zscaler™

White Paper

Why IT Leaders Should Consider a Zero Trust Network Access Strategy

Enabling digital business while protecting data

While technology has long been considered an engine necessary to keep the business moving forward, it is now recognized as a true business driver, capable of creating new efficiencies and revenue opportunities. Similarly, the role of the IT leader has evolved, with CISOs, CIOs, and CTOs joining the executive suite to focus on and lead technology initiatives.

The major factors in this shift have been the explosion of enterprise public cloud adoption, including Azure, AWS, and Google Cloud, and the widespread use of employee-owned (BYOD) mobile devices for work. Companies are leveraging these technologies to optimize business processes and deliver products and services more quickly and at a lower overall cost.

But what about the risk that they introduce?

Because of the shift toward cloud and user mobility, the traditional security perimeter that once protected users and internal services within the corporate network is gone.

Because of this, when asking for a budget for new IT to support cloud and mobility, they must help the boardroom see the connection between risk and its potential impact on the businesses' revenue. They need to effectively communicate the cost of a data breach, the cost of downtime of critical infrastructure, and the cost of loss of brand reputation. In essence, IT must drive a business–value conversation that execs will understand.

IT leaders should start by first understanding their company's risk portfolio and determine how risk averse their business is. Their business–critical apps may be SOC1 or ISO 27001 compliant and require additional layers of security. These are considered critical infrastructure. There may be certain countries, such as China, that must be isolated from other countries. With legacy infrastructure needing continuous evaluation for patches, one missed firewall configuration could mean big problems for the business.

The Challenges Technology Leaders Must Overcome

When it comes down to it, in order to enable key business initiatives and bridge the gap between business needs and IT capabilities, IT leaders must choose technology that helps them overcome their challenges and allows them to:

1. Make it easy to get work done and minimize stress for your workforce
2. Deliver a superior user experience for employees and third parties
3. Reduce the risks that can threaten productivity, IP, and the company's reputation
4. Be adaptive and agile to empower a dynamically changing business
5. Accelerate digital transformation through the adoption of the public cloud

Identifying the technologies that will achieve these goals is a difficult task as, at times, the desired outcomes of one solution may add complexity to another. For example, the decision to adopt cloud services and mobile technologies achieves the goal of a streamlined user experience, but what about the goal of minimizing the risk of a cybersecurity attack? IT leaders must strike a careful balance between accelerating the adoption of new technologies and ensuring the security of sensitive data. Therefore, choosing the right technology at the right time is critical.

The value of ZTNA for the business

Gartner recommends that IT leaders adopt ZTNA as part of a security service edge (SSE) strategy to provide flexible, secure hybrid workforce connectivity. ZTNA services provide secure access to private enterprise applications for remote and in-office users without the need for traditional VPN technologies.

ZTNA services create an identity and context-based, logical-access boundary around an application or set of applications. The applications are hidden from discovery, and access is restricted via a trust broker to a set of named entities. The broker verifies the user identity, context, and policy adherence of the specified participants before brokering the connection. This removes the application assets from being visible to the Internet and significantly reduces the surface area for an attack.

Gartner

By 2025, at least 70% of new remote access deployments will be served predominantly by ZTNA as opposed to VPN services—up from less than 10% at the end of 2021.

Earlier, we discussed the five key factors that IT leaders must consider when adopting new technologies. Let's take a look at how ZTNA plays a role in enabling each:

1. Improved productivity:

Three out of four in-office, full-time employees are **planning to quit this year,** adding to the tens of millions who have already made the switch during the pandemic-driven Great Resignation. With the mass reshuffling of the workforce, employers are rethinking how to retain and attract talent, and IT leaders can use technology to help stop the bleeding while laying the groundwork for the future of work. ZTNA's ease-of-use offers significant benefits to users since it eliminates the headache of launching a VPN client every time the user logs into the network, keeping productivity high and frustration to a minimum. The simplicity of cloud-delivered, software-only ZTNA makes it easy to set up and deploy. This simplicity allows IT to adopt secure—even on mobile devices—cloud-application technology while maximizing productivity for the IT staff and the entire organization.

2. Provide superior user experiences:

Today, users are working from anywhere: in-office, at home, and even on the road. These users are often a mix of employees and third parties, both of which expect frictionless access to applications regardless of their device, location or network. ZTNA ensures that each user has a fast and completely seamless experience. It also eliminates the need for a VPN and inconvenient log-ins while supporting third-party users and all device types without the need for an endpoint agent.

Moreover, clientless ZTNA leveraging policy-based access to private apps increases productivity as users can connect to applications from any device, regardless of location.

3. Reduce risk:

Security remains a concern for cloud adoption and remote work as they can increase the probability of an attack against business-critical apps and infrastructure if not handled with care. Traditional, network-centric technologies such as VPNs and firewalls are excessively trusting and should be avoided. These solutions place remote users directly onto the network, which requires VPN servers to listen for inbound calls from the Internet. This is why VPNs have become a trojan horse for ransomware. This means that whether remote or local, the user has lateral access across the network. This is the case with both employees and third parties who could have weaker security practices. ZTNA services use zero trust-based policies to provide only authorized users (based on identity and device posture) connectivity to specific private apps running in a public cloud, private cloud, or datacenter. The recent evolution of ZTNA from primarily providing connectivity to fully integrated security to protect applications against insider threats and advanced attackers helps organizations improve their overall security posture.

4. Cloud-delivered agility and scale:

Today, the amount of employees, user devices, applications, and traffic continues to grow. Cloud-delivered ZTNA services are hosted by the vendor, so increasing scale is no longer a concern for IT. As demand increases, the ZTNA service handles the additional load automatically. There is no need to deploy additional hardware or virtualized firewalls, which will slow down public cloud adoption projects. More agility and more scale are critical to an IT leader's success, and ZTNA provides this.

5. Accelerate digital transformation:

Today, cloud and mobility are priorities for the majority of enterprise teams. However, with the wrong solutions in place, it can take months or even years to leverage the cloud securely across a global user base. This is partially due to the complexity involved in using traditional network and security technology to provide access to cloud apps from unmanaged user devices. ZTNA uses software to reduce complexity, thereby reducing implementation time from months, or years, to just hours. With ZTNA, organizations can quickly reap the benefits of the cloud and improved mobility.

> “With the changes we’ve made on our journey to the cloud, I’m confident we’ll be in a strong position to handle whatever comes along. In the end, this experience will have a long-lasting impact and will ultimately change legacy mindsets. We are opening eyes to new ways of working while showing the impact of technology and the resilience and creativity of our workforce.”
>
> — **Alex Philips,** Chief Information Officer, National Oilwell & Varco

Learn more about ZTNA

Zero trust network access services are a valuable tool for enterprise IT leaders. At Zscaler, we have developed a ZTNA service called Zscaler Private Access (ZPA). The service uses our global cloud to provide seamless, secure access to internal applications. Exactly what’s needed to help IT go from “cost center” to boardroom hero.

Be sure to check out Paychex’s story from Carlos Cong, Sr. Manager, Enterprise Technology Services, as they simplified and accelerated their M&A IT integrations with ZTNA.

Watch CMA-CGN’s Story

Have your team take a free 7-day test drive of Zscaler’s ZTNA solution.

Start a 7-day ZTNA Demo

Have additional questions? Feel free to reach out directly to our ZTNA experts at **sales@zscaler.com.**

zscaler™ | Experience your world, secured.™

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world’s largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com