puredome

PureDome's ZTNA Solution

Securing Remote Access to Enterprise Resources

In the face of escalating cyber threats and a projected annual cost of **$10.5 trillion by 2025,** traditional network security models proved inadequate. The evolution led to the emergence of Zero Trust Network Access (ZTNA), challenging the implicit trust within network perimeters. Adopting a "never trust, always verify" approach, ZTNA offers a paradigm shift in securing remote access, acknowledging the shortcomings of conventional security measures.

Why Is Secure Remote Access So Essential?

With remote work increasingly prevalent across industries, as evidenced by recent McKinsey data indicating that 58% of Americans work from home at least one day a week, secure remote access has emerged as a crucial information technology (IT) tool for numerous organizations.

58%
of Americans
work
from home

Here are some main reasons why secure remote access should be a priority for your business:

- Facilitates flexible work arrangements, boosting employee productivity and collaboration.
- Ensures data protection and compliance, minimizing the risk of cyber threats and unauthorized access.
- Safeguards sensitive information, maintaining business continuity and resilience in an interconnected world.
- Enhances company agility, attracting top talent and adapting to evolving work dynamics.

Principles of Zero Trust Network Access

The Zero Trust Network Access (ZTNA) model challenges traditional security by adopting a "never trust, always verify" approach. Key principles include rigorous identity verification through various means, context evaluation based on user, device, and network factors, and behavior monitoring using advanced tools for anomaly detection and threat response. This multifaceted strategy enhances organizational security in the dynamic threat landscape.

Aspect	Core Principle
Identity Verification	The foundation of ZTNA includes multi-factor authentication, biometrics, device certificates, and more.
Context Evaluation	Considers user location, device health, time of day, and network context for access decisions.
Behavior Monitoring	Continuous monitoring using anomaly detection, UEBA, and EDR tools to identify and respond to threats.

Components of Zero Trust Network Access

These components collectively embody the principles of Zero Trust, offering organizations a comprehensive toolkit to navigate the cybersecurity landscape effectively.

Identity and Access Management

- Utilizes multi-factor authentication and advanced biometrics for user validation.
- Enables dynamic provisioning and de-provisioning based on roles, reinforcing the principle of least privilege.
- Employs granular access controls, limiting exposure and enhancing security.

Network Segmentation

- Implements micro-segmentation at the application level to curtail lateral movement.
- Detailed access controls operate on a micro-segment level, preventing unauthorized access.
- Leverages technologies like SDN and Zero Trust Architecture for adaptive access controls.

Continuous Authentication

- Utilizes behavioral analytics to detect anomalies and trigger real-time alerts.
- Adapts access policies based on user behavior and contextual factors for enhanced security.
- Relies on advanced technologies like machine learning and risk-based authentication for dynamic verification.

Least Privilege Access

- Enforces role-based access controls for specific, tailored access rights.
- Implements Just-in-Time provisioning to grant access only when necessary, enhancing efficiency.
- Utilizes privilege elevation mechanisms for temporary, task-specific access, maintaining flexibility and security.

Micro-Segmentation

- Adopts application-centric segmentation, tying access controls directly to specific applications.
- Implements dynamic policies for real-time adaptation to evolving situations.
- Minimizes lateral movement by confining users and devices to designated segments with fine-grained access control.

Why Does Your Business Need To Implement ZTNA?

If your business faces challenges with traditional security models, leaving it vulnerable to evolving cyber threats and sophisticated attacks, and struggles with maintaining control over user and device access in the era of remote work, implementing Zero Trust Network Access (ZTNA) is a critical solution to address these pain points and enhance overall cybersecurity resilience.

Robust Security: ZTNA adopts a "never trust, always verify" approach for enhanced protection.

Remote Work Enablement: Ideal for secure access in remote or distributed work scenarios.

Dynamic Access Controls: Streamlined Access Controls: Ensure that only authorized users can access Protected Health Information (PHI) with our simplified network access controls.

Limited Attack Surface: Micro-segmentation confines and prevents lateral movement, reducing risks.

Regulatory Compliance: Ensures adherence to regulations with precise access controls.

Scalable Solution: Adapts seamlessly to changing user roles and access needs

Advanced Threat Defense: Utilizes cutting-edge tech to detect and thwart sophisticated attacks.

Cloud Security: Tailored for secure access in cloud environments, safeguarding data integrity.

A Quick Look Into PureDome’s ZTNA

By prioritizing identity verification and contextual factors like location, time, and user behavior - PureDome ensures that users and devices securely access resources - even in a dynamic, cloud-centric environment.

Feature	Description
Authenticate & Authorize	Seamless integration with identity providers like Okta or Azure eliminates manual account management and ensures controlled access.
Network Segmentation	PureDome gateways segment extensive networks, providing least privilege access control for improved performance, security, and administration.
Reporting & Logs	Centralized admin reports offer visibility into access requests, feature usage, admin/member activity, access analytics, and device activity.
Device Health Checks	Enforce security policies for compliant device connections, ensuring granular control over users and devices in BYOD environments.

Take the next step in your Zero Trust strategy with PureDome's ZTNA

Identify
everything that users may need remote access to

Monitor
all access attempts no matter where they're from

Adjust
access privileges to boost productivity while minimizing risk and exposure

Enforce
policies to limit user access to specific resources

Book a demo to learn more, or get started for free today.

Sources:

https://www.globenewswire.com/news-release/2020/11/18/2129432/0/en/Cybercrime-To-Cost-The-World-10-5-Trillion-Annually-By-2025.html#:~:text=Every%20U.S.%20business%20is%20under%20cyberattack&text=18%2C%202020%20(GLOBE%20NEWSWIRE),%243%20trillion%20USD%20in%202015

https://www.business.com/articles/secure-remote-access/