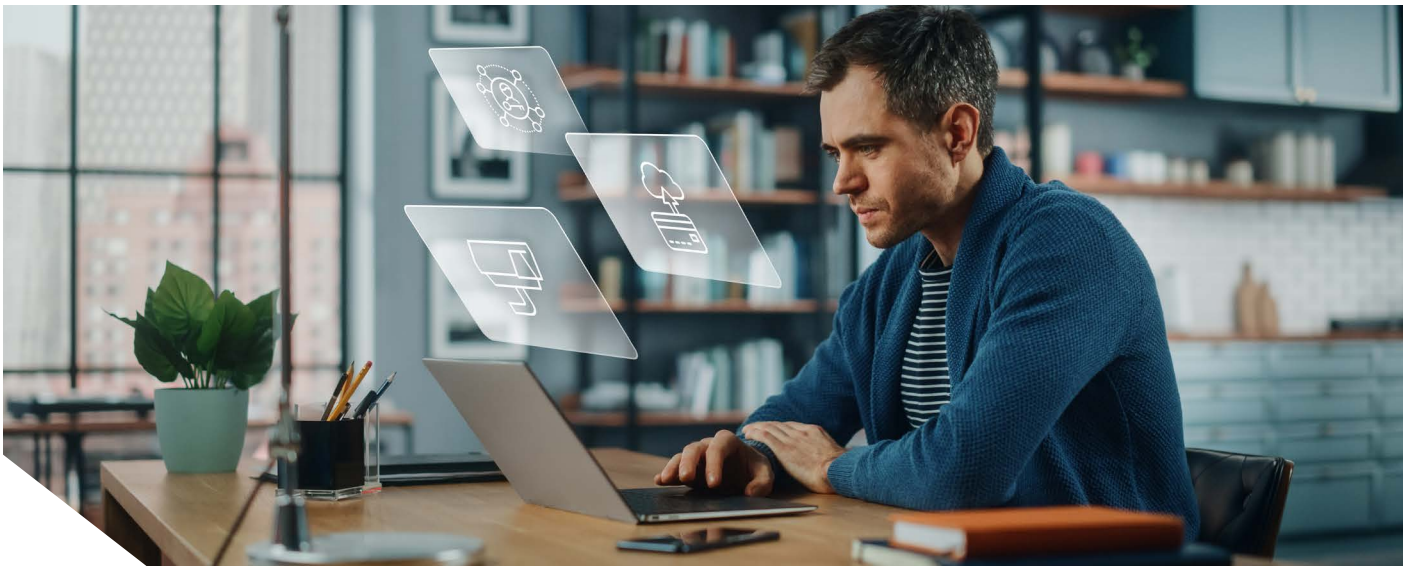


Bolstering Enterprise Security Using Zero Trust Architecture

Deploying a zero trust model for 5G Wireless WAN provides greater security and easier management than traditional VPNs

Overview

Protecting critical information and infrastructure is increasingly difficult for enterprises managing complex networks, replacing data centers with cloud-based applications, and balancing a "work from anywhere" mentality. Vast quantities of data are being stored on-premises and in the cloud and sent back and forth through wide-area networks (WAN). These ever-expanding attack surfaces pose harmful risks to an organization's security. To combat these risks, organizations must move beyond traditional security models to build adaptive zero trust networks.

What has led to zero trust?

To understand the value of zero trust, it's helpful to review virtual private networks (VPNs), a security model that has been a corporate standard for decades. In a traditional network setting, VPNs use encryption to connect branch offices and remote users to a corporate data center. Within VPN architecture, if a hacker connects to a site, they may be able to move laterally and compromise the network. This is why hackers work so hard to get employees' usernames and passwords, and why legacy VPNs don't fit the needs of modern organizations.

VPNs are complex to manage and their security falls short when it comes to protecting large enterprise networks. In addition, any troubleshooting takes a substantial amount of time, which most IT teams don't have. In short, facing an increasing attack surface, the efficacy of VPNs has dwindled. As a result, many enterprises have sought a simple-to-manage security model that replaces traditional VPNs while still allowing employees and others to work securely from any network or location.

What is zero trust?

A zero trust security model — as the name implies — is built on the guiding principle of "never trust; always verify," meaning it assumes that anyone attempting to access a network or application has a hostile intent and must be restricted through ongoing verification.

Zero trust network architecture masks public facing IP addresses and applies microsegmentation and adaptive verification policies on a per-session basis while taking into account a combination of the user's identity, location, device, time and date of request, and previously observed usage patterns. These security evaluations consider whether a user has changed locations, when they last attempted to access an application, if they're using a new device, and if they exhibit abnormal behavior, such as rapidly altering or deleting data.

Once verified, a secure tunnel can be created from the user's device to the requested resource. This authenticated tunnel prohibits public discovery or lateral movement to other resources on the network and ultimately decreases the likelihood of cyberattacks.

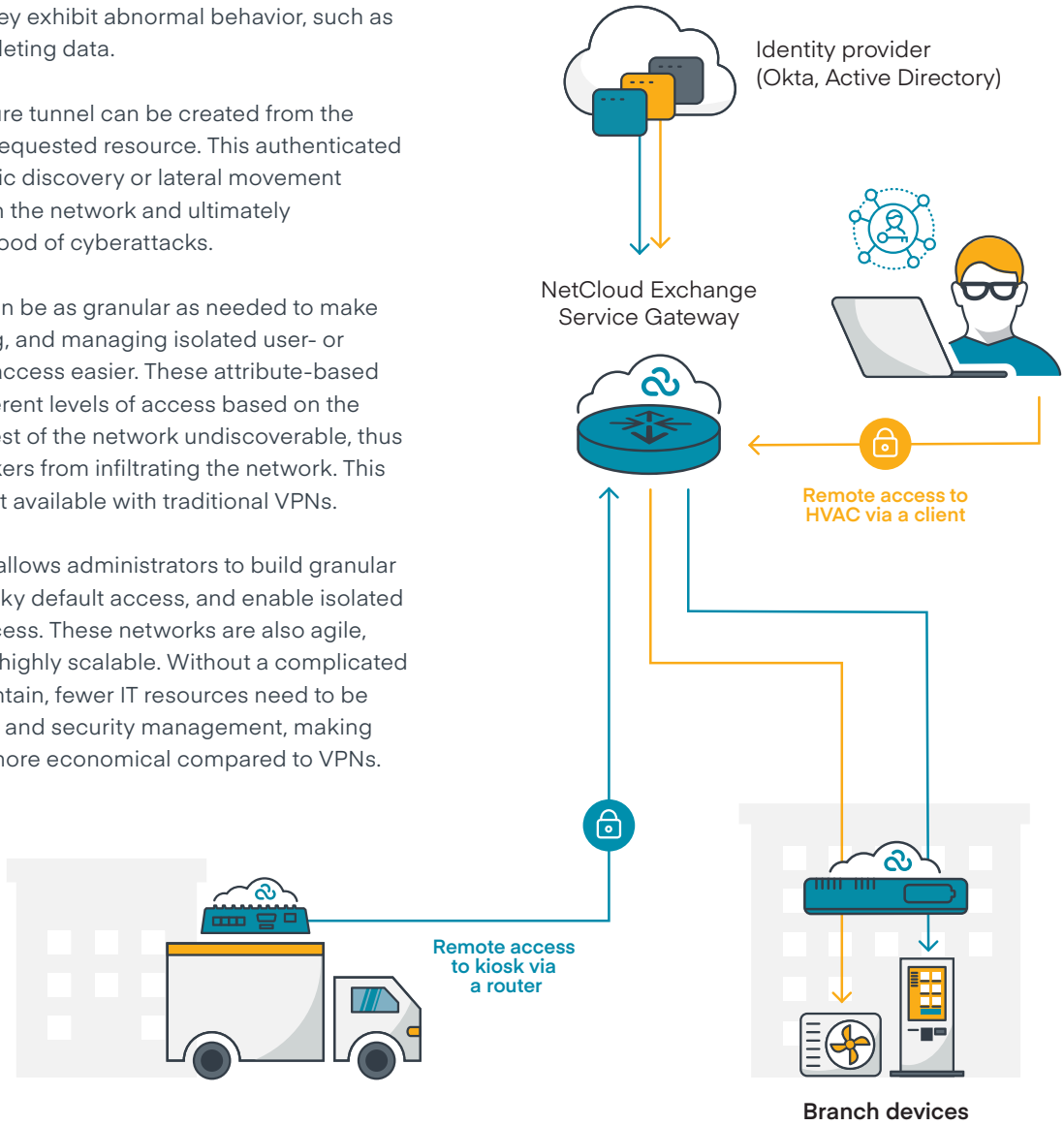
Zero trust policies can be as granular as needed to make identifying, assigning, and managing isolated user- or device-to-resource access easier. These attribute-based policies provide different levels of access based on the user and make the rest of the network undiscoverable, thus helping prevent hackers from infiltrating the network. This level of security is not available with traditional VPNs.

A zero trust solution allows administrators to build granular policies, eliminate risky default access, and enable isolated user-to-resource access. These networks are also agile, quick to deploy, and highly scalable. Without a complicated infrastructure to maintain, fewer IT resources need to be dedicated to training and security management, making zero trust solutions more economical compared to VPNs.

What is ZTNA?

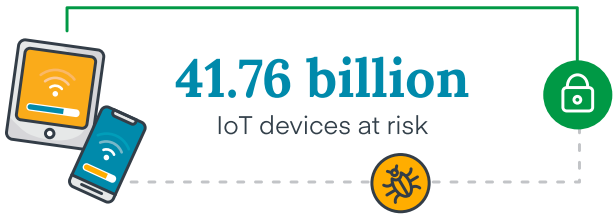
A zero trust network eliminates default access by giving users and devices access only to the resources they need to do their job. This infrastructure establishes secure connections across distributed sites and the users and IoT devices within them.

Zero Trust Network Access (ZTNA) extends secure, isolated user-to-resource connections to third-party contractors, suppliers, and certain employees and IT users accessing the network through a client. It also allows remote users to securely access the network through specific routers.



How the right zero trust solution protects IoT devices

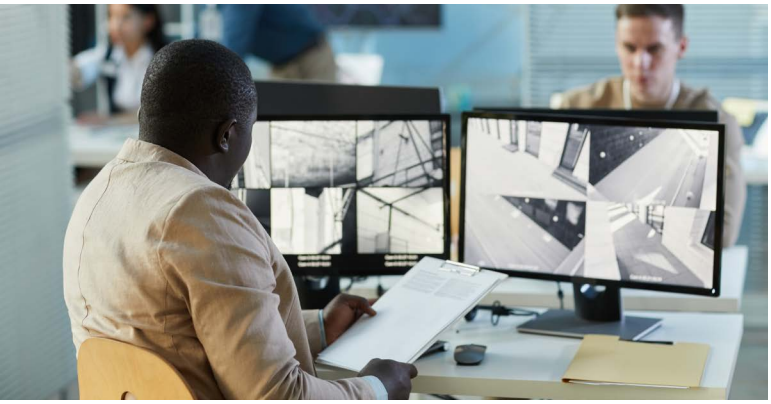
There are an estimated 41.76 billion IoT devices globally in 2023. With the rise in the number of IoT devices comes increased security risk, as video surveillance cameras, kiosks, digital signs, and more are especially vulnerable to security threats.



Why are IoT devices vulnerable to attack?

By nature, IoT devices are simple machines. As such, they lack sufficient processing power to run on-board security. Most industry security solutions require that a device runs an agent or browser extension for protection. IoT devices can't run security agents and don't support browsers, making these solutions useless for IoT security. The default passwords on IoT devices are seldom changed and updates are not often installed. Most importantly, IoT devices typically broadcast their IP addresses, making them an easy target for IP scans. With a zero trust network and no visible IP address, IoT devices become invisible to the outside world.

For IT teams to effectively manage distributed IoT networks, organizations need to implement data security practices that simplify the setup and maintenance of IoT security solutions. With advanced policies, organizations can securely connect third parties to remotely manage devices. Zero trust architecture is an ideal replacement solution for VPNs.



Why is IoT remote access important?

Third-party contractors and suppliers are a vital part of business for many enterprises seeking ways to save money through outsourcing. However, granting setup, troubleshooting, management, and operating access is a risk — one that is becoming increasingly common as more enterprises add 5G to their infrastructure and WANs continue to transform.

For example, many organizations use video surveillance systems for safety and security purposes to provide real-time monitoring and recording of activities within and around the premises. But, like most IoT devices, these cameras often require ongoing management and maintenance.

Businesses can opt to have a third party remotely manage their cameras to reduce costs associated with on-site visits and enhance operational effectiveness. Secure IoT remote access using policies built on zero trust principles establishes an isolated connection between the contractor and the video system. This means they can securely monitor live video feeds, review footage, adjust camera settings, and perform necessary maintenance and troubleshooting without physically being on site, and without gaining access to other resources on the network.

Using zero trust remote access can be a convenient and cost-effective way to manage IoT devices, and it reduces risk from third-party access.

Many companies still use traditional encrypted VPN tunnels for third-party access, which could allow contractors to move laterally once they have access to the network. A zero trust network minimizes this risk by only allowing access to specific resources.

Many enterprises are eager to dip their toes into zero trust, but where do you start? Replacing a VPN with a zero trust network can be a daunting task, historically requiring tedious IP address management to ensure no duplicate addresses on the network. This process can be made easier by using named-based routing, which does not require unique IP addresses for each device on the network.

How to extend the zero trust network to those managing data remotely

Let's go back to IoT remote access. Enterprises need a ZTNA solution that manages user-to-resource (or IoT-device-to-resource) connections and extends secure access to third party contractors, suppliers, and certain employees without giving them access to other resources on the network. ZTNA allows companies to evolve to user-based access policies, enabling remote access from either a router or client.

For example, consider HVAC systems, which are found in virtually every enterprise building to help control temperatures and air quality and create a healthy working environment. Like video cameras and other IoT devices, contractors can access HVAC systems remotely via a client, giving them access to monitor and adjust temperature settings, control ventilation and air quality, and receive real-time alerts regarding system performance and maintenance requirements.

Modern-day organizations should always have their guard up when it comes to protecting their network, which is why ZTNA solutions verify first then grant access. ZTNA continuously verifies users as conditions change, such as the location of where the user is logging in from and the time of day they are logging in. These changes in user context are important to monitor and integral to the values of zero trust.

Integrating zero trust into enterprise use cases

Zero trust networks are becoming essential to enterprise business. As enterprise workers become increasingly remote and workforce diversity expands to include contractors along with part-time and temporary workers, the security, flexibility, and scalability of cloud-delivered ZTNA will make it an important part of any network.

The practice of replacing implicit trust with identity- and context-based trust is extremely powerful, which many enterprises already recognize. An estimated 60% of businesses will embrace zero trust as a starting point for security by 2025, according to Gartner.

2x

by 2025, the number of remote workers is expected to be nearly double what it was pre-pandemic.

Future Workforce Report

Remote work access

Remote work isn't slowing down anytime soon. According to the Future Workforce Report, by 2025, the number of remote workers is expected to be nearly double what it was pre-pandemic. In the age of wireless and hybrid WAN connectivity and remote workforces, secure connectivity should be a top priority for IT teams.

A work-from-anywhere model means employees request access to sensitive information from locations with unique IP addresses to get their jobs done. Using a zero trust solution enables companies to replace these IP addresses with personified titles like "Samantha's house" to simplify configuration and management.

Widely distributed kiosks

Companies in nearly every industry use kiosks to make their services easier to access. As enterprises scale and manage thousands of geographically dispersed kiosks, network security is increasingly at risk. For example, a kiosk operating on a large, shared network segment might be monitored by a third-party consultant. If the consultant were granted access to the network, rather than a specific resource, they could move laterally and potentially compromise other resources on the network. ZTNA helps secure the network and consultant and employee access.

On-premises access

In the past, on-premises access primarily referred to large headquarters filled with employees who would connect to the company network from their cubicles. Today, an on-premises zero trust solution also refers to internally hosted LANs — or private cellular networks — that cover a variety of spaces, including manufacturing floors, classrooms, sports arenas, and more.

For these use cases, it is vital to ensure your private network edge security solution includes a zero trust strategy that can enforce custom access policies for all users and endpoints on the network.

With a proper zero trust solution in place, there is no such thing as a shared segment — only completely isolated connections between the consultant and the kiosk and the internal employee and the kiosk. The consultant and the employee are never on the same segment and are entirely blind to one another, preventing the consultant from accessing resources they are not authorized to access.

Selecting and implementing a zero trust strategy solution

Determining the scope and attributes of a zero trust network requires a closer look at what the future holds for your business — whether that means network expansion or adding IoT and mobile devices to your network.

To properly protect their networks, IT and security leaders must sift through a growing number of zero trust product and service offerings and drill down to the capabilities and use cases that best align with the needs of their business. Here are some questions for potential buyers to explore when implementing a zero trust strategy.

No. 1

What are your zero trust use cases?

Narrowing down your use case portfolio will help determine what type of solution your organization needs. For example, enterprises need to distinguish between site-to-site or remote access use cases. This could be anything from connecting IoT devices, vehicles, kiosks, retail outlets, and more. It could also mean providing secure remote access functions to internal or third-party users. Zeroing in on use cases will make a difference when looking for a solution to best fit the needs of your business.

Regarding WAN edge security, most organizational zero trust needs will fall into three primary use cases:

- Extended workforce, remote access, and "bring your own device" (BYOD)
- Privileged remote access
- On-premises access

No. 2

How will your remote access users and resources connect to the network?

When considering the location and connectivity options for users and endpoints, a ZTNA solution can be either agent-based or agentless.

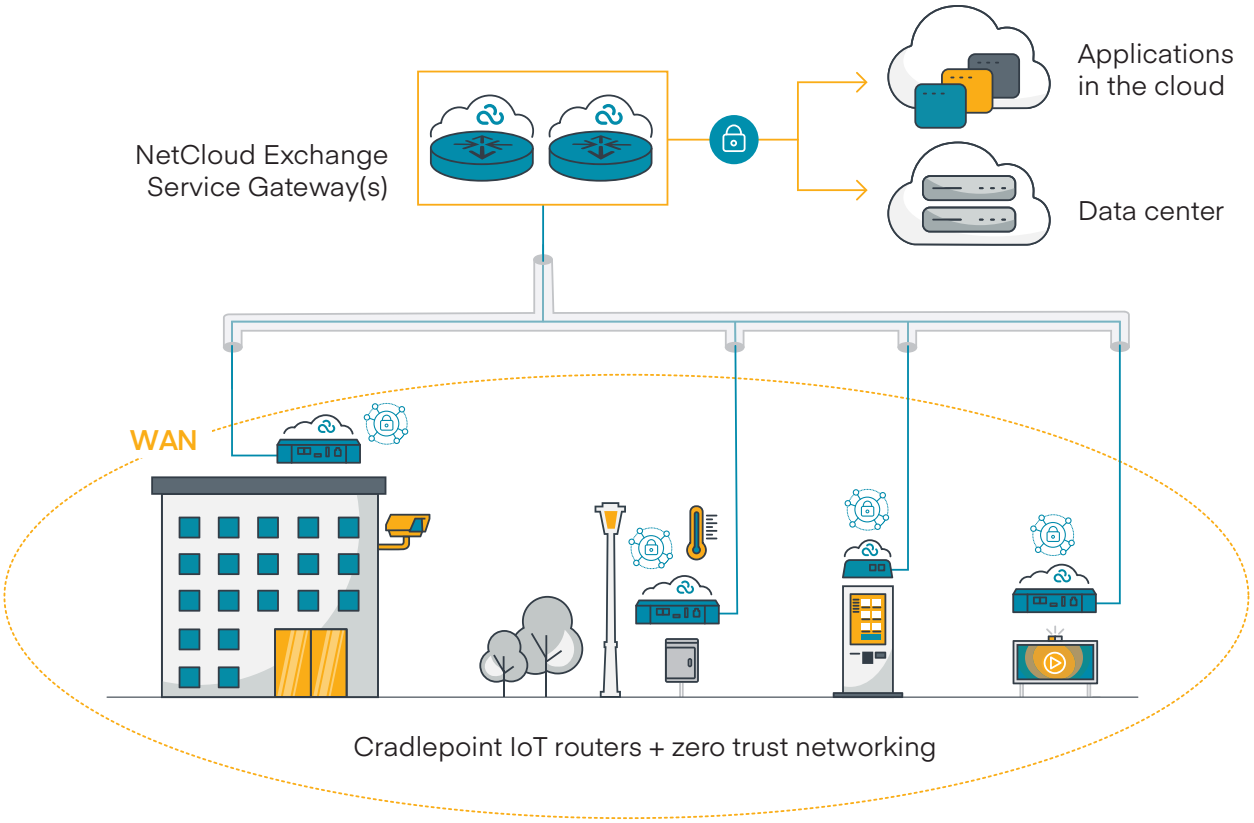
An agent-based ZTNA strategy requires that an agent be installed on every device to perform required security functions. This can lead to a lack of control over which devices and applications can take advantage of ZTNA, particularly in the instance of third-party remote access. Agent-based systems are often support-intensive and can be cost-prohibitive.

Agentless ZTNA is an agile solution and the only available option if an agent cannot be deployed to the endpoint, such as in the case of BYOD, contractor access, or remote or specialized locations. Agentless zero trust solutions rely on a web-based portal for user authentication and access, making them simple to manage from a single pane of glass.

No. 3

How will your zero trust solution be deployed and managed?

Very lean IT teams are quickly becoming the norm. With limited resources, it makes sense to look for a zero trust solution that is deployed and managed from a single pane of glass. This cuts down on training and ongoing maintenance costs and contributes to the good mental health of the IT team, as well as their available bandwidth to focus on strategic planning and other projects.



Capitalize on the agility of zero trust

Flexible deployment for a 5G or LTE solution starts with a wireless router built to complement a zero trust network. With the right products and services in place, all devices behind these routers can be protected, regardless of location, creating a platform for your enterprise to grow securely. To simplify deployment and management, a zero trust solution for Wireless WANs should:

1. Build a secure end-to-end zero trust network through a single platform, replacing cumbersome traditional VPNs.
2. Ensure features such as automation, intuitive orchestration, and name-based routing are included as part of the offering.
3. Extend secure, isolated user-to-resource access to third party contractors and IT users.
4. Provide lean IT staff with real-time visibility and control of user-based access policies and all WAN networking and security events through a single pane of glass.

Learn more at **cradlepoint.com**