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 navigating a "work from anywhere" mentality. Vast quantities of data are stored on-premises, in the cloud, and are sent across 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 malicious user connects to a site, they may be able to move laterally and compromise other prize assets on 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, especially when scaling the network, and their security is insufficient 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 foolproof 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 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. Some zero trust solutions also mask public-facing IP addresses. These security evaluations consider the following: whether a user has changed locations, when they last attempted to access an application, if they’re using a new device, the posture of that 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.

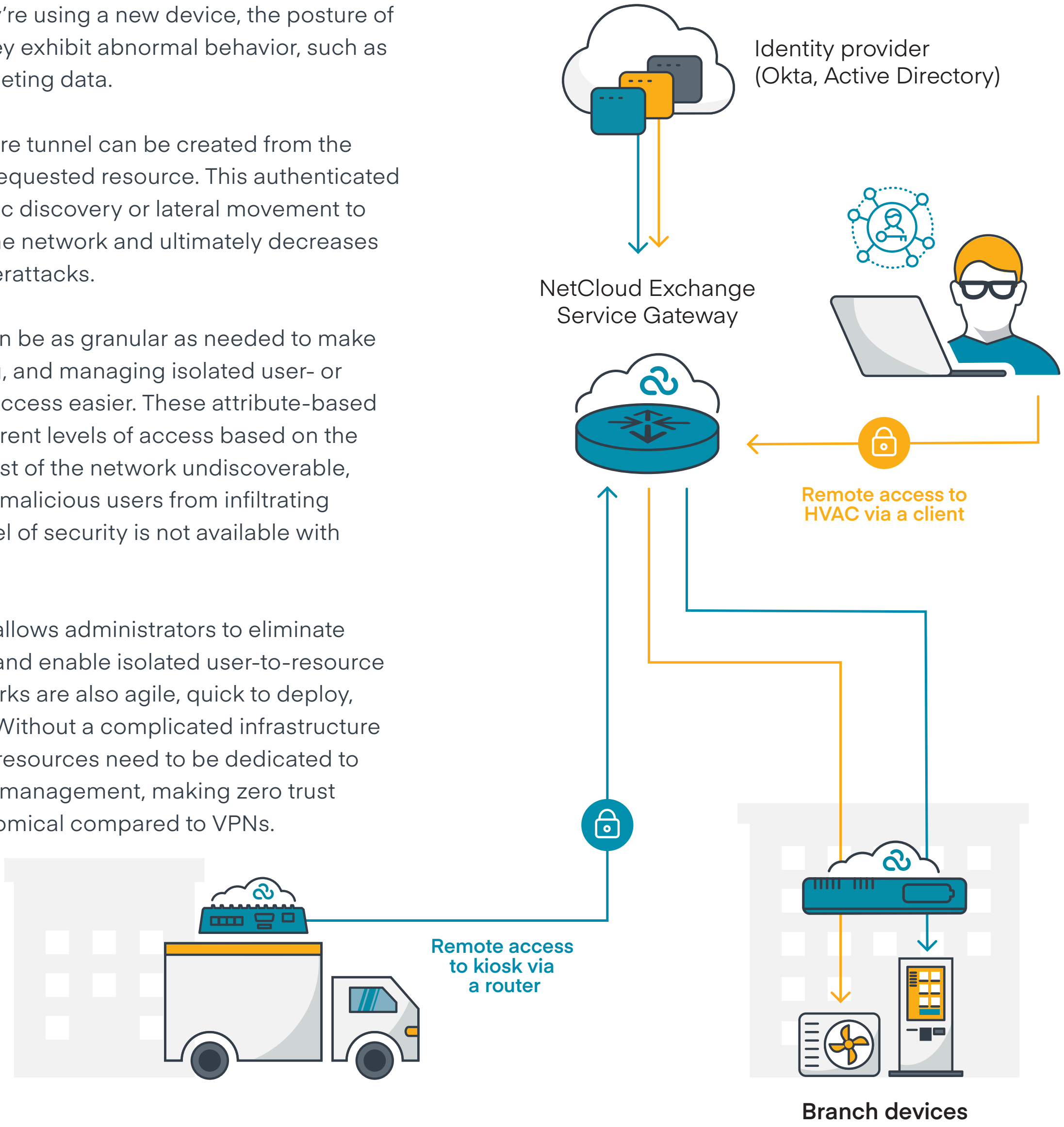
Zero trust policies can be as granular as needed to make identifying, assigning, and managing isolated user- or device-to-resource access easier. These attribute-based policies provide different levels of access based on the user and make the rest of the network undiscoverable, thus helping prevent malicious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

A zero trust solution allows administrators to 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

With the continued rise in the number of global IoT devices comes increased risks, 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 have been vulnerable when they haven't been 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 granular 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.

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

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.

Extending zero trust to web-based scenarios

No matter how many training certifications employees and contractors are put through, it's easy to mindlessly click on a malicious link or download an attachment riddled with malware. Internet-based attacks can occur during uploads, downloads, copy/paste functions, video conferences, and more. Protecting networks from these attacks requires a zero trust approach through the lens of isolation.

Using digital air gaps to protect networks

Network isolation typically refers to creating a digital air gap, where data and systems are separated, operating in distinct, self-contained environments that can't be accessed from adjacent networks. This limits the lateral movement of threats within a network, reducing the likelihood of widespread compromise.

Creating a digital air gap between a website and a user's device ensures every session operates within a secure cloud container, maintaining logical isolation. This means users engage with content solely through a virtual browser confined within the isolated cloud container and are not directly connected to the isolated application. This provides a crucial defense against web-based threats. Even if a website is compromised, the device remains protected thanks to the isolation, providing true zero trust protection.

Types of zero trust internet security

Secure web and email access

To neutralize potential threats before they reach users' devices, email and web content must be isolated using technologies such as remote browser isolation (RBI) to create a digital air gap. Website code — including sites opened from email links — is executed in an isolated virtual browser in the cloud. Then, only safe rendering data is streamed to device browsers where users can interact just as they would with native web content.

Using policy-based controls, enterprises can regulate access to specific sites or categories based on individual or group permissions. When dealing with untrusted sites, a read-only mode is enforced, thwarting any attempts by users to enter credentials.

Content disarm and reconstruct (CDR) can be deployed to inspect documents before download to eliminate any potentially malicious content. Data loss prevention (DLP) mechanisms can also be put in place to safeguard against the accidental leakage of sensitive data.

Virtual meeting security

The convenience of virtual meeting applications such as Google Meet, Zoom, and Teams does not come without challenges. Cybercriminals exploit these platforms to steal data, gain access to internal IPs, and deliver malware.

Virtual meeting isolation (VMI) is designed to tackle these issues head-on using a proactive approach that isolates meeting activities within secure cloud containers. This provides a robust defense, complete with granular control over participants' actions, restrictions on file uploads, and thorough scanning of links and uploads for potential malware and sensitive data. With VMI, organizations can enjoy the benefits of virtual collaboration without compromising on data integrity or security.

Generative AI data loss prevention

In today's work environment, isolating generative AI (GenAI) and content has become crucial, as sensitive data entered into GenAI apps can be incorporated into datasets, risking exposure to other users through future responses. Using GenAI isolation, users can engage with websites such as Bard and ChatGPT in a protected virtual browser environment. Here, stringent controls over data loss protection, data sharing, and access policies can be enforced, while user interactions maintain a completely standard appearance.

By proactively preventing the submission of sensitive information — such as proprietary data or personally identifiable information (PII)— to GenAI platforms and other applications fueling large language models, GenAI isolation significantly reduces the likelihood of exposure and potential data breaches.

Application access for unmanaged devices

Giving third-party contractors and "bring your own device" (BYOD) employees access to an enterprise network can be risky, which is why it's important to utilize web application isolation (WAI), especially for unmanaged devices. Privileged Remote Access brings applications into a secure cloud environment, granting access while maintaining security. Equipped with features like blocking file transfers, copy/paste controls, malware sanitization, and read-only mode, WAI prevents hackers from being able to attack and breach corporate web or cloud applications.

PRA is simple. No intricate device configurations, complicated setups, special browsers, or cumbersome clients are needed. Contractors can seamlessly use their standard browsers, while IT takes the reins in establishing and enforcing access policies behind the scenes.

Integrating zero trust into enterprise use cases

Zero trust networks are essential to enterprise business. As 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 zero trust will make it an important part of any network supporting offices, temporary locations, and more.

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. Beyond traditional fixed sites, zero trust solutions provide fundamental security for:

60%

of businesses will embrace zero trust by 2025

Access to work from anywhere

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

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 with employees to the company network from their cubicles. Today, an on-premises zero trust solution also refers to internally hosted LANs — or private cellular networks — covering a variety of spaces, including manufacturing floors, classrooms, sports arenas, and more.

For these use cases, it is vital to ensure your private network solution includes a zero trust strategy in which connections between consultants and devices and employees and devices are completely isolated. The consultants and employees are never on the same segment, preventing the consultant from accessing resources they are not authorized to access.

When offices, pop-ups, rural locations, and temporary sites use a mix of wired and wireless WAN connections, lean IT teams require a zero trust solution that allows them to manage all locations and scenarios from one spot.

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. 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.

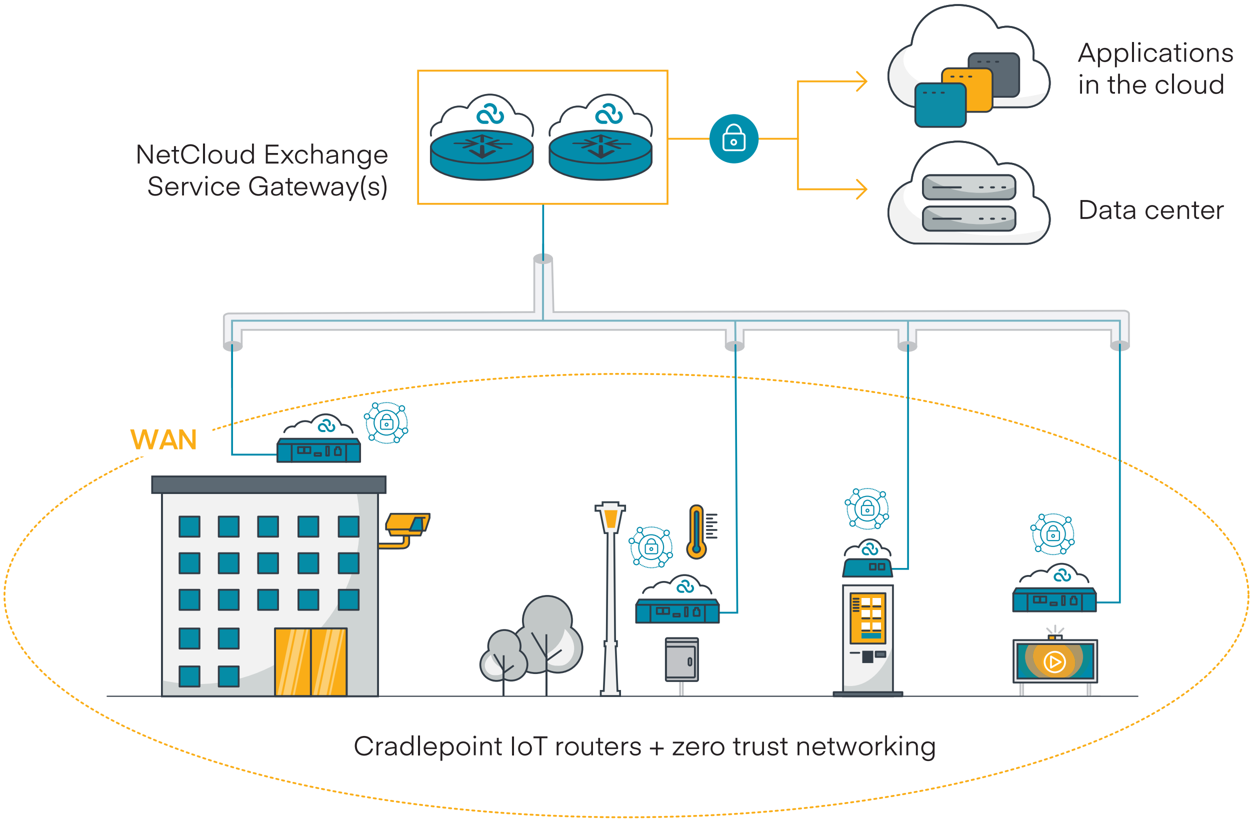
An agent-based ZTNA strategy requires that an agent be installed on every device to perform required security functions. This can lead to a lack of control over which devices and applications can take advantage of ZTNA, particularly in the instance of third-party remote access. Agent-based systems are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