# Strengthen security through a persistent connection to your endpoints.

## Absolute® Data & Device Security complements Dell Data Security Solutions

The mobile workforce is here to stay. To address the challenges of mobility, in partnership with Absolute we offer a solution that provides a persistent, self-healing connection to all your endpoints and the data that they contain. This means that you're always in control, even if a device is off network, lost, or stolen.

Absolute Data & Device Security (DDS), formerly Absolute Computrace®, complements data security solutions from Dell by addressing additional security risks including rogue employees, lost/stolen devices, and end user error. Absolute supports a wide range of devices and operating systems – so your people can work where they want and how they want.

## Control and secure devices on and off the network

With Absolute, it's all about the connection. By maintaining a two-way connection with each device, you have the insight you need to assess risk and apply remote security measures so you can protect each endpoint and the sensitive data it contains. This valuable insight is delivered through a cloud-based console that requires no additional IT infrastructure.

Concerned about offline devices without Internet access? Offline policies allow you to automatically freeze devices that are offline for a specified period of time.

## Eliminate worst-case scenarios

Prevent and mitigate security incidents with proactive security policies and heightened visibility across groups, users, and devices.
Identify suspect devices, then take action. Not only can you remotely discover what's on the device, but you can also locate it, freeze it, retrieve data, or delete data remotely.

## Protect your business with endpoint security including remote device freeze and data delete

**Reporting & Analytics**
Collect information from each device, including historical data. Identify events that could be precursors to security incidents, such as non-compliant software and hardware installations, and changes to IP address, location, and user.

**Geotechnology**
Track recent and historic locations of assets on Google Maps™. Create geofences with corresponding out-of-bounds alerts, and investigate security risks.

**Risk Assessment and Response**
Set policies for events that correlate with elevated security risk and receive notifications when they occur. Remotely recover or delete data, set policies to protect devices, freeze a device and communicate status, produce audit logs, and use certified data delete to decommission devices.

**Endpoint Investigations**
Determine if vulnerable data was accessed, and decide if data breach notification is required. Locate and recover missing or stolen devices.

Persistence is embedded into the core of most computers, tablets, and smartphones at the factory.

Once activated, it provides you with a reliable two-way connection so you can confidently manage mobility, investigate potential threats, and take action if a security incident occurs.

Learn More at absolute.com

## I have data encryption. Why do I need Absolute?

Although the data on a missing or stolen device may be protected by encryption, there are scenarios in which you may need more information, or you need to protect against internal threats.

Absolute provides visibility across complementary security solutions and the ability to reach out to the device with preemptive actions.

## Absolute Data & Device Security is available in three editions:

**Standard**
Best for organizations that do not plan to monitor security behavior, but need to respond to user-reported incidents.
Includes hardware reporting, offline device policies, device freeze, and data delete capabilities.

**Professional**
Adds software and security reporting, along with geotechnology and geofencing to document and mitigate device drift.
Proactive alerting, event calling, custom alerts, and remote file retrieval are also included, along with a connector to send security data to SIEM solutions.

**Premium**
Everything in Professional, plus Endpoint Investigations by Absolute security professionals using proprietary forensic tools.
Includes device theft investigation and recovery in coordination with local law enforcement.

More information on Absolute DDS editions at:
absolute.com/en/products/dds/editions

## Technical Requirements

Absolute DDS agent:
- Windows 7, 8, 8.1, and 10 (32 and 64 bit)
- Mac OS X 10.6 or later
- Android 2.3 or later
- Internet connection

Absolute cloud-based console:
- Google Chrome (Windows and Mac)
- Mozilla Firefox (Windows and Mac)
- Windows Internet Explorer
- Microsoft Edge (Windows 10)
- Safari (Mac)

## The Absolute difference

With Absolute, endpoints are under your control, whether or not they are on or off the network. You'll have tools to proactively manage your users and data, and you'll be equipped to handle security incidents.

**Lifecycle Security**
Apply a layer of security across the entire lifecycle of each device and receive alerts if specific conditions occur. Secure new devices in transit, validate end users, inventory hardware and software, blacklist applications, set certified end of life data delete protocols, and take other security measures.

**Risk Assessment**
Monitor device activity and status, and receive alerts if specific conditions occur. Locate non-compliant devices, control offline devices, receive blacklisted application install alerts, flag rogue employees, and receive alerts for complementary security technologies such as encryption, anti-malware, and SCCM.

**Risk Response**
Remotely invoke security commands and other measures to avoid a significant security incident. Send messages to end users, lock and unlock devices, establish chain of custody, conduct internal investigations, remotely retrieve and delete endpoint data, and prove that that endpoint data and corporate networks were not accessed while a device was at risk.

**Enterprise Class Architecture**
Manage an entire deployment of devices and operating systems from a single cloud-based console.

You can run filtered reports across thousands of devices, create and execute commands such as a data delete or device freeze, and set customized alerts. The Absolute global monitoring center is enterprise-grade and ISO certified, with millions of devices contacting the Absolute Monitoring Center daily.

**Comprehensive Security, Complementary Technology**
Dell and Absolute have a long partnership spanning more than 20 years. The security tools that we offer allow you to maintain a layered defense and take action to remediate potential security breaches.

**Learn more at Dell.com/DataSecurity**