APPLICATION PERSISTENCE

SELF-HEAL YOUR MISSION-CRITICAL APPLICATIONS

"We use Application Persistence to ensure our VPN technology is maintained on each endpoint. This provides our remote workers with a reliable connection to our network with no interruption to productivity."

ALLEGIS GROUP

EVERY APP FAILS — EXCEPT THOSE BACKED BY PERSISTENCE®

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.

Application Persistence finally makes the self-healing endpoint a reality. By extending Absolute's firmware-embedded Persistence® technology, **it allows applications to heal themselves.**

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.

And because Persistence® is embedded in the firmware of your devices, your applications can still revert to the gold image **after any attempt to remove or compromise them.**

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 unbreakable 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

EDITIONS

Application Persistence 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.

APPLICATIONS SUPPORTED

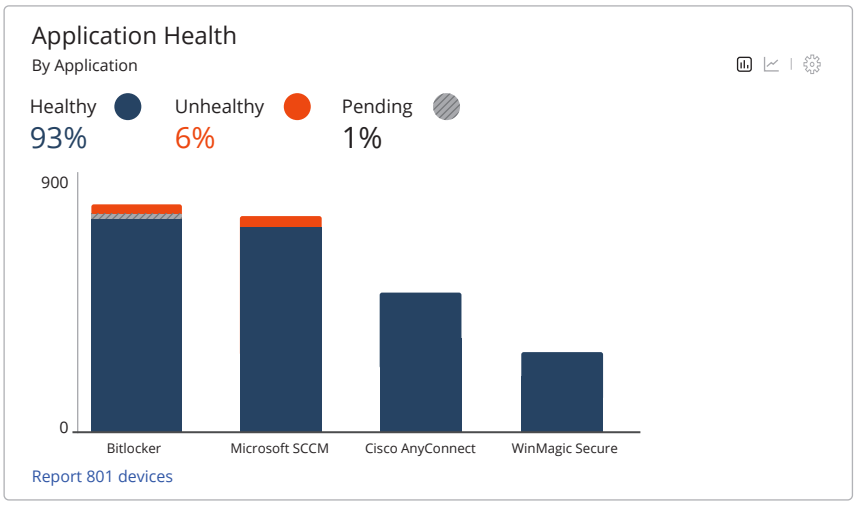
Application Persistence can make any application resilient on your endpoints. Popular apps among Application Persistence users include, but are not limited to:

- **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 Antivirus, 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, Workspace One and Microsoft SCCM.*
- **VPN:** Let your employees to access corporate resources without compromising security. *Examples includes Cisco AnyConnect, F5 BIG-IP Edge Client, Pulse Connect Secure*
- **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.*

Note: Outside the Absolute console, other applications can be supported through an engagement with the **Absolute Professional Services** team.

The library 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 Persistence.

As Application Persistence stands up 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 Persistence dashboard.



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

PERSISTENCE TECHNOLOGY

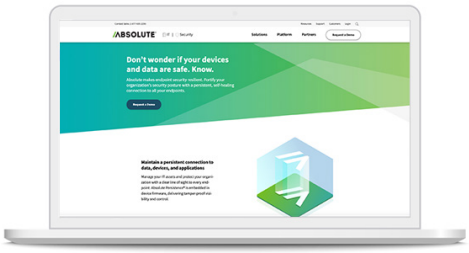
Persistence® technology is already embedded in over one billion devices, as a result of our partnership with device manufacturers from around the world. This is the only technology that, once activated, will survive attempts to disable it — even if the device is re-imaged, the hard drive is replaced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

Ensure your business-critical applications are there when you need them most. Application Persistence is available to new and existing Absolute customers. Once our Endpoint Security solution is deployed, Persistence® is activated, giving Application Persistence the power to automatically self-heal any critical application.

Visit **absolute.com** for more information.

REQUEST YOUR DEMO TODAY

See how Absolute can transform your organization's IT and Security



REQUEST DEMO