How Does Zero Trust Network Access Increase Your Cyber Security

328 S. Jefferson St., Suite 603,
Chicago, IL 60661
312.753.7880
info@CloudSourceServices.com
www.cloudsourceservices.com

Today's businesses need all the tools like zero trust network access (ZTNA) you can find to increase your cyber security. Why? Experts expect the total worldwide damage from cyber crime in 2021 to total $6 trillion. That means that if cyber crime were a country, it would be the third-largest economy right behind the U.S. and China.[1]

Defeating an enemy that powerful is a challenge every company faces, with no exception. Cyber criminals are attacking businesses of all sizes and in all industries – and the problem is just getting worse. Since the pandemic sent workers home, they needed access to business systems, and the digitization of the business environment has exploded. Experts say that cyber crime skyrocketed 600% during the pandemic,[2] and there's no indication that it will slow down.

Protecting your company's network using zero trust network access will give you an advantage over the cyber criminals. ZTNA gives you cyber security scalability and flexibility, and an effective way to protect your network that you can't find in frequently used network access technology like virtual private networks (VPNs).

With today's technology, there is no perimeter because your data is in public and private clouds, on your premises, or in a data center. Using ZTNA, you have a way to protect your network regardless of where your data is stored or how the user is accessing it.

ZERO TRUST NETWORK ACCESS: AN OVERVIEW

Traditionally, cyber security was heavily focused on protecting a network's perimeter. It made sense since everyone was working in the office and accessing company data using endpoints that were located in the office. If a cyber criminal wanted to break into your servers, they'd need to find a way in through one of those endpoints.

Today, however, there really isn't a defined perimeter in most networks. Data and applications that your business needs to continue operating can be located anywhere, and the users who need access can use a variety of devices and a range of access methods.

You can't afford to allow access only through your company network if you want to be competitive in today's digital culture. You need to switch to a strategy that restricts access to your data and applications, rather than one that is focused on securing your network's perimeter.

To understand zero trust, it's easiest to start by describing the way things work in a network that is not zero trust. In standard network access procedures, once a user has been verified as an authorized user of the network, that user can access anything connected to the network. As you can see, that approach puts a lot of trust in the user and gives them a great deal of power, whether the user is an employee or a cyber criminal.

The principle behind a ZTNA approach is to not trust a user with any access other than the minimum they need to do their jobs. A ZTNA approach authenticates the user, their device, and the context of the request for access before allowing the user to access an application or service. The technology also monitors users and devices for changes. If changes occur, the ZTNA will adjust the access allowed.

ZTNA technology also gives you the ability to define application access very specifically in situations where a user needs access to part of an application rather than the entire thing. This is another way that ZTNA improves your cyber security.

ZTNA PROVIDES THE SAME SECURITY FOR EVERYONE, EVERYWHERE

Since networks are so crucial to your business, they need to give your users easy access that doesn't reduce productivity. Unfortunately, that's not always possible when different products are used to control access to different systems.

An employee must learn the different protocols for accessing systems depending on whether the application they need is running in the cloud or on-premises. There may even be differences depending on whether the user is working from the office or from home. This approach typically causes confusion, reduces security, frustrates your employees, slows down workflow, and reduces productivity.

You don't want to force your users to use one access approach if they're in the office, and different protocols if they are working from home, in a coffee shop, or on the road. You also want to avoid having different network procedures for your on-premise systems and your cloud systems.

ZTNA solves these problems by providing a single centralized controller that applies the same security for everyone, regardless of their location or the system they need to access. It's a security-driven approach that addresses the need for exceptional cyber security to ward off attacks by cyber criminals. Security solutions must be integrated with the network to avoid gaps that can create vulnerabilities hackers easily find and exploit.

When you use one approach for network access, you also simplify work for your IT team. The team doesn't need to use different dashboards or track different policies for multiple types of access. They can configure one type of access technology, which typically reduces the possibility of errors. It's also much easier to troubleshoot when problems arise. The team will have complete visibility into the transactions the network is handling to make spotting and fixing problems faster and easier.

DOES YOUR BUSINESS NEED ZERO TRUST NETWORK ACCESS?

There are a number of trends that are moving many leaders to take advantage of ZTNA. In a recent global survey, it was found that 72% of respondents either had plans to implement ZTNA or had already adopted it.[3] This is a trend that experts see as continuing.

Businesses are concerned about the complexity of configuring VPNs for remote users. In addition, a VPN gives a user access to a part of your network. With that access, a hacker can search the network to find opportunities for staging an attack, typically called a lateral network attack surface. VPNs also can't give you an opportunity to reduce your vulnerability to attack by segmenting applications.

Given the state of world politics and the increase in cyber threats, the U.S. federal government has taken steps to improve security by moving to ZTNA. A recent Office of Management and Budget (OMB) report indicates that the government can't depend on perimeter-based cyber security technology to protect critical applications and data. The OMB is requiring federal agencies to implement zero-trust strategies.[4]

Many organizations have been working to improve cyber security by upgrading their approach to identity management. Businesses have been putting systems such as access management and multi-factor authentication in place. As one of the foundations of zero-trust strategies, this trend is taking leaders to the next step, which is ZTNA. The pandemic also prompted many businesses to look at technologies such as microsegmentation to improve the security of their local networks.

In the face of all these trends, it's difficult to think of good reasons not to move to ZTNA.

FINAL THOUGHTS

The world of cyber security is continuing to evolve, but some things won't change.

- Cyber threats will continue to increase.
- Being hit by a cyber attack will continue to be debilitating and costly.
- Hackers will continue to get better at finding and exploiting vulnerabilities.
- The challenge of supporting remote workers will continue because the hybrid workforce is becoming more entrenched as the workforce of the future.
- Applications will continue to move to the cloud.
- Network perimeters will continue to disappear.

There are many benefits to switching to ZTNA, some of the most important benefits are:

- You'll have protection against low-level and advanced cyber threats.
- You'll do a better job of supporting remote workers without impacting their productivity.
- You'll reduce your risk by closing gaps and controlling lateral access on your network.

- You'll have protection for your applications and data, whether it's in the cloud, in multiple clouds, or in some combination of clouds, on-premises, and in data centers.
- Your IT team will have tools to manage your network centrally.

Contact us to learn more about ZTNA or to get started with these leading-edge cyber security solutions that meet today's challenges.

SOURCES

1. https://cybersecurityventures.com/cybersecurity-almanac-2022/
2. https://www.cloudwards.net/cyber-security-statistics/
3. https://www.statista.com/statistics/1228254/zero-trust-it-model-adoption/
4. https://www.cnbc.com/2022/03/01/why-companies-are-moving-to-a-zero-trust-model-of-cyber-security-.html

328 S. Jefferson St., Suite 603, Chicago, IL 60661
312.753.7880 | info@CloudSourceServices.com
www.cloudsourceservices.com

Cloud
Source