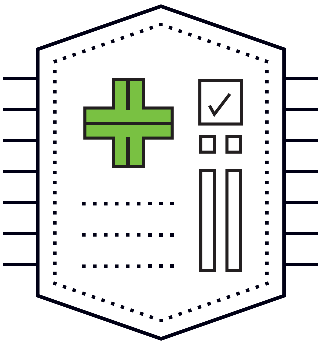
ABSOLUTE SELF-HEALING ENDPOINT SECURITY



UNCOMPROMSED VISIBILITY & REAL-TIME REMEDIATION

Absolute combines cloud-based Device & Data Security with patented embedded Persistence technology, giving you always-on visibility and real-time remediation to protect devices, data, applications and users — on or off your network.

With Application Persistence, endpoint security applications can now self-heal when attempts are made to compromise them, for a more resilient security ecosystem.

> "Absolute provides a feature-rich set of functionality to support IT professionals' need for endpoint contextual awareness and resiliency. It also maintains its heritage of enabling IT teams to maintain device visibility and deliver IT asset management capabilities."
>
> IDC 2016

SEE WHAT OTHERS CANNOT SEE
SECURE WHAT OTHERS CANNOT SECURE

Dark endpoints — devices that are off the network, lost, stolen, or operating without effective security controls — are breeding grounds for security breaches. Fractured visibility across layers of devices, applications, data, and users presents far too many opportunities for attackers and even insiders to perpetrate devastating breaches.

When a device goes dark, no matter what the reason, you have a limited window to take action and mitigate the risk. Absolute identifies those off-the-grid dark endpoints and reduces the likelihood that a dark asset turns into a breach vector. This uncompromised visibility and real-time remediation is what sets us apart. We maintain a constant connection with your endpoint devices, whether or not they're connected to your corporate network. And we give you the power to remediate a breach by healing endpoint agents, freezing or wiping data, and locking down rogue devices.

When a device goes dark, no matter what the reason, you have a limited window to take action and mitigate the risk. Absolute identifies those off-the-grid dark endpoints reduces the likelihood that a dark asset turns into a breach vector. This uncompromised visibility and real-time remediation is what sets us apart. We maintain a constant connection with your endpoint devices, whether or not they're connected to your corporate network. And we give you the power to remediate a breach by healing endpoint agents, freezing or wiping data, and locking down rogue devices and data.

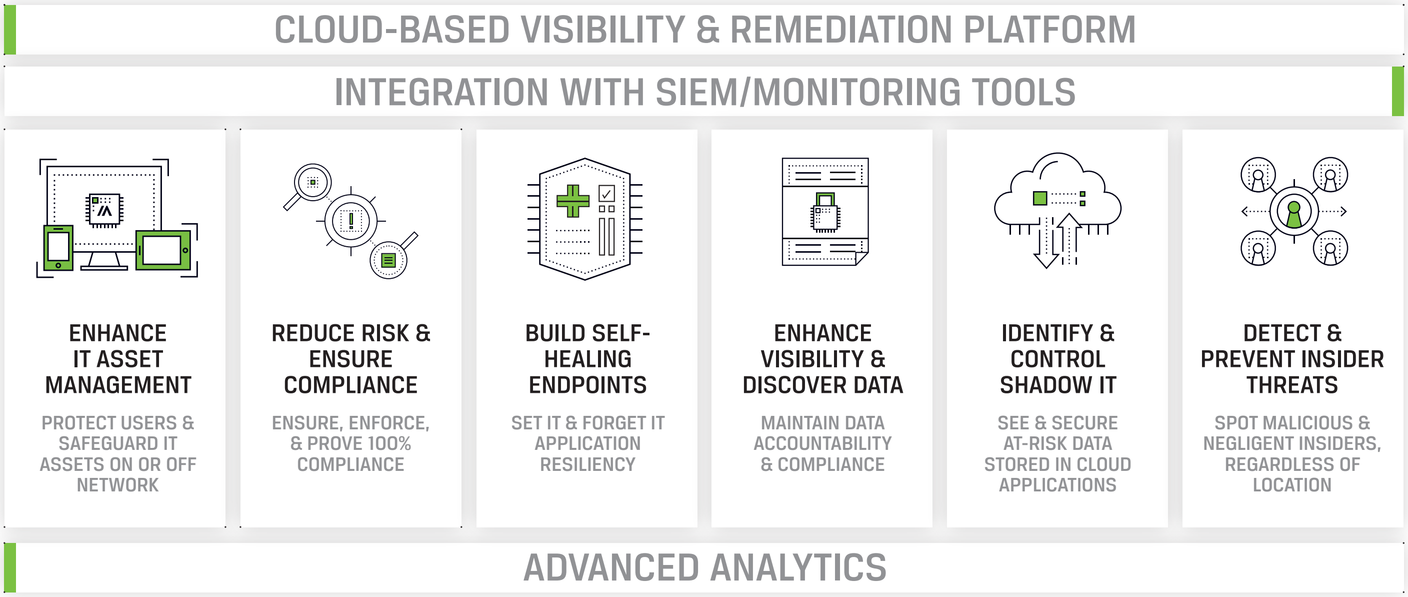
Eliminate Dark Endpoints, Identify At-Risk Data, and Ensure Compliance, with Absolute's Cloud-based Solution

With the cloud-based Absolute Data & Device Security (DDS), you can see and control what others can't, via our own cloud-based console, or as an integrated feed for SIEM solutions such as RSA Security Analytics, Splunk, HP ArcSight, and others. Absolute DDS can be quickly deployed throughout your organization without costly staff and infrastructure resources, or difficult-to-enforce changes in user behavior. With our solution, there is zero impact on the user and administrator.

The Absolute platform is always available for visibility and real-time remediation of devices, applications, data, and users, thanks to a two-way connection [NOTE: in the draft, "connection" is split between two lines. Never do that in public-facing docs.] with Absolute's self-healing embedded Persistence technology. You get the awareness to understand, quantify, and manage your risks for absolute control — on or off the network. Our exclusive Security Vitals Dashboard gives you at-a-glance, actionable insights to diagnose and improve the health of your security posture. With Absolute DDS you will:

- **Automatically remediate breaches to mitigate disruption and losses.**
- **Assess, improve, and monitor endpoint health via an intuitive Security Vitals Dashboard that provides actionable diagnostic intelligence at a glance.**
- **Identify and safeguard data from a single cloud-based console wherever that data may be stored — on or off network.**
- **Withstand user errors or malicious attacks, quickly return to an original safe state, and ensure compliance.**
- **Activate and deploy instantly, with Absolute Persistence is already embedded in your endpoints.**
- **Deliver immediate value and improvement of overall compliance.**
- **Increase the effectiveness and efficiency of IT and security staff.**

THE ABSOLUTE SELF-HEALING ENDPOINT SECURITY SOLUTION



CLOUD-BASED VISIBILITY & REMEDIATION PLATFORM

INTEGRATION WITH SIEM/MONITORING TOOLS

ENHANCE IT ASSET MANAGEMENT
PROTECT USERS & SAFEGUARD IT ASSETS ON OR OFF NETWORK

REDUCE RISK & ENSURE COMPLIANCE
ENSURE, ENFORCE, & PROVE 100% COMPLIANCE

BUILD SELF-HEALING ENDPOINTS
SET IT & FORGET IT APPLICATION RESILIENCY

ENHANCE VISIBILITY & DISCOVER DATA
MAINTAIN DATA ACCOUNTABILITY & COMPLIANCE

IDENTIFY & CONTROL SHADOW IT
SEE & SECURE AT-RISK DATA STORED IN CLOUD APPLICATIONS

DETECT & PREVENT INSIDER THREATS
SPOT MALICIOUS & NEGLIGENT INSIDERS, REGARDLESS OF LOCATION

ADVANCED ANALYTICS

SELF-HEALING EMBEDDED PERSISTENCE®

Enable Self-Healing Applications with the Unstoppable Power of Application Persistence

Organizations invest in endpoint controls and applications to protect their most critical assets, but full application availability and integrity is required to remain effective. However once deployed, devices get re-imaged, malware disables applications, registry files become corrupted, and we all know the impact of negligent or malicious users. Critical applications such as VPN, anti-virus, encryption, systems management, and other controls that have historically been too easily compromised, have left IT and security pros flying blind — until now.

With Application Persistence, the exclusive Absolute advantage — true, self-healing capabilities for data and devices — is now available to third-party endpoint applications. For the first time, both enterprises and ISVs can build complete application resiliency, prove compliance, and eliminate blind-spots, with firmware-level visibility and zero-touch remediation.

- **Automatically remediate disabled controls to mitigate dark endpoints and losses.**
- **Ensure endpoint applications are always available and effective.**
- **Minimize security risks, by maintaining critical security controls on devices.**
- **Mitigate financial and reputation risk by ensuring compliance.**
- **Painlessly activate the security capabilities already embedded in your devices.**

/ABSOLUTE

Always There. Already There.

absolute.com

United States Headquarters
11401 Century Oaks Ter Ste 430
Austin TX 78758
1 800 220 0733

Sales
1 877 600 2295
sales@absolute.com

Canadian Headquarters
1400-1055 Dunsmuir St.
Vancouver, BC V7X 1K8
1 800 220 0733