Absolute Persistence:

The firmware-embedded technology at the core of Absolute

WHITEPAPER

ABSOLUTE®

CONTENTS

In our business, it's what happens in the background that counts. Maybe it's a security officer who knows that, even though a criminal has stolen a computer, the IT department can still remotely delete every trace of corporate data on it. Or perhaps it's when the CTO realizes that the annual three-month, 12-person physical inventory cycle can be replaced with a report that takes just minutes to run.

More than 1 billion devices around the world host our patented Persistence technology. Persistence is the linchpin of Absolute, the uniquely-embedded technology that gives peace of mind to security and IT teams.

A CLOUD-BASED SOLUTION FOR A MOBILE WORKFORCE

The modern workforce isn't tethered to a desk: people work in transit, on the road, from home, and across multiple office locations, using many given factors to connect. As a result, an average of 51% of an organization's devices can't be seen at any given moment.[1]

Persistence gives organizations and individuals the ability to reach and connect with all of their devices – regardless of network, user, or any changes that have been made to the device. This gives administrators the confidence of always knowing where a device is and what condition it's in.

But Persistence enables much more than just visibility. To explain that, we'll show you how it works.

AN ELEGANT INTEGRATION OF HARDWARE AND SOFTWARE

Step 1 — Hardware

Absolute has partnerships with dozens of the world's largest computer manufacturers. Each of them builds the Persistence module directly into the firmware of their devices before they leave the factory. To date, Persistence is embedded in over 1 billion laptops, desktops, tablets, and smartphones — all you need to do is activate it.

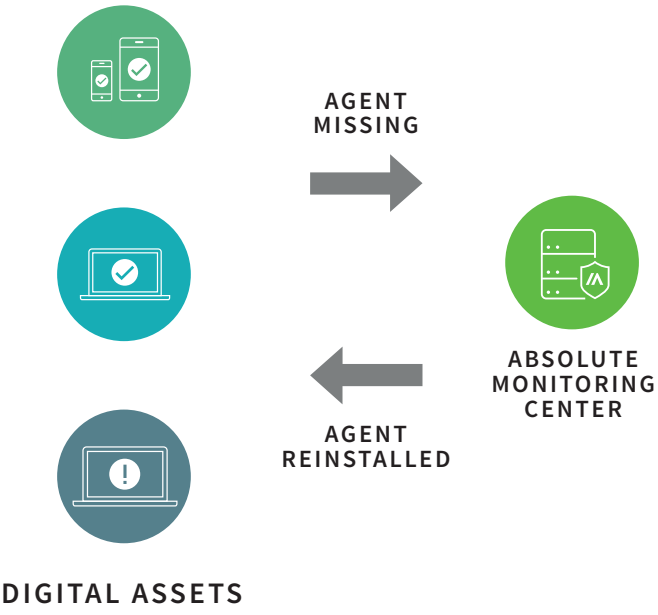
Step 2 — Software

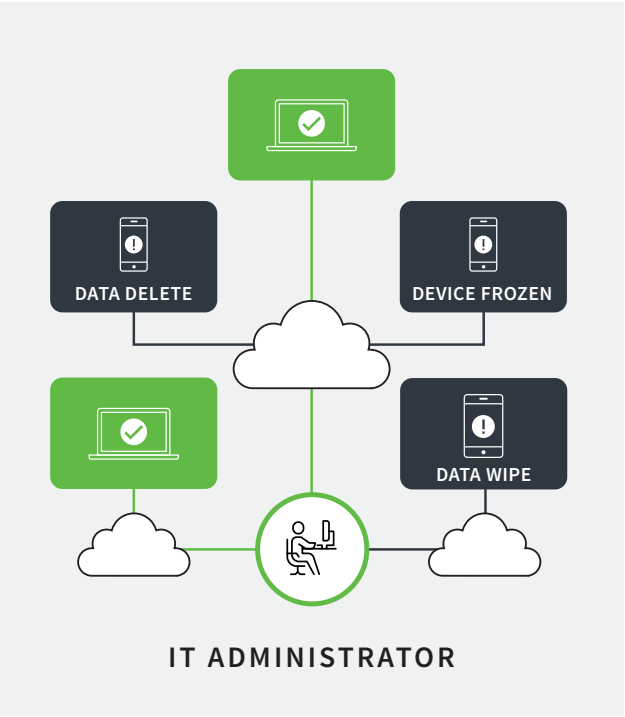
When a licensed Absolute agent is installed for the first time, the agent creates a two-way digital tether between the activated device and the cloud-based Absolute console. Hundreds of data points related to hardware and software are transmitted to administrators in real time.

And it's a two-way street: the same connection can be used to query and remediate at scale, remotely wipe or delete sensitive data, lock down compromised devices, and many other remote commands.

Step 3 — Persistence

The Persistence module constantly monitors the health of the software agent and automatically performs a reinstall whenever it is disabled or removed (either accidentally or maliciously.) Even if the firmware is flashed, the device reimaged, the hard drive replaced, even if a tablet or smartphone is wiped clean to factory settings — when the Persistence module detects removal, it always reinstalls the agent.





The only way to stop the continuous stream of data and control is to perform an authorized deactivation through the Absolute console.

CYBERSECURITY IS GETTING MORE COMPLEX AND EXPENSIVE

- *70+ percent of breaches originate on the endpoint*
  — IDC, 2016
- *$6 billion of cybercrime damages will be accrued annually by 2021*
  — Annual Cybercrime Report 2017, Cybersecurity Ventures
- *63% of companies can't monitor off-network endpoints*
  — Ponemon Institute 2017
- *55% of vulnerable endpoints contain sensitive data*
  — Ponemon Institute 2017
- *51% of an organization's devices can't be seen at any given time*
  — Ponemon Institute 2017
- *10 security agents are installed on the average device* — Absolute Endpoint Security Trends Report, 2019
- *5,000+ common vulnerabilities and exposures (CVEs) found on the top 20 client applications in 2018*
  — MITRE.ORG
- *50%+ of attacks target the application layer*
  — Verizon Data Breach Report
- *42% of endpoints have encryption failures at any given point in time*

— Absolute Endpoint Security Trends Report, 2019

MITIGATE YOUR DATA AND COMPLIANCE RISKS

Being on the right side of compliance has never been more critical: ransomware attacks are on the rise, with ransom payments totaling almost $1 billion worldwide as of 2019. Add in the cost of disruption and compliance fines, and it's easy to see why corporate, healthcare, education and governmental organizations all need to improve visibility into their device fleets and maintain their security controls.

And over 12,000 organizations trust Absolute to mitigate those risks. Whether it's a device changing location, a hardware swap, an unknown user accessing the device, or the inevitable failure of security vitals such as AV, encryption and VPN, Persistence helps them identify and seamlessly eliminate threat vectors, protecting their fleets from potential calamity.

We couldn't call it Persistence if it didn't persist — so yes, it even works when a device is missing or stolen. Thieves, rogue employees, and corporate criminals have all tried to

break the connection to no avail. Instead, their activities were monitored, recorded, and used against them in a court of law. We've provided forensic evidence to close to 5,000 law enforcement members around the world, allowing them to recover over 28,000 stolen devices.

From a governance, risk management, and compliance perspective, Persistence can mitigate most risk scenarios relative to the endpoint. This is more important than ever in an era where data is arguably the world's most valuable resource. Persistence helps you maintain compliance and resume normal business operations in the face of incidents that would previously have been catastrophic.

FUTURE-PROOF YOUR IT ASSET MANAGEMENT

Deployments are more complex than ever: desktops, tablets, PCS, and phones all make up the typical organization's device fleet, and our data indicates that the average device has 10 security agents installed at once. Keeping up with basic IT and security requirements is difficult enough. Connecting to and protecting all of these devices, apps, and data? Sometimes it can seem impossible.

The only thing that hasn't changed is the need for the organization to secure and manage endpoints so that the organization is protected.

The only thing that hasn't changed is the need to secure and manage endpoints so the organization is protected, business data is secured, and end user productivity is supported with seamless workflows and up-to-date devices.

Persistence extends across multiple form factors and operating systems, providing the consistent connection IT and security teams needs to do its job.

For more information about Persistence and our products, visit **absolute.com/platform/persistence**

REFERENCES

[1] The Cost of Insecure Endpoints, Ponemon Institute 2017

/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