Inside Application Persistence:

Enabling Application Visibility and Integrity on Endpoints

WHITE PAPER

ABSOLUTE®

CONTENTS

Absolute's unique, patented Persistence technology maintains a direct two-way connection between the Absolute solution and the endpoint device, enabling the reporting and remediation of critical applications to ensure the security posture of the organization

ABSTRACT

This document details how Absolute® Application Persistence® helps organizations address pressing security concerns regarding application visibility and vulnerability. Organizations in industries such as healthcare, education and financial services, to name a few, are dealing with ever-growing security challenges on their endpoint devices.

Not only is their critical data at risk, but lateral movement across the endpoint into the corporate network becomes a potential concern, due to the non-compliance of critical applications, including anti-virus/anti-malware, encryption and VPN. Additionally, the increasing types of endpoints and the advent of remote work has heightened the complexity of monitoring machines across the fleet.

Absolute Application Persistence leverages Absolute's Firmware Persistence™ technology, embedded in the BIOS of close to 1 billion devices, to automatically monitor and remediate endpoint device applications in cases of non-compliance.

SECURITY CHALLENGES AT THE APPLICATION LAYER

Corporations today deploy a standard set of applications across their endpoints to secure devices, protect sensitive data and maintain uninterrupted workforce productivity. Examples include Anti-Virus, Anti-Malware, Encryption, Systems Management, VPN and Patch Management tools to name a few.

Despite this, organizations are still under constant danger of cyberattacks occurring through malicious intruders or internal threats due to the disabling or tampering of such critical applications. The issue of inadvertent user behavior such as the disabling of applications by negligent users is one that administrators face regularly. Reimaging of machines, malware intrusion, corrupted registry files or lax users can all affect the health of security applications that organizations have invested in, leaving the endpoint and corporate network under threat.

According to a study conducted by the Ponemon Institute, "traditional endpoint security approaches are ineffective and are costing (average) enterprises $6 million annually in poor detection, slow response and wasted time."[1] Additionally, the advent of remote work and bring your own device (BYOD) schemes heighten the chances of endpoints going off the network completely making endpoint and application visibility increasingly challenging. The Ponemon study further states that 63% of companies cannot monitor off-network endpoints whilst 55% of such endpoints usually contain sensitive data.[2]

Despite the investment in the latest security tools, administrators know that applications inevitably encounter issues leaving security vulnerabilities on the Application Layer. This leaves concerns regarding compliance and data breaches that could result in serious financial penalties, reputation damage and lost business.

Historically, administrators have conceded that there is no real manual solution to this prevalent problem. Enterprises today, however, trust automation tools that monitor and remediate applications instantly to solve this pressing issue, as illustrated by the 61% of organizations in the Ponemon study that highlighted the importance of automated solutions in their endpoint security arsenal.[3]

Absolute's Application Persistence provides self-healing capabilities to endpoint agents across the device fleet regardless of whether the machine is on or off the corporate network through automated, zero-touch remediation of critical applications.

APPLICATION PERSISTENCE

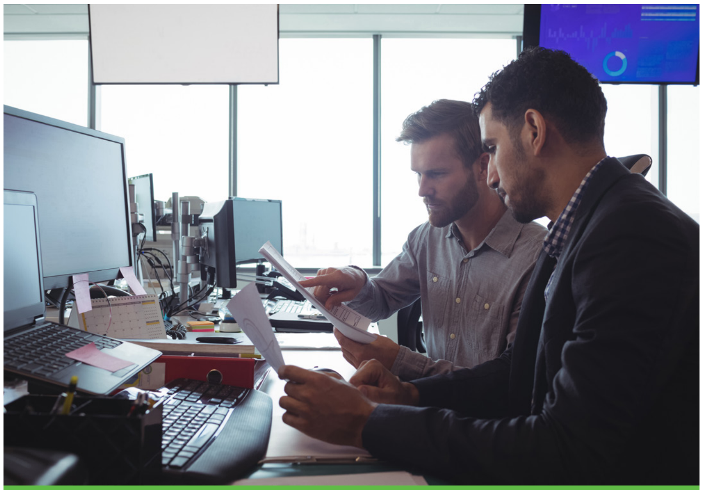
Absolute's unique, patented Persistence technology maintains a direct two-way connection between the Absolute solution and the endpoint device, enabling the reporting and remediation of critical applications to ensure the security posture of the organization. Firmware Persistence being embedded in the BIOS of machines manufactured by all major OEMs (over 1 billion devices worldwide) enables unparalleled endpoint and application visibility.

Application Persistence runs periodic health checks across the device fleet and seamlessly remediates applications that are either not installed, not running or missing critical operational files or directories.

Additionally, Application Persistence sends regular updates on the compliance status of applications across all managed devices to a secure Absolute data center. Through this, the administrator has the ability to actively monitor compliance at the fleet level, without having to worry about individual instances of application non-compliance on specific endpoints whenever they occur.

Benefits of Application Persistence include:

- Ensuring and proving compliance through self-healing endpoint agents and standardized application version deployment.
- Eliminating blind spots through uninterrupted visibility of any application regardless of the device being off-network.
- Ensuring optimal threat detection and response with instant remediation of existing controls and reporting of corrective measures taken.
- Maximizing staff productivity by guaranteeing VPN access and the availability of all business-critical applications at all times.
- Ensuring application integrity by maintaining health and efficacy.
- Validating that asset management and other important applications are present across the fleet and are functioning correctly.
- Peace of mind and operational efficiency relying on automatic, zero-touch, built-in resilience that leverages the only security solution embedded in the firmware of the devices you already have.



After activation, Application Persistence periodically reports the compliance status of each configured application back to an Absolute server whilst remediating applications whenever cases of non-compliance arise.

COMPATIBILITY

Application Persistence is supported on all devices having the following configuration:

- Absolute security agent
- Operating System: Windows 7 or higher

ACTIVATION

Absolute's console must be installed on each endpoint for an organization to leverage Application Persistence. Once Absolute is installed on the endpoint, policy files that contain application instructions and configurations are then downloaded. After activation, Application Persistence periodically reports the compliance status of each configured application back to an Absolute server whilst remediating applications whenever cases of non-compliance arise.

FUNCTIONALITY

Remediation Action Overview

The specific remediation actions that the Application Persistence (AP) engine takes in cases of application non-compliance can be summarized by the three following buckets:

- **Report:** The AP engine runs health checks on the endpoint to deduce whether the application is installed and running appropriately. This includes, but is not limited to, checking if the application is listed in the Windows Registry, if the application folder has all critical files and operational subdirectories intact and if the application's services are running smoothly.

- **Repair**: If the AP engine deduces non-compliance during the Report phase, it will attempt to remediate the application through steps taken within the confines of the endpoint device. This includes, but is not limited to, restarting the application's services as well as running the cached MSI package to install (if the application is missing) or reinstall the application (if critical application files are missing).
- **Reinstall:** If the *Repair* phase fails to remediate the application, the AP engine will attempt to download the application's installer from a preset URL on a customer hosted web server, perform a hash check to authenticate the contents of the downloaded installer and run a fresh installation on the endpoint device.

Device Policy Setup

In order to activate Application Persistence, the administrator must create a device policy through the Absolute console that specifies the applications to be persisted and the configurations specifying the remediation actions taken in case of non-compliance (either to only Report, only Report and Repair, or to Report, Repair and Reinstall). The administrator then assigns the Device Policy to a subset or all of the managed devices in their fleet.

After device boot-up, Absolute's Persistence technology embedded in the BIOS firmware ensures that the Absolute OS agent is healthy and running on the device.

Application Health Monitoring and Remediation Process

1. After device boot-up, Absolute's Persistence technology embedded in the BIOS firmware ensures that the Absolute OS agent is healthy and running on the device.
2. The OS agent then downloads the XML-based policy file that provides configurations and instructions on how to persist each specific application. The user sets these configurations prior to activating Application Persistence.
3. The AP engine runs application health checks periodically as per the Report remediation action discussed above, and sends appropriate compliance status updates to the Absolute data center. This includes, but is not limited to, the following:
   a. Checking if the application is installed on the endpoint device by inspecting the Windows registry.
   b. Checking if any critical files are missing in the application directory.
   c. Checking if the application executable and custom services are running on the device.
4. In cases of non-compliance, the AP engine runs the Repair remediation action (if defined to do so by the user in the device policy) to attempt remediating the application from within the confines of the machine. If remediation is successful, the AP engine sends updates to the Absolute data center detailing the appropriate issue and actions taken. This includes, but is not limited to, the following:
   a. If the application is not installed, attempting to run the application's cached MSI installer package to install the application.
   b. If the application is installed but has critical files missing in the application directory, attempting to run the cached MSI installer package to reinstall the application.
   c. If the application is installed but not running, attempting to restart the application's executable file and custom services.
4. In case the Repair action (step 4) fails in remediating the application, the AP engine will attempt to download an installer from a specified URI, authenticate the installer

through a hash check and run the installation as per the Reinstall remediation action. The AP engine then sends updates to the Absolute data center regardless of whether the Reinstall actions are successful or not.

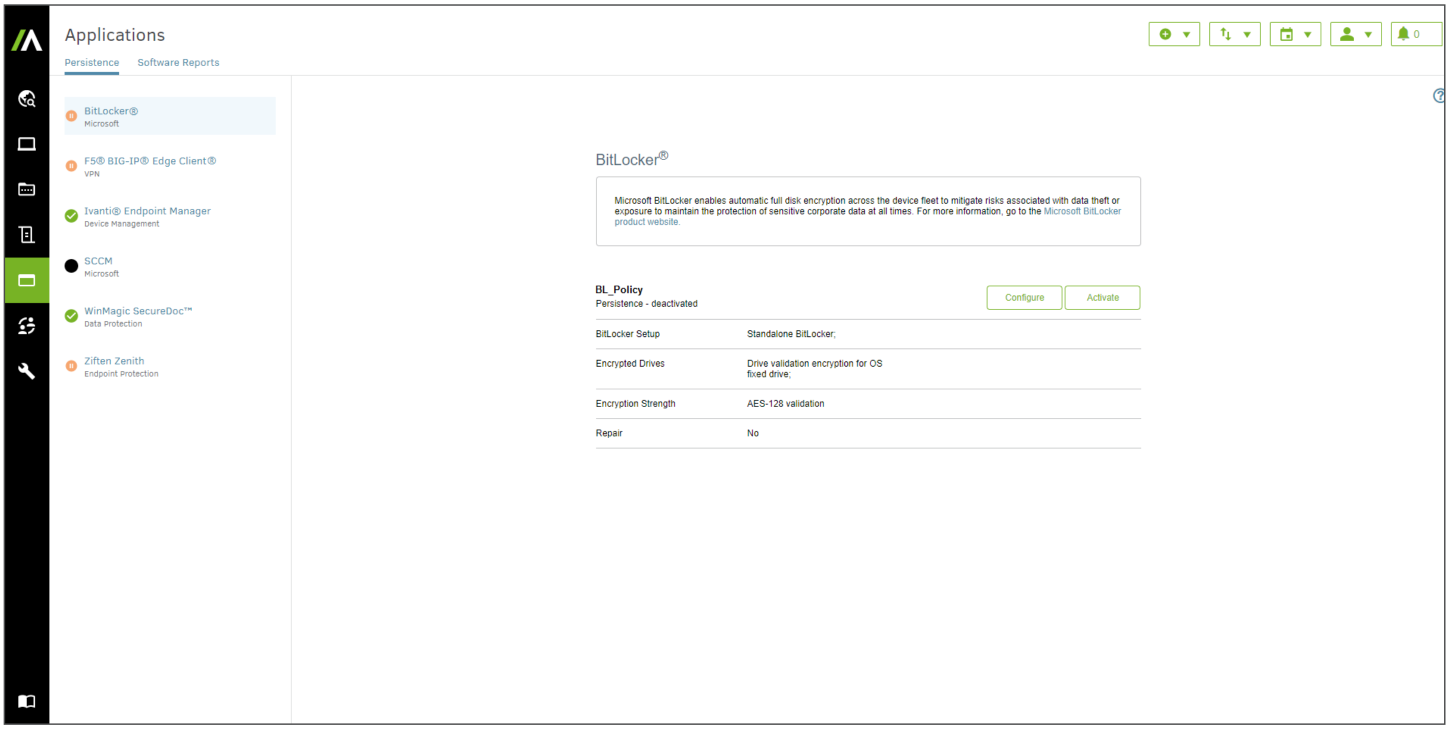
Reports

Through the Absolute console, the administrator has the ability to view customized reports specifying the compliance status of all critical applications persisted within their device fleet. This information can then be utilized to identify machines encountering most non-compliance instances and to enforce risk mitigation strategies to alleviate security concerns on the corporate network.

USER EXPERIENCE

Absolute's user interface is designed for administrators to efficiently set up and leverage Application Persistence through the seamless defining of application policy standards, assigning of endpoint devices to policy groups and viewing of application compliance status updates through periodic reports.

Through the Absolute console, users can actively configure and monitor all the applications within their subscribed module, as shown below. All pictures shown are for illustrative purpose only. Actual product may vary due to product enhancements.

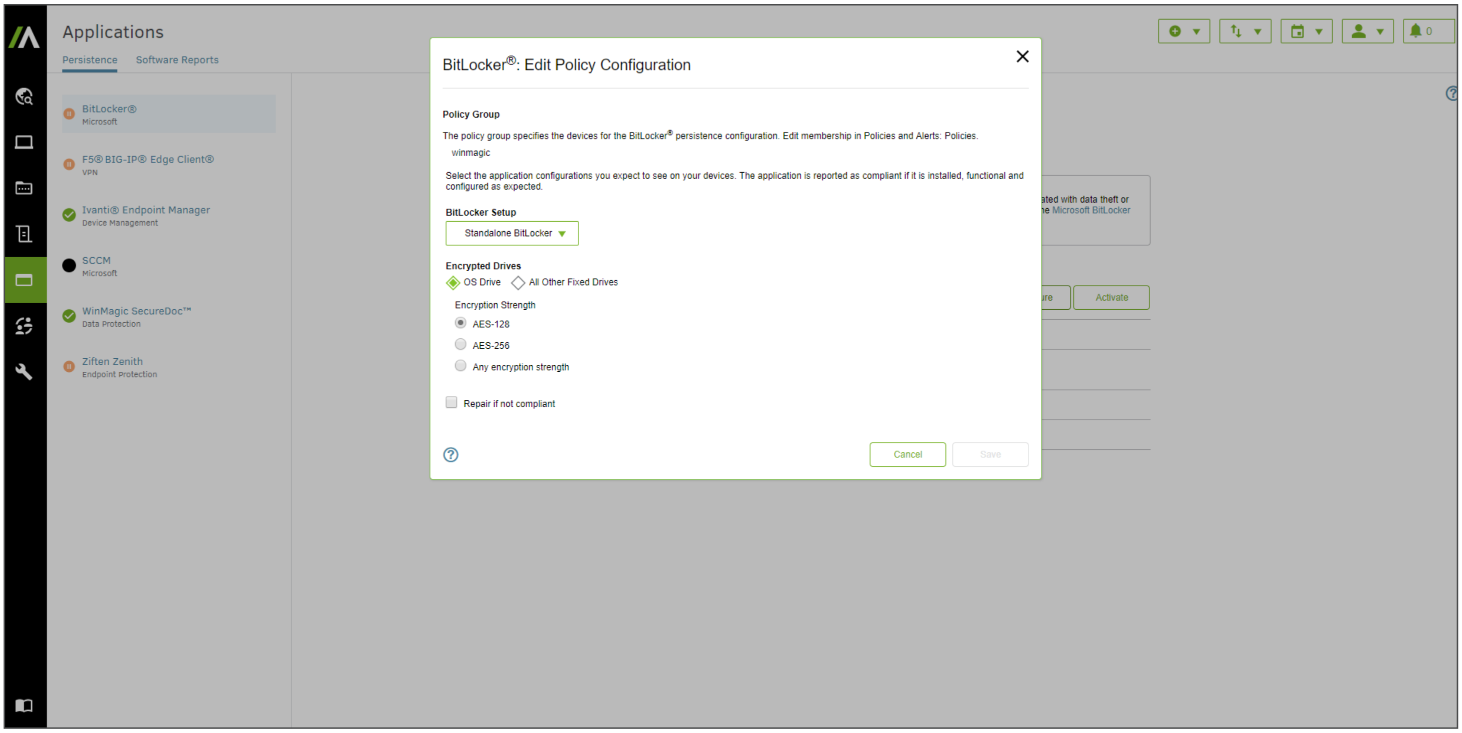


Microsoft BitLocker enables automatic full disk encryption across the device fleet to mitigate risks associated with data theft or exposure to maintain the protection of sensitive corporate data at all times. For more information, go to the Microsoft BitLocker product website.

BL_Policy
Persistence - deactivated

BitLocker Setup	Standalone BitLocker;
Encrypted Drives	Drive validation encryption for OS fixed drive;
Encryption Strength	AES-128 validation
Repair	No

Figure 1: Persistence tab within the Absolute console enabling users to monitor configured applications.



BitLocker®: Edit Policy Configuration

Policy Group

The policy group specifies the devices for the BitLocker® persistence configuration. Edit membership in Policies and Alerts: Policies.

winmagic

Select the application configurations you expect to see on your devices. The application is reported as compliant if it is installed, functional and configured as expected.

BitLocker Setup

Standalone BitLocker ▼

Encrypted Drives

◆ OS Drive ◇ All Other Fixed Drives

Encryption Strength

● AES-128

○ AES-256

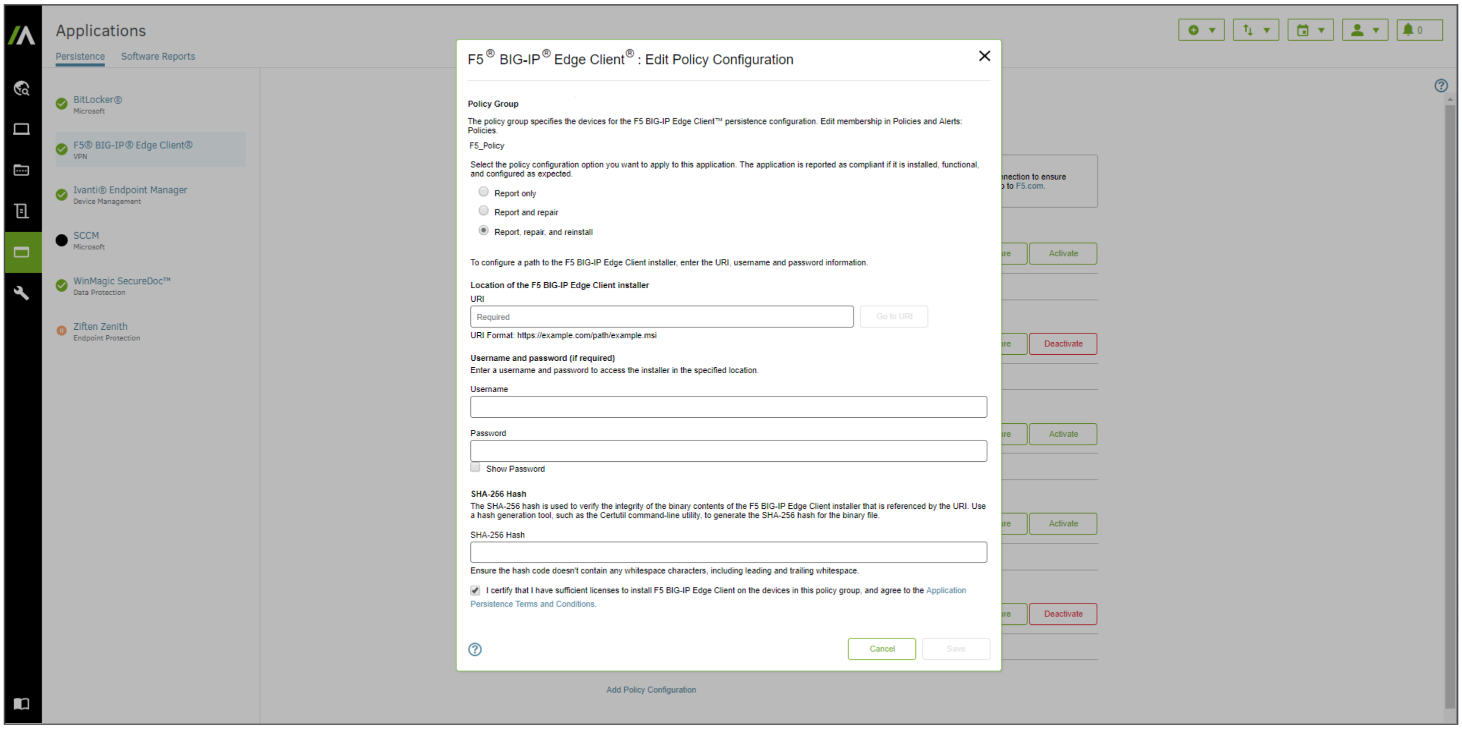
○ Any encryption strength

□ Repair if not compliant

Cancel Save

Figure 2: Window to add policy configurations and assign device policy groups to applications.

Additionally, the user has the ability to specify the remediation actions taken for each application in cases of non-compliance, as shown below. By selecting to "Report, Repair and Reinstall", the user can specify a URL location for the AP engine to download the application's installer and the SHA-256 Hash to authenticate the downloaded installer.



F5® BIG-IP® Edge Client®: Edit Policy Configuration

Policy Group

The policy group specifies the devices for the F5 BIG-IP Edge Client™ persistence configuration. Edit membership in Policies and Alerts: Policies.

F5_Policy

Select the policy configuration option you want to apply to this application. The application is reported as compliant if it is installed, functional, and configured as expected.

○ Report only

○ Report and repair

● Report, repair, and reinstall

To configure a path to the F5 BIG-IP Edge Client installer, enter the URI, username and password information.

Location of the F5 BIG-IP Edge Client installer

URI

Required | Go to URI

URI Format: https://example.com/path/example.msi

Username and password (if required)

Enter a username and password to access the installer in the specified location.

Username

Password

□ Show Password

SHA-256 Hash

The SHA-256 hash is used to verify the integrity of the binary contents of the F5 BIG-IP Edge Client installer that is referenced by the URI. Use a hash generation tool, such as the Certutil command-line utility, to generate the SHA-256 hash for the binary file.

SHA-256 Hash

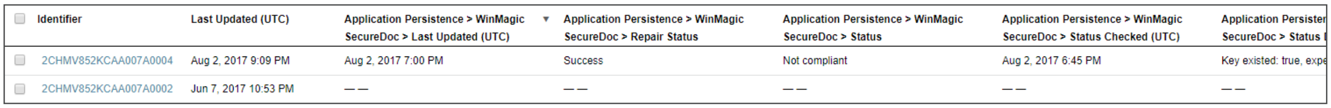
Ensure the hash code doesn't contain any whitespace characters, including leading and trailing whitespace.

☑ I certify that I have sufficient licenses to install F5 BIG-IP Edge Client on the devices in this policy group, and agree to the Application Persistence Terms and Conditions.

Cancel Save

Figure 3: Report and Repair configuration window.

Users can monitor the compliance status of applications at the device level through Application Persistence reports, as shown below.



☐	Identifier	Last Updated (UTC)	Application Persistence > WinMagic SecureDoc > Last Updated (UTC) ▼	Application Persistence > WinMagic SecureDoc > Repair Status	Application Persistence > WinMagic SecureDoc > Status	Application Persistence > WinMagic SecureDoc > Status Checked (UTC)	Application Persister SecureDoc > Status I
☐	2CHMV852KCAA007A0004	Aug 2, 2017 9:09 PM	Aug 2, 2017 7:00 PM	Success	Not compliant	Aug 2, 2017 6:45 PM	Key existed: true, expe
☐	2CHMV852KCAA007A0002	Jun 7, 2017 10:53 PM	——	——	——	——	——

Figure 4: Application Persistence compliance report.

APPLICATION CATEGORIES

Application Persistence is available for the following security software categories that represent tools most commonly used in the industry today.

Device Management

Ensure visibility and the ability to manage all endpoints across the device fleet. Enable customized reporting and alerts in case of non-compliant events.

- ITAM
- System Management

Data Protection

Ensure critical data protection and encryption measures are always present, always functioning. Enable customized reporting and alerts in case of non-compliant events.

- Encryption
- Data Loss Protection

Endpoint Protection

Ensure security investments and controls are always in place and functioning continually. Validate to regulators, audit, senior management and board of directors.

- Anti-Virus/Anti-Malware
- Continuous Visibility
- Threat Detection

VPN

Ensure control and visibility of off-network devices. Ensure encrypted and approved channels of communication and data transfer are always functioning.

- SSL VPN
- Secure Mobility

[1] The Ponemon Institute. New Ponemon Study Finds Traditional Endpoint Security Approaches Are Ineffective, Costing the Average Enterprise $6 Million+ Per Year. N.p., 13 June 2017. Web. 20 June 2017.

[2] “The Cost of Insecure Endpoints.” The Ponemon Institute, 13 June 2017. Web. 19 June 2017.

[3] “The Cost of Insecure Endpoints.” The Ponemon Institute, 13 June 2017. Web. 19 June 2017.

The information in this white paper is provided for informational purposes only. The materials are general in nature; they are not offered as advice on a particular matter and should not be relied on as such. Use of this white paper does not constitute a legal contract or consulting relationship between Absolute and any person or entity. Although every reasonable effort is made to present current and accurate information, Absolute makes no guarantees of any kind. Absolute reserves the right to change the content of this white paper at any time without prior notice. Absolute is not responsible for any third party material that can be accessed through this white paper. The materials contained in this white paper are the copyrighted property of Absolute unless a separate copyright notice is placed on the material.

/ABSOLUTE®

ABOUT ABSOLUTE

Absolute enables a world where security and IT professionals always retain control over their devices and data. We're the first and only company to offer uncompromised visibility and near real-time remediation of security breaches at the source.

Absolute Persistence® returns devices to their desired state of safety and efficacy after malicious attacks or user error, thanks to our unique location in the firmware of more than 500 million devices built by most of the world's top device manufacturers.

EMAIL:
sales@absolute.com

SALES:
absolute.com/request-a-demo

PHONE:
North America: 1-877-660-2289
EMEA: +44-118-902-2000

WEBSITE:
absolute.com