OpenVPN Whitepaper

Zero Trust Network Access (ZTNA) and its Adoption

September 2022

Zero Trust Network Access (ZTNA) and its Adoption

ABSTRACT

The complexity and cost of ensuring network security and remote access for employees and key business partners can overwhelm smaller businesses. Higher cloud adoption, a distributed workforce, mobile employees, the proliferation of Internet of Things (IoT) devices, and increasingly sophisticated cyberattacks make traditional methods of ensuring secure communications across your organization overly complex and expensive. Zero Trust Network Access (ZTNA) reduces the surface area for attack by following zero trust tenets to provide access to applications. ZTNA from OpenVPN Cloud creates a private, secure overlay network for businesses, which connects all of their applications, private networks, workforce, and IoT devices together without needing to own and manage a multitude of complex and hard-to-scale security and data networking gear.

Differing Definitions of Zero Trust and ZTNA Cause Confusion

The genesis of ZTNA came from John Kindervag's original work on zero trust model while at Forrester in 2010. According to Gartner:

Zero trust network access (ZTNA) makes possible an identity- and context-based access boundary between any user and device to applications. Applications are hidden from discovery and access is restricted via a trust broker to a set of named entities. The broker dynamically verifies identity -- context for policy adherence of specified participants and devices before allowing access -- and limits lateral movement in the network.

A white paper written by the NIST* on planning for a zero trust architecture states that zero trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources. A zero trust architecture (ZTA) uses zero trust principles to plan industrial and enterprise infrastructure and workflows. Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned).

* https://csrc.nist.gov/publications/detail/white-paper/2022/05/06/planning-for-a-zero-trust-architecture/final

Zero Trust Network Access (ZTNA) and its Adoption

Some of the key zero trust tenets the white paper points to as applicable for access to resources, are:

All resource authentication and authorization are dynamic and strictly enforced before access is allowed. Dynamic enforcement means that other factors such as endpoint and environmental factors impact authentication and authorization policies.

All data sources and computing services are considered resources. All components — mobile devices, data stores, compute resources (including virtual), remote sensors/actuators, etc. — are resources and need to be considered.

All communication is secured regardless of network location. Appropriate safeguards should be in place to protect the confidentiality and integrity of data in transit.

Access to individual enterprise resources is granted on a per-session basis. In an ideal zero trust architecture, every unique operation would undergo authentication and authorization before the operation is performed. This level of granularity may not always be possible and other mitigating solutions, such as logging and backups, may be needed to detect and recover from unauthorized operations.

Zero Trust Network Access (ZTNA) and its Adoption

Access to resources is determined by dynamic policy — including the observable state of client identity, application/service, and the requesting asset — and may include other behavioral and environmental attributes. This may include meeting requirements such as client software versions, patch level, geolocation, historical request patterns, etc. Note that it may not be possible to perform all checks at the time of each access request; some policy checks may be performed on an independent schedule (e.g., daily software versioning checks).

> While a plurality of organizations think of zero trust as a strategy, 56% continue to equate it with technology — whether segmentation-centric or identity and access-focused.

According to research by ESG*, there is no universal agreement as to exactly what zero trust means and how it should be implemented. While a plurality of organizations think of zero trust as a strategy, 56% continue to equate it with technology — whether segmentation-centric or identity and access-focused.

* ESG, a division of TechTarget, is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community. ESG surveyed 421 IT and cybersecurity professionals at organizations in North America (US and Canada) personally responsible for driving zero-trust security strategies and evaluating, purchasing, and managing security technology products and services in support of these initiatives and published their findings in a Research Report: The State of Zero-trust Security Strategies, April 12, 2021.

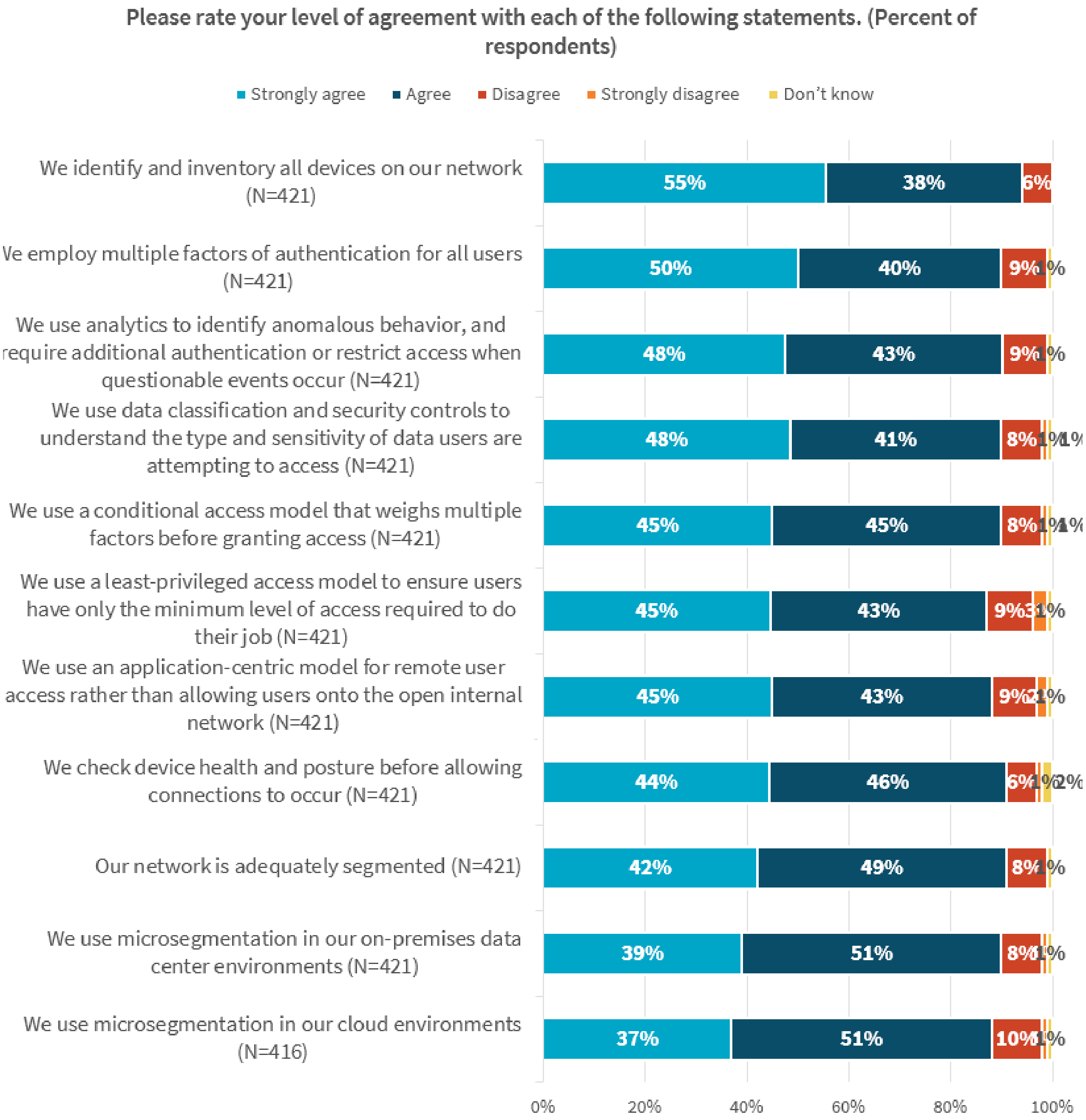
Important Aspects of Zero Trust are Less Likely to be Implemented

The same ESG study indicates that more than half of respondents strongly agree that their organizations identify and inventory all devices on the network and employ multiple factors of authentication for all users. However, other important aspects of zero trust, such as least privilege, conditional access, application-centric access, and analysis of device health and posture, are slightly less likely to be in place. The result is that, as far as zero trust has come in awareness and adoption, many organizations still have far to go in applying it pervasively across the enterprise.

> Implementing Zero Trust for a specific use case is the starting point for many

While nearly all respondents that ESG surveyed at organizations have begun to implement zero trust say they have a formalized, documented strategy that guides their cybersecurity program at least some of the time, this does not mean that such a strategy started the initiative. Indeed, many (53% and 50%, respectively) indicate that zero trust began with a specific use case and/or that a strategy was built around tools already in place in the environment. So, while critical to longer-term success with zero trust, a broad, formalized strategy is not required to begin. The breadth of technologies required, the number of teams with input into strategy creation and decision making, and potential complexity as the initiative is broadened all contribute to some organizations deciding to maintain a more focused approach to zero trust.

Important Aspects of Zero Trust are Less Likely to be Implemented



ZTNA Using OpenVPN Cloud

OpenVPN Cloud offers businesses a cloud-delivered service that integrates virtual networking with essential Secure Access Service Edge (SASE) capabilities such as firewall-as-a-service (FWaaS), intrusion detection and prevention system (IDS/IPS), DNS-based content filtering, and zero trust network access (ZTNA). Using OpenVPN Cloud, businesses can easily deploy and manage a secure overlay network that connects together all of their applications, private networks, workforce, and IoT devices without owning and managing a multitude of complex and hard-to-scale security and data networking gear. OpenVPN Cloud can be accessed from more than 30 worldwide locations.

We can see from ESG research that ZTNA could mean different things to different policymakers. The ZTNA policies can be made very complex and a variety of different tools can be leveraged to provide authentication and authorization context for these policies. OpenVPN Cloud keeps things simple and focuses on the three main aspects of ZTNA:

Application access isolated from network access: OpenVPN Cloud hides all applications from public view and discovery by allowing you to continue hosting applications on your private networks and avoid exposing them to the internet. All users, whether remote or on-site, need to authenticate and connect to one of the 30+ worldwide PoPs OpenVPN provides to even have the opportunity to use the applications. On connection, even authenticated users do not get access to the whole private network. In fact, our solution does not even need the IP address subnets of your connected private networks to use for routing. None of your private networks' IP address subnet ranges are exposed as routes to the connecting devices, thus the notion of lateral movement is completely eliminated.

ZTNA Using OpenVPN Cloud

Identity-based least privilege access control: All applications, not just web apps, can be configured using the domain name of the application or service. Additionally, a firewall can be applied around the application to allow only specific application protocol access. Once the applications are configured, least privilege access can be provided to them based on the identity of the user and the user's membership to a specific Group or Role.

Continuous authentication and authorization: Authentication takes place during every connection attempt to OpenVPN Cloud. Zero trust access policy enforcement is continuous. Any change in the access policy is enforced in near real-time.

In addition to the above, OpenVPN Cloud provides many features that differentiates it from other ZTNA offerings:

Bi-directional Accessibility Most ZTNA solutions only allow for devices to access network resources. IT apps (for example, software update server) on the network cannot initiate communication to devices. That is not the case with OpenVPN Cloud. It supports these network-initiated flows and can also apply policies around it.

Restricted Internet Access General internet access from special purpose connected devices or users can be restricted. This locks down the device and allows it to only reach a set of authorized private and trusted public destinations.

ZTNA Using OpenVPN Cloud

ZTNA for IoT IoT devices can authenticate using digital certificates and get access to applications based on identity-aware policies.

ZTNA for Server to Server communications or API communications Servers and other API originators or endpoints can be given a unique identity and, therefore, identity-based access policies.

ZTNA Between Sites Typically, ZTNA is about providing users access to applications. But what if all devices on a network need access to applications hosted on a different network? OpenVPN Cloud can do that, too. For example, a network at a Branch location can get access to only authorized applications hosted at the Headquarters.

Automatic Network Segmentation Accessing applications using their domain names is ideal, but if access is needed using destination IP addresses, OpenVPN Cloud automatically segments the routes to those IP addresses based on the requesting entity's identity and access controls.

Access to Applications Hosted on Networks with Overlapping IP Address Subnets Acquisition of another company or use of multiple IaaS providers brings with it the challenge of connecting to networks that might use the same IP address subnets. Even with networks whose IP addresses overlap, OpenVPN Cloud provides access using patent-pending application name domain routing.

ZTNA Using OpenVPN Cloud

Protection of Access to SaaS Apps OpenVPN Cloud secures SaaS application access by tunneling traffic to those application domain names via a customer-owned internet gateway while allowing other internet traffic to use local direct internet access. An additional layer of protection is added by restricting SaaS login access to the IP address of the internet gateway.

Peer-to-Peer Communications Enforces policies that determine whether a group of devices can communicate with each other or another group of devices directly.

Self-service Scaling Immediate, on-demand scaling, up or down, of the number of connections needed for ZTNA.

Get Started

We make getting started with OpenVPN Cloud as easy as possible by offering three free connections. Follow the steps below to create an account, use your free connections as long as you like, then scale from free to paid when you're ready. Our Technical Support team is available 24/7 to guide you through every step of set-up and configuration and answer any questions you may have.

- ✓ Create an OpenVPN Cloud account, and select an identity for your Cloud (for example, cyberone).
- ✓ Go to the Shield section, and turn ON blocking of dangerous and unwanted categories.
- ✓ Download and launch the OpenVPN Connect app.
- ✓ Add a profile in the Connect app by using your OpenVPN Cloud URL (for example, cyberone.openvpn.com), authenticate, and select a Region to connect.

Have any questions? Feel free to contact us at: sales@openvpn.net