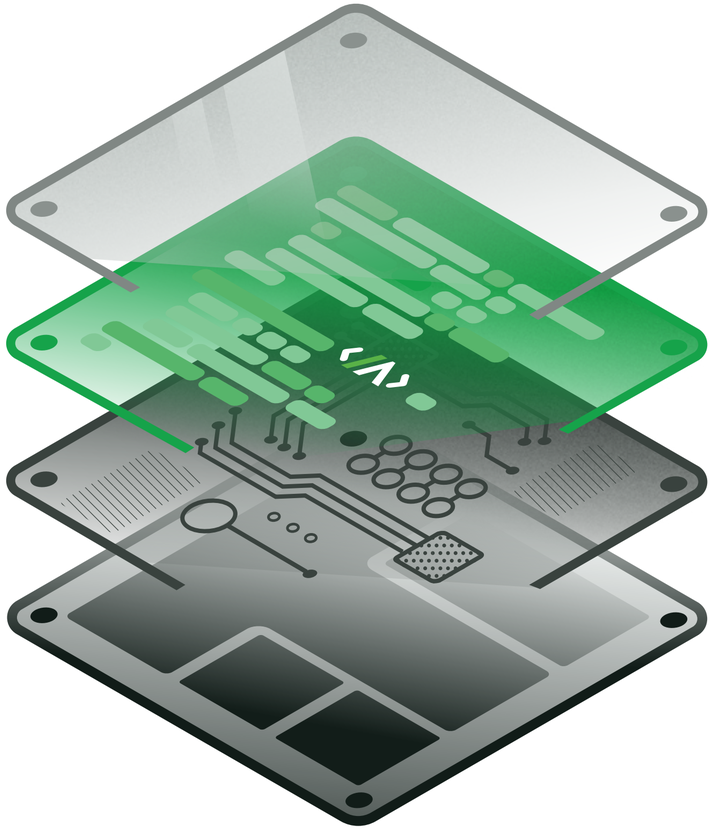
The catalog of industry-leading applications is continuously expanding. With an active Absolute Resilience subscription, you automatically gain self-healing capabilities for any subsequent application that you add to your fleet. As your capabilities grow, so do those of Application Resilience.

As Application Resilience maintains the health of your most vital applications, you can confidently measure their ROI by actively monitoring and reporting on their health across your device fleet with our Application Resilience dashboard.



Application Resilience dashboards to quickly monitor and assess the state/health of your applications

* Outside the Absolute Application Resilience catalog, other applications can be supported through an engagement with the Absolute Professional Services team.



Persistence® Technology

Persistence® technology is already embedded in over 600 million devices, as a result of our partnership with device manufacturers from around the world. This is the only technology that, once activated, will survive attempts to disable it — even if the device is re-imaged, the hard drive is replaced or the firmware is updated. No other technology provides this firmware-embedded resilience.

How to Take Advantage of Application Resilience

Application Resilience is flexible and adapts to your specific deployment environment. If you want crystal-clear reporting for your mission-critical applications, that function is available through an Absolute Visibility or Control license.

Absolute Resilience grants your apps the ability to self-heal and reinstall themselves, as well as all the features of Visibility and Control.

ABSOLUTE®

Trusted by nearly 21,000 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