Two Options for Application Hardening and Resilience

WHITE PAPER

ABSOLUTE®

Introduction

As an independent software vendor (ISV), your customers rely on you to deliver value – by making their operations more effective, efficient, and secure. But without the means to ensure the ongoing health and performance of your applications, can you be certain that value is realized?

When applications and security controls fail, it's rarely an issue of quality. Users remove them. Hackers disable them. They can interfere with one another, causing damage and decay. With infinite configurations to test, solving for every variable is not possible and even the best applications introduce risk of their own.

Leading system manufacturers like Dell®, Lenovo®, and HP® have long recognized the value of Absolute – embedding our Absolute Persistence® technology in over half a billion devices to offer their customers continuous visibility and control over their endpoint environments.

The **Absolute Application Persistence™ Partner Network** extends the same advantages for software providers to:

- Monitor the health and performance of their applications and automatically restore, repair, or reinstall with Absolute's undeletable connection.
- Get application insights across their customer base with continuous intelligence and detailed reporting on usage, versions, and performance-impacting events to cost-effectively fine-tune application performance.

Don't risk your reputation on code-based application hardening. Secure your application and your customers with firmware-based Application Persistence.

You and your customers can be confident that your application is always installed, fully operational, and delivering its intended value whether included alongside category-defining applications in our Absolute Resilience® endpoint security solution, integrated with Application Persistence-as-a-Service (APaaS) directly – or both — by partnering with Absolute.

Why harden your applications and assure they continue functioning across disruptions, unintentional decay, or malicious actions?

The Need for Application Hardening and Resilience

Ultimately, customers rely on your security and business applications to protect their endpoints from cyber risks and empower their employees to remain productive. However, maintaining application integrity across an entire device fleet can be challenging and costly.

This holds especially true in today's work-from-anywhere era. The need to support and secure remote workforces has led to an increase in the average number of applications installed per endpoint. With this comes an accompanying risk of friction, failure, and non-compliance.

According to the Absolute 2021 Endpoint Risk Report, enterprises now have an average of 96 unique applications per device, including 13 mission-critical applications.

- The number of security controls has increased to 11.7 per device, with most devices containing multiple controls with the same function.
- 100% of devices have at least one encryption application installed; 60% have two or more.
- 100% of devices have at least one endpoint management control; 52% have three or more.
- 59% of devices have at least one identity and access management (IAM) solution installed, 11% have two or more.

It's worth noting that this increased complexity is itself a security risk — as each new control adds friction to the endpoint environment, increasing the likelihood of collision and decay.

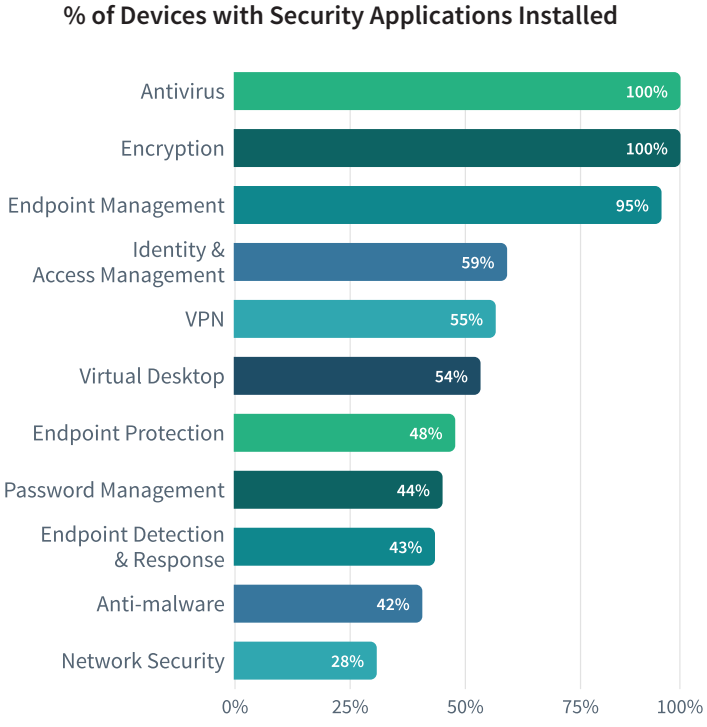

FIGURE 1: Percentage of devices with security apps

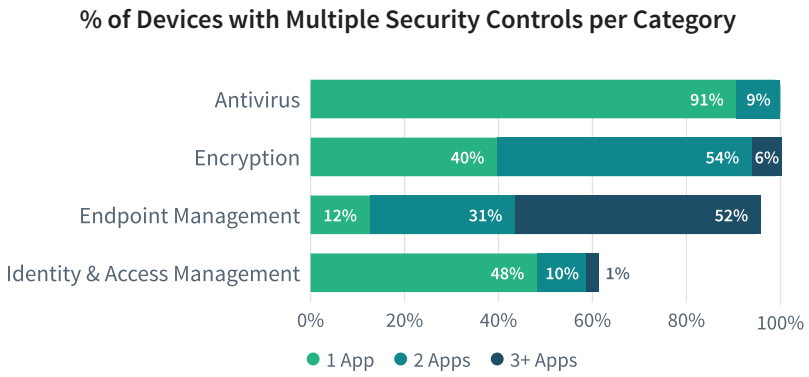

FIGURE 2: Percentage of devices with multiple security controls per category

Your customer's security posture is only as good as the applications that support it. Regrettably, failing applications continue to undermine the best efforts of many security teams.

Left unchecked, every one of the 11.7 security controls deployed on the average device is a potential attack vector. Complex environments cause security controls to collide and decay. Their effectiveness measurably degrades over time and users wanting to circumvent restrictions may attempt to disable or remove them altogether.

With sophisticated attackers seeking access by any means, simply deploying protections such as encryption, VPN, anti-virus, and anti-malware — and trusting that they remain effective — is no longer enough for your customers. To truly defend the endpoint and realize a return from their security investments, your customers expect your applications' effectiveness are continuously monitored and maintained. More and more customers are demanding their ISVs deliver application hardening and resilience as part of their overall offerings.

In organizations without application hardening and resilience in place, one in four devices reported unhealthy applications at any given time, including critical protections.

While faulty implementations, poor integrations, and lackluster maintenance by your customers might contribute to these shortcomings, more commonly these factors influence the integrity and efficacy of security and business applications:

- Re-imaging of an end user's device where often the software is not re-installed.
- Critical files are corrupted when new third-party applications are installed or updated.
- Negligent users damage or remove applications unknowingly.
- Malicious insiders and/or hackers disable security applications to bypass security controls.

So, how do you assure that your software continues to function across disruptions, unintentional decay, or malicious actions that are fundamental to its operations?

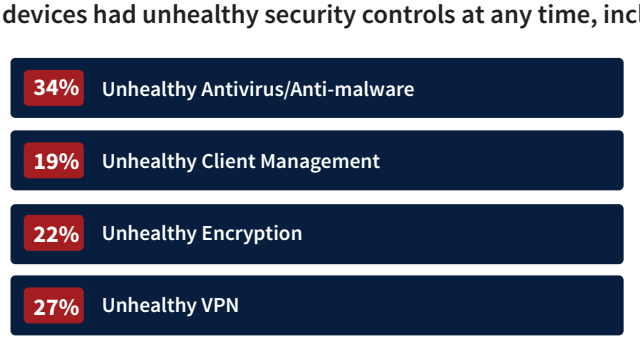

FIGURE 3: Efficacy of security controls

Application Hardening via Kernel Driver

While most ISVs have not taken special measures to harden their applications, a smaller number of vendors leverage a kernel driver approach to harden their applications and minimize the risk of tampering. These vendors typically provide mission-critical security applications, like anti-virus and anti-malware solutions, that are otherwise an easy target for threat actors to tamper with.

Kernel driver hardening uses specific kernel configuration options to limit or prevent certain types of cyberattacks. As an ISV, you can use these options to create a more secure application by building upon the operating system kernel. These sets of processes resident in memory provide a low-level abstraction layer between your application and the computer hardware. The kernel mediates access to the CPU, file systems, network sockets, memory, etc.

An ISV's kernel driver can intercept process, I/O, and registry requests from third-party application programs, including operating system applications running in "user space," such as Microsoft Windows File Explorer, and deny these operating system requests.

Leveraging a kernel driver, your application can protect its processes from termination, its files from modification, and protect its registry configuration. The registry may contain application-specific configuration and is also used by the Windows operating system to define the services to run at system boot.

However, software security practitioners are often torn between choosing performance or security. Ultimately, a misbehaving and conflicting kernel driver can crash the operating system or cause a severe loss of functionality. A poorly configured kernel driver can impact overall system performance. This can cause significant issues, as OS kernels are sensitive to the smallest performance regressions. This makes it difficult to develop innovative kernel hardening mechanisms, as they inevitably incur some run-time performance overhead.

Employing a kernel driver can have a substantial impact on other applications or system processes. Software security practitioners are often forced to whitelist other applications (e.g., Windows File Explorer, Microsoft Endpoint Configuration Manager, core security applications such as anti-malware and anti-virus) to avoid disruptions and assure user productivity, which in reality pokes holes in your hardening strategy.

Establishing a kernel driver approach to harden your application requires specialized skills and knowledge. The return on the incremental investment is primarily limited to preventing accidental tampering of your software, whereby specific services, files, or registry keys are protected against software collision or decay. Unfortunately, it doesn't take care of malicious activity. A simple Google search reveals many options on how to disable applications that have been hardened using kernel drivers. In fact, a threat actor could simply wipe the hard drive and the kernel driver's effectiveness would be lost, as the file is deleted.

Ultimately, kernel drivers can provide some degree of resilience. But they are fragile in much the same way the applications they're supposed to protect are, in that a kernel driver does not have self-healing capabilities to return to an original state of integrity.

So, how can your application developers assure that your software survives even the most severe disruption?

Beyond the Kernel Driver: Firmware-Embedded Application Persistence

The most severe disruption is the re-imaging of a device or swapping out the hard drive, and while drastic, it happens more often than you would think. In those cases, it doesn't matter what your customer had installed on their devices and if one of the applications was hardened by a kernel driver or not. None of the files would be there anymore.

A firmware-level Persistence technology can overcome this as the embedded micro executable would start before the OS kernel starts. It would load instructions into the OS kernel's memory space that would determine what process should run first upon finishing the boot-up of the device. It is resilient to human error, malicious actions, software collisions, and normal decay.

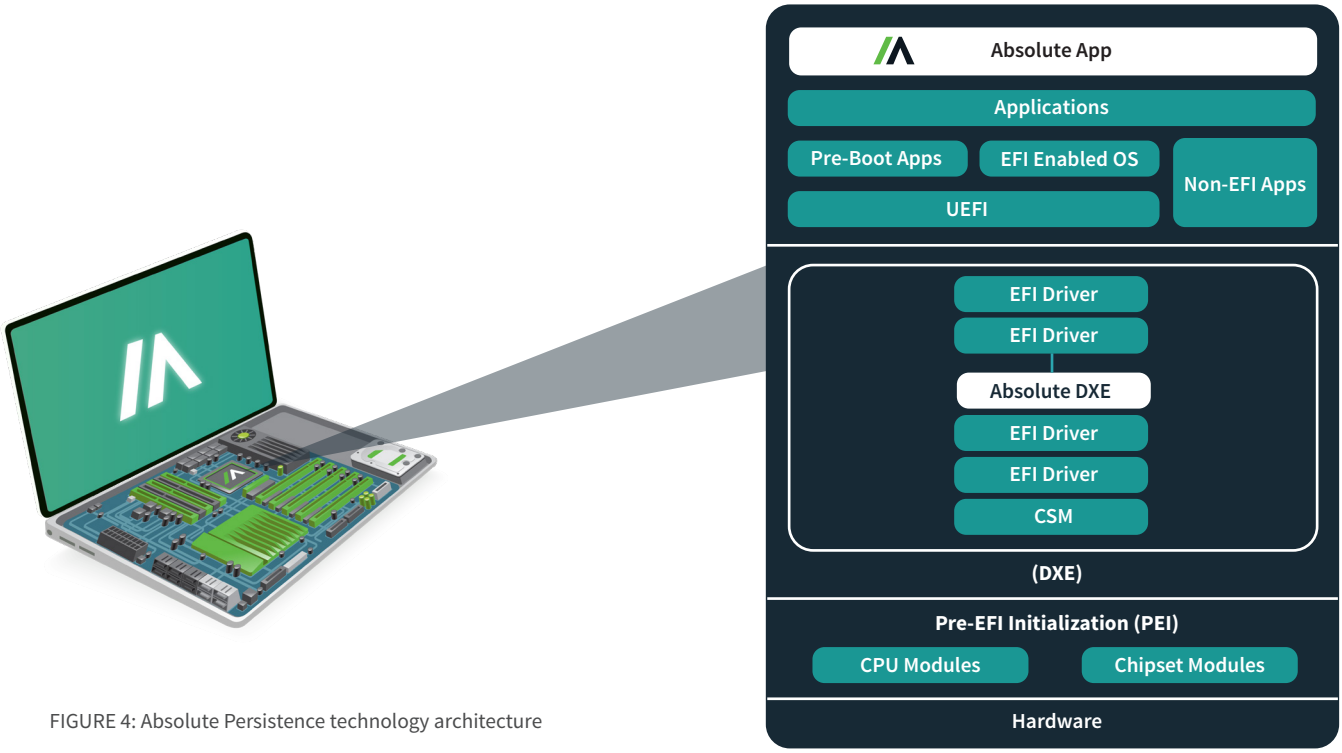

FIGURE 4: Absolute Persistence technology architecture

The permanent presence of the Persistence technology is guaranteed by the root of trust inherited by the fact that the firmware-embedded micro executable is signed by Microsoft, assuring that it is trusted upon start-up.

Now, how can you envision this to work in practice and what are the components that Absolute delivers?

Leading system manufacturers factory-embed our trusted Absolute Persistence® technology into a privileged section of their devices' firmware called the UEFI (or BIOS). Upon start of a Windows device, it loads the Absolute Rpcnet Agent, which is a little micro executable that is embedded into our firmware component. The Absolute Rpcnet Agent then communicates with the Absolute Persistence technology embedded in the firmware of those Windows devices. This enables the activation and enrollment of the device to an Absolute account. It is also used to install the other agent, the Absolute CTES Agent.

The Absolute CTES Agent is installed through the Absolute Rpcnet Agent to deploy components and execute actions based on specific features activated by an end user organization's IT administrator through the Absolute Console or pre-configured when delivered as part of the ISV's application installer package.

The CTES Agent checks pre-defined conditions for your application that define its integrity and health, ranging from registry values, presence of key files and their hashes, metadata attributes, services status and port status down to the user that has been assigned. Should any of those attributes mismatch the pre-defined policy, your application would automatically be repaired or reinstalled.

Absolute Persistence technology runs regular health checks on the Absolute Rpcnet Agent and repairs or reinstalls it whenever it is tampered with. The Absolute Rpcnet Agent in turn, does the same for the Absolute CTES Agent when necessary. This self-healing connection from the Absolute Persistence technology embedded in the device's firmware is the foundation to harden your applications and make them resilient to any external factors.

The two agents communicate with Absolute's cloud-based servers primarily through search.namequery.com via ports 80 and 443. The Absolute Agent binaries are coded-signed and white-listed with all the major anti-virus and anti-malware vendors. Through our relationships with those vendors, we regularly engage in whitelisting programs to ensure our respective products function effectively together. This equips your customers with the necessary in-depth defense to protect against today's dynamic cyber threats.

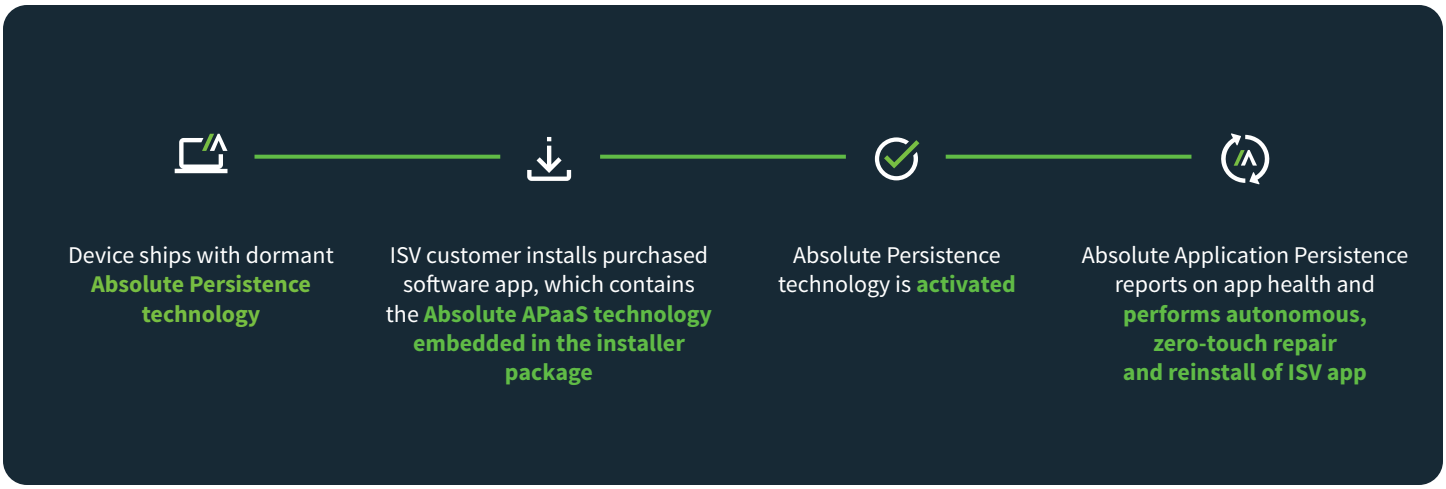

FIGURE 5: Application Persistence-as-a-Service – How it Works

Application Hardening and Resilience Made Simple

This undeletable line of defense is delivered as part of the Absolute Endpoint Resilience solution or built directly into your software via our Application Persistence-as-a-Service (APaaS) to seamlessly repair and heal the applications your customers depend on.

When delivered as part of the Absolute Endpoint Resilience solution, Absolute creates an Application Persistence Module that defines the attributes for the integrity and health of your application. This module is added to the Absolute Application Persistence Library, accessed by joint customers through the Absolute Console. From there, the customer can select which applications to persist and what actions to take – be it just to report on the health of the application, to repair the application, or even reinstall it, if a repair attempt failed.

For APaaS partners, we simply extend our undeletable line of defense of self-healing to nearly any application – not just security applications. You can deliver Application Persistence to your entire customer base without them having to subscribe to any of Absolute's services. Absolute generates an Activation Utility that you embed into your installer package that upon installation of your software would activate the Absolute Persistence technology, and from thereon would harden your application and reinstall without end user intervention.

It's your choice if you wanted to make this capability part of your standard offering, or if you select to create a premium offering.

APaaS partners also receive telemetry data (e.g., data on repairs and re-installs, app versions used in the wild, data on repairs and re-installs by app version, app integrity, top failure reasons) to get insights into your application's health across your customer base – to understand what is failing and why – for continuous improvement.

WHAT CUSTOMERS HAVE TO SAY

> *We use Absolute Application Persistence to ensure our VPN technology is maintained on each endpoint. This provides our remote workers with a reliable connection to our network with no interruption to productivity.*

ALLEGIS GROUP

> *The application repair and reinstall is exceptionally powerful. Not only does it supplement SCCM… but it keeps SCCM itself running and functioning correctly.*

Ogletree Deakins

Your customers will thank you, as they:

- **Ensure application integrity** by maintaining health and efficacy.
- **Increase operational efficiency** by relying on automatic, zero-touch, built-in resilience.
- **Maximize productivity** by guaranteeing availability of mission-critical applications and reducing IT helpdesk tickets.
- **Increase ROI** for existing security and software investments.
- **Maintain compliance** with internal policies, industry standards, and government regulations.

With Absolute APaaS, focus on your core business while we take care of your application hardening and resilience.

- **Stand out from the pack** with differentiation against competition by assuring application uptime and integrity.
- **Access rich application health telemetry** to allow for cost-effective application performance tuning.
- **Lower development cost** by leveraging Absolute's field-proven technology instead of investing in code-based application hardening and maintaining the code.
- **Improve customer satisfaction** through better return on investment and reduced support calls.
- **Focus on what you do best** and let Absolute deliver Application Persistence for your apps at scale.

Deliver on Your Value to Customers

Considering today's dynamic threatscape, it's not surprising to see that end user organizations select software vendors who demonstrate a commitment to secure coding practices and have a strong track record of maintaining the integrity and health of their applications. Ultimately, organizations truly value the efficacy and return on investment of their software purchases. It's vital for ISVs to either "build or buy" Application Persistence capabilities when developing software.

Absolute Application Persistence for ISVs delivers many benefits beyond a traditional kernel driver approach and delivers telemetry data to fine-tune application performance for the future. Instead of investing in application hardening and maintaining code, leverage Absolute's field-proven technology to assure application uptime and integrity.

WHAT YOUR PEERS HAVE TO SAY

> *Our customers rely on our application continuously throughout each day to ensure **only authorized users** are accessing their systems and sensitive data. Plurilock is excited to partner with Absolute to add **persistence capabilities** to our endpoint agent as a new offering for our customers.*

Ian L. Paterson,
CEO,
Plurilock Security

> *Through APaaS, we are able to extend Absolute's **undeletable line of defense** and self-healing capabilities to our application to ensure it stays up and running. This gives us the confidence, and the validation, that we are delivering on our promise of keeping customers' highly sensitive data secure.*

Dexter Caffey,
CEO and Founder,
Smart Eye Technology

ABSOLUTE® PERSISTED

To join our network of customer-centric vendors and resilient applications that drive productivity, ensure security, and deliver peace-of-mind, visit:

Become an Absolute Application Persistence Partner

Don't take our word for it.

Connect with **Lawrence Pingree**, Managing Vice President for emerging technologies at Gartner, to set up an inquiry call on the advantages of firmware-embedded Application Persistence.

Engage with **Andrew Hewitt**, senior analyst at Forrester Research, who is conducting a study on self-healing applications.

/ABSOLUTE®

ABOUT ABSOLUTE

Absolute Software (NASDAQ: ABST) (TSX: ABST) accelerates customers' shift to work-from-anywhere through the industry's first self-healing Zero Trust platform, ensuring maximum security and uncompromised productivity. Only Absolute is embedded in more than half a billion devices, offering a permanent digital connection that intelligently and dynamically applies visibility, control, and self-healing capabilities to endpoints, applications, and network access to ensure their cyber resilience tailored for distributed workforces. Trusted by nearly 16,000 customers, G2 recognized Absolute as a leader in Zero Trust Networking in the Fall of 2021. For the latest information, visit **absolute.com** and follow us on **LinkedIn** or **Twitter**.

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