

Absolute Application Health

GENERAL INFORMATION

What is Absolute Application Health?

Absolute Application Health offers Absolute Resilience customers the ability to track the health of a wide range of applications beyond security applications currently supported through the Absolute Application Resilience Catalog. This new capability provides health monitoring support for over 2,000 Windows and Mac applications in total and enables practitioners to diagnose application failures. They can subsequently use this information to take swift remedial action to bring the application back to a state of efficacy, thus maintaining end user productivity and/or the organization's security posture.

How is Absolute Application Health offered to customers?

Absolute Application Health is offered as a product feature available through eligible Absolute Resilience licenses. Customers with an Absolute Resilience subscription can activate the feature and get access to integrated reports and widgets through the Absolute Console showcasing the health of applications installed across their devices.

Note – Absolute Application Health is not available with the following Resilience licenses:

- › Absolute Resilience for Education
- › Absolute Resilience for Student Devices
- › Absolute Resilience for Chromebook

What pain points does Absolute Application Health solve for customers?

Absolute Application Health addresses the following pain points in gaining visibility into application health in today's work from anywhere environment.

- Applications routinely failing on remote endpoints due to a variety of reasons, including but not limited to:
 - › An application is not being installed or being incorrectly installed after a device reimage or as a result of a malfunctioning Endpoint Management tool.
 - › Critical application files being corrupted while new third-party apps are installed or updated.
 - › An end user negligently disabling or uninstalling an application that was provisioned or certified by the IT team.
- Inability to accurately track the health of installed security, business, productivity, communication, and other applications being utilized within an organization.
- Lack of visibility into granular application failure reasons on individual devices to aid in the remediation of the application.
- Inability to track the spread of installed application versions across a fleet of remote endpoints.

What benefits does Absolute Application Health offer to customers?

Absolute Application Health helps IT and security practitioners yield the following benefits:

- Helps IT teams maintain end user experience across their remote workforce by ensuring they can access core business/productivity, file sharing, browser, data backup, and communication/messaging applications to remain productive.

- Helps IT and security teams maintain the organization’s security posture by ensuring critical security applications such as endpoint protection/anti-malware, encryption, patch management, data loss prevention, and VPN tools are healthy and indicate any degradation in application health.
- Helps reduce helpdesk tickets from end user-related application failures, thereby boosting the IT team’s efficiency.
- Helps identify potentially problematic or faulty applications in relation to making decisions on application renewal or subscription termination.

What applications are supported through Absolute Application Health?

Absolute Application Health provides health monitoring support for over 2,000 Windows and Mac applications, including the most used business, productivity and security applications. Examples of categories of supported products include:

- Anti-Malware; Anti-Phishing; Public File Sharing; Backup; Firewall; Messenger; Cloud Storage; Data Loss Prevention; Patch Management; VPN; Virtual Machine; Health Agent; Remote Desktop Control; Peer-to-Peer Agent; Web Browsers; Web Conferencing.

Check out the [Absolute Help](#) for a full list of supported applications.

HOW APPLICATION HEALTH WORKS

How is Absolute Application Health different from Absolute Application Resilience?

Absolute Application Health extends Absolute’s application health monitoring capabilities beyond the security products currently supported through the [Absolute Application Resilience Catalog](#). Some key differences between Application Health and Application Resilience are described in the matrix below.

Application Health	Application Resilience
Support for 2,000+ Win and Mac applications (as of October 2023). Including business, productivity and security apps.	Support for 80+ (as of October 2023) security focused applications such as Endpoint Protection, Endpoint Detection and Response, Unified Endpoint Management, Data Loss Prevention, etc.
Application health monitoring and access to granular failures reasons. IT can leverage the information to fix issues separately through their Endpoint Management, Application Management or other designated tools.	Application health monitoring as well as automated remediation (repair and reinstall).
Activation of policy across all installed applications detected on devices.	Configuration and activation of policies for specific applications.
Interactive reports and widgets showcasing installed app versions, overall app health and reasons for failure on individual devices.	Interactive reports and widgets showcasing overall app health, reasons for failure on individual devices and the status of remediation attempts.

Note – Application Health and Application Resilience can be enabled at the same time for apps that are supported by both, resulting in unified reporting under the Applications report through the Absolute Console.

What checks does Absolute Application Health perform to deduce whether an application is healthy?

Application Health performs a few different checks to determine the health of an application. These can be described through the following categories.

- ✓ **Installation health** – whether the application has been installed on the device correctly (e.g., application directories and files and executable file signatures)

- ✓ **Running state health** – whether agent-based applications are running on the device correctly (e.g., core agent, services/processes)
- ✓ **Configuration health** – if the application has been configured on the device correctly. (e.g., for Anti-Virus/Endpoint Protection, this can be whether real-time threat prevention is active.)

How often does the Absolute Agent scan for Application Health updates?

The Absolute Agent checks for updates every 15 minutes and sends an update if a change is found. The agent will send a complete scan every 24 hours, even if there has been no change.

CONFIGURATION AND REPORTING

How is Absolute Application Health configured through the Absolute Console?

Application Health can be configured and activated through the “Installed Applications” policy under “Policies > Policy Groups” page, with “Include Health Data” selected. Once the policy is configured and activated, the following will occur:

- The activated policy will trigger a Custom Data Collector (CDC) component to be downloaded on devices. This component is about 50MB and will be downloaded on devices with active Installed Applications policies over a period of 6 hours. This may generate significant network traffic for large deployments. This download is not required for organizations that use the Full Agent Installer or use the Absolute DataExplorer feature.

The Application Health related reports and widgets (as described in the next question below) will be populated with data collected from devices that have the policy active.

Note – Given the size of the endpoint component, it is recommended that you activate the feature on a group of devices before doing so across your entire fleet. You can do this by creating a Custom Policy Group for the limited devices you would like to test the feature on and activate the “Installed Applications” policy for that specific Custom Policy Group. You can then either choose to add more devices into this Custom Policy Group or activate “Installed Applications” on a different Custom Policy Group with other devices.

How are application health tracking and failure reasons offered through the Absolute Console?

Application health monitoring is offered through the following four distinct views through the Absolute Console:

1. **Viewing Application Health via the Assets pane** – This view provides a list of all applications installed across your devices, application publisher information, the number of devices on which each app is installed, and the health of the application on devices where it is installed.
2. **Viewing a specific application’s health** – Provides a summary of the application’s deployment across your devices, the application’s health across devices and the breakdown of the different versions. This list can be filtered to show only certain devices having a specific version of the application installed or devices on which the application has failed.
3. **Viewing the health of applications on a specific device** – This view provides a list of all applications installed on a specific device as well as each app’s health status. In addition, you can also view information about the application’s publisher, version(s), when the application was installed, and the install location.
4. **Viewing the Installed Applications Report** – This report is available through the Reports section of the Absolute Console. It provides a tabular list of all your devices and applications installed on them. Like other views, the report provides app health details, failure reasons, app versions installed as well as app publisher information.

For further details on activating and utilizing the Application Health reports and widgets, check out the [Absolute Help](#).

