Pulse Secure®

Pulse Zero Trust Access

Cloud-delivered Secure Access Service for Hybrid IT Environments

Highlights

Holistic visibility, compliance and enforcement for users, devices, applications and gateways

Direct, trusted device-to-application access with Dark Cloud support using Software Defined Perimeter architecture

Seamless, secure access to corporate applications in the data center and cloud

Flexible, per-user subscription licensing and lifecycle management for enterprise scale deployments

Customer Value

End-to-end Zero Trust access with reduced attack surface

Single-pane-of-glass visibility, policy management, and analytics

Greater governance and compliance

Lower total cost of ownership and increased productivity

Solution

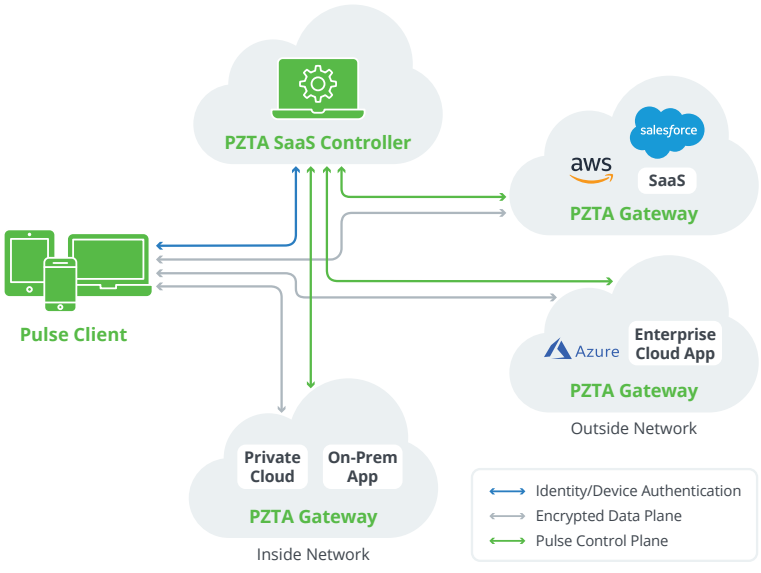
The PZTA cloud-based service — aligned to the Zero Trust Network Architecture — enables software-defined access, continuous authentication, and Dark Cloud support. It consists of the ZTA Controller which is hosted and managed by Pulse Secure, the ZTA Gateway which can be deployed in the cloud or on-premises by the customer, and the ZTA Client installed on users' devices.

- Zero Trust Access as a Service
- End-to-end visibility and enforcement
- Unified Client: Windows, macOS, iOS, and Android
- Broad ecosystem integration
- Comprehensive analytics and reporting
- Rapid deployment, flexible licensing

Zero Trust Access for a Hyper-connected World

Digital transformation has triggered a new era of hyper-connectivity between users, devices, applications and infrastructure. Enterprises need to enable secure access, protect users and applications, and manage cybersecurity risk in increasingly distributed networks with few, if any, boundaries. Today, endpoints, applications, and services are operating outside the traditional perimeter, placing more emphasis on Zero Trust approaches. Organizations are seeking end-to-end secure access solutions that address these new challenges — rather than continuing to add multiple point products to fill gaps. This piecemeal approach is cumbersome and costly to manage, introduces additional security issues, and adds to a broad range of inefficiencies and risks.

Pulse Zero Trust Access (PZTA) solves the secure access challenge in the hyper connectivity era by providing direct, trusted access to applications and resources across hybrid IT environments. It delivers holistic visibility, end-to-end analytics, endpoint compliance, and adaptive enforcement. With continuous entity authentication and robust ecosystem integration, PZTA offers an access service that provides easy and protected connectivity, administration efficiency and deployment flexibility to meet your needs on-premises or in the cloud.



Use Case Overview

Pulse Secure's Zero Trust Access (PZTA) platform enables diverse users from any location to securely access any public, private, and hybrid cloud applications as well as data center resources. As enterprises continue to evolve with mobile workforces and hybrid IT adoption, PZTA enhances security and productivity, increases visibility, and greatly enhances administrator and user experience as part of an extensible Zero Trust platform.

Zero Trust Access to On-premises, SaaS and Hybrid Cloud Applications

Pulse Zero Trust Access enables Zero Trust secure access to your organization's applications in the data center, private cloud and public clouds. The ZTA Client offers continuous user and device authentication and always-on protected access to corporate applications through an encrypted data channel between the ZTA Client on the user's device and the ZTA Gateway closest to the application. The application servers are protected and hidden which reduces security risks, known as Dark Cloud support.

CHALLENGES	PULSE ZERO TRUST ACCESS
Difficult to manage resources in the cloud	With PZTA, managing and accessing resources in the cloud are exactly the same as managing and accessing resources that are on-premises – with the same level of visibility, compliance, enforcement and analytics. The user never accesses the application server directly. When an application is moved from on-premises to the cloud, the next time the user attempts to access this application, the ZTA Controller will direct the user ZTA Client to the ZTA Gateway closest to this application.
Keeping user and application traffic within my organization's network	PZTA separates the control plane and data plane based on SDP architecture. All user and application traffic only flows through the ZTA Gateway which is deployed in the customer's own VPC or data center, and the data traffic never flows to the ZTA Controller.
Increase productivity	For administrators, the ZTA Controller is the centralized place to configure end-to-end Zero Trust access policies that tie users, devices, gateways and applications no matter the application or device type, or user location. For end users, regardless of the type of applications they are trying to access or where they are accessing them from, the access mechanism remains the same. This simplifies, yet unifies, user and administrator experience, increasing productivity for the organization.
Ensure access security when integrating acquired companies	Instead of allowing complete network access to different locations, PZTA allows administrators to specify what resources will be shared among different user groups in different locations by adding them to the centralized secure access policy. If a higher level of separation is desired, administrators can choose to configure a separate gateway or set up the different BU (business unit) as another tenant in a multi-tenant configuration.

Visibility, Enforcement and Compliance Reporting

Pulse Zero Trust Access provides a single pane-of-glass visibility of all users connecting from any of their devices regardless of their location, and the location of applications and resources. IT and Security administrators and leaders can view real time status and historical trends from the various interactive dashboards provided in the PZTA portal and receive pre-defined and custom reports at their convenience.

CHALLENGES	PULSE ZERO TRUST ACCESS SOLUTION
Visibility gaps	PZTA provides holistic visibility of users, devices, infrastructure and applications. All access is authenticated and authorized by the ZTA Controller. All access activities are captured in the Pulse ZTA dashboard and logged for reporting and auditing purposes.
Allowing BYOD is necessary but poses a security risk	Using PZTA, BYOD devices may benefit from the same level of Zero Trust access as corporate-owned devices. Every time users from a personal device attempt to access a corporate application, the device compliance status together with other security posture checks, such as location, time of the day, user behavior, will be assessed before access is granted.
Ensuring user and endpoint access compliance	PZTA dynamically authenticates the user, device and security posture against granular access policies before, and during, the connection. PZTA will inform the user of the violation or can execute pre-defined endpoint remediation to users that are denied or allow only reduced access to applications and resources.

Automated Anomaly Detection and Mitigation

What is secure and normal varies by organization. Pulse Zero Trust Access continuously learns and adapts by observing where users log in from, what devices they normally use and what applications they usually access. Administrators are alerted when there is an anomaly from normal user behavior, and can select a pre-set response or suggested mitigation action on the fly.

CHALLENGES	PULSE ZERO TRUST ACCESS SERVICE
Detecting and preventing credential theft by malicious insiders for purposes of stealing valuable data	Traditional perimeter defenses make it difficult to detect and pinpoint credential theft by malicious insiders. PZTA can alert security administrators that the employee in question is using a different device and logging in from a different location. Then, the administrator can either take pre-set enforcement actions such as requiring MFA or manually suspend access temporarily until the situation is resolved.
Administrators would like to restrict access when employees travel to high risk locations	This is easily implemented with PZTA. When the user location changes, the list of accessible applications are dynamically updated. Access to sensitive applications can be temporarily removed when the employee is traveling in high-risk locations or when employees are using devices that do not meet all the compliance requirements.

User Behavior Analytics

Every user attempt to access an application is sent to the ZTA Controller for authentication and authorization. In this process, PZTA applies extensive learned usage and behavior information to enhance the user experience, improve visibility and proactively take preventive actions to minimize potential security risks.

CHALLENGES	PULSE ZERO TRUST ACCESS SOLUTION
Measuring employees' risk factors	PZTA assigns a "risk score" to every user based on their current and past behavior and usage. This score is assessed dynamically and reflects both user action and potential risk factor. Based on the score, administrators can take a differentiated approach to users.
CIO would like to see the utilization rate of deployed resources	PZTA can provide comprehensive usage trends and detailed usage reports to help CIO and C-level executives understand what applications are being utilized the most. The solution supports various real-time queries using the ZTA analytics GUI to zoom into user group, location, resources, gateways or even individual users. This information can then be applied for resource and budget planning.
Administrator wants to know where to deploy network assets	From the PZTA usage report, administrators can obtain detailed information on which physical location users travel to, and which ZTA Gateways they are accessing they are accessing (down to user group or individual user level). The administrator can use this information to best match bandwidth to maximize user experience and reduce operational overhead.
Make employees more productive	By getting a 360-degree view on how, where and when users are accessing resources and applications, IT teams can define best practices such as when to schedule maintenance to minimize disruption, and what priority to upgrade devices and applications, etc. This will further improve user experience and productivity.

Zero Trust as a Service

Pulse ZTA is a service provided by Pulse Secure. The ZTA Controller is globally hosted and managed by Pulse Secure.

Available On-Premises and in the Cloud

ZTA Gateways can be deployed in customer's VPC in public cloud or in a private environment.

SDP and Dark Cloud

Adheres to SDP architecture with invisible applications only accessible after user and device have been authenticated and authorized.

Extensive Integration

Extensive set of APIs allows easy integration with ecosystem partner's solution.

Microservices Architecture

Containerized microservices composed of small, independent processes for maximum scalability and performance.

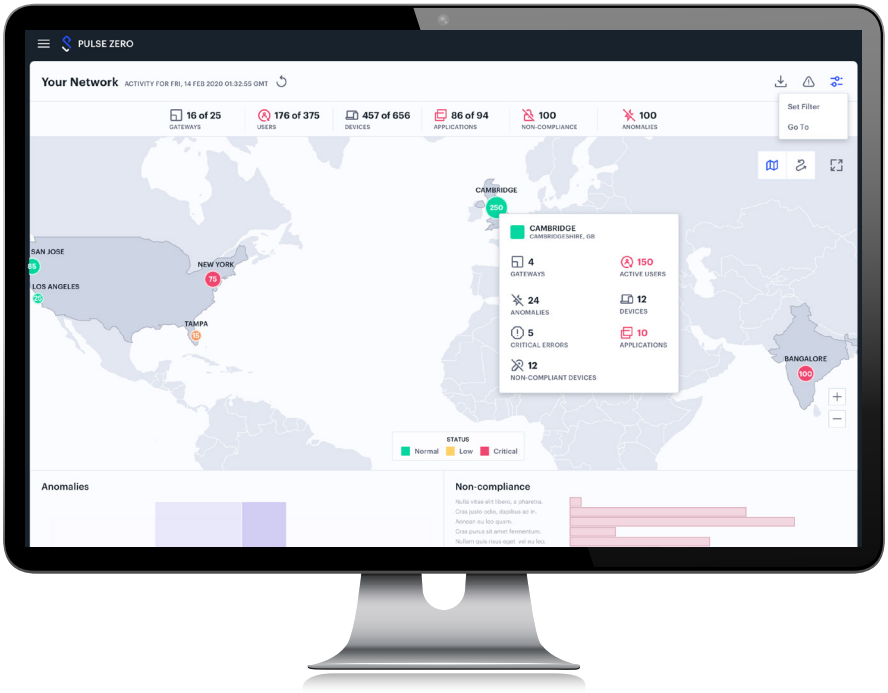
FEATURE	ADVANTAGE
End-to-End Access Policy	For every resource or resource group, administrators can define a set of end-to-end access policies. This eliminates the distinction between remote users and those on the corporate network, BYOD and corporate-owned devices, and whether applications or resources reside in the data center or cloud.
Dark Cloud	The ZTA Client will always request access through the ZTA Controller without knowledge of where the protected application server and resources reside. Once access is granted, the headless gateway establishes an encrypted data tunnel to the client to access the application. This Dark Cloud functionality drastically reduces the attack surface.
Single pane-of-glass Visibility and Compliance	Provides administrators with single pane-of-glass for holistic visibility and compliance reporting of users, devices, applications and infrastructure across all user groups, locations, device types, on-premises and cloud resources.
Separation of Control and Data Plane	The control plane is limited to authentication and authorization between the ZTA Client and ZTA Controller. The user and application traffic are sent directly between the user and designated gateway after being allowed by the controller. This separation reduces the risk of losing user data and optimizes user experience.
Adaptive SSO	Through SAML 2.0, PZTA integrates with popular identity solutions and services to provide SSO to supported SaaS and 3rd party applications. Administrators also have the option to enable adaptive SSO based on additional security postures such as location, time of day, user behavior, etc.
Endpoint Compliance	PZTA ensures access compliance and reduces endpoint security threats such as malware by authenticating the user and their device's security posture against granular access policies before granting access. Stateful endpoint security compliance checks reduce the possibility of introducing malware or other device security threats.
User Behavior Analytics	User behaviors and usage information are dynamic and constantly changing. PZTA leverages the analytical data to reduce security risks, detect anomalies, optimize user experience and adapt to the needs of an increasingly mobile workforce.
Data Privacy and Sovereignty	All user and application data are fully encrypted between client and gateway. Application data is never shared on the Pulse-Secure hosted data plane.
On-premises and Hybrid Cloud GW	Gateways can be deployed in public cloud, private cloud or customer data centers. This hybrid IT flexibility allows organizations to take advantage of the most optimal traffic and bandwidth conditions to reduce latency and keep data within the trusted domain as much as possible.

How Pulse Zero Trust Access Works

PZTA is based on the SDP architecture that embraces a Zero Trust approach to secure access. It consists of the ZTA Controller which is hosted and managed by Pulse Secure, the ZTA Gateway which can be deployed in a VPC (AWS/Azure public cloud, hosted private cloud, or on-premises) and the ZTA Client which is the same unified Client as the Pulse VPN/NAC Client.

Each and every time a user wants to access a protected application or resource from their device, the ZTA Client initiates a session with the ZTA Controller to request access. The ZTA Controller, upon validating the user's credentials, device compliance, and other security postures (such as location or behavior), will authorize the ZTA Gateway closest to the requested application or resource, allowing encrypted data communication with the ZTA Client. Throughout the communication, the endpoint security posture is continually being assessed to ensure the session is secure.

This Zero Trust access flow is the same regardless whether the user is inside or outside the corporate network, whether the user is using a corporate-owned device or personal device (BYOD), or whether the user is accessing a SaaS application or an on-premises resource.



PZTA administrator portal provides at-a-glance views of users, locations, anomalies, and more

Key Benefits of Pulse Zero Trust Access

Simplified User Experience

The ZTA Client is the same, proven Pulse VPN/NAC unified Client that is being used by 20M+ Pulse customers today. It supports popular operating systems such as Windows, macOS, iOS, and Android, and enables multi-factor authentication (MFA), Single Sign-on (SSO) and VPN services to ensure user experience is simplified as organizations implement PZTA or migrate from VPN to PZTA.

End-to-end Secure Access Policy

With PZTA, administrators simply publish an end-to-end secure access policy that defines which user/user group can access the application/resource. Regardless whether the users are remote or on-premises, whether they are using their own devices or corporate owned devices, or whether they are accessing applications in the data center or in the cloud, every time the user chooses to access a resource from the endpoint device, they will be authenticated and authorized based not only user credentials and device compliance, but also other security postures such as location, user behavior, etc. This is Zero Trust access at work.

Reduction of Attack Surface

Leveraging Software Defined Perimeter (SDP) architecture, the PZTA service provides a much-reduced attack surface. The end-user device never connects to the application or resources directly — it can only initiate all access requests through a secure connection with the ZTA Controller. The ZTA Controller maintains the list and mapping between gateway and protected applications. Only upon successful authentication and authorization, will the ZTA Client be able to establish an encrypted data tunnel with the corresponding ZTA Gateway. Once the access is complete, the data tunnel is terminated. When the end user wishes to re-establish the connection, they will need to again be authenticated and authorized by the ZTA Controller. This dramatically reduces the attack surface and potential vulnerabilities by shielding ZTA Gateway and application servers from untrusted hosts and devices.

Holistic Visibility and Compliance

Pulse ZTA provides a single pane-of-glass for visibility and compliance for CIO, CSO and IT administrators. From the PZTA dashboard, administrators have a holistic view of users, devices, gateways, applications and their status, as well as overview statistics. With a single click, administrators can zoom into any area of interest to see what caused any alert or compliance failure. Administrators, supervisors and executives can start their work day by browsing a pre-defined report with customized filter and format from the PZTA dashboard.

User Behavior Analytics

With all access going through the ZTA Controller, a wealth of user behavior information on both the macro- and micro-level can be collected and machine-learned. There are many practical applications of in-depth behavior analytics, such as detecting anomalies automatically when there is a change in behavior from normal routines, or when there is a suspicion based on location, device or activities. In fact, PZTA will assign a unique "risk score" to every user based on their usage pattern and history. Administrators can restrict certain applications based on threat scores or limit access based on location, device type and security posture.

Users	Devices	Applications	Infrastructure
• Employees	• Mobile	• SaaS & Cloud Native	• On-Premises
• Contractors	• PC/Mac	• On-Premises	• Cloud
• Guests	• Corporate	• 3rd Party	
	• Personal	• Custom	

Pulse Secure®

Corporate and Sales Headquarters
Pulse Secure LLC
2700 Zanker Rd. Suite 200
San Jose, CA 95134
(408) 372-9600
info@pulsesecure.net
www.pulsesecure.net

ABOUT PULSE SECURE

Pulse Secure, LLC offers software-defined Secure Access solutions that provide visibility and easy, protected connectivity between users, devices, things and services. The company delivers suites and a SaaS platform that uniquely integrate cloud, mobile, application and network access control for hybrid IT. More than 24,000 enterprises and service providers across every vertical rely on Pulse Secure to empower their mobile workforce to securely access applications and information in the data center and cloud while ensuring business compliance. Learn more at www.pulsesecure.net.

linkedin.com/company/pulse-secure
www.facebook.com/pulsesecure1
twitter.com/PulseSecure
info@pulsesecure.net

VERSION 07272020