ABSOLUTE®

2023 RESILIENCE INDEX

A False Sense of Security Imperils Digital Enterprises

Executive Summary

In the fourth year of our recurring research of endpoint resilience trends, we analyzed anonymized data from 14 million Absolute-enabled devices active across customer organizations in North America, Europe, and APAC, as well as data and information from trusted third-party sources.

This report examines the state of resiliency in the new work-from-anywhere model by assessing its complexity, continuity, and compliance posture. The findings affirm that despite the long-standing belief that deploying more security solutions will result in greater protection against threats, the truth of the matter is very different.

As a result, organizations are looking for ways to securely connect their employees to corporate networks and resources. This is driving a new *comply to connect* trend that balances security and cyber resilience to ensure your employees can confidently get to work, and keep working, no matter where risk finds them.

Read the 2023 Resilience Index to learn how to:

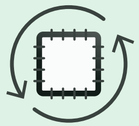
1. Assess complexity in your environment and evaluate your cyber resilience posture.
2. Gain an understanding of the connectivity and compliance practices needed today.
3. Learn how Absolute makes your existing security work.

Securing the Remote and Hybrid Workforce

As businesses and employees adjust to post-pandemic norms, one point becomes clear: hybrid work is here to stay and is no longer just an employee perk but an employee expectation. According to Gartner[1] by year-end 2023, 48% of knowledge workers will be working hybrid and fully remote (up from 27% in 2019), with 39% of those employees working hybrid, which is up from 12% in 2020.

1 Gartner; Forecast Analysis: Knowledge Employees, Hybrid, Fully Remote and On-Site Work Styles, Worldwide, January 2023

WINDOWS 10
ON A MAJORITY OF ENTERPRISE DEVICES



OS VERSIONS & PATCHES

800+
BUILDS/PATCHES

14
VERSIONS

The Landscape Is Messy

The new work-from-anywhere model is putting a strain on IT and security teams and creating unprecedented complexity. Employees shifting between corporate and off-corporate networks are creating visibility and control challenges, which are impacting those teams' ability to diagnose and remediate end user issues and minimize cybersecurity risks. In addition, they have to deal with a broad mix of networks, hardware, operating system (OS) versions, and patches.

As an example, more than 80% of devices use the Microsoft® Windows® OS, with the large majority on Windows 10. At first glance, this might appear homogenous and easy to manage; however, the reality is that IT practitioners are struggling to keep their employees' endpoints up to date with 14 different versions and more than 800 builds and patches present.

DEVICES

> 80%  **WINDOWS DEVICES** IN VERY LARGE ORGANIZATIONS

< 20%  **CHROMEBOOKS** IN VERY LARGE ORGANIZATIONS

Source: Absolute Device Telemetry Data

INCREASED DEVICE MOBILITY OPENS NEW VULNERABILITIES

4 LOCATIONS
ENTERPRISE DEVICES

Remote employees' multiple locations add further to this already significant level of complexity. They are now performing significant work on networks their organizations do not own or control, which dramatically increases an organization's risk exposure. And even within locations, users may often switch between devices and networks—from a laptop on their favorite coffee shop's Wi-Fi to a mobile device on a carrier's cellular network, all while trying to run a productive online meeting on the drive back home, for example. Thus, it's not surprising that Absolute's customers' average number of enterprise device locations has grown 15% year-over-year, with an average of four locations per device in February 2023.

15%
GROWTH OF ENTERPRISE DEVICE LOCATIONS YEAR-OVER-YEAR

Source: Absolute Device Telemetry Data

ON ENTERPRISE DEVICES THERE ARE

67 APPS

OF ALL TYPES (PRODUCTIVITY, SECURITY, NON-WORK APPS ETC.) ON AVERAGE

Adding to the complexity, IT and security teams must deal with is the number of installed applications on devices. According to Absolute device telemetry data, there are 67 applications installed on the average enterprise device, with 10% of those devices having more than 100 applications installed.

10%

OF ENTERPRISE DEVICES HAVE

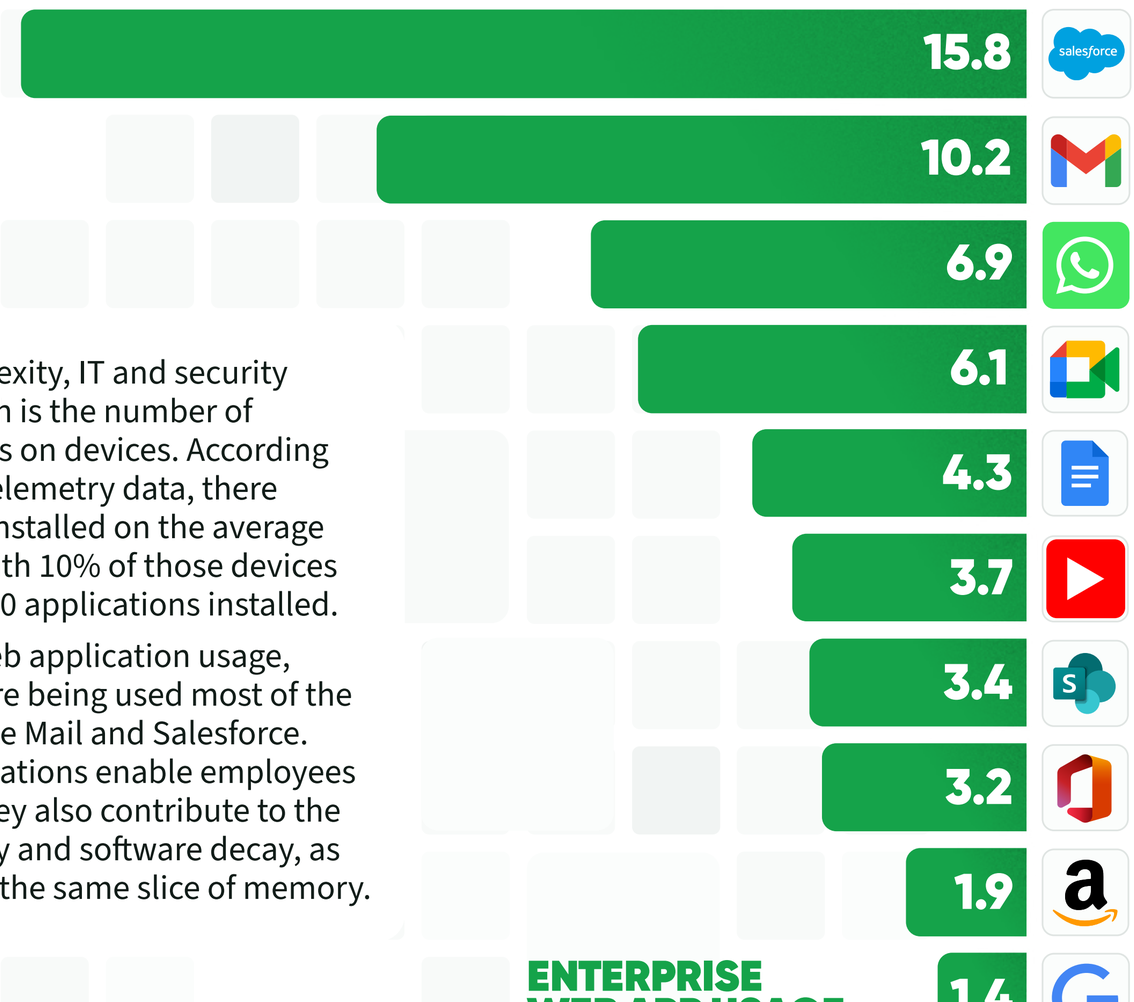
100 APPS

OR MORE

When it comes to Web application usage, enterprise devices are being used most of the time to access Google Mail and Salesforce. Many of these applications enable employees to be productive. They also contribute to the increased complexity and software decay, as they all compete for the same slice of memory.

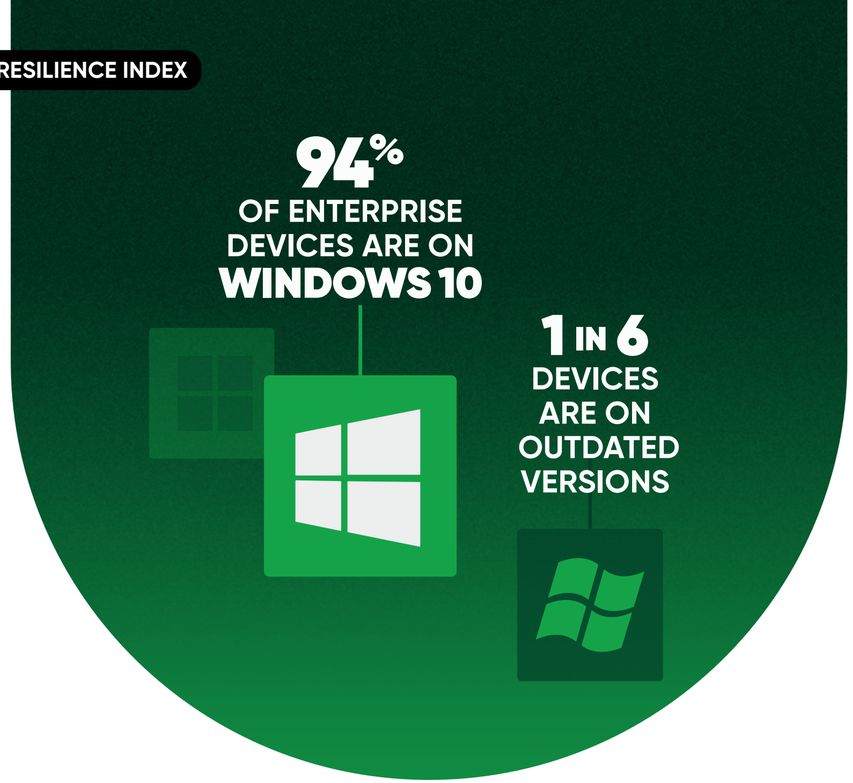
ENTERPRISE WEB APP USAGE

(IN HOURS)



SOURCE:
Absolute Device Telemetry Data

ALL THIS UNDERLINES THE **COMPLEXITY** LANDSCAPE



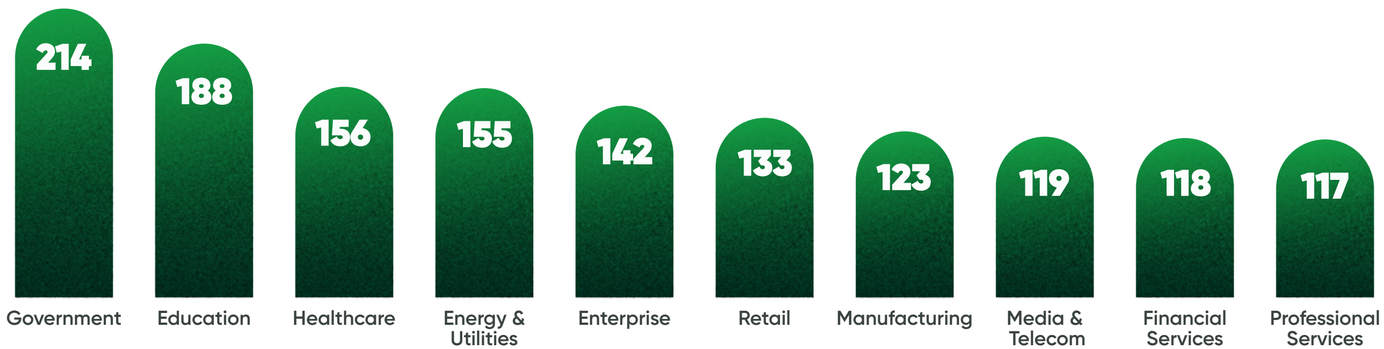
Furthermore, the sheer number of applications installed on enterprise devices - as well as the variety of operating system versions and builds – make it difficult for IT and security teams to maintain those apps or patch them. This situation negatively impacts their ability to minimize exposure to known vulnerabilities.

This assumes that IT is trying to proactively manage as many as 50 to 100 applications. More likely, they are managing a much smaller subset and the rest are “shadow applications” that are not actually being managed or patched but may still be running in the background. This exposes organizations to further risk and consumes even more system resources.

WINDOWS 10 PATCH AGE

DAYS BY VERTICAL

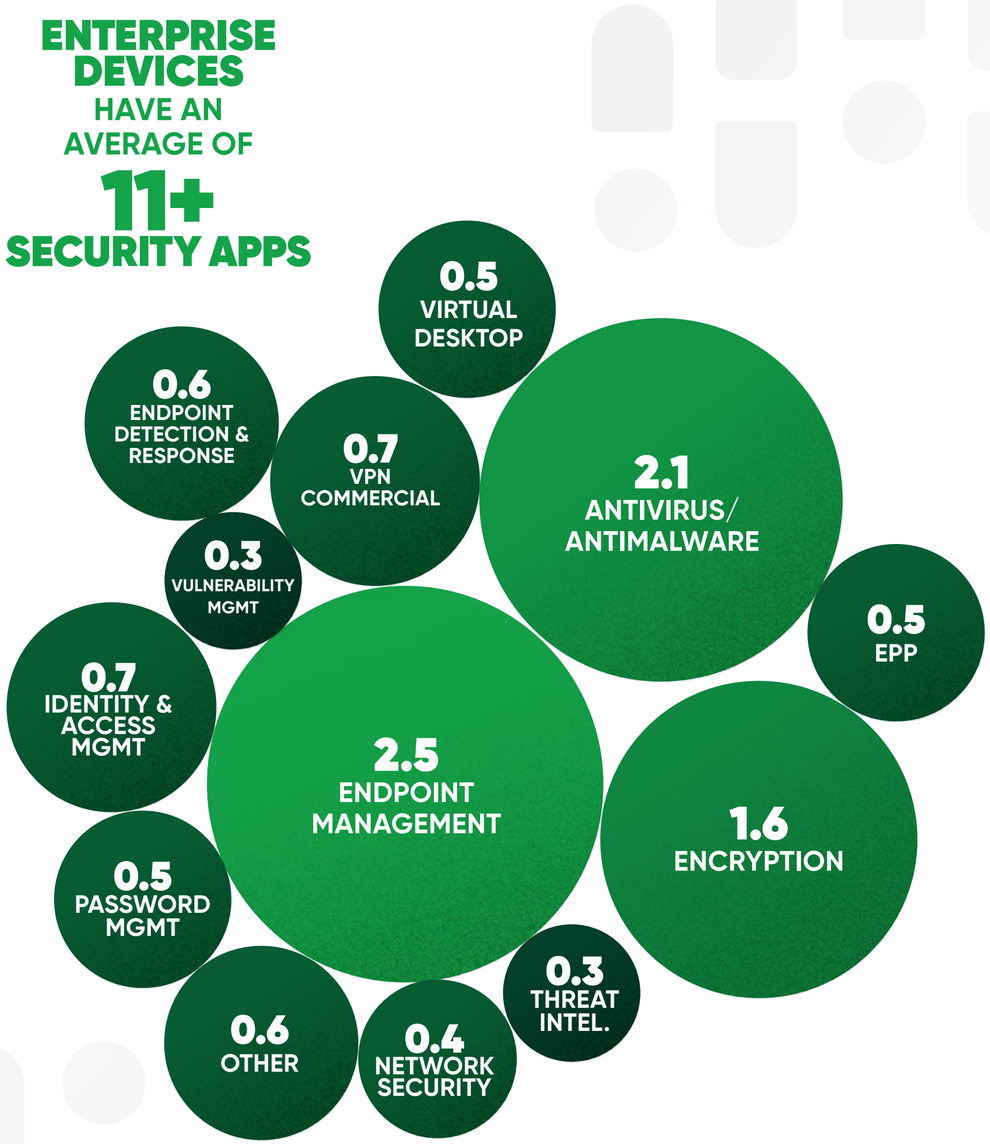
THE WORST OFFENDERS ARE EDUCATION AND GOVERNMENT



DAYS BY SIZE

VERY LARGE ACCOUNTS ARE THE WORST OFFENDERS

Source: Absolute Device Telemetry Data



A False Sense of Security

A long-held belief among enterprise organizations is the more you spend on IT and security technology, the stronger your security posture will be. So, to address a new challenge or threat, we purchase more solutions. We are spending tens of billions of dollars annually on endpoint security alone. In turn, it's not surprising that there are more than 11 security applications installed on the average work-issued laptop.

Notably, enterprise devices on average have more than one security application installed to deal with endpoint management, anti-virus, anti-malware, and encryption, which are considered essential security controls by many industry standards (e.g., ISO/IEC 27001, NIST CSF, PCI DSS, GDPR) and government regulations (e.g., HIPAA, HITECH, FISMA). This indicates that many organizations lack insights into the software inventory across their device fleet, are running more software than is needed, or simply believe that the more tools deployed, the safer they are.

Source: Absolute Device Telemetry Data

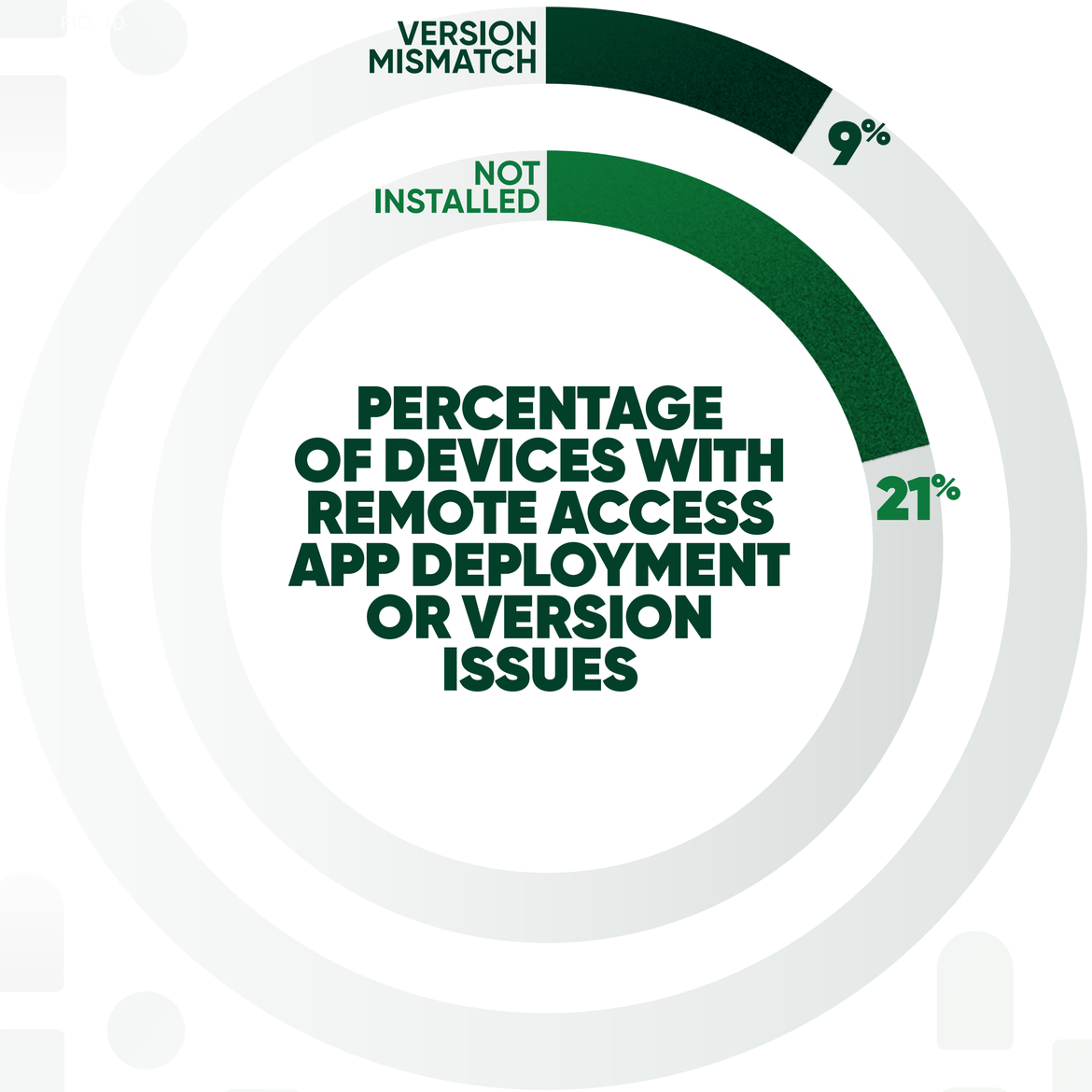
Security Applications' Efficacy Varies Widely

Unfortunately, you can't secure and ensure the efficacy of what you can't see. An enterprise's security posture is only as strong as the security controls that support it. If left unchecked, every security control deployed on the endpoint represents a potential vulnerability if it is not running and able to perform its job. Common decay, unintentional deletion, or malicious actions all impact the integrity and efficacy of security applications and endpoint management tools.

Some might suggest that guaranteeing peaceful co-existence should fall to the solution providers themselves. But when you consider the number of permutations based on the number of tools, the number of versions and builds for each of them, and the number of operating system versions and builds, it is impossible for any solution provider to do so. And this is to say nothing of the constant stream of threats from malicious actors that they must also stay on top of in order to protect their end customers.

IT and security practitioners agree that security tools like Endpoint Protection Platform (EPP), Endpoint Detection and Response (EDR), anti-virus, etc. are essential to defend against attacks, and therefore should always be running and up to date. Absolute's data shows that 25 - 30% of devices had unhealthy security controls.

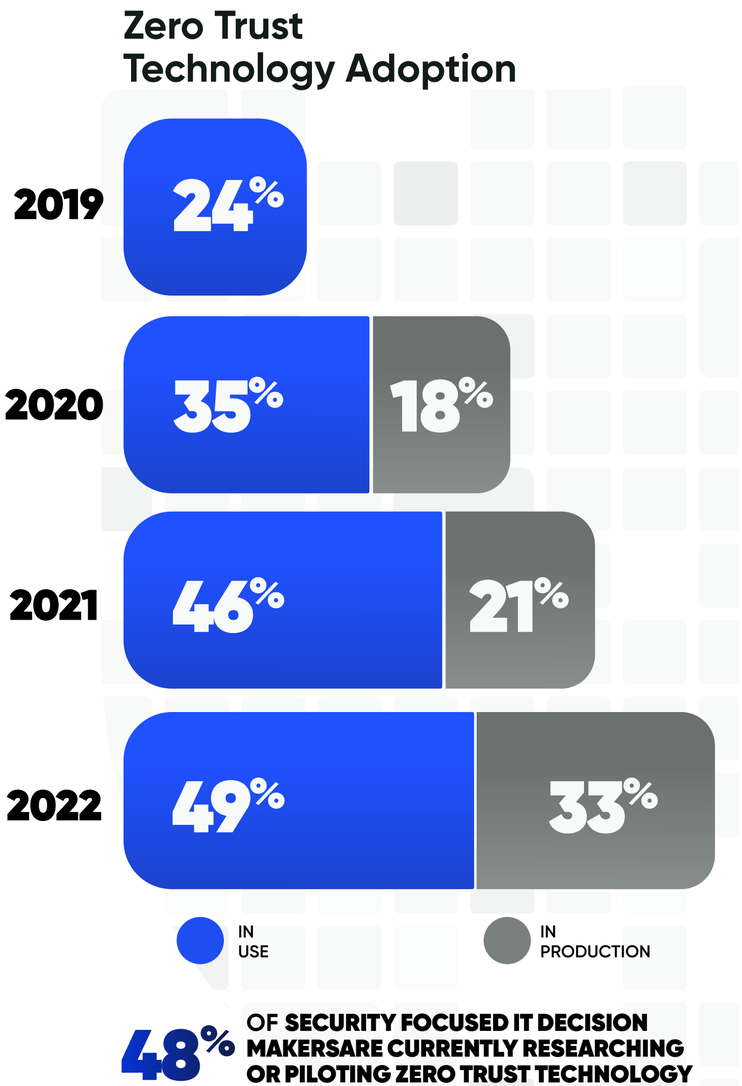
Source: Absolute Device Telemetry Data



Source: Absolute Device Telemetry Data

We cannot forget about remote access and Zero Trust Network Access (ZTNA) applications, as they have become the lifeline to enterprises. Mobile workers require secure, but frictionless access to corporate resources that nowadays can reside anywhere. That's why these technologies have become the intersection between endpoints and corporate networks, as we're seeing a strong adoption within the enterprise. In turn, it is essential that the integrity of these tools is not tampered with.

However, our data shows these critical tools are either not installed or are not at the required version level on more than 30% of devices, exposing organizations to unnecessary risk.



Cyber Resilience: the New Strategy to Cope With Increased Threats

Considering the implications of the findings above, it is apparent that it's no longer a matter of 'if' but 'when' an organization will suffer a breach. This means that instead of exclusively focusing efforts on preventing an attack, it's important to develop a plan to reduce the impact when a successful attack occurs. This is why many forward-thinking organizations are adopting a new strategy to cope with today's increased cyber threats, called *cyber resilience*.

Step One: Zero Trust, We Must

The acceleration of cloud adoption and the shift to work-from-anywhere have diminished the common perimeter defense, leaving organizations more vulnerable than ever before. A first step in this new era is to apply Zero Trust principles, which goes together with cyber resiliency.

Forrester defines Zero Trust as an information security model that denies access to applications and data by default. Threat prevention is achieved by only granting access to networks and workloads utilizing policy informed by continuous, contextual, risk-based verification across users and their devices. Zero Trust advocates three core principles: all entities are untrusted by default, least privileged access is enforced, and comprehensive security monitoring is implemented.

Zero Trust architectures and technologies are steadily working their way into corporate security, and Zero Trust is finally replacing the old perimeter-centric approach. In a 2022 Security Priorities Study by Foundry (formerly IDG Communications), 32% of respondents said they are researching Zero Trust technologies and 16% cited that they are "piloting" them[2].

2 Source: Foundry (formerly IDG Communications), Security Priority Study, 2020 - 2022

IN TODAY'S THREATSCAPE, YOU MUST ASSUME ATTACKERS ARE ALREADY IN YOUR NETWORK...

ZTNA, the Logical Starting Point For Zero Trust

Deciding where to start the journey to Zero Trust can be challenging. A guiding factor should be understanding your cyber adversary and assessing their exploitation tactics, techniques, and procedures (TTPs). In this context, it is important to understand that the modern definition of the Zero Trust pillars extend beyond the network and encompass today's ever-expanding attack surface.

The easiest way for attackers to gain access to sensitive data is by compromising a user's identity. In fact, a study by the Identity Defined Security Alliance (IDSA) reveals credential-based data breaches are both ubiquitous (94% of survey respondents experienced an identity-related attack) and highly preventable (99%)[3]. In this context, ZTNA helps you move away from the dependency on username/ password and instead rely on contextual factors, like time of day, geolocation, and device security posture, before granting access to enterprise resources.

However, human error, malicious actions, and decayed, insecure software often impede the efficacy of Zero Trust technology. Thus, the National Institute for Standards and Technology (NIST) has been propagating the use of self-healing or resilient cybersecurity systems.

What ultimately differentiates self-healing cybersecurity systems is their relative level of ability to prevent the same factors that they are built to protect against: human error, decay, software collision, and malicious activities. In the end, they are just another software application. It is therefore important to select solutions that can persevere in the face of hostile external factors. To achieve this state of hardening, self-healing capabilities should be embedded in the firmware of the endpoint, shielding it from any intentional or unintentional manipulation.

3 Identity Defined Security Alliance (IDSA), Identity Security: A Work In Progress

How to Become Cyber Resilient to Secure a Hybrid Workforce

Even once Zero Trust principles are established, organizations need to be prepared for the worst-case scenario and therefore balance defensive measures with cyber resiliency. This is reflected in many recommendations from MITRE[4], NIST, global analyst firm Gartner, and even the US White House, which calls for cyber resiliency in their ambitious National Cybersecurity Strategy. The White House strategy reflects a widely held belief in the US government that market forces have failed to keep the nation safe from cyber criminals and state-sponsored attacks.

The director of the US Cybersecurity and Infrastructure Security Agency, was quoted recently: “We often blame a company today that has a security breach because they didn’t patch a known vulnerability…What about the manufacturer that produced the technology that required too many patches in the first place?”[5] Many took that to mean that the accountability for maintaining cyber resiliency should be shifted to vendors who need to step up to the challenge.

According to MITRE, cyber resilience (or cyber resiliency) “is the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on cyber resources.”[5] The need for cyber resilience arises from the growing realization that traditional security measures are no longer enough to protect systems, data, and the network from compromise. The objective of cyber resilience is to ensure that an adverse cyber event, whether intentional or unintentional, does not negatively impact the confidentiality, integrity, and availability of an organization’s business operation.

4 MITRE, Cyber Resiliency Overview, January 2020
5 Cyberscoop; CISA director urges tech sector to stop shipping unsafe products, February 27, 2023

> "Collectively we can deliver better compliance, and greater continuity in the face of complexity – cyber resiliency is a team sport."

Christy Wyatt
President and CEO, Absolute Software

Absolute Software: Making Security Work

Absolute is known as the pioneer of endpoint and network resilience and our **Persistence® technology** has been embraced by the **world's leading system manufacturers** (e.g., Dell, Lenovo, HP, Microsoft, etc.) for many years, delivering cyber resiliency to millions of users.

Embedded in more than 600 million devices, Absolute enables visibility and control across endpoints, applications, and network connections. Leveraging our unique self-healing capability, customers can protect devices, data, and users and ensure that critical security controls operate at maximum effectiveness, while also delivering an optimal remote and mobile user experience.

As we shared earlier in this report, our unique position in the firmware of millions of active devices demonstrates how **Absolute Application Resilience™** delivers the ability to monitor application health. We can automatically repair and/or re-install unhealthy third-party applications listed in the Absolute Application Resilience catalog to restore them to healthy operations.

Ultimately, it's all about strengthening an organization's compliance posture, assuring secure and reliable network access, and making sure that employees can confidently get to work, and keep working, no matter where risk finds them.

With Absolute Application Resilience, we see initial app health scores leap from less than 50% to close to 100%, unassisted by IT.

Improving security uptime means closing the gap between cyber risk and cyber resilience.

The Power of Cyber Resilience and Application Resilience

As IT and security practitioners know, there are only a small number of tools needed to minimize your risk exposure at the frontend of the cyber-attack chain: EPP or EDR as well as remote access solutions. Without the help of these tools, you cannot remain as functional and operational as you should be. And it's not just about ensuring defensibility but leveraging the same tools in your recovery efforts in the case of an attack. These activities are often an afterthought and overlooked. However, security efficacy plays a big role here.

To illustrate the power of Application Resilience, we assessed the application health for the top security vendors across EPP/EDR and Remote Access who are cited as leaders in industry reports and are used by Absolute customers: Cisco, Citrix, CrowdStrike, Microsoft, Netskope, Palo Alto Networks, SentinelOne, Sophos, Trend Micro, and Zscaler. We then compared this to their application health once Application Resilience policies were applied. The following results are anonymized and in random order:

	Non-Resilient Apps Percentage of Healthy* Devices	Resilience-Enabled Apps Percentage of Healthy* Devices	Efficacy Gains in Percentage Points
Endpoint Protection Platform / Endpoint Detection & Response			
Vendor A	95%	**96%**	1%
Vendor B	70%	**94%**	24%
Vendor C	47%	**99%**	52%
Vendor D	49%	**100%**	51%
Vendor E	89%	**93%**	4%
Remote Access			
Vendor F	75%	**90%**	15%
Vendor G	73%	**93%**	20%
Vendor H	85%	**97%**	12%
Vendor I	53%	**98%**	45%
Vendor J	76%	**99%**	23%

*App health is a representation of whether an app is installed at all, installed at an organization's desired version level, and if services are running that are required to allow the app to function as intended, as well as many other conditions.

Absolute advances cyber resiliency in the face of growing IT and security complexity—

uniquely defending and protecting your collaboration, technology, and security resources from the firmware up, while empowering the performance agility and operational continuity that leading enterprises require today. Leveraging our device-embedded Absolute Persistence technology and extending its self-corrective recovery capabilities via Absolute Application Resilience, both enterprises and security vendors can optimize application efficacy and strengthen security and compliance posture. With Absolute, you neutralize digital disruption and transform the mobile user experience, so your people can confidently get to work, and keep working, no matter where risk finds you.

Report Methodology

We analyzed anonymized data from 14 million Absolute-enabled devices active during the period of February through April 2023, across customer organizations in North America, Europe, and APAC, as well as data and information from trusted third-party sources.

Enterprise Resilience Index

Enterprises can evaluate their cyber resilience through these three lenses: complexity, compliance, and continuity.

COMPLEXITY

Focuses on application health, and includes number of endpoint controls, number of devices and users and number of OS platforms.

Ask these questions to learn more about your state of complexity.

1. What is the percentage of devices by OS that are behind on patching?
2. What is the number of security controls per device?
3. Are we testing/using the optimal combinations of anti-virus/anti-malware and encryption apps?

COMPLIANCE

The scorecard that focuses on risk and encryption.

Ask these questions to learn more about your state of compliance.

1. Is your sensitive data encrypted across all endpoints as well as while in transit or in motion?
2. Do you have insights into the efficacy of your security controls at any given time?
3. Do you know at any given time where all your company-assigned devices are located and if they contain any sensitive data?

CONTINUITY

Includes mobility, app health, and availability.

Ask these questions to learn more about your state of continuity.

1. Do you have any insights into network coverage gap or quality of connection that would allow you to enforce SLAs?
2. Do you have any ways to communicate with end users without having to rely on your email system?
3. Do you have automated ways to repair and/or reinstall mission critical applications that would either prevent attacks or help with the recovery efforts?

ABSOLUTE®

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.

Trusted by nearly 20,000 customers, G2 recognized Absolute as a Leader for the thirteenth consecutive quarter in the Spring 2023 Grid® Report for Endpoint Management and as a Leader for the third consecutive quarter in the Grid Report for Zero Trust Networking.

Request a Demo

Nasdaq | ABST TSX | ABST