WHAT IS ZERO TRUST NETWORK ACCESS? ZTNA EXPLAINED

Zero trust network access attempts to solve the most basic security problem, which is:

How can you secure systems, services, applications, and data that can be accessed anywhere, anytime, by any user using any device, on an organizational network and in the cloud?

This article introduces zero trust network access (ZTNA) and how it shores up network resource security. We will look at:

- Perimeter security
- What ZTNA is
- How ZTNA works
- Flavors of ZTNA

Where perimeter security falls apart

Many organizational networks still rely on traditional perimeter security to protect data and applications from bad actors and malware attacks.

Perimeter networks use a castle-and-moat concept. Like a moat surrounding a castle, a perimeter network is surrounded by DMZ security barriers. Firewalls, VPNs, edge servers, and other devices residing in the DMZ attempt to keep bad guys out and let good guys in. Anyone who crosses the DMZ moat—good or bad—is generally considered trusted and able to reach the assets behind the DMZ. Perimeter security's access model is **Trust, but Verify.**

Unfortunately, in perimeter networks, trust is vulnerability. Behind the DMZ, everything is considered trusted. Users and devices can move freely inside the network—this is called lateral movement. Hackers can infiltrate, access, and extract data *anywhere* in the network, if they can just get past the perimeter.

Traditional perimeter networks by themselves create a threat-conducive environment. Users, apps, and data reside on premises *and* in the cloud. Any user can access these, anywhere, anytime, using both approved and unsecured, unpatched BYOD equipment. Pervasive cloud access has made perimeter boundaries fuzzy or altogether non-existent—all the easier to breach.

With resources and services residing in multiple locations inside the physical network and in the cloud, threat attack surface areas have expanded. Security access capabilities need to evolve beyond using only perimeter security.

What is Zero Trust Network Access?

The zero trust network security model is **Never Trust, Always Verify**. The ZTNA philosophy assumes there will always be attackers originating from both outside and inside the network. No user or device should be automatically trusted, even when they get past the DMZ. This directly contrasts the Trust, but Verify model of traditional perimeter security.

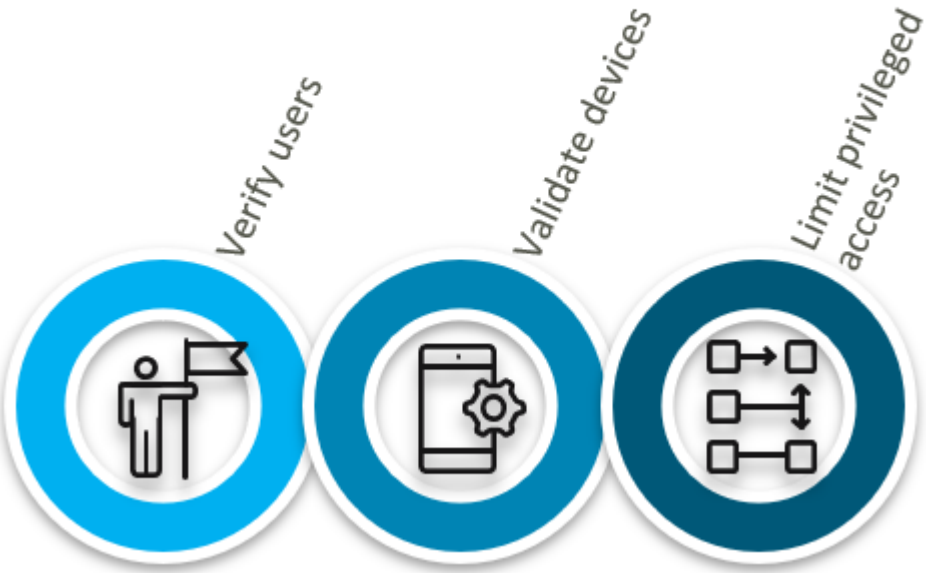
Zero trust networks require verification whenever a user or device requests resource access, regardless of whether the requester sits inside the organizational network. ZTNA does not rely on a DMZ perimeter consisting of VPNs, firewalls, edge servers, and other security devices protecting restricted resources.

How does ZTNA work?

ZTNA products and services create an environment that defends both your physical (on premises) and logical (cloud-based) resources. Applications are non-discoverable (hidden) and access is verified by a trust broker, who allows or denies access using these three key steps:

bmc

Zero Trust Security Model: 3 Steps



1. Verify users when they sign on to the system.
2. Validate devices before entering the network. Ensure that incoming devices are known, trusted, and up to date on patches and security.
3. Limit access based on principle of least-privilege (POLP). The user or device is only given as much authority as needed to access the requested resource, based on roles.

ZTNA is not a single technology philosophy. Rather it encompasses a range of technologies for verifying the requesting user or device and providing access. The table below shows some of the different technologies used in ZTNA environments and how they are used to allow or deny resource access.

bmc

Zero Trust Network Access

Technology used in ZTNA	What it does	Network protection provided
Multi-Factor Authentication (MFA) 2-Factor Authentication	After the user signs on to the resource, they must also enter an access code that was sent to their registered phone number or email. Entering the requested code verifies the user identity and enables user access.	User verification
Network Access Control (NAC)	Enforces and verifies user and device identities. NAC profiles users, devices, and operating systems to ensure they comply with all required security policies. NAC can also block, isolate, and repair non-compliant entities.	User verification Device verification
Device Access Control	Ensures only authorized devices are allowed access, using techniques such as digital keys or matching media access controls (MAC) addresses for every allowed device.	Device verification
Privileged Accessed Management (PAM)	Ensures that every user and device only get the POLP access they deserve, minimizing lateral movement across the network.	Limited access via Principle of Least Privilege
Microsegmentation	Using network virtualization, microsegmentation divides your workloads into unique and granular segments that contain their own security policies and are isolated from the rest of the on premises and cloud network. Microsegmentation reduces the total attack surface of the network and severely limits server to server threats.	User verification Device verification Limited access via Principle of Least Privilege

ZTNA product flavors

ZTNA products are available in three different flavors:

- **As a cloud service**, usually delivered as an Infrastructure as a Service (IaaS) offering

- **As a standalone offering**, where customers must deploy and manage the product themselves
- **As a hybrid service**, combining cloud service and stand-alone offerings

According to the recent Market Guide for Zero Trust Network Access, Gartner estimates that 90% of its clients are implementing ZTNA in its as-a-service flavor. Many major networking vendors offer ZTNA products, including:

- Akamai
- Broadcom
- Cisco
- Google
- Microsoft
- Palo Alto Networks
- Verizon

The future of ZTNA

Implementing ZTNA security is a possible solution for redefining and centering security around network resource needs, instead of the DMZ. Unlike perimeter security, ZTNA reduces insider threat risks by always verifying users and validating devices before granting access to sensitive resources. For outside users, services are hidden on the public internet, protecting them from attackers, and access will be provided only after approval from their trust broker. With ZTNA, reducing unearned trust improves security.

With digital transformation efforts, many organizations will have more systems, applications, and data in the cloud than they have in their on premises networks. Cloud-based ZTNA services, in particular, migrate verification, validation, and privilege assignment services to where the user is: the cloud.

There are network and Internet issues to consider when implementing ZTNA, including:

- Latency in contacting trust brokers
- Redundancy of ZTNA components

Trust brokers should not become single points of failure. In general, a zero trust network should remain secure when any individual account or endpoint is compromised.

ZTNA services will not replace perimeter security overnight. Castle and moat security will continue to be used in the right settings. Over time, however, organizations will implement security models such as ZTNA to provide safer targeted access to valued resources and eliminate issues with automatic trusted access.

Additional resources

For more on this and related topics, explore these resources:

- BMC Security & Compliance Blog
- SecOps Trends of 2020
- Introduction to Identity and Access Management
- Kerberos Authentication: What It Is and How It Works

- Security Analytics: An Introduction
- What Does a Network Operation Center (NOC) Engineer Do?