Pulse Secure®

Demystifying Zero Trust Network Access (ZTNA)

A Strategy for Evolving Secure Access

Today, being hit with a data breach is almost inevitable. No organization is immune: Facebook, Marriott, and even government agencies have been victimized. Now, experts are predicting more serious repercussions than data theft including data and system manipulation, and full exposure of company secrets and intellectual property. At the same time difficulties in enforcing data protection have never been more challenging—and more urgent.

Most attacks result from compromised credentials, vulnerable endpoints, unmanaged IoT devices, or unprotected access to applications and resources. Attackers gain an entry point to a network and begin to discover resources and expand control. But organizations are also vulnerable to unintentional mistakes: in a recent study, human errors were the second largest cause of data breaches.[1]

[1] 2017 Cost of a Data Breach Study by Ponemon

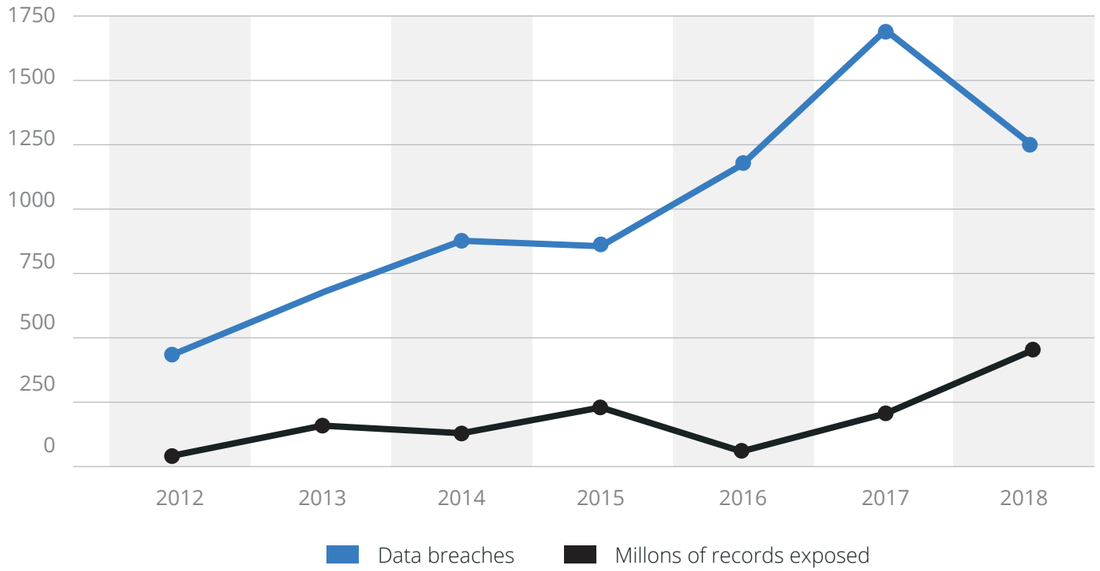
Protecting Data and Access in a Digital World

- Trust is no longer determined by location or IP address
- Secure access must evolve to the cloud where users and applications are moving
- There isn't a distinction between "inside" the network or "outside" the corporate network any more

Ensuring security compliance

- Dynamic endpoint visibility and policy enforcement regardless of user, app, and device location

Annual number of data breaches and exposed records in the United States from 2005 to 2018 (in millions)



Data Breaches by the Numbers

$3.86 million	the average global cost of a data breach in 2018 according to Ponemon Institute
291	records are stolen or exposed every single second
$600 billion	the annual cost of cybercrime to the global economy according to the Center for Strategic and International Studies

Secure Access by the Numbers[2]

48%	of organizations want to improve endpoint security, remediation prior to access
45%	of organizations fear unauthorized app/resource access including lax authentication or encryption
44%	want to fortify network and cloud access visibility and resource segmentation

[2] 2019 State of Enterprise Secure Access, IDG

Locking down valuable resources and applications is now imperative. But how can you attain vital, new levels of security without completely disrupting your digital business initiatives, confusing your employees, breaking infrastructure and requiring a massive resetting of your existing defenses?

The Solution is to implement Zero Trust

Zero Trust is a network security model that trusts no one, regardless of their location. Increasingly, trust can no longer be established based on whether a user is "inside" or "outside" the network. Every user is vetted before – and during – a connection, and every connection is governed by a policy that controls what resources can be accessed.

Leveraging Zero Trust means that enterprises enhance their security posture by:

Validating
users, and their devices' security posture

Controlling
access through granular policy enforcement

Protecting
and encrypting data transactions

What is Zero Trust Network Access (ZTNA)?

ZTNA is also known as Software-defined Perimeter (SDP). It uses a centralized policy controller that allows or denies a connection to specific applications. These applications are hidden from discovery, significantly reducing the attack surface. Before granting access, the controller leverages extensive authentication and authorization to ensure the validity of the connection, such as device type, date and time, and location. Only when all conditions are met is the connection granted; otherwise, a default "deny" posture is assumed.

What's the difference between Zero Trust as a security model and Zero Trust Network Access as a security architecture?

Zero Trust Model	Zero Trust Network Access Architecture
No "inside" or "outside" distinction	Centralized authentication of user, devices, applications, and stateful device security compliance checks
Authenticate everything before and during access	Centralized policy enforcement and separated control and data planes
Policy-based access through identity, role, device configuration as well as device security state, application, behavior, and other parameters	Granular segmentation based on per-application, per-user, and per-device connectivity
Trust established closest to resource	Significantly reduced threat surface by mitigating numerous APTs, malware, DDoS attacks and rendering resources "dark"

Is it possible to augment your secure access architecture to achieve a Zero Trust model without the extreme of throwing out your existing investments?

Zero Trust delivers several important capabilities:

Zero Trust Network Access (ZTNA)—also known as Software Defined Perimeter (SDP)—can be gradually deployed, even in complex organizations.

A hybrid model that encompasses both Zero Trust and ZTNA is possible.

ZTNA's architecture lends itself to improved performance and scalability.

Pulse Secure's dual-mode capability offers investment protection, enabling you to use VPN and ZTNA architectures simultaneously.

Zero Trust Network Access extends these tenets by centralizing policy enforcement so that every user – and their device – is governed by a granular policy for every resource they access. It authenticates every user *before* the connection is made, ensuring that unauthorized users or devices are unable to access any resource whatsoever.

Moreover, it also re-verifies a device's security posture during a connection to determine if the security state is no longer acceptable. In such cases, devices can be quarantined or remediated, depending on a policy set by the administrator.

Finally, ZTNA renders resources "dark". In other words, no DNS, internal IP address, or visible port information is communicated until proper authorization takes place. So, unauthorized users can't traverse the network, "looking" for resources to infiltrate. This reduces the attack surface significantly by mitigating or eliminating numerous threats like APTs and malware.

Pulse Secure Zero Trust Capabilities

Pulse Secure delivers a comprehensive approach to Zero Trust:

- **User identity, including multifactor authentication**
- **User role and permissions**
- **Type and location of the device used for access**
- **Stateful device compliance checks before, and during, a connection**
- **Type of network used (e.g. public hotspot)**
- **Per-application/per-resource rules and permissions**
- **Granular policy enforcement**

With Pulse Secure, you get Zero Trust today and can implement ZTNA architecture when and where you need it.

1. Pulse Secure is a pioneer of VPN technology. Our proven expertise has been in establishing secure, protected connections—coupled with the most advanced modes of user and device authentication, authorization and verification.
2. Despite the new prominence of the term, Zero Trust has always been built into our Secure Access platform.
3. Pulse Secure's Zero Trust addresses immediate access issues and data protection concerns. At the same time, it enables organizations to implement ZTNA for specific use cases as necessary.
4. With Pulse Secure, enabling Zero Trust does not require changes to existing security or networking infrastructure, and it will only fortify access to designated resources while preserving user experience.

> **Zero trust network access replaces traditional technologies, which require companies to extend excessive trust to employees and partners to connect and collaborate. Security and risk management leaders should plan pilot ZTNA projects for employee/partner-facing applications.**
>
> Market Guide for Zero Trust Network Access, April 29, 2019, Gartner

Unique Advantages of Pulse Secure Zero Trust Solutions

Enhanced user experience:
Pulse's unified client offers easy and seamless access options for multiple applications simultaneously.

Simultaneous dual-mode connectivity:
Deploy industry-leading SSL VPN and ZTNA on the same virtual or physical appliance depending on how you want to treat individual applications or resources. For example, certain legacy or non-sensitive applications may not warrant ZTNA and the additional requirements for access control.

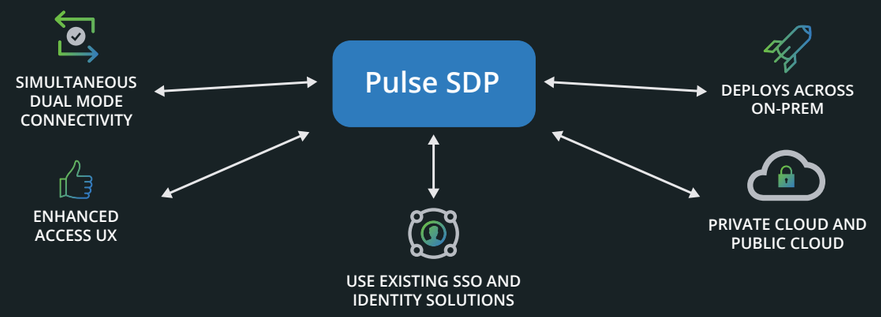
Deployable across the entire infrastructure:
Pulse SDP can be used on all networks and data centers—on-premise, private cloud and public cloud.

Integration with existing SSO and identity solutions:
Pulse Secure Zero Trust preserves integrations with identity solutions from providers such as Okta, Ping Identity and Microsoft ADFS. In addition, Pulse SDP augments these identity-based integrations by supplementing multi-factor authentication (MFA) with in-depth device- and host-based security compliance checks.

Comprehensive Endpoint Compliance:
Offering the most comprehensive device compliance for mobile, IoT and laptop/desktop devices, Pulse Secure employs an array of agent and agent-less client assessment techniques to ensure that only compliant devices connect to your network.

Powerful, granular role-based access control:
A high-performance policy engine, wizard policy editing, and SSO capabilities enable unified access closest to applications residing in multi-cloud or data centers.

Flexible Deployment:
Pulse Secure offers the industry's most flexible, scalable deployment options to choose from: data center hardware or virtual appliances and private cloud, public cloud or SaaS. Pulse Secure has been deployed among the largest enterprises and service providers in the world due to proven performance and scale.



Getting Started

With the influx of BYOD and IoT, the increase in workforce mobility, and the rise in malware, Zero Trust is more critical than ever. But it's easier than you might think to implement.

Zero Trust is first enabled by our unified client. Leveraged across our portfolio, it enables consistent, streamlined user experience and consistent policy control across multiple platforms (Windows, macOS, iOS, Android). Client can be agent or agentless.

Our Host Checker feature uses the client to query endpoint devices for an acceptable security posture before the device is allowed to connect – and it continues to check even during the secure connection. This prevents malware (like WannaCry or NotPetya) and other endpoint exposures from penetrating your network.

Next, our traditional Secure Access solution has integrated multi-factor authentication and authorization (MFA) and single sign-on (SSO) features designed to ensure every user is vetted and secured.

Once users are connected, centralized policy management and enforcement governs specific resources and applications your mobile workforce can access, and prevents unauthorized users from accessing sensitive data.

Finally, Pulse Secure's advanced SSL encryption technologies protect all data transactions. With features like Always On, On Demand, and Per-application VPN, data-in-motion is kept secure and compliant.

Extending Zero Trust

With a simple software upgrade, Pulse SDP extends Zero Trust by rendering resources and applications "dark" (minimizing malware penetration and lateral spread), and centralizing policy controls that make it possible to isolate applications, allowing only specific users and specific devices access. The whole solution is optimized for a streamlined user experience, enhanced security compliance, and a reduced total cost of ownership.

Pulse Secure is the only vendor to offer dual-mode support, making it possible to have traditional VPN and SDP operating simultaneously. Moreover, our deployment flexibility with physical, virtual, and cloud appliances offers true Hybrid IT protection, securing sensitive data across data center and cloud.

Learn how Pulse Secure can boost worker productivity, strengthen your network security profile, and enhance security compliance at www.pulsesecure.net.

ABOUT PULSE SECURE

Pulse Secure provides easy, comprehensive software-driven Secure Access solutions for people, devices, things and services that improve visibility, protection and productivity for our customers. Our suites uniquely integrate cloud, mobile, application and network access to enable hybrid IT in a Zero Trust world. Over 20,000 enterprises and service providers across every vertical entrust 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.