

DATA SHEET

Absolute Investigations

**Unbreakable Device Visibility and
Expert Investigators: The Perfect Team**



When one of your devices is stolen or missing, Absolute is the only solution that combines the power of firmware-embedded Persistence technology, which maintains a self-healing connection to all of your devices to track them at all times, even off the corporate network or in the hands of an unauthorized user, with an in-house expert team to conduct the investigation for you, at your explicit request.



When a security incident occurs, the Absolute Investigations team works on behalf of Cigna-HealthSpring to gather evidence from the endpoint.

CIGNA-HEALTHSPRING

Uninterrupted Assistance throughout the Investigation Process

- ✓ Absolute's Investigations team has access to proprietary tools that can gather identifying information about the person using the errant device and determine its location.
- ✓ Once an identification is made by one of our investigators, a comprehensive written report is prepared and forwarded to the appropriate law enforcement agency.
- ✓ The Absolute investigator maintains regular contact with the detective assigned to the case to advise them of any changes, and to ensure that your case remains a priority.
- ✓ This proven methodology provides you with the greatest opportunity to have your device recovered and returned to you, mitigating the potential regulatory compliance risk, preserving your organization's financial resources, and ensuring business continuity.

Investigate the Root Cause to Prevent Further Incidents

In addition to recovering the missing or stolen asset, Absolute's investigators are also typically able to establish links from a device user back to your location, and conclusively determine that the user of the device was a current or former employee, contractor, temporary worker, patient, student, construction/maintenance worker, housekeeper, or visitor.

Finding out about the root cause of an incident will allow you to address organizational vulnerabilities that threaten your sensitive data, such as personally identifiable information (PII) or electronic protected health information (ePHI), as well as your physical assets, and prevent similar incidents in the future.



Requirements

- ✓ Access to Absolute's Investigations team requires the installation of the Absolute software agent onto each device.
- ✓ This will activate Persistence technology from Absolute, which is embedded in the firmware of the device at the factory.
- ✓ Persistence technology triggers an automatic reinstallation of the Absolute software agent if it is removed from an endpoint, resulting in a trusted, selfhealing connection to each device regardless of user, location or network.
- ✓ Access to Absolute's Investigations team also requires the purchase of a Resilience license.

A Team Of Expert Investigators At Your Disposal

Our expert Investigations team has a combined total of nearly 65 years of experience in locating our customers' missing and stolen devices. Most investigators came to Absolute after full careers with various local, state, and federal law enforcement agencies in the U.S., Canada, and the U.K. All of this investigative experience has led to the successful recovery of over 56,000 of our customers' missing or stolen devices in over 127 countries around the world.

As a result of these years of experience, Absolute's Investigations team can also provide you with practical advice on best practices to help maintain your asset inventory, by detecting suspicious activity on a device, such as a change in user name or hard drive, the installation of a new operating system, or a change in geolocation. Our investigators have extensive experience in discretely dealing with an extremely wide gamut of situations, and always strive to implement solutions that are in your best interest.





ABSOLUTE[®]

Trusted by nearly 21,000 customers, Absolute Software is the only provider of self-healing, intelligent security solutions. Embedded in more than 600 million devices, Absolute is the only platform offering a permanent digital connection that intelligently and dynamically applies visibility, control and self-healing capabilities to endpoints, applications, and network connections – helping customers to strengthen cyber resilience against the escalating threat of ransomware and malicious attacks.

[Request a Demo](#)