SOPHOS
Cybersecurity delivered.

Why ZTNA Matters: The future of secure networks

ZTNA secures remote access, defends against ransomware

A Sophos Whitepaper. February 2022

When it comes to cybersecurity, it all comes down to risk and trust. Do you trust the user who just logged on to the network, or the one who is trying to access the corporate applications? How about the email that appears to be from your business partner but includes requests that seem unusual, perhaps indicating a business email compromise attack. Trust but verify became a popular slogan in the 1980s, but today the pendulum has moved to Never Trust; Verify Everything.

The zero-trust model requires that anyone on the network must be authenticated in order to gain access, but that is not all. Any attempt to access a network resource, such as a server, application or data, requires the device or application used to access the resource must also be validated for compliance, then reauthenticated and validated each time a new request is made.

From a cybersecurity standpoint, trust is earned, not given. Each time the user, device and application attempt an action on the network is made, the authentication process must be run again.

What is ZTNA?

Zero Trust Network Access (ZTNA) is founded on the principle of zero trust or "trust nothing, verify everything." This provides significantly better security by effectively treating each user, device and application like their own perimeter on their own micro-segment of the network and constantly assessing and verifying identity and health to obtain access to corporate applications and data. Users only have access to applications and data defined explicitly by their policies, reducing lateral movement and the risks that come with it.

Ransomware victims have much greater familiarity with the ZTNA approach, likely driven by their desire to prevent a subsequent attack. We will go into details on that and a look at how Sophos users view and use ZTNA technology a bit later in this document.

ZTNA is a fundamental component of a Secure Access Service Edge (SASE) security framework that describes how network and cloud security are converging into a single, cloud-delivered platform. SASE, first described by Gartner in 2019, essentially is a merger of traditional wide-area network (WAN) management and security capabilities using cloud-native architectures. In addition to ZTNA, the SASE architecture includes cloud-access security brokers, firewall-as-a-service, intrusion prevention systems and secure access gateways.

Cloud management offers tremendous benefits from being able to be up and running instantly, to reduced management infrastructure, to deployment and enrollment, and enable access anywhere. One of the key advantages of cloud management is being able to log in and begin instantly, without adding additional management servers or infrastructure. Cloud management also offers instant secure access from anywhere on any device, supporting the way you want to work. It also makes it easy to enroll new users wherever they happen to be in the world.

Implementing ZTNA, however, is a crucial component to improve security for remote users and a significant security upgrade in a pandemic-driven, remote-user network environment, as well as protecting the corporate network from malware and ransomware attacks.

Deconstructing the VPN threat

As horrible as the pandemic has been on a human level, it has had an unexpected but significant benefit to improving remote access: the deployment of ZTNA as a replacement for the vulnerable VPN. The pandemic forced millions of workers to move out of the friendly confines of their corporate network and work from home, creating millions of vulnerable, new endpoints, often outside the control of the corporate IT staff.

These endpoints are ripe targets for attackers, since a sizable percentage might not have corporate-class endpoint protections. Additionally, the millions of newly minted remote users created a huge burden on corporate VPNs that often had not been tasked with such heavy workloads.

ZTNA delivers on the principles of zero trust while replacing problematic VPNs, a traditional approach for connecting remote users to the corporate network. Technologically, VPNs have three serious drawbacks for today's largely remote workforce.

First, VPNs are not designed to scale to meet the demands of large enterprises with a comparatively substantial number of remote employees. Second, VPN client software, which often is old, neglected and complicated that makes them potential targets for attackers. VPNs also tend to have security vulnerabilities since they were designed to use the traditional username/password approach to security. Finally, users who access networks using VPNs effectively have the run of the network once they connect, much like a workstation inside the perimeter firewall. Depending on the internal network controls, this could be problematic.

Let us look at each of these issues and how ZTNA addresses them.

VPNs do not scale well. Among the limitations are the maximum bandwidth of VPNs, which are often limited to 1Gbps, exposed ports that can be exploited, potential man-in-the-middle attacks, and over-privileged access. Additionally, VPNs are designed VPN's user volume handle a specific amount of volume from remote users and cannot scale up or down dynamically. Should the volume be too high, for example, some users would not be able to access the VPN until others dropped off.

Second, the U.S. National Security Agency cited VPN vulnerabilities in several cybersecurity advisories over the years and in 2019, the Canadian Centre for Cyber Security released guidance that said three popular VPN products had multiple indicators of compromise for detecting malicious activities. These included credential resets and vulnerable proprietary SSL and TLS VPN protocols.

Finally, VPNs provide no filter when dropping a user on to a network. Essentially, the user has all the privileges as if they were a workstation behind the corporate firewall.

One can reduce the threat of remote access tools providing an attacker the ability to move about a network in two ways: First, require every entry onto the network to authenticate the user, device and software only to a specific, micro-segment of the network. Even if the attacker successfully gains access, movement is limited. Second, significantly restrict privileges of anyone on the network. If the attacker cannot see the network due to limited privileges, they cannot traverse it.

According to The Forrester NewWave: Zero Trust Network Access, Q3 2021, "With ZTNA, users can access on-premises applications using Zero Trust principles while allowing their two-way video conference traffic to go directly out to the internet, thereby improving security posture and employee experience," the report states. "Ultimately, ZTNA reduces the need for employee VPNs and makes way for infrastructure and security teams to adopt cloud-delivered networking and security capabilities."

The Zen of ZTNA

From a corporate governance perspective, managing who is on the network and what they are doing are among the key corporate concerns. Having policies and procedures that determine how a company operates and solid, ethical business practices that lead to financial viability are the purpose for the corporate governance function. One could have bad actors mucking around the network, compromising or stealing confidential data, installing ransomware and other malware programs, or simply sitting in stealth mode waiting for a more opportune time to attack. This not only could violate compliance regulations and cost the company substantial amounts of money, but it can reduce the market value of a company significantly.

Deploying a zero-trust network model in general and ZTNA specifically not only can identify intruders on the network, malicious and benign applications, and users that do not belong, and significantly reduce the attack surface of a corporate network, further improving the company's overall risk profile.

When users access the corporate network equipped with ZTNA, devices access the network resources on their own micro-segmented perimeter that is constantly validated and verified. With zero trust, users are no longer "on the corporate network" per se with all the implied trust and access that usually comes with it. Rather, they have access only to those portions of the network for which they and their devices have been authenticated. That is not the case with legacy VPN connections.

In a traditional network where corporate firewalls keep attackers out, but few defenses are in place once a user's credentials are accepted, attackers can move freely, looking for elevated credentials that allows them to access more secure parts of the network seeing data to steal, copy, corrupt or encrypt for a ransom.

Implementing a zero-trust infrastructure not only makes credential theft less valuable, the corporate firewall becomes only the first of many defenses to data and applications. Even if a work-from-home employee's computer is breached, the user's credentials would not be sufficient once the attacker accessed the greater corporate network.

Instead, the ZTNA approach only gives them access to a limited portion of the network. This assumes they had the credentials to authenticate themselves, the device and software for an approved application or data.

Overcoming ransomware

According to the Sophos The State of Ransomware 2021 report, 37% of respondents suffered a ransomware attack in the prior year, with 54% of them saying the cybercriminals succeeded in encrypting their data. From a data loss perspective, there was good news as 96% of respondents said they got at least some of their data back. However, the bad news is that paying the ransom rarely gets all your data back: on average, only 65% of the encrypted data was restored after the ransom was paid.

The average ransom paid by mid-sized organizations in 2020 was US$170,404, the report noted. However, this is just part of the overall remediation bill. The average cost to rectify the impacts of the most recent ransomware attack (including downtime, people time, device cost, network cost, lost opportunity, ransom paid and other costs) was US$1.85 million, more than double the US$761,106 cost reported in 2020.

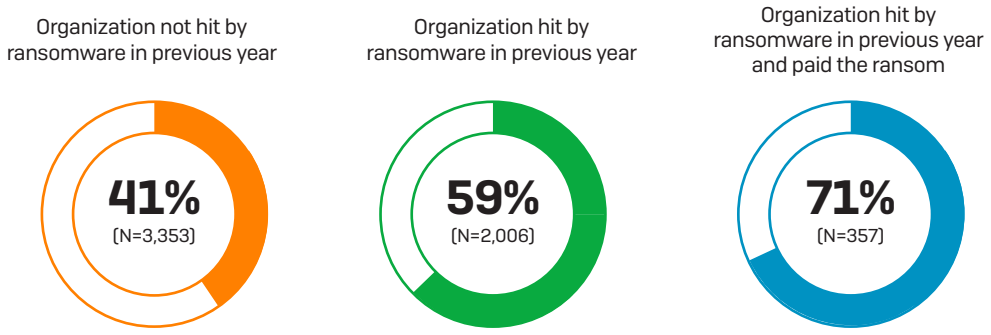
In a recent survey of 5,400 IT professionals worldwide conducted by Vanson Bourne and underwritten by Sophos, 20% of respondents said they already have implemented a zero-trust approach, with another 41% saying they have already begun implementing zero trust and expect to have it completed by early 2022. An additional 20% indicate the expect to be done by early 2023.

ZTNA solutions eliminate a common vector of attack for ransomware and other network infiltration attacks. Since ZTNA users are no longer 'on the network' but rather are on a micro-segment of the corporate network, threats that might otherwise get a foothold through a VPN have nowhere to go with ZTNA.

Ransomware attacks drive ZTNA adoption

The survey shows that IT professionals in organizations that had been hit by ransomware in the previous year are almost 50% more likely be 'very familiar' with the ZTNA approach than those whose organizations had not experienced an incident (59% vs 39%). This rises to 71% among those whose organizations had been hit and they paid the ransom.

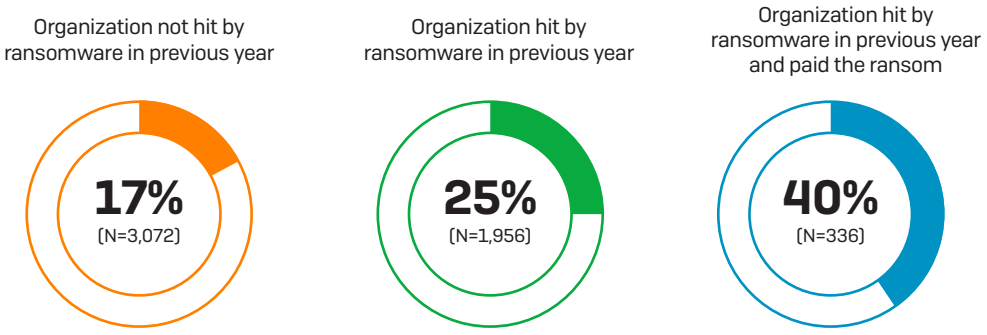
Percentage of respondents that consider themselved 'Very familiar' with the Zero Trust Network Access (ZTNA) approch



Further illustrating this point, just 10% of ransomware victims have little or no familiarity with ZTNA, compared with 21% of those whose organization has not fallen victim.

The survey also showed that ransomware victims are more advanced in their zero trust adoption. One quarter (25%) of those whose organization experienced a ransomware attack in the previous year have already fully adopted a zero-trust approach, rising to a full 40% of those whose organizations were hit and paid the ransom. In comparison, just one in six (17%) of those that had not experienced an attack have already fully migrated to this approach.

Percentage of respondents whose organizations have alredy adopted a zero trust approch



Additionally, ransomware victims have different motivations for adopting ZTNA.

- Respondents were asked about their motivations for adopting a zero-trust approach and, while there were several commonalities, there were also clear areas of difference To improve our overall cybersecurity posture' was the most common motivator among both victims and non-victims
- The second most common motivator among ransomware victims was the desire to 'simplify our cybersecurity operations' (43%), potentially reflecting that complex security had contributed to their previous attack
- Ransomware victims were also much more likely to say that 'to move from a CAPEX to an OPEX model´ was one of the main factors behind their adoption of a zero-trust approach (27% vs. 16%, and rising to 34% among those that had been hit by ransomware and paid the ransom)
- Ransomware victims are also heavily motivated by 'supporting our move to increased use of the cloud' (42%). This dropped to 30% among those that had not experienced a recent attack

Looking forward

The benefits of a zero-trust environment can be difficult to explain to senior management and shareholders, in that it can be challenging to prove an attack was unsuccessful or simply never occurred because the attacker was stopped before they could deposit their malware. That said, it is possible to demonstrate that zero trust significantly reduces risk and reduced risk can be monetized by the enterprise.

Reducing corporate risk, for example, can lead to lower premium costs and better terms for cyber insurance and potentially to higher valuation for a company. Cyber insurance brokers and carriers recognize that lower risk leads to fewer claims, leading to fewer and lower insurance payouts. As a result, the cyber insurance industry is currently reevaluating and modifying its terms and conditions for writing such policies, offering better terms for companies that proactively reduce their risk.

In the U.S. Presidential Executive Order on Improving the Nation's Cybersecurity issued by President Joseph Biden in May 2021, the order states that federal government "must adopt security best practices [and] advance toward Zero Trust Architecture…." Adoption of a zero-trust model by the nation's largest employer underscores the recognition that this approach is seen as the way forward to reduce risk.

Gartner agrees that zero trust is the cybersecurity path for the future. "Both for large enterprises who are part-way through their could journey and those who are just getting started, protecting data has to be a top priority," the company said. According to Gartner, 82% of companies plan to let their employees work remotely for some time. "As companies start to incorporate remote workers into their long-term plans, security has become a priority. However, many companies are beginning to realize their traditional approaches to security are not suitable for the cloud-native remote workforce," Gartner wrote.

Forrester also agrees, noting that zero trust secures resources rather than the physical network. "In its simplest forms, the zero trust model shifts focus from various types of authentication and access controls to tailed controls around sensitive data stores, applications, systems and networks," Forrester wrote. "These controls leverage identities, commission/decommission users and broker their access based on defined roles."

If the future is zero trust, then it all begins with controlling who is on the network, what they can access and how. That is the *raison d'être* of ZTNA and why it is critical to the future of cybersecurity.

Learn more at
sophos.com/ztna

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North America Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

22-02-06 EN (MP)