Uncompromised visibility and real-time remediation of breaches at the source, made possible by self-healing endpoint security from Absolute

Augment your security strategy with Absolute®, an adaptive endpoint security solution that can eliminate blind spots and address breaches in real time. Absolute provides a persistent connection to your endpoints and the data they contain. This means that you're always in control, even if a device is off your corporate network, lost, or stolen.

Add Absolute (formerly Computrace®) to your security lineup in order to strengthen your security stack, ensure compliance, and remediate with lightning speed.

See and secure data and devices, on and off your network

You can't secure what you cannot see. With Absolute, you have uncompromised visibility and control of your endpoints by maintaining a reliable two-way connection with each device. This persistent connection allows you to assess risk and apply remote security measures. This visibility and control is delivered through a cloud-based console that requires no additional IT infrastructure.

Endpoints activated with Absolute check in with the cloud-based monitoring center periodically (the default is set to every 24 hours) and deliver critical health and security information.

With Absolute, you can audit and correct non-compliance remotely and resolve security issues quickly with case-specific compliance and security posture detail. Concerned about offline devices without internet access? Offline policies allow you to automatically freeze devices that do not connect to the internet within a set time period.

Respond immediately in the case of a potential loss or breach, by reviewing the last known state of a system, determining if risk is present, and taking action remotely. You can choose to execute a NIST-compliant hard drive wipe; freeze a system and send a message to the user; or engage Absolute expert investigators to assist with remotely-conducted forensic investigations and device recovery (some conditions apply).

The advantage of Persistence technology

The self-healing two-way connection with endpoints and the data they contain is made possible by patented Persistence® technology from Absolute.This technology is embedded into the core of Dell PCs and most other computers, tablets and smartphones, so it can be activated across an existing population of devices.

When the firmware agent in the core of a device is activated by installing the Absolute client, self-healing endpoint security takes effect. The two-way connection is designed to withstand firmware and application tampering, hard drive removals, and OS reinstalls.

Prove compliance and value of existing IT investment

Absolute not only allows you to see and control devices on or off network, but also strengthens your existing security stack. Through reporting, alerts and SIEM integration, Absolute can validate the status of other installed security applications and prove compliance of secured devices. Furthermore, Absolute includes SCCM repair capabilities to enable consistent management of clients.

Self-healing Absolute technology can be extended to make other mission-critical applications in your enterprise resilient, including security, endpoint management, and VPN apps.

Visibility and Remediation with Absolute

Proactively protect an entire deployment of devices and operating systems from the Absolute cloud-based console. The Absolute global monitoring center is enterprise-grade and ISO certified, with millions of devices contacting the Absolute Monitoring Center daily.

Reporting & Analytics

- Collect information from each device, including historical data.
- Identify activities and precursors to security incidents, such as non-compliant software and hardware installations and changes to IP address, location and user.
- Integrate with SIEM or use the Absolute Security Vitals Dashboard.

Geotechnology

- Track recent and historical locations of devices on Google Maps^{TM}.
- Create geofences and out-of-bounds alerts based on corporate policies and investigate devices entering unauthorized locations.

Risk Assessment

- Preempt security incidents by setting policies and alerts for events that correlate with elevated security risk.
- Locate noncompliant devices, receive blacklisted application install alerts, and flag rogue employees.
- Validate and monitor the status of critical applications including SCCM.

Risk Response

- Enable adaptive security measures.
- Set offline policies to ensure the automatic protection of devices.
- Recover or delete data, freeze a device and communicate status, produce audit logs, and use certified data delete to decommission devices.
- Gather insights and remediate devices anytime, anywhere via the Absolute Reach script-and-query tool.
- Prove that that endpoint data and corporate networks were not accessed while a device was at risk.

Endpoint Data Discovery

- Identify and remediate non-compliant data.
- Discover sensitive data including personal health information and personally identifiable information on devices and assess the associated risk.
- Discover sensitive data synced with cloud storage applications.

Endpoint Investigations

- Prevent, identify, and eliminate insider threats.
- Leverage the Absolute investigations team to determine the cause of an endpoint security incident, Locate and, if necessary, recover missing or stolen devices.
- Determine if a data breach notification is required.

Absolute editions

Visibility (Standard)

- Best for organizations looking for dependable asset tracking, on and off the network.
- Includes hardware and software reporting and analytics; device location mapping, logging and reporting; and call history and loss control reports.

Control (Professional)

- For organizations who want visibility into security risk and the ability to control and remediate devices and data.
- Reporting and controls encompass device usage, device location (geofencing), adjacent security software health, encryption status, the presence of cloud sharing, SCCM self-healing, and security dashboards.
- Includes a connector to send security data to SIEM solutions.

Resilience (Premium)

- Includes everything in Professional, plus the ability to discover sensitive data on endpoints and the expert services of the Absolute investigations team.
- Investigation services include forensic investigations and device theft investigation and recovery in coordination with local law enforcement (some conditions apply).

Services for Education (US and Canada)

- Specialized services and a device recovery guarantee are included with Absolute Resilience (Premium) for Education. Premium editions. Some conditions apply.

Technical requirements

Absolute DDS agent

- Windows 7, 8, 8.1 and 10 (32 and 64 bit)
- Mac OS X 10.6 or later
- Android 4.4.2 or later
- Internet connection

Absolute cloud-based console

- Windows Internet Explorer
- Microsoft Edge (Windows 10)
- Mozilla Firefox (Windows and Mac)
- Google Chrome (Windows and Mac)
- Safari (Mac)

Solutions for iOS and Chromebooks

Absolute also offers solutions to track and secure Chromebooks and iOS devices in the Absolute cloud-based console. Ask your sales representative for more information.

Learn more at Dell.com/DataSecurity