Zero-Trust Access: Enable and Protect Business Innovation

Fortinet and NTT deliver secure access everywhere

The Notion of Digital Trust Must Be Redefined

Traditional access control strategies tend to broadly trust a user or device across the network, once access has been provided through the traditional network perimeter. In the past, employees primarily connected to the network while in a corporate or branch office. Today, however, many users access the corporate network from remote locations. In addition, users are increasingly connecting to resources beyond the traditional network perimeter, including public and private clouds.

Networks Attract Cyberattacks

Legitimate network users, along with bad actors, can jeopardize business networks and data, compelling IT administrators to place identity and access management (IAM) at the center of security operations programs. Since credentials can be stolen and used to gain access, IAM is not enough. Secure access solutions must not only extend beyond people, but also adopt a "least-privilege" model.

A zero-trust access (ZTA) approach can continually verify who and what is using the company's digital resources.

IT needs this visibility and control to protect their business made more vulnerable through digital transformation initiatives. Using a zero-trust approach that covers these three areas is a good first step:

- Users on the network
- Devices on the network
- Users and devices off the network

It should be noted that a fragmented approach to ZTA leaves security gaps, is more costly to employ, and is more cumbersome to manage.

Challenges to Achieving Comprehensive ZTA

Integrating a solution to close security gaps can be difficult due to:

No central network and/or security strategy

Organizational resistance across IT teams

Still too dependent on traditional VPN

Lack of access to skilled resources

Lack of budget to make IT changes right now

Lack of qualified vendors with a complete solution

Attempt to bring together fragmented solution approach

No unified definition on ZTA

Fortinet and NTT Have You Covered

Fortinet and NTT have the experience and qualifications to implement a zero-trust solution that provides comprehensive visibility and protection across devices, users, endpoints, clouds, and infrastructures with a "never trust, always verify" strategic approach to security.

The Fortinet Zero-Trust Access framework leverages a tightly integrated collection of security solutions that enable organizations to: identify and classify all users and devices seeking network access; assess their states of risk and compliance with internal security policies; automatically assign them to zones of control; and continuously monitor them, both on and off the network. This holistic approach ensures that legitimate users and devices are protected from attacks and that only those that have been appropriately verified can only access the resources relevant to their work and their role.

NTT provides a comprehensive zero-trust solution in addition to services ranging from consulting, design planning, implementation, and managed services. NTT experts work with organizations to identify and resolve access-control issues across their entire environments.

Zero-Trust Access Use Cases

Identity and Access Management
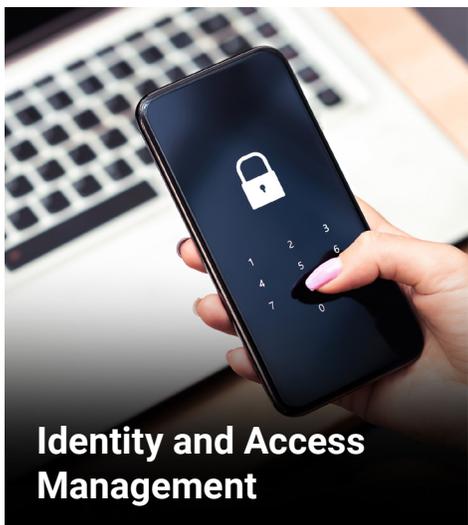
Identify and verify users entering the network with high reliability. Centralized authentication includes SSO, certificate management, and guest management. MFA confirms identity with a second factor.

Endpoint and Device Protection
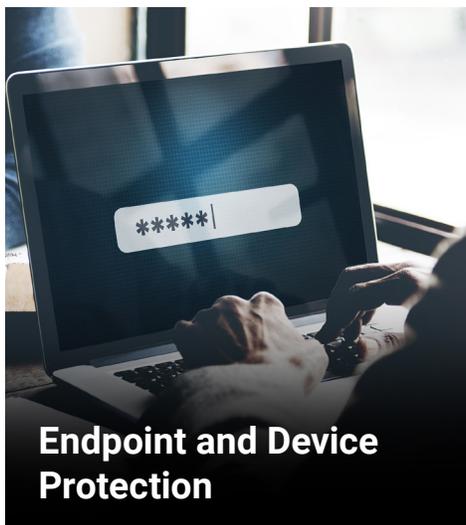
Identify and secure unknown endpoints and devices entering the network. Integrated endpoint visibility, control, and advanced protection ensure organizations are secure.

Remote Access and Application Access
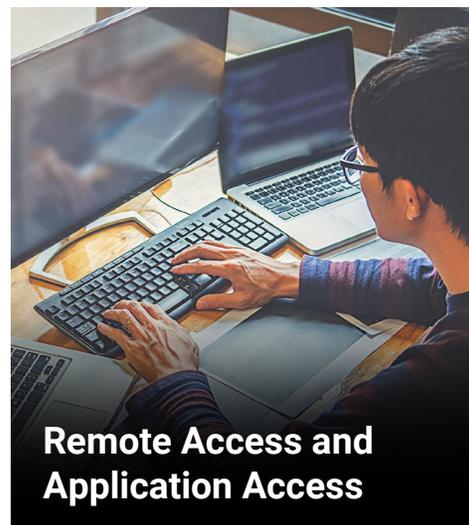
Grant access on a per-session basis to individual applications only after devices and users are verified. This policy is also applied when users are on the network, enabling the same zero-trust model no matter the user's location.

Fortinet and NTT help organizations assess, design, plan, implement, and manage their on-premises and remote workforces over a converged network. The Fortinet-NTT partnership takes advantage of Fortinet's advanced technologies and NTT's global managed cybersecurity services to deliver a complete, efficient, and cost-effective solution that protects the network from indiscriminate access to critical resources, regardless of the user's or application's location.

Next steps

For additional information on cybersecurity solutions, visit www.global.ntt and learn how to protect your digital and physical assets.