Absolute DDS

Adaptive Security for the Endpoint

"At Under Armour, one of the most important things for us is intellectual property. We use Absolute to protect all of our computers including those in our innovation and design departments."

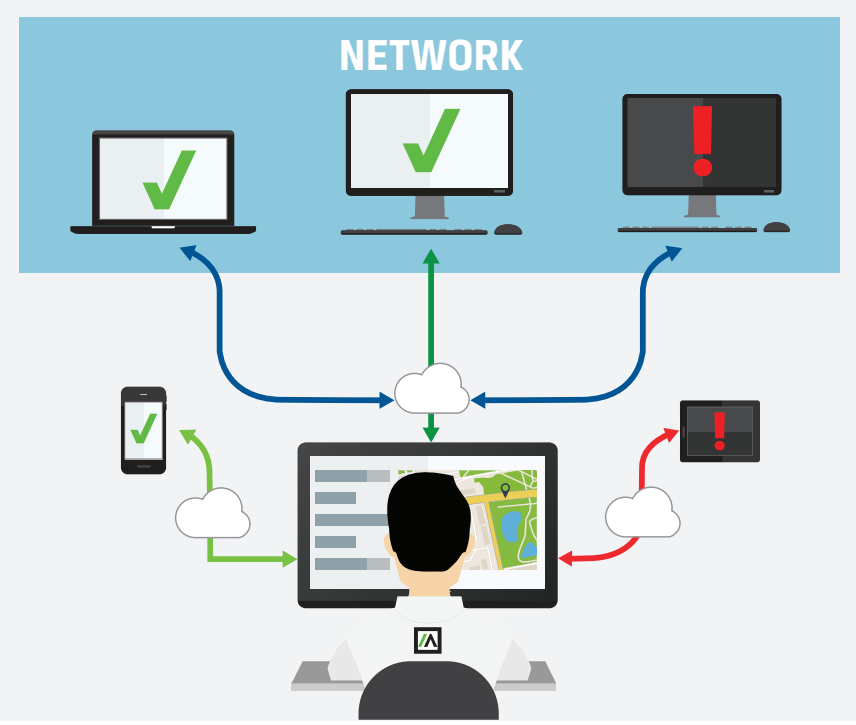
Ben Snyder

UNDER ARMOUR

DATASHEET

Absolute® Data & Device Security (DDS), formerly Absolute Computrace®, is an adaptive endpoint security solution. It provides you with a persistent connection to all of your endpoints and the data they contain. This means you're always in control, even if a device is off the network or in the hands of an unauthorized user.

And let's face it, with most employees using multiple devices and accessing sensitive data from just about anywhere in the world, being in control is a welcome change.



Control and secure devices on and off the network.

With Absolute DDS, 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.

Absolute DDS

Adaptive Security for the Endpoint

Absolute DDS provides a full complement of endpoint security features and remote capabilities so that you can control and secure business data and devices:

REPORTING & ANALYTICS

Collect incredibly accurate information from each device, including historical data. Determine what's installed on a device. Identify events and activities that could be precursors to a security incident including changes to IP address, location, and user; non-compliant software/hardware installations; and many more. Receive a notification if these activities occur.

GEOTECHNOLOGY

Track assets on a Google Map™, including recent and historical locations. Create geofences based on corporate policies. Investigate devices that are out of bounds or entering an unauthorized location.

RISK ASSESSMENT

Identify risk conditions and receive a notification if these conditions occur. Key security data integrates automatically with SIEM solutions. Validate the status of complementary security applications such as encryption, anti-malware, and SCCM. Use these reports to prove to auditors that security measures were properly implemented and in place at the time of a security incident.

RISK RESPONSE

Remotely recover or delete data. Set policies to ensure offline devices are automatically protected. Freeze a device and communicate with the user to verify status. Produce an audit log to prove data on a compromised device was properly secured, not accessed, and safely deleted. Use certified data delete workflows to decommission a device.

ENDPOINT INVESTIGATIONS

Leverage the Absolute Investigations team to determine the cause of an endpoint security incident. Identify and eliminate insider threats. Refine best practices so the same incident does not reoccur. Determine if data was accessed during an incident, and whether or not a data breach notification is required. Recover stolen devices.

PERSISTENCE TECHNOLOGY

DDS relies on patented Persistence® technology by Absolute. 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.

For a list of Persistence-enabled devices, visit ***absolute.com/core***

SYSTEM REQUIREMENTS

Absolute DDS supports:

Details available at
absolute.com/sysreq