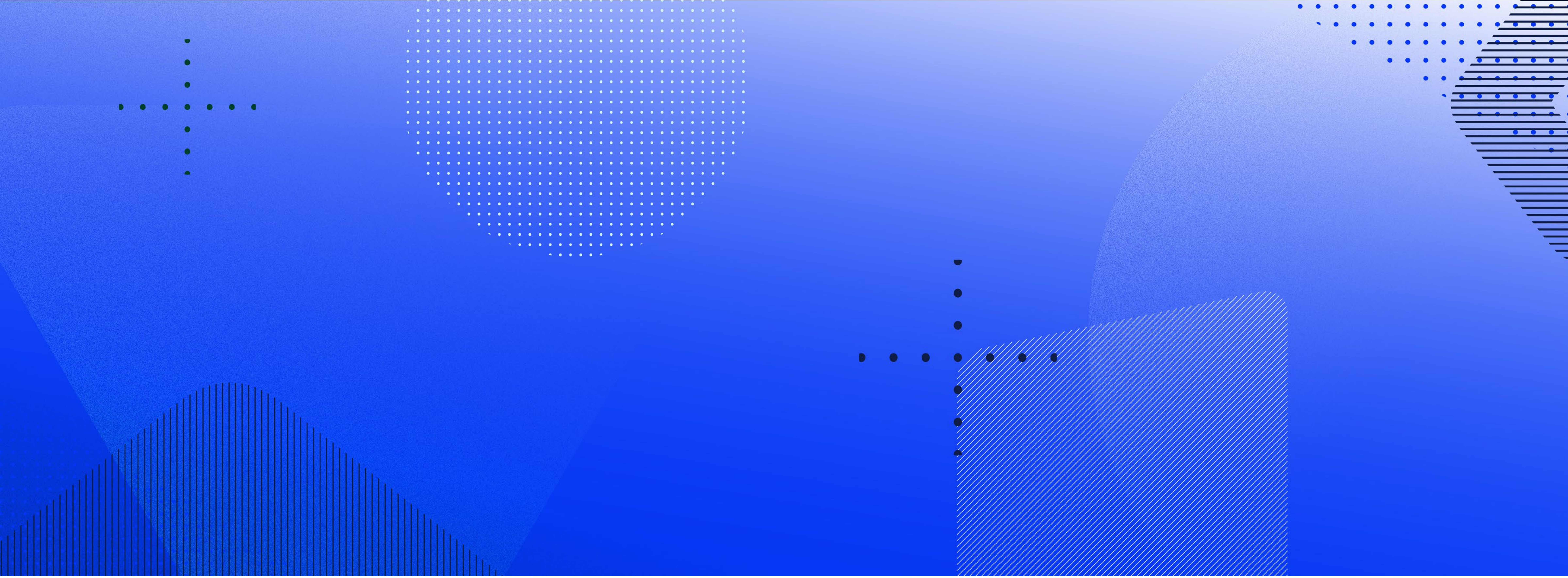


WHITE PAPER

Absolute Secure Access with ZTNA Policy

This document discusses the operational and technical capabilities of Absolute Secure Access. It is intended as a resource for network administrators and technical evaluators seeking a deeper understanding of how Absolute Secure Access can enforce Zero Trust Network Access (ZTNA).

absolute.com

ABSOLUTE®

Contents

> "Zero trust requires that the degree of trust granted to users and devices need be explicitly granted, continuously calculated, and then adapted to allow the right amount of access only for as long as necessary."
>
> -NEIL MACDONALD, GARTNER[1]

Zero Trust Summary

A Zero Trust approach to remote connectivity increases security by severely restricting access to each resource, ensuring that every communication between individuals and resources is authorized. With a Zero Trust approach in place, even if an attacker managed to breach a single resource, they could not access other resources. In Zero Trust parlance this is called "darkening resources" and "limiting lateral movement."

Using a medieval castle analogy, a Zero Trust approach surrounds every single resource with its own sentry, moat, and castle wall. Instead of granting broad permissions to access many resources, a Zero Trust approach uses strong, multi-factor authentication to verify identity, then only grants access to specifically authorized resources (micro-segmentation) and nothing else.

There are no more "keys to the kingdom" because Zero Trust puts a separate secure perimeter around every resource. Each resource has its own key and a custom list of people and conditions authorized to access it. If you are not on the list and the conditions are not met, you can't access the resource even if you have the key.

Absolute Secure Access Overview

Absolute Secure Access provides Zero Trust Network Access (ZTNA) capabilities implemented as a software-defined perimeter (SDP) with powerful mobile edge security, reliability, micro-segmentation control, and visibility.

The solution is purpose-built to secure remote access for hybrid organizations where people are working in-office, at home, remotely, mobile on-the-go, or as contractors. It provides centralized Zero Trust policy administration but enforces security on the mobile endpoints, creating a resilient, software-defined perimeter. It offers powerful security and management for remote connectivity over networks that are not under organizational control such as home, Wi-Fi, carrier, enterprise, satellite, and cable networks to provide authorized, Zero Trust access to organizational and cloud resources.

Numerous security parameters and AI-powered services enable unlimited combinations to evaluate when to block, secure with a tunnel, send outside a tunnel, and report on each application connection as well as security event.

Absolute Secure Access is the only undeletable secure access technology capable of automatically repairing or reinstalling itself if tampered with, accidentally removed, or has otherwise stopped working. This ensures that it remains healthy and delivers its full intended value.

[1] www.darkreading.com/remote-workforce/companies-struggle-zero-trust-attackers-adapt

Architectural Overview

The primary software components in Absolute Secure Access are Absolute VPN, Absolute ZTNA, and Absolute Insights™ for Network. They provide a ZTNA solution implemented as a software-defined perimeter.

Absolute VPN

Provides security and confidentiality for data in motion by authenticating and encrypted tunneling. The tunnel is particularly resilient, making network and application sessions resistant to disruption, keeping workers productive, especially when networks are not performing optimally.

Absolute ZTNA

Provides authentication, encryption, AI-powered reputation services, context-aware policies, distributed firewall rules, forward and reverse proxies, mobile optimized secure tunnel, network access control (NAC), network diagnostics, network optimizations, and rich metadata publishing including location, devices, networks, applications, and flows.

Absolute Insights For Network

Absolute Insights for Network offers dashboards and monitoring capabilities across endpoints and networks, allowing organizations to proactively monitor, investigate, and remediate access, security and performance issues quickly and at scale, even on networks that are not company-owned or managed. It aggregates the security, connectivity, and flow metadata into dashboards for threat analysis, network performance, cost control, inventory, and system status. Absolute Insights for Network provides advanced data visualizations that guide Zero Trust policy creation, refinement, and enforcement in Absolute Secure Access.

Centralized Administration

Policies defined by an administrator are automatically deployed and enforced on mobile perimeter devices, creating a distributed defense system. Policies can be defined and applied system-wide, to groups of users or devices, as well as to individual users and devices.

Absolute Secure Access maintains policies and distributes them seamlessly to the Secure Access clients. Updates and modifications to policies are applied within seconds.

Zero Trust Network Access In a Software-Defined Perimeter

Absolute Secure Access is uniquely differentiated from competitors’ solutions by an architecture with endpoint enforcement, forward and reverse proxies, and a host of capabilities that strengthen security, improve the user experience, and act intelligently and dynamically as conditions, behaviors, and the threat landscape change. These capabilities are discussed in detail in the sections below.

Absolute Secure Access Endpoint Architecture

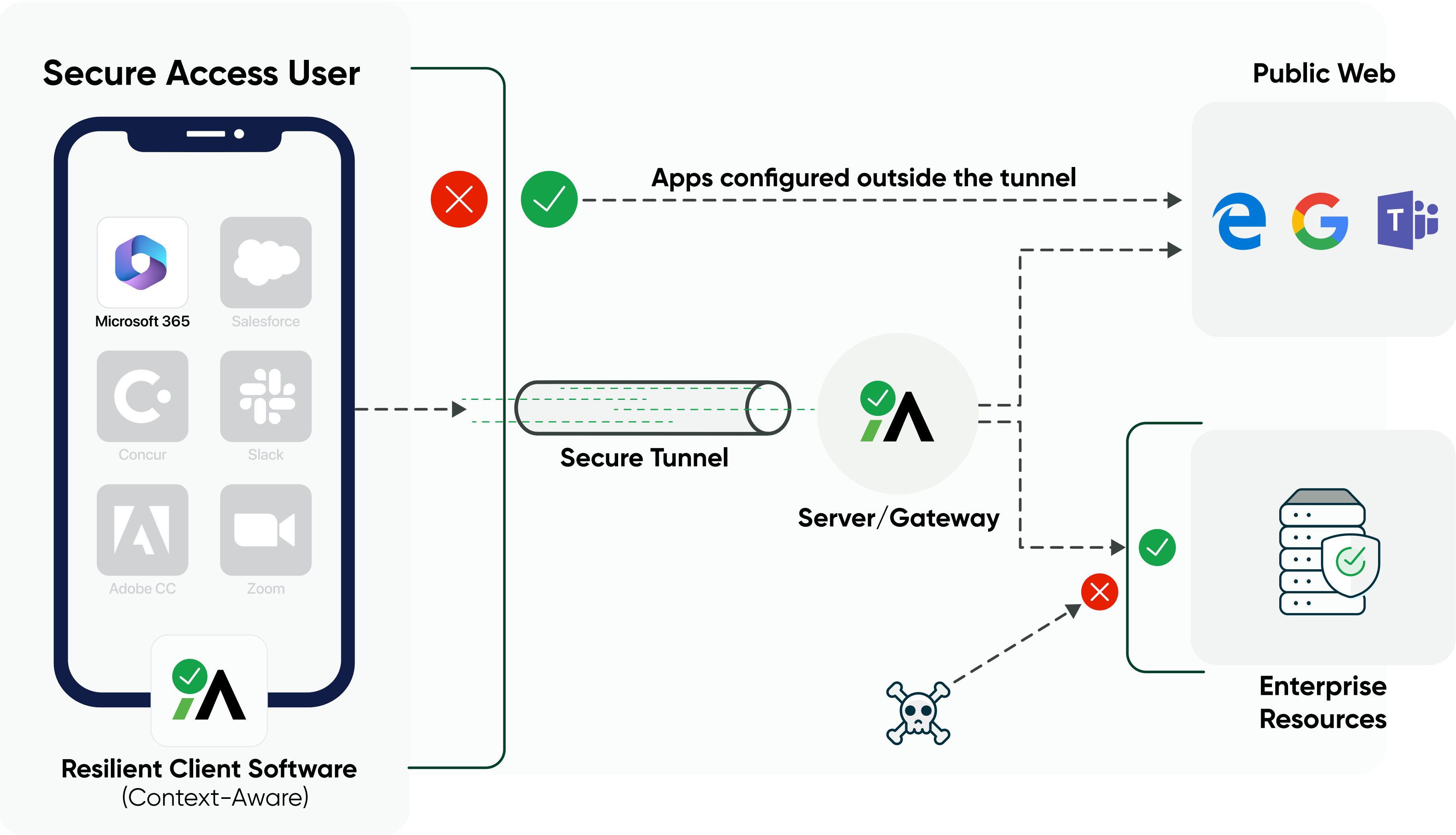
Inside each endpoint is a context-aware policy engine that dynamically enforces Zero Trust policies and distributed firewall rules; a local proxy; a mobile-optimized, secure tunnel; and a network diagnostics and telemetry engine. Windows clients also have Network Access Control (NAC) and can automatically repair or reinstall themselves if tampered with, accidentally removed, or otherwise stop working. This ensures that the Windows clients remain healthy and deliver their full intended value.

Productivity and User Experience

Users are more likely to run security software when it makes them more productive and improves their experience. With optimizations and integrated diagnostics, Absolute Secure Access improves network reliability, reduces data transfer times, reduces time to identify and repair outages with integrated diagnostics, and even prevents applications and TCP connections from failing through roaming and coverage gaps.

Resilient Client

On Windows, if the client is tampered with, Absolute Application Resilience proactively and automatically heals the client. On mobile platforms, tampering can be prevented by deploying to devices managed by an Enterprise Mobility Management/Mobile Device Management system.



Endpoint Functionality

Context-Aware Policy

Determines client behavior based on the user, device, network, application, flow, website and domain reputation, as well as time of day. These policies are centrally configured and pushed down to clients within seconds. Context-aware policy enforces Zero Trust principles and other rules.

AI-Powered Reputation Services

Enforces reputation policies that prevent users from connecting to malicious websites and domains and enforces appropriate use policies by domain category.

Network Access Control

Audits and enforces the security posture of Windows client devices before they are authorized to connect to an Absolute Secure Access proxy server and continues to monitor their security posture for the duration of their connection.

Distributed Firewall

Secures traffic entering and leaving the device as authorized by the Zero Trust policies. Every flow is blocked or allowed based on rules that automatically respond to changing conditions on the mobile device.

Secure Tunnel

Encrypts, secures, and hides applications, meta data, flows, microflows, and sensitive information.

Network Resilience and Roaming

Keeps applications and TCP connections alive on slow or saturated networks, in coverage gaps, and during network transitions.

Network Optimizations

Improves user experience on unreliable networks for tunneled flows.

Diagnostics

Proactively diagnoses network issues and improves performance on poorly performing networks.

Data Intelligence

Gathers information on device telemetry, applications, processes, networks, flows, reputation, etc. to enhance security, control, and visibility.

So What?

Your Employees Take Their Armor With Them

Application flows are monitored and protected even when data is not sent to the cloud. The security stays persistent and active on the device using integrated policy, distributed firewall, local proxy, mobile optimized secure tunnels, and network diagnostics.

Least Privileged Access and Context-Aware Policy

With Absolute Secure Access, the endpoint can detect if it is on a high-risk network and subsequently add an extra layer of encryption, using a secure tunnel. It can even treat the same application differently on different platforms. Other solutions do not have access to endpoint context and are unable to make these important Zero Trust policy distinctions.

With Absolute Secure Access, dynamic Zero Trust policies can be created that are appropriate for the user and endpoint environment. Enforcement changes as the environment changes.

Compliance and Network Access Control

The additional context gained by being on the endpoint enforces compliance and network access control. Network Access Control (NAC) capabilities audit and enforce the security posture of endpoints before they are authorized to connect to your resources and continue to monitor compliance throughout the duration of the connection.

Reduced Attack Surface

Many ZTNA/SDP solutions share a common weakness: they route all data through the provider's data center. When all data is hair-pinned for security, the data center(s) become a potential attack surface. Absolute Secure Access reduces the attack surface with deep continuous analysis and policies where your data originates – at the endpoint.

For data sent to the Absolute Secure Access Cloud, a walled garden single tenant design ensures privacy and security. Your data is never comingled or accessible by other customers.

Network-Independent Security

Connections are secured regardless of what network the device attaches to—home or public Wi-Fi, carrier, LAN, or any other IP-based access network.

Improved Performance With Reduced Latency

Voice, video, and other applications are extremely sensitive to latency. Routing all data through a provider's cloud creates choke points, adding hops, latency, and inefficiency. The choke point architecture also needlessly increases mobile data usage and degrades the end user experience.

Absolute Secure Access reduces latency by managing flows both inside and outside the tunnel using context-aware policies. You decide what to send to the cloud and what to send outside the tunnel for improved performance. Secure flows going outside the tunnel are routed directly to their peers without a chokepoint for optimal efficiency. Regardless of how you choose to route your data, tunneled or not, you get full visibility and control.

Scalability

The flexibility to route data and flows outside the tunnel increases scalability by removing choke points and potential bottlenecks. Customers who self-host Absolute Secure Access in their private cloud or data center can significantly reduce the amount of cloud egress data and associated costs.

Productivity and User Experience

For traffic configured inside the tunnel, sophisticated traffic optimizations ensure application stability and connection resilience between the endpoints and the servers; application and TCP connections stay resilient even through coverage gaps and poorly performing networks. When your network is at its worst, Absolute Secure Access is at its best using patented technology to improve performance.

Always-On Data Intelligence and Absolute Insights For Network

Unlike other ZTNA solutions where only data routed to the cloud is visible, Absolute Secure Access collects metadata from every endpoint all the time. Whether you choose to tunnel or directly route an application, you still get all the policy control and visibility.

Zero Trust Policy Examples

Prevent Lateral Movement of Malicious Software

Limit authorized application access by users, devices, user groups, device groups, networks, and destinations. For example, you can restrict access to Saleforce.com to only authorized employees on the sales team. For these same employees you can also restrict all other applications. If a machine becomes compromised, the process-level restrictions block the malicious software from accessing the network or other machines.

Hide Applications With Secure Tunnels

Prevent malicious actors from accessing sensitive information by securely tunneling application flows. Even if an application already encrypts its data, tunneling with Absolute Secure Access hides information that malicious actors can use to craft attacks by deducing which applications you are using. For example, detect when a user roams from a low-risk corporate network to a high-risk public network and begin tunneling sensitive application information transiting public networks. Zero Trust policies can still be enforced for tunneled applications.

Manage by Application

Manage by application and process name for easier administration. Authorize access to applications with an “allow list” and prevent access to applications on a “block list.”

A few examples:

- ✓ Allow Chrome and block Firefox
- ✓ Allow Webex and block YouTube
- ✓ Block YouTube on a carrier network but allow it on Wi-Fi
- ✓ Allow Netflix but only on Wi-Fi during non-business hours

Use Advanced Data-Driven Enforcement

Artificial intelligence is used to assign a risk score of low, medium, or high to each domain, allowing flexibility to create risk-based policies. For example, if a destination host’s risk is high, block access and inform the user; if it is medium, allow access but warn the user.

Absolute Secure Access detects malicious URLs, malware sites, phishing and other frauds, bot nets, proxy avoiders and anonymizers, adware, open HTTP proxies, as well as confirmed and unconfirmed SPAM sources.

There are also 56 predefined Web categories for creating Zero Trust policies. Using categories, you can create policies such as if the destination is “weapons” block the connection.

There are customizable classifications for approved, legal liability, and other sites, each of which can contain any number of the 56 predefined categories. You can then block all connections to the legal liability category and report on attempted access. Each list is customizable because organizations view the same activities differently. If you are a police agency, detectives may need to access sites discussing weapons, ammunition, and bombs. If you are an airline, accessing these sites would be alarming.

Protect Mobile Phones, Tablets, and Laptops

Policies can be used on iOS, Android, Windows, and Mac OS, treating each platform uniquely and differently. For example, on phones you can block malware URLs embedded in text messages to prevent smishing attacks.

Enforce Compliance With Network Access Control

Detect devices with out-of-date operating systems, anti-malware reference files, disabled firewalls, and poor security posture to prevent network access until remediation is completed.

For non-compliant devices, you can allow access only to remediation servers until corrected or allow employees to continue working but with limited access. For example, if anti-virus signatures are more than seven days old, send a reminder message telling the user to update; if they are more than 21 days old, quarantine the device. The same capability can be used to automatically download and install updates and operating system patches during times that will not impede worker productivity.

Manage Down to the Flow Level

You can treat flows within a single application differently to maintain secure access while improving performance. For example, often voice and video are already encrypted and run over UDP ports 3478-3481. Policy can be used to tunnel application authentication but route voice and video directly, outside the tunnel to improve performance.

Improve Employee Productivity and Experience

Absolute Secure Access uses customizable diagnostics and patented optimizations to proactively improve the user’s experience on poorly performing networks. For example, policies can detect when the network is performing poorly and automatically tunnel all traffic to take advantage of the link optimizations and connection resilience. The tunnel prevents applications’ TCP connections from dropping during coverage gaps and roaming, compresses data, and adds real-time traffic optimizations such as those for voice and video applications.

Endpoint Functionality Details

Context-Aware Policy

Zero Trust policies can be simple or complex using the following building blocks:

- Destination risk
- Destination type
- Application name
- Username
- Device name
- Time of day
- Network name
- SSID, BSSID
- Protocol
- IP address
- Port number
- Device ID
- Interface name
- Interface speed
- Interface type
- Metered interfaces
- Interface plug-and-play
- NAC status
- Operating system version
- Client version
- Battery status
- Registry key value
- Destination domain
- Destination reputation
- Active Directory group
- Externally defined condition

Some of the policy actions available include the following:

- Allow
- Block
- Route inside the tunnel
- Route outside the tunnel
- Reauthenticate user
- Data collection on/off
- Diagnose network problems
- Run bandwidth test
- Start application
- Set quality of service parameter

Network Access Control

The Network Access Control audits and enforces the security posture of Windows devices before they are authorized to connect to an Absolute Secure Access proxy server. The device's security posture is continuously monitored while it remains connected.

NAC module policies can audit and monitor attributes of the following:

- Anti-virus and Anti-spyware
- Files
- Firewall
- Processes
- Registry key
- Windows update
- Absolute Secure Access version
- Operating system
- External conditions

Authentication

Absolute Secure Access offers five authentication modes that can be assigned globally, to groups, or to individuals:

- ✓ User
- ✓ Multi-factor
- ✓ Unattended
- ✓ User required/device optional
- ✓ Device only

Absolute Secure Access supports the following authentication protocols:

- ✓ SAML
- ✓ NTLMv2
- ✓ RADIUS EAP TLS, GTC, PEAP, MSCHAPv2
- ✓ RSA SecureID

Cryptography

Absolute Secure Access employs standards-based, cryptographic algorithms to secure communications between its clients and proxies, including FIPS 140-2 validated and Suite B 128-, 192- or 256-bit keys and cryptographic algorithms.

Localization

Absolute Secure Access clients are localized and available on all supported platforms in English, French, Italian, German, Spanish, and Japanese.

The administrative consoles for Absolute Secure Access and Absolute Insights for Network are localized and available in English and Japanese.

Certifications

Absolute Secure Access cryptographic modules are FIPS 140-2 validated on each platform. Furthermore, Absolute Secure Access has been certified to Common Criteria EAL 4+ on all platforms, the highest certification available for a software product.

In addition, the Absolute Secure Access Cloud is SOC 2 certified.

Absolute Insights for Network

Absolute Insights for Network has over 50 dashboards for analyzing threats, performance, cost control, and inventory that can inform policy creation. Each dashboard provides filters for focusing the data on users, devices, groups, and operating systems.

Some of the security-related dashboards include the following:

- ✓ Reputation risk level
- ✓ Reputation category
- ✓ Severe and high risk
- ✓ Destinations
- ✓ Low security networks
- ✓ Insecure Wi-Fi
- ✓ Failure locations
- ✓ Failure type
- ✓ Coverage by location

Deployment Options

Absolute Secure Access supports three deployment options:

- **Secure Access Cloud (SaaS)** – the SaaS infrastructure and network for Absolute Secure Access and Absolute Insights for Network are deployed and hosted by Absolute. The customer manages system settings, policies, and day-to-day administration. Infrastructure patches and updates are deployed to each customer's cloud instance regularly by Absolute. Absolute is responsible for maintaining overall system uptime, scalability, and availability. The customer is responsible for the daily administration and operations of the system.
- **Absolute Secure Access SaaS** – hosted and managed by Absolute partners. Responsibilities for deployment, configuration, and day-to-day administration vary by service provider.
- **Absolute Secure Access software** – the customer deploys the SaaS platform infrastructure and networking for Absolute Secure Access and Absolute Insights for Network in their cloud, virtualized or physical data centers. The customer manages the system settings and policies. The customer is responsible for all aspects of the system infrastructure, configuration, and daily operations.

Absolute Secure Access Cloud SaaS Hosted and Managed by Absolute

Absolute Secure Access is available from Absolute as a cloud SaaS. Secure Access Cloud is deployed in Microsoft Azure and leverages Azure's security model.

In an Absolute Secure Access Cloud deployment, the customer only administers Absolute Secure Access and Absolute Insights for Network configuration and services to their end users. Absolute manages the cloud-native infrastructure, including scale, regions, zones, load-balancing, routing, failover, and uptime.

Absolute Secure Access Related Information

Additional information can be found on **www.absolute.com** and in the **Absolute Secure Access Systems Administrator Guide** and **Absolute Insights for Network Systems Administrator Guide**.

Private Walled Garden

Each customer's Absolute Secure Access Cloud instance is a private walled garden with dedicated resources for the highest level of security and performance. Customer data is never comingled with other customers. Unlike many other cloud services, nothing is shared between customer instances, including gateways, routers, firewalls, VLANs, databases, and services.

Disaster Recovery and Geographic Redundancy

Absolute Secure Access Cloud uses availability zones and multi-region redundancy for high reliability. Availability zones are physically separate locations within a geographic region, providing resilience from disasters or other wide-scale network outages. Availability zones are equipped with independent power, cooling, and networking infrastructure. In addition to redundant availability zones in each region, Absolute Secure Access Cloud offers geographic failover and disaster recovery between multiple regions including North America, Europe, South America, and Asia.

Supported Client Operating Systems

iPhones, iPads, Macs, Android phones and tablets, and devices running Windows desktop operating systems are all supported.

Don't Forget About Endpoint Security

It has become abundantly clear that widely distributed, hybrid work environments are here to stay and, as a result, organizations are seeking security approaches that fully integrate endpoint and access assessments to ensure that Zero Trust principles are fully applied. Absolute's unique ability to enable visibility and self-healing from the endpoint to the network edge means we can offer you truly differentiated solutions to maximize security as well as assure uncompromised productivity and network performance for your end users.

The underlying foundation of a reliable and productive work-from-anywhere environment is anchored around your employees' endpoints, as well as secure and reliable network connectivity that allows them to exchange information and access enterprise resources independent of their location.

As shown in this white paper, Absolute Secure Access provides reliable network connectivity for users to gain secure access to critical resources in the public cloud, private data centers, or on-premises.

Beyond the capabilities offered by Absolute Secure Access, we can also help you make your devices resilient. Considering that endpoints serve as the main points of access to an enterprise network, many threat actors exploit the security gaps of endpoints. Often the efficacy of established security controls on endpoints has been impeded – this can occur due to decay, software collision, or simply because a threat actor turns them off to operate without disruption and risk of detection.

That's where the Absolute Secure Endpoint product line can help. It enables your IT and security personnel to monitor and address computers' problems and enables the laptops and their mission-critical applications to self-heal.

Differentiation

Absolute Secure Access has a unique approach to Zero Trust. This table outlines some of the key differences and advantages of Absolute Secure Access when compared to other common ZTNA solutions.

	Common ZTNA Solutions	Absolute Secure Access	Absolute Secure Access Benefits
Traffic Routing	*Traffic is hair-pinned through a cloud chokepoint*	**Traffic routes selectively, dynamically and optimally, balancing security and performance. Only traffic tunneled by policy is routed to the gateway.**	Significantly better network performance, decreased data usage, and improved employee productivity. All traffic, whether tunneled to a gateway or routed directly is monitored and reported.
Tunnel	*All traffic*	**Selective, per-tunnel, per-app, and per-flow ZTNA policy.**	Protects application and meta data from attackers. Tunnel is flexible and dynamic, allowing ZTNA policies to be applied inside and outside the tunnel. Customers can implement ZTNA policies regardless of how where they are in the journey to ZTNA.
Optimizations	*None*	**Native network performance optimizations for modern edge networks**	Improves worker productivity by adding fault tolerance and optimizing throughput in challenging network conditions.
Enforcement	*Centralized enforcement at the cloud chokepoint*	**Endpoint enforcement, distributed on each device**	Reduced attack surface. Creates an SDP. Local firewall protects the device. Highly scalable because the compute load is distributed on each device.
Cloud Architecture	*Multi-tenant with shared compute resources*	**Single-tenant, walled-garden with dedicated compute resources**	Less susceptible to system-wide outages. Data cannot be comingled. More performant with dedicated resources – no "noisy neighbors"
Resilient, Self-Healing Windows Client	*None*	**Self-healing, resilient Windows client**	An undeletable app that automatically self-heals to ensure a secure perimeter that is running and healthy.
Network Resilience	*None*	**Network session resilience and link optimizations**	Ensures that application sessions are not disrupted even during network outages, network roaming, and coverage gaps. Offers the most productive experience for end users.
Telemetry	*Basic telemetry*	**Rich telemetry**	Absolute Insights for Network offers rich telemetry information spanning performance, threat defense, cost control, and inventory of devices, users, applications, and network adapters, affording the insights necessary to fine-tune and benchmark the effectiveness of your access policies.
Connection Diagnostics	*None*	**Proactive diagnostics**	Absolute Secure Access automatically interrogates a device's connectivity stack tracing connection problems to their source, automatically fixing them when possible, and always reporting on probable cause. It can also run throughput tests to actively measure and report connection performance.

ABSOLUTE®

Trusted by more than 18,000 customers, 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.

Request a Demo

Nasdaq | ABST   TSX | ABST