ABSOLUTE: SECURITY & PRIVACY OVERVIEW

INFOSHEET

TABLE OF CONTENTS

INTRODUCTION 2

OVERVIEW 2

- Absolute the Company 2
- Absolute Platform 2
- Persistence Technology 2
- Data Centers 3
- Privacy Policy 4

DATA & INFORMATION 4

- Device Data Attributes Collected (Standard) 4
- Device Data Attributes Collected (Optional) 5
- Data Protection 6
- Information Security Management System 6
- Information Security Policy 6
- Tools & Services for Data Protection 6
- Processes & Procedures for Data Protection 6
- Procedural Controls 7
- ISO 27001 Certification & Audits 7
- ISO 9001 Certification & Audits 7
- Federal Information Processing Standard 8

CUSTOMER ROLES AND RESPONSIBILITIES 8

INTRODUCTION

This document is intended for customers and agencies wishing to evaluate and advise on the use of the Absolute platform. The document provides information about:

- Absolute: the company and solutions
- Data collected
- Processes and technology used to protect data
- Roles and responsibilities of Absolute customers

OVERVIEW

Absolute the Company

Absolute is the new standard for endpoint visibility and control, delivering always-connected IT asset management and self-healing endpoint security to protect devices, data, applications and users—on and off the network. Bridging the gap between IT operations and security, only Absolute gives enterprises visibility they can act on to assess every endpoint, remediate vulnerabilities and at-risk data, and ensure compliance in the face of insider and external threats. Absolute's patented Persistence technology is already embedded in the firmware of more than one billion PC and mobile devices and trusted by over 20,000 customers worldwide.

Absolute Platform

Absolute gives you the power to see, manage and secure every endpoint, everywhere. That's because only Absolute is always-connected to every endpoint, unlike traditional endpoint security solutions that are constrained by network dependencies and contingent upon healthy endpoint agents.

With Absolute, no endpoint device will ever go dark giving enterprises highly-assured IT asset management, self-healing endpoint security, and data visibility and protection.

The basic components of the Absolute solution include:

- **Persistence technology** built into the firmware of most devices at the factory (Persistence remains dormant until the Absolute agent is installed)
- **Absolute agent** installed onto devices by the customer
- **Monitoring center** operated by Absolute to which the agents connect periodically (referred to as 'agent calls' to the monitoring center)
- **A web-based console** that customers use to log in to their Absolute environment

Persistence Technology

Persistence is the only technology that keeps you in complete command with a self-healing, two-way connection to any endpoint or application — even if they are off the network. It's a fundamentally new approach to security, leveraging our privileged position embedded in the firmware of billions of endpoints. It's also the advantage behind the Absolute platform.

The power of Persistence can also be extended to your critical applications, providing resiliency and availability with Application Persistence.

How Persistence works:

1. OEMs embed Persistence technology into the firmware of devices at the factory
2. Once the Absolute software agent is installed, Persistence is activated
3. An automatic reinstallation is triggered if an Absolute software client or an application supported by Application Persistence is removed from a device
4. The reinstallation will occur even if the firmware is flashed, the device is reimaged, the hard drive is replaced, or if a tablet or smartphone is wiped clean to factory settings

Data Centers

When selecting a physical environment provider for the data centers, Absolute recognizes the benefits of housing production infrastructure using vendors that follow best practices in network infrastructure and physical security. The following selection criteria is selected:

- Data center outsourcing and infrastructure must form the core of the provider's business, and they must have industry-leading expertise in technology and security
- The provider is assessed against SSAE16 at least annually, has strong financial viability, business continuity planning in place, and rigorous personnel standards
- The facilities have excellent physical security, including solid building infrastructure, cages, biometric entry-control, man-trap entry preventing tailgating, and CCTV
- The provider offers onsite services, including 24 x 7 onsite security with monitoring and response procedures, and network management with appropriate service level agreements (SLA's)
- The facility has strong network and power infrastructure, including dual power sources, UPS, HVAC, fire suppression, network redundancy and appropriate bandwidth availability

Absolute procures and uses its own servers and hardware, co-located in the data center, and managed by permanent employees of Absolute who are background-checked periodically.

These and the following practices are in place to ensure the security of customer data so production services can be maintained at close to 100% uptime targets:

Operating Environment and Patching Process

In most cases, a critical security patches are deployed within a 30-day window from its release. This supports a thorough internal and public evaluation of the patch prior to implementation. Critical patches are examined immediately to determine whether they should be deployed on an expedited schedule. The Absolute server infrastructure resides behind perimeter firewalls, permitting external access only through ports 80 and 443, further limiting vulnerabilities.

Security of Code Management

Code that is placed into the product environment is carefully managed:

- **Policy:** A software development and release methodology are mandated. This includes segregated development, test, and production environments, as well as a QA process and limited release publication authority.
- **Process:** A Gatekeeper process is implemented that requires approvals from a number of teams, before a Development Release is moved into production. As part of this process, the gatekeeper checklist documents are logged against the release candidate.
- **Tools:** Microsoft tools are used for software configuration management
- **Permissions:** Product network folder access is restricted to select employees

Incident and Issue Management

Redundancy and fail-over is built into the production infrastructure. The Operations team is also prepared to respond to hardware and software failures with a documented incident and issue management plan as back-up. The plan includes architecture, automated / manual monitoring, response, escalation of incidents, and the recovery steps required for an extensive set of issues.

Privacy Policy

Absolute will only use and disclose personal information for the purposes for which it was collected or as required or permitted by law. Before Absolute uses or discloses personal information for any other purpose Absolute obtains consent.

- Absolute does not sell customer information to third parties
- Absolute does not share customer information with outside parties who may wish to market their products
- Absolute is committed to protecting customer information in every transaction, at every level of the organization

Absolute's Privacy Policy is published on the corporate website and is publicly available. The policy states that Absolute will only collect personal information for the following reasons:

- To develop, manage and deliver our products and services to our customers
- To ensure high standards of service to customers
- To contact our customers, either directly or through one of our resellers, to offer them the option to renew services
- To contact customers with product and service updates, upgrades and enhancements
- To meet regulatory requirements
- To verify a customer's identity
- To contact our customers directly about products and services that may be of interest

Absolute will collect personal information directly from the individual concerned unless authorized by that individual to collect it from a third party or as otherwise permitted by law. We will only collect personal information through lawful methods and we will not collect information indiscriminately.

The policy states that:

"Absolute's products and services help keep assets safe and secure and our products are designed to help protect your privacy. Using a very small software agent, our products allow your computer to call into our confidential and secure monitoring center on a regular basis and transmit to our servers certain information relating to your computer (including IP address, computer name, user name, list of hardware and installed software). With your consent and participation, certain of our products may also collect additional asset-related information for certain other purposes designated by you, such as hardware/software inventory, lease management, PC migration and software license compliance.

"If you report your computer as lost or stolen, with your consent we may collect further information from the lost or stolen computer in order to determine its location. Once we have gathered sufficient information to determine its location, we may compile such information and deliver it to a law enforcement agency having jurisdiction over the individual in possession of the lost or stolen computer. The law enforcement agency may then use this information to attempt to recover the lost or stolen computer."

DATA & INFORMATION

Device Data Attributes Collected (Standard)

Absolute collects many data points from your devices to offer you visibility and insight into your entire deployment. These data points are collated and presented to you in the predefined and customized reports you create within the console.

A list of the data attributes is available: **Absolute Data Points Collected**.

Information on Absolute reports by device OS can be viewed in the **Absolute Product Feature Support Matrix**.

Device Data Attributes Collected (Optional)

Geotechnology

Geolocation can be enabled in the Absolute console once the customer has signed a separate authorization agreement which requires that they obtain approval from their employees to enable the feature. Without this, there is no geolocation information collected or made available.

For assets that meet the Geolocation system requirements, and for which Geolocation has been enabled, the Absolute DDS agent collects location data approximately every hour from the client, using GPS and Wi-Fi triangulation technology. Using this data, the following reports can be generated:

- **Device Location Report:** Shows the most recent location of all assets with location data
- **Device Location History Report:** Shows the location history of an individual asset

These reports are based on the historical latitude and longitude data available for the device and do not provide real-time tracking functionality.

Endpoint Data Discovery

Endpoint Data Discovery is a unique data security feature available within the Absolute platform. Endpoint Data Discovery allows you to set policies to scan your managed Windows and Mac devices for data-at-risk. This EDD component of the Absolute agent is responsible for silently scanning files stored on your devices to detect content that is confidential or at risk. When you activate an Endpoint Data Discovery policy, the component is deployed automatically to each device after the next successful agent call. A full scan of each device is performed. During the scan, the component opens each file on the hard drive, scans files for specific pieces of information (matched tokens), masks tokens where applicable, encrypts these matched tokens, and uploads it to the Absolute Monitoring Center using a secure connection.

The documents that have been identified as containing matched tokens such as credit card numbers and social security numbers are not stored by Absolute after a match is found.

Once matches are identified on the endpoint, the matched tokens are first encrypted at the endpoint before being sent to the DDS console. All matched tokens are encrypted using RSA 2048 bit encryption, including those tokens matched using the built-in rules and custom rules. Additionally, any matches of credit card numbers and social security numbers using the built-in rules (Credit Card Numbers, Social Security Numbers, Personal Health Information, Personal Financial Information) are also first masked at the endpoint before being encrypted, such that only the first four digits of a match are sent and the remaining digits masked using the * symbol. Note that masking is applied to the built-in rules listed above, but not to tokens matched by custom rules. However, all matches are encrypted, regardless of whether they matched using built-in or custom rules. Only roles of 'Security Administrator' are able to view the results of matched tokens in the Absolute console. When matches are viewed, they are only decrypted for viewing within the current session of the browser and never decrypted at the Absolute Monitoring Center.

For more infomation on Endpoint Data Discovery, reference the **FAQ**

Investigative Services

Certain Absolute product editions include Investigative Services delivered by the Absolute Investigations team. These services can be leveraged to investigate a stolen device. The service operates in parallel to the local criminal justice procedure, and begins with the customer filing a theft report with their local police.

The Investigations team relies on information collected from the machine through the use of patented forensic tools. These tools may retrieve data stored on the device by the current user in order to determine the unauthorized user's identity. This data is stored in a segregated system available only to the Absolute Investigations team.

Data Protection

Absolute exceeds industry best practices to ensure our systems are:

- **Secure:** Data is protected and viewed only by the owner, or those employees delivering Absolute services on a need-to-know basis
- **Accurate:** Data is not corrupted, so it is not liable to be inadvertently misinterpreted or misused
- **Available:** Data is available for customer decisions, and for Absolute service delivery in a prompt fashion, particularly for transactions that are of an urgent nature

Information Security Management System

In order to deliver on our promise of secure, accurate, available systems, Absolute implements an Information Security Management System (ISMS).

Absolute's IT team follows ISMS processes for its internal IT systems as well as the production monitoring centers used to deliver the Absolute platform.

The documentation included in the ISMS falls broadly into the following categories:

- Policy documentation including corporate information security, codes of conduct, technical operations team security and ISMS policy
- HR policies and procedures, including employee on-boarding and separation, and badges for physical access
- ISMS statements of applicability and scope for clarity of the included systems and information assets
- Extensive operational procedures including incident management, work order and corrective action procedures, vulnerability management, capacity and database management, backup, restore, and recovery procedures

Information Security Policy

The Absolute Information Security (IS) policies and practices are promoted within Absolute in the following ways:

- Employees are provided a policy manual on commencement of employment
- Policies are highlighted on the company intranet
- Reminders of best practices are provided during company meetings and via company-wide email

There are a number of processes included in the ISMS but the most important aspects include:

- Deployment process to provide for stable, predictable, and secure installation of new or updated software into the monitoring center
- Internal audit process (annually) to review and improve policy, process, procedures, and controls
- Corrective action procedure to track and act upon non-conformities or areas of improvement

Tools & Services for Data Protection

Tools and services used by Absolute to support the protection of stored data include:

- External vulnerability scans
- Firewalls
- Anti-virus / anti-malware

Processes & Procedures for Data Protection

Important processes and procedures are supported using logs, documents and systematic tools. Examples of the tools in use include:

- Help desk ticketing application that provides a trail for all incidents and issues raised with the IT team
- Deployment tracker to provide a listing of each modification to the production environments, with the associated work order etc.

Procedural Controls

Data Access

Access to Absolute databases and systems is granted to its employees only in the following scenarios:

- System access is available for Sales and Finance to process orders and review account status
- System access is available for Support and Technical Account Management to reproduce issues and to help customers
- System access to the investigative files is available for Investigations staff (TRMS is a separate system for managing stolen device investigations)

Data Delete

The deletion of data on a customer's laptop is a sensitive transaction, and is controlled with the following steps:

- Customer must file an authorization form
- Service can only be authorized by the Security Administrator designated by the customer
- A soft token or RSA token is required
- An email is sent to the designated Security Administrator when the Data Delete is initiated
- An email is sent to multiple addresses if the Security Administrator email address is changed

For more information about the data delete capabilities, reference the **FAQ**.

Investigations Reporting and Forensics

The involvement of the customer is required when Absolute is involved in a sensitive transaction. In the example of investigational reporting:

- The customer must file a tools authorization form
- The deployment of forensic tools is in the hands of the customer (triggered on submitting an investigational report)
- The use of forensics tools is available to Investigators

ISO 27001 Certification & Audits

ISO/IEC 27001 certification was awarded to Absolute. This certification recognizes our implementation of an effective ISMS that complies with one of the most stringent international standards.

Read additional information about BSI Group.

ISO 27001 requires that a company use a systematic approach to managing sensitive information and ensuring data security. It comprises 10 detailed control categories: information security policy, security organization, asset classification controls, personnel security, physical security, communication management, access controls, system deployment, continuity planning, and compliance.

ISO 9001 Certification & Audits

ISO/IEC 9001 certification was awarded following audits conducted by BSI Group and recognizes our Investigations team for consistently meeting customer and applicable statutory and regulatory requirements. To qualify for ISO 9001 certification, eight quality management principles were met: customer focus, leadership, involvement of people at all levels, process approach, system approach to management, continual improvement, factual approach to decision making, and mutual beneficial partner relationships.

Federal Information Processing Standard

The Federal Information Processing Standard (FIPS) Publication 140-2 is a US government security standard that specifies the security requirements for cryptographic modules protecting sensitive information. The National Institutes of Standards and Technology (NIST) **publishes the list of vendors with validated FIPS 140-1 and 140-2 cryptographic modules**. Absolute Encryption Engine is validated FIPS 140-2.

CUSTOMER ROLES AND RESPONSIBILITIES

Software Installation and Removal

While Persistence technology is built into most devices at the factory, Persistence is only active when a customer installs and activates the Absolute DDS software agent on the device. The **Absolute Service Agreement** mandates that the customer *"must correctly install the Client Software on the Customer Computer to be protected."*

Similarly, the customer has the obligation to *"ensure that you have completed the removal of the Absolute Technology from a Customer Computer prior to your sale or transfer of such Customer Computer to another party".*

Compliance Relating to Employees and Personal Data

Customers that use Absolute's products and services are legally required by the **Absolute Service Agreement** to *"comply with all applicable laws, including without limitation all applicable local, state, national and foreign laws, treaties and regulations ("Laws"), including without limitation those related to data privacy, international communications and the transmission of technical or personal data, as well as the Privacy and Security Policy then in effect".* Customers must consult the laws of their jurisdiction to ensure they are in compliance with laws concerning the consent of their users or employees, personal information collection and other pertinent regulations.

Compliance Relating to Geotechnology

Before activating the Geolocation feature, customers must complete and sign the Absolute Security Administrator and Geolocation Authorization Agreement, which contains the following commitment:

"By activating or using the Geolocation features, you agree that you will only use the Geolocation Tracking Feature (a) with the unambiguous consent of all users and possessors of tracked assets, and (b) in accordance with all applicable employment, privacy, and other laws."

Once the feature is activated, and before the customer may view the Geolocation data in the DDS console, the customer is reminded of the commitment with an on-screen click-through form, stating:

"Determining the location of computing devices may by implication also determine the location of individual persons who use or possess those devices. The law of your jurisdiction likely requires the consent of such individuals before their movements may be legally tracked. By using the Geolocation Tracking Feature, you promise that you will only use the feature (a) with the unambiguous consent of all users and possessors of tracked assets, and (b) in accordance with applicable laws, including those regarding privacy and data security."

For further information on Absolute solutions and customer privacy, please contact your Absolute sales representative: **absolute.com/contact**