The value of Zero Trust in a WFA world

How your organization can better understand, take advantage of, and implement a ‘Zero Trust’ security strategy in today’s Work from Anywhere (WFA) world.

Introduction to Zero Trust

The often used, rarely fully understood term 'Zero Trust' is one that now dominates many conversations in the cybersecurity world. The term was coined back in 2010 by Forrester Research and over 12 years later, it has emerged as a leading security model to address modern, hyper-connected infrastructures.

Defining 'Zero Trust' is relatively simple. The concept revolves around the notion of 'never trust, always verify'. Any device or user attempting to gain access to a network or application must always be authenticated and their identity validated before 'trust' or access is given.

Zero Trust wasn't always the norm across IT and security teams. Historically, a traditional perimeter was used to gauge if a device or user was 'trusted'. For example, in most cases, any user connecting from inside an organization's corporate office network or 'perimeter' was implicitly trusted and wouldn't require any sort of validation to connect to an enterprise application.

This kind of model now presents its fair share of challenges, especially with an increasing number of employees working outside of the four walls of the office. Zero Trust security does away with the traditional office 'perimeter', and essentially allows IT teams to set their own requirements for contextual identity verification across their workforces.

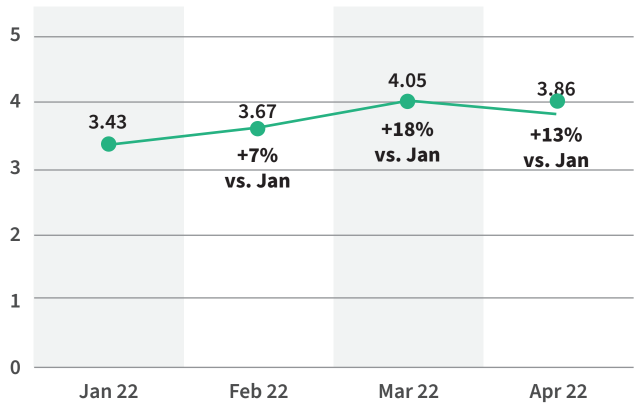
Why Zero Trust remains critical

2020 changed the nature of network and endpoint security indefinitely. The COVID-19 pandemic mandated a sudden shift to 100% remote work. This was something very few organizations were prepared for. In fact, many continue to struggle to effectively protect endpoints and remote connections in the new ‘work from anywhere’ world.

One might wonder if the remote working concept is here to stay. After all, many employees have now returned to the office. Aggregated data from the global network of Absolute-enabled devices indicates there could be a continued trend of working ‘from anywhere’:

Figure 1

Average Number of Enterprise Device Locations (by Month)



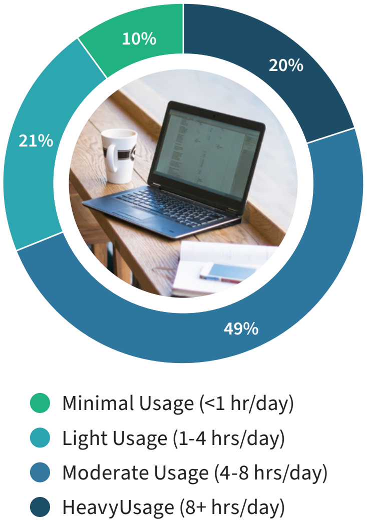
Enterprise devices are becoming more mobile in new Work from Anywhere era

Analysis based on Enterprise devices with geolocation data present in each respective month, representing 5.1M devices. Geolocation methodologies include Wi-Fi Positioning/Triangulation, GPS, Windows Location API, and Google’s Geolocation API (in that priority).

Looking at data gathered over the past few months, there has been a notable increase in the number of locations enterprise devices are connecting from. Increases of 7%, 18% and 13% respectively have been noted from January to February, March and April of 2022.

Figure 2

Average Enterprise Device Usage (over 30 day period)



Enterprise devices are being used heavily

1 in 5 devices are used heavily and nearly **70% of** devices are used **4+ hours/day**

Data as of 2022-04-19. Device usage data averaged across the last 30 days. Includes 30-day active devices: Enterprise – 4.2M devices

Not only that, but these devices are being used for a considerable number of hours each day. 70% of enterprise devices are being used for more than 4 hours per day. This indicates that these Absolute-enabled devices are allowing workers to be productive, everywhere they go.

But what does this mean for security?

The risk of remote work

Moderate to heavy enterprise device usage in an increasing number of locations points to an increase in risk for organizations.

A recent study from NetMotion by Absolute indicated that 97% of surveyed IT experts believed that remote workers are exposed to at least some added risk, with roughly 47% believing that the risk was either high or extremely high.

Why is this the case? There are a myriad of reasons why remote work is considered riskier than working within the confines of an office. These include but aren't limited to:

Security event response is difficult without physical proximity

Challenging to identify ransomware and other malware attacks

High risk access requirements with legacy remote access

Devices are not always kept up-to-date and configured

Limited network security protections, wider attack surface

Reduced telemetry when diagnosing potential issues

Lost, misplaced and stolen devices difficult to recover

Mobile phishing attacks rampant (multiple form factors and devices)

These risks ultimately result in a heightened chance of a malicious third-party gaining access to sensitive corporate data, applications, or networks. To account for this increased risk perpetuated by the new way of working, a comprehensive security strategy is required that validates the identity of workers regardless of where they are.

The current state of endpoints and access

How are organizations currently dealing with this increased risk across their now inherently mobile workforces? The following key data points pulled from millions of Absolute-enabled devices globally speak for themselves.

16% of Enterprise devices are unencrypted

Data pulled from >4.2M Absolute-enabled active enterprise devices

1. Unencrypted devices

An unencrypted enterprise device can carry a substantial risk for an organization. This risk becomes even greater if the device is being used outside the perimeter of the corporate network.

The fact that it's unencrypted means that any communications sent from or received to the device are not secured. If the device is connected to a corporate-owned network this is not necessarily an issue; however, any other network connected to is an opportunity for the device's data to be compromised.

With more locations and networks being used for day-to-day work, these unencrypted devices must be identified and ideally locked down to prevent compromise.

13% of Enterprise devices are not connected to corporate domain

Data pulled from >4.2M Absolute-enabled active enterprise devices

2. Invisible devices

A device not connected to a corporate domain is a concern to any IT team. It essentially means the device is operating off the company's radar without any checks or balances by IT or security. If this computer, laptop, or mobile device does have sensitive data stored or downloaded, this means it could be comprised without the company's knowledge.

Obviously, it's important that organizations can recognize such devices and take steps to ensure they connect to the corporate domain as soon as possible.

2 out of 3 Enterprise devices are running OS versions 2+ behind

Enterprise devices are **77 days** out of date with current patching

Data pulled from >4M Absolute-enabled active Windows 10 devices

3. Devices out of date

Running an out-of-date OS or a device without the latest patches isn't necessarily a threat to the company, however it likely means that the device is vulnerable. Microsoft releases Windows patches and OS updates to protect against known vulnerabilities that hackers can take advantage of to exploit endpoints. Therefore, going without an update, while seemingly harmless, can be detrimental.

Working outside of the office and on various insecure network only increases the likelihood that a vulnerable device will be exploited. IT teams require visibility into endpoints to determine if updates need to be pushed automatically, depending on their risk appetite.

Given these stats, it's clear that many organizations either don't have the means to mitigate their risk today or they can be doing more to protect and control their workers' remote endpoints and remote access.

Applying Zero Trust

Unfortunately, implementing a Zero Trust security strategy isn't something that can be accomplished with the purchase of one solution (as much as some companies may try to convince you this is the case). After all, Zero Trust is a concept, one that demands that no trust is given without thorough validation of identity. A complete stack of security solutions are required to ensure this is the case.

A good first step to practicing a Zero Trust security posture is adopting a Zero Trust network access (ZTNA) solution. Gartner recently published its **latest Market Guide on ZTNA** documenting the continued maturation and growth of the market. They recognized Absolute as a representative vendor alongside other major players in the space.

Absolute is doing something incremental when it comes to Zero Trust. Not only is the focus on securing and validating the contextual identity of every connection to the corporate network (secure access) but this validation now also extends to the security of the endpoint. Absolute has brought to market, the industry's first self-healing **resilient Zero Trust solution**.

Secure Access

Secure access has been a key component of IT strategies for years, but ever since the pandemic, it has come to the forefront of importance for organizations. Most companies have gone from having 1 or 2 centralized offices to hundreds of individual home office setups. Securing and recognizing every single one of those home office connections to the corporate network is essential in the context of ensuring Zero Trust (and avoiding data breaches).

This is exactly what the Absolute Secure Access product line enables, providing a real-time analysis of every connection to ensure verification based on a number of factors (including date, time, location, privileges etc.). This analysis is seamless and does not inhibit the performance of the network or the endpoint. Absolute's Zero Trust policies are enforced at the closest possible point to the end user (at the endpoint) to avoid any latency or data transgression. This meets the most advanced NIST SP 800-207 Zero Trust Architecture recommendations. In addition, Absolute Secure Access actively improves the end user experience using low level data optimization techniques.

This description likely sounds like many other ZTNA solutions on the market, however Absolute goes one step further providing resilience. What does this mean?

Secure Endpoint

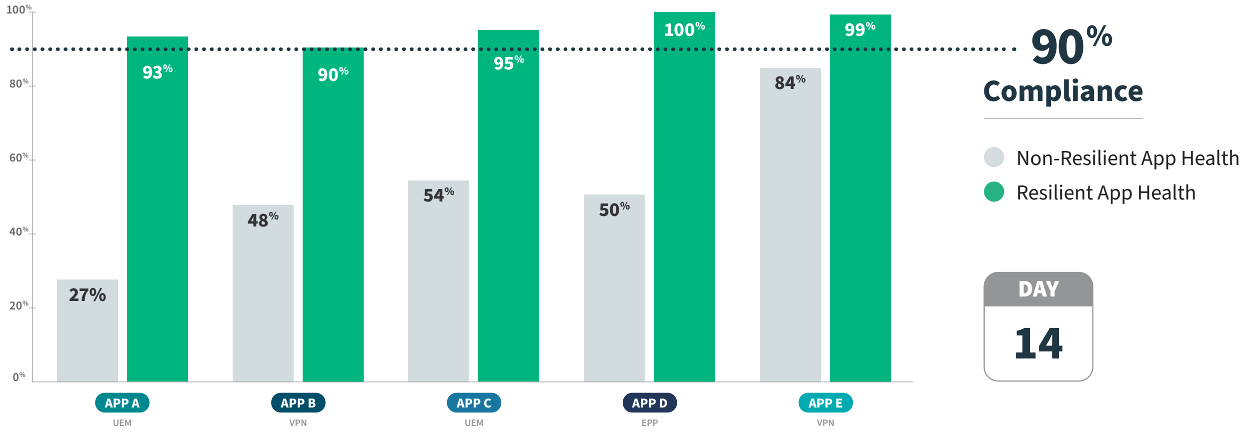
Any form of defense that lives on an endpoint can only be effective if it remains operational, and functions as intended. Oftentimes employees can unintentionally compromise the integrity and efficacy of these security applications by doing something as simple as installing an unsupported third-party application on their work device. And with phishing and other attacks becoming more widespread, bad actors have proven to be incredibly creative when exploiting vulnerabilities or human error to bypass controls and maliciously disable security applications.

The Secure Endpoint product line, featuring resilience, completely changes the narrative: Absolute Persistence® technology, which is embedded in the firmware of endpoints, is fiercely resilient and the only solution to survive attempts to disable it, even if the device is re-imaged, the hard drive is replaced, or the firmware is flashed. Based on its unique position in the firmware, Absolute extends its undeletable line of defense of self-healing to third-party applications, assuring that they remain installed, healthy, and effective to counteract human error, malicious actions, software collisions, and normal decay. This means that if someone were to uninstall the Secure Access solution from a device for any reason, or if malware were to compromise the integrity of the application, an admin is able to pre-emptively set up policies that will automatically fix or reinstall the solution when the device restarts.

Let's take a closer look. Evaluating the health of applications with and without Absolute's Application Resilience technology, over the course of two weeks shows how applications can become unsafe exceedingly quickly without intervention:

Figure 3

Security Health and Stability Improvements with Automated Remediation

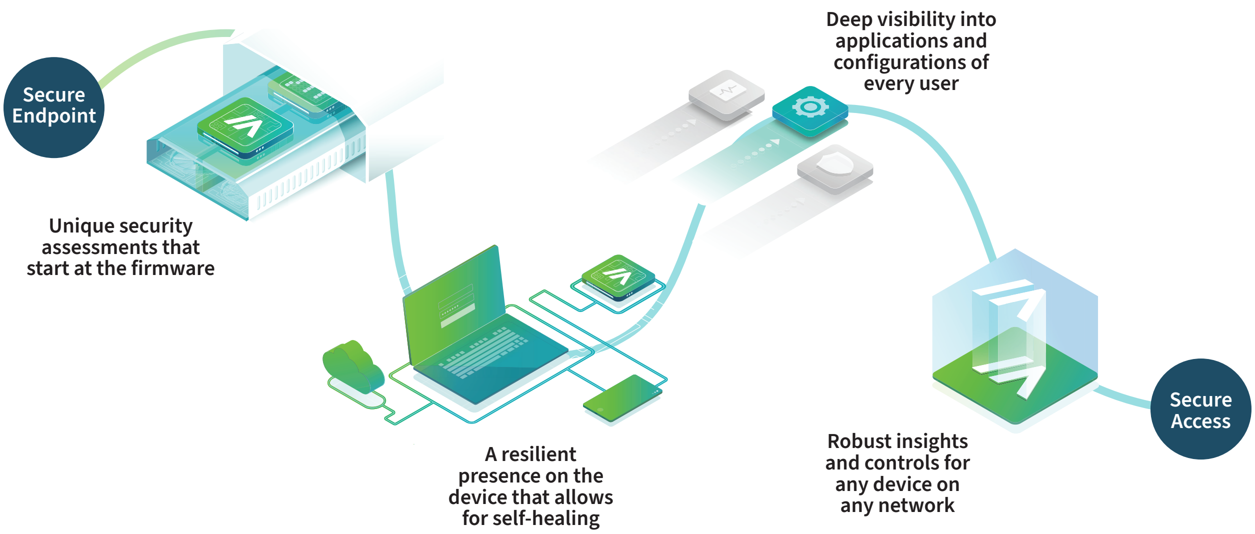


Analysis based on 5 applications across 3 product categories (EPP, VPN and UEM) over 14 days and 3.1B records

Ensuring resilient Zero Trust today

If you're ready to start your journey to resilient Zero Trust, it's as easy as having a conversation with one of our specialists.

Zero Trust Security at Every Level


Secure Endpoint
Unique security assessments that start at the firmware
A resilient presence on the device that allows for self-healing
Deep visibility into applications and configurations of every user
Robust insights and controls for any device on any network
Secure Access

See how you can leverage the power of Absolute to ensure the security of your work-from-anywhere workforce.

Book a demo

Report methodology: To develop this report, we analyzed anonymized data from nearly five million Absolute-enabled devices active across 12,000 customer organizations in North America and Europe as well as data and information from trusted third-party sources.