



Absolute® Data & Device Security Support Service

Care Pack, part of HP Care

Service benefits

Lifecycle security

Apply a layer of security across the entire lifecycle of each device and receive alerts if specific conditions occur. Some examples include securing new devices in transit; validating end users; and performing hardware/software inventories, blacklisted applications, and certified end-of-life data delete protocols.

Risk assessment

Monitor device activity and status, and receive alerts if specific conditions occur. Examples include noncompliant device location; the status of complementary security technologies such as encryption, anti-malware, and SCCM; offline device control; blacklisted applications; sensitive data stored in cloud storage applications; and rogue employees.

Risk response

Remotely invoke security commands and other measures to avoid a significant security incident. Some examples include end-user messaging, locking a device until its status is confirmed, definitive proof that endpoint data and corporate networks were not accessed while a device was at risk, remote retrieval and deletion of endpoint data, chain of custody, and endpoint investigations. Initiate commands directly from the DDS environment, cloud storage applications, and certain SIEM applications.

Service overview

The strategic global relationship between Absolute® and HP Care provide your organization with world-class hardware technology and endpoint security and management for your devices.

Absolute® provides persistent endpoint security and data risk management solutions for computers, tablets, and smartphones. Its solutions offer a unique and trusted layer of security, so customers can manage mobility while remaining firmly in control. With over 30,000 commercial customers worldwide and more than 20 years of experience in the industry, Absolute® is a leader in device security and management tracking.

Absolute® Data & Device Security (DDS) provides your organization with actionable intelligence to prove compliance and deliver comprehensive visibility and control over your devices and data—anytime, anywhere.

Absolute® Data & Device Security Support Service offers multiple service levels of Absolute® DDS products to meet your business needs.

Persistence technology

HP devices have Persistence® technology embedded in their firmware. Once activated, it provides a reliable two-way connection, so you can confidently manage mobility, investigate potential threats, and take action if a security incident occurs. The ability to communicate with endpoints—regardless of user or location—means that you can receive timely device and event information. Most importantly, you can apply remote security measures to protect each device and the data it contains. No other technology can do this. For a complete listing of HP devices with Persistence technology embedded in the firmware, visit: absolute.com/en/partners/oem/hp

Table 1. Service features matrix

	Device Theft Investigation & Recovery	Healthcare Endpoint Investigations	Safe Schools**	Software Asset Reports	Security Reports	Geotechnology	Geofencing	Data Delete	Device Freeze	End User Messaging	Endpoint Data Discovery
Absolute DDS Premium***	•			•	•	•	•	•	•	•	•
Absolute DDS Professional				•	•	•	•	•	•	•	
Absolute DDS Standard								•	•	•	
Absolute DDS for Education Premium	•		•	•	•	•	•	•	•	•	•
Absolute DDS for Education Professional				•	•	•	•	•	•	•	
Absolute DDS for Education Standard				•		•					
Absolute DDS for Healthcare Premium*	•	•		•	•	•	•	•	•		•

* Available in the US only

** Safe Schools is available in North America and the UK only

*** Includes Mobile Basic, Mobile Standard, and Mobile Premium features

Specifications

Table 2. Service features

Feature	Delivery specifications
Capability overview	Depending on the Absolute® DDS Support Service purchased, the following features may apply:
Reporting and analytics	Collect highly accurate information from each device, including historical data, the status of security applications, and determine what's installed on a device. Build flexible with custom rules to search for data specific to your organization. Receive reports on cloud storage applications. Identify events and activities that could be precursors to a security incident, including changes to IP address, location, and user; noncompliant software/hardware installations; and more. Receive a notification if these activities occur.
Geotechnology	Track assets on Google Maps™, including recent and historical locations. Create geofences based on corporate policies, and 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 security information and event management (SIEM) solutions. Maintain direct mapping and integration between key security data and security information and event management solutions (SIEM). Validate the status of complementary security applications such as encryption, anti-malware, and System Center Configuration Manager (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. Execute these measures directly from the Absolute® DDS console, cloud storage applications, and SIEM solution applications. Produce an audit log to prove that 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.
Device Theft Investigation & Recovery	Leverage the Absolute® Investigations team to determine the cause of an endpoint security incident, identify and eliminate insider threats, refine security best practices, and determine if data was accessed during an incident, and whether or not a data breach notification is required.
Healthcare Endpoint Investigations	Leverage the HealthCare Information Security and Privacy Practitioners (HCISPPs) and ASIS Certified Protection Professionals (CPPs) on 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.
Absolute Safe Schools	Absolute® Safe Schools is an integrated program that works in conjunction with existing Absolute® theft recovery technology. Overseen by the Absolute® Investigations team, Absolute® Safe Schools can help keep students, school environments, and devices safe.

Feature	Delivery specifications
Software Asset Reports	Collect incredibly accurate information from each device, including historical data. Determine what's installed on a device to ensure compliance.
Security Reports	Identify risk conditions and receive a notification if these conditions occur. Key security data integrates automatically with SIEM solutions including ArcSight. 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.
Endpoint Data Discovery*	Scan devices for sensitive data, on or off the network. Use pre-built rules or create custom rules to search for specific data. Leverage these search capabilities to scan cloud storage application folders.
Geofencing	Create geofences based on organizational policies and receive an alert to investigate devices that are out of bounds or entering an unauthorized location.
Data Delete	Remotely delete data from at-risk devices.
Device Freeze	Remotely freeze suspicious devices until the status can be verified.
End User Messaging	Remotely communicate with end users to verify the status of a device.
Cloud Storage Application Reporting	Detect folders on devices associated with cloud storage and any sensitive data they contain.

* Only applicable with certain editions

Customer responsibilities

Product and factory installation information

The Customer must register the covered hardware and Care Pack immediately after purchase, using the registration instructions provided by HP.

In addition, to be eligible for the Absolute® DDS Support Service, the Customer must work with Absolute® to install the necessary software on the required Customer's device. None of the services can be provided until the Absolute® software agent is installed. The Customer will receive a welcome email from Absolute® (fulfillment@absolute.com) with instructions on how to download and install the Absolute® software agent.

Alternatively, HP can pre-install Absolute® DDS on the Customer's devices before deployment via factory installation. The Customer should contact an HP sales representative for more information on this option.

The Absolute® software agent must be installed by the Customer before the service can be activated. In order to use security features such as geotechnology and risk response, the Customer must first sign a pre-authorization agreement and follow other instructions.

For additional information regarding customer responsibility, service limitations, and other terms, please visit the Absolute® Software Service Agreement page: absolute.com/en/partners/oem/hp

Support

Absolute® is committed to providing customers with world-class support. Solutions and help for Absolute® products is available from the Absolute® online support resources page: absolute.com/support

Absolute Investigations

Absolute® customers that engage with the Absolute® Investigations team are able to adjust their infrastructure and immediately remove points of weakness, reducing the risk to the organization and precluding corporate liability.

Absolute® DDS customers can take advantage of endpoint investigations delivered by the Absolute® Investigations team. They will help customers 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

To learn more, download the Absolute® Investigations datasheet: absolute.com/en/resources/datasheets/absolute-investigative-services

Coverage

Table 3. Product coverage by geographic region

Type of Care Pack service sold	Americas				EMEA	APJ
	U.S.	Puerto Rico	Canada	LAR	EMEA	APJ
Absolute DDS Premium*	•	•	•	•	•	•
Absolute DDS Professional*	•	•	•	•	•	•
Absolute DDS Standard*	•	•	•	•	•	•
Absolute DDS for Education Premium**	•	•	•	•	•	•
Absolute DDS for Education Professional	•	•	•	•	•	•
Absolute DDS for Education Standard	•	•	•	•	•	•
Absolute DDS for Healthcare Premium	•					

Legacy Computrace Mobile functionality is now fully supported across all Absolute® DDS product editions.

* Available in the US only

** Safe Schools is available in North America and the UK only

Learn more at
hp.com/go/pcandprintservices

Sign up for updates
hp.com/go/getupdated



Share with colleagues



Rate this document

HP Services are governed by the applicable HP terms and conditions of service provided or indicated to the Customer at the time of purchase. The Customer may have additional statutory rights according to applicable local laws, and such rights are not in any way affected by the HP terms and conditions of service or the HP Limited Warranty provided with an HP product.

© 2016 HP Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Google Maps is a trademark of Google Inc.

4AA2-1087ENUC, November 2016

