HP Absolute Security

Service overview

Together, HP and Absolute provide a robust security solution to protect data and devices—on or off the corporate network.

Absolute provides endpoint persistence, intelligence, and resilience. The cloud-based platform maintains a constant connection to devices through self-healing Absolute Persistence® technology. This unique and trusted platform is embedded into many HP devices, allowing IT professionals to monitor, manage, and secure their entire endpoint population.

Choose from three levels of service based on your IT and business needs:

- Absolute Visibility service
- Absolute Control service
- Absolute Resilience service

Service benefits

- Persistence: Security built into devices helps ensure they are always protected and easy to manage
- Intelligence: Visibility over an entire endpoint population addresses blind spots and improves compliance
- Data protection: Locate, lock, and delete data on devices—on or off the corporate network
- Resilience: Self-healing endpoint controls trigger a rebuild, reinstall, or restoration of endpoint agents to ensure security measures work as intended

Service highlights

Apply a layer of security across the entire lifecycle of each device and receive alerts if specific conditions occur. Some examples include:

- Secure new devices in transit
- Validate end users
- Perform hardware/software inventories
- Certify end-of-life data delete protocols

Service features and delivery specifications

Absolute Persistence® technology

Absolute Persistence® technology is a patented security solution that provides a continuous, reliable, two-way connection between devices, data, and the Absolute console.

The ability to communicate with endpoints—regardless of user or location—allows remote security measures to be applied to protect devices and the data they contain.

Absolute invest heavily in maintaining relevant product and company authorizations, accreditations, and certifications. To learn more, visit https://www.absolute.com/platform/certifications/.

Risk assessment

Monitor device activity and status and receive alerts if specific conditions occur. Examples include:

- Non-compliant device location
- Unhealthy status of encryption, anti-malware, SCCM, or other complementary security technologies
- Devices that haven't connected for a prolonged period of time
- Blacklisted applications
- Sensitive data stored on devices or data that is using cloud storage applications
- Rogue employees

Risk response

Invoke security commands and other measures remotely to mitigate security incidents. Examples include:

- Locking a device until its status is confirmed
- Definitive proof that endpoint data was encrypted and not accessed at the time of the incident
- Remote deletion of endpoint data
- Endpoint investigations and risk analysis
- Running query or remediation scripts remotely on any number of devices, to gather information or fix vulnerabilities, and confirming successful execution

Absolute Visibility Service

See all devices on and off your network, and collect 500+ hardware, software, security, usage, and geolocation data points automatically, with 365 days of historical logs—all with SOC2 compliance levels 1 and 2. Datapoints include:

- Hardware inventory details on 25+ PC OEMs
- Installed applications inventory (over 2,000 applications detected)
- Device location and history
- Application health monitoring
- Automated and customizable alerts
- Persistence® technology
- Encryption status and process monitoring

Absolute Control Service

Go beyond device tracking with the ability to take remote action to remediate endpoint risks immediately. This includes all Absolute Visibility features, plus:

- Device freeze—on-demand or offline
- Full or selective data deletion with full wipe-with industry certifications
- Granular geo-fences from office, building, metro, country-in 120+ countries
- Geo-fencing to detect device movement, take action, and create automated actions with custom messaging
- Take ServiceNow action, along with other 3rd party API integrations

Absolute Resilience Service

Establish resilient security by ensuring critical third-party apps remain active at all times. Remotely identify and protect sensitive data, gather precise insights, or remediate endpoint vulnerabilities. This includes all Absolute Visibility and Control features, plus:

- GDPR compliance
- Investigate and recover stolen devices
- Self-heal third-party applications across many companies
- Remotely scan for sensitive and at-risk files, locally and in the cloud
- SCIM 2.0 integration providing expanded compliance with regulators
- Run PowerShell or BASH scripts on any device
- Perform risk analysis on suspicious devices with recommendations from experts

Visit absolute.com/platform/editions for a detailed comparison between Absolute Visibility, Absolute Control, and Absolute Resilience. Visit absolute.com/hp to request a demo.

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

Absolute Investigations

Absolute customers who 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 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

Download the Absolute Investigations datasheet for more information: absolute.com/resources/datasheets/absolute-investigative-services

Customer responsibilities

You must register the covered hardware and Care Pack immediately after purchase, using the registration instructions provided by HP. For security and compliance purposes, only the end customer's (account administrator) email address may be entered during the registration process, which enables Absolute to complete license fulfillment. Failure to register using the end customer's email may result in failure of license fulfillment.

In addition, to be eligible for the HP Absolute Security Service, you must work with Absolute to install the necessary software on the required device. None of the services can be provided until the Absolute software agent is installed. You 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 on your devices before deployment via factory installation. Contact an HP sales representative for more information on this option.

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

Terms and conditions apply

See complete Care Pack terms and conditions.
For more information on HP Services, contact any of our worldwide sales offices or resellers or visit hp.com/go/services

Sign up for updates hp.com/go/getupdated

4AA2-1087ENW, May 29, 2024