Seven Principles of the Zero Trust Security Model

A zero trust framework delivers secure access to all corporate apps, modernizes IT security, and allows businesses to securely support a hybrid workforce

White Paper

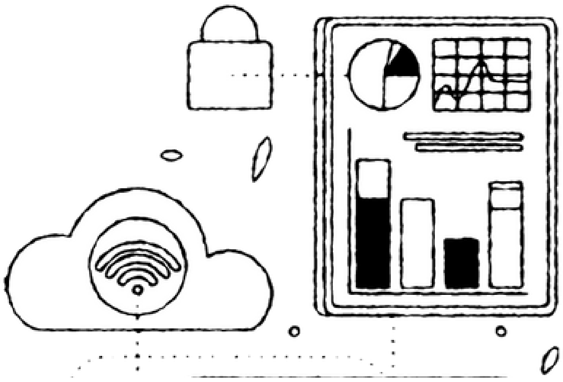
The reality is that today's fast-paced, hybrid work environment leaves businesses vulnerable to security breaches. More and more employees now rely on their own unprotected devices for work, leveraging SaaS and web-based apps to access valuable enterprise assets and data. By logging into the corporate network to accomplish work tasks, those employees are also unknowingly increasing the attack surface.

For channel services providers, this expanded threat area presents the newest opportunity to share the value of seamless security solutions. Regardless of the size of the customer, employing a zero trust network access (ZTNA) solution provides unmatched security and peace of mind.

To showcase the value of the ZTNA "trust none, verify all" approach, highlight these seven security principles that illustrate how ZTNA insulates business data from malicious activity.

1 Secure Communications

Also known as perimeter-less security, ZTNA takes the "never trust, always authenticate" approach to security when it comes to allowing a user access to a network. Explicit permission must be granted for every session — even if the same user or device was previously verified. Users operating in a ZTNA environment won't even be aware of applications and services within a business framework unless they're granted access through individual permission protocols.



2 Evaluate on a Per-Session Basis

The dynamic nature of distributed compute environments and a remote workforce makes user and device trust a critical priority. As a result, every single login or access request should be protected by authentication protocols. Unprotected cloud-based architectures are vulnerable to bad actors and a barrage of threats, from poor access management to data loss and breaches. Plus, just because a device or identity was trusted during a previous session doesn't mean it should be automatically granted immediate access the next time access is requested. ZTNA provides additional protection simply by questioning access every single time.

3 Monitor Resources — When Everything is a Resource

Business networks can be accessed by a virtually limitless number of devices. Whereas endpoint user workstations and servers were once the extent of connected equipment, today's dynamic cloud computing services can execute specific permissions to other devices.

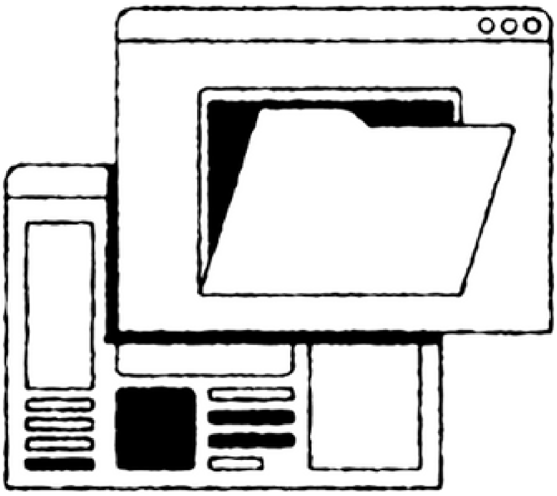
To maintain a line of sight into the security of the connected devices accessing corporate data, the best approach is to implement varied and compounding authentication protocols. Employing the Principle of Least Privilege (PoLP) safeguards data by ensuring that every module (from processes to users to programs) must only be able to access the information and resources necessary for an assigned task.

4 Monitor, Measure, Repeat

The zero trust approach is designed to be taken literally. By employing continuous monitoring of enterprise apps, businesses safeguard against possible malicious entry from unauthorized users. Applications are highly vulnerable to cyberattacks, and it should be of paramount importance for every organization to keep a watchful eye on each request to access them.

Even one successful attempt at unauthorized access can wreak havoc on infrastructure. In a traditional perimeter-based model like VPN, once a hacker gets access through an app they're able to move laterally, and in most cases, access the entirety of the network.

By stopping bad actors at the application level, ZTNA solutions can prevent threats from ever gaining a foothold within the corporate network.



Are you a Citrix partner? Scan the QR code to watch **Citrix Made Simple ZTNA**

5 Be Dynamic

A dynamic, adaptable policy should govern both behavioral and environmental attributes. Risk factors such as location and device posture should be used to trigger protocols that make access control decisions automatically.

Parameters surrounding user information and location, the device from which they are requesting access, and any associated security clearance can be automatically diagnosed. A result of full access, limited access, or no access at all can be governed autonomously by detection protocols.

Utilizing multi-factor authentication (MFA) measures is one example of how governance applications can limit access when necessary.

6 Enforce Strictly

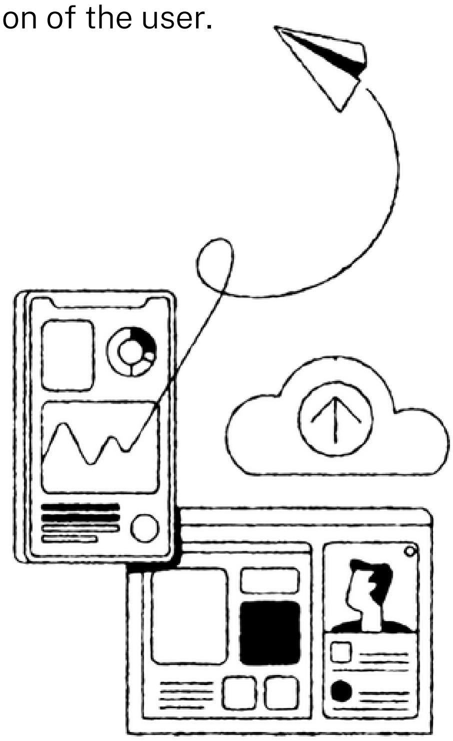
Both authentication and authorization should be dynamic and strictly enforced before access is granted. By ensuring that security checks are constant — and constantly evolving — a business is protected by an ongoing cycle of scanning users.

These protocols evaluate the trustworthiness of authentication attempts by leveraging signals and security checks before determining whether access is granted. This iterative process, initiated as soon as an employee or new device creates an account with associated permissions, does not stop for the lifecycle of the hardware or the association of the user.

7 There is no such thing as "too much"

Today's IT infrastructure environments are subject to a near-constant stream of possible threats, and businesses must maintain rigorous monitoring to stay ahead of potential vulnerabilities.

To illustrate the importance of ZTNA implementation, talk to your customers about whether their company is currently following the seven principles of the zero trust model.



Learn more about Citrix ZTNA
citrix.com/solutions/zero-trust-network-access