

Why IT leaders  
should consider  
a zero trust network  
access strategy



## Enabling business while also 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, capabilities, and revenue opportunities as well. The role of the IT leader has similarly evolved, with CISOs, CIOs, and CTOs now part of the executive suite due to a new strategic focus on technology.

The major factors in this shift have been the explosion of enterprise public cloud adoption, including Azure and AWS, 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 mobility, the traditional security perimeter that once protected users and internal services within the corporate network is to a large extent gone.

Because of this, when asking for 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 if critical infrastructure and the cost of loss of reputation. In essence, have and IT 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 crown jewel apps may be SOC-1 or ISO 27001 compliant and require additional layers of security. These are considered critical infrastructure. There may be certain countries, like China, that must be isolated from other countries. With legacy infrastructure one missed FW configuration could mean big problems for the business.

IT leaders should consider cloud-delivered services that are hosted by a cloud security provider, can scale to meet user demand, and provide global availability for users across a variety of public cloud or datacenter environments.

**“By 2023, 60% of enterprises will phase out most of their remote access virtual private networks (VPNs) in favor of ZTNA.”<sup>1</sup>**

– Gartner

<sup>1</sup> Riley, Steve; MacDonald, Neil; and Orans, Lawrence, “Market Guide for Zero Trust Network Access,” Gartner, April 2019.

## Challenges that 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. Solve the IT skills shortage, allowing the enterprises to make the most of talent on hand**
- 2. Deliver a superior user experience for employees and key company stakeholders**
- 3. Be adaptive and agile to empower a dynamically changing business**
- 4. Reduce the risks that can threaten productivity, IP, and a company's reputation**
- 5. Accelerate the adoption of public cloud and mobile devices**

Identifying the technologies that will achieve these goals is a difficult task, as the goals can seem at odds. The decision to adopt cloud services and mobile technologies, for example, achieves the goal of a streamlined user experience, but what about the goal of minimizing the chance of a security attack? IT leaders must strike a careful balance between accelerating the adoption of new, enabling technologies, and ensuring the security of sensitive data. Choosing the right technology at the right time is critical.

**“Security leaders should deploy technology that facilitates digital business access to applications while shielding them from many kinds of prevalent attacks that are common on the cesspool that is the modern internet.”<sup>1</sup>**


<sup>1</sup> Riley, Steve; MacDonald, Neil; and Young, Greg, “It’s Time to Isolate Your Services From the Internet Cesspool,” Gartner, September 2016.

## The value of ZTNA for the business

Zero trust network access (ZTNA) services, also known as a software-defined perimeter (SDP), are a set of technologies built to provide fast, secure access to private applications without placing a user on the network. 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 allowing brokering the connection. This removes the application assets from being visible to the Internet and significantly reduces the surface area for attack.

These are more than just cool security technologies though, they're good for business too. 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. Solves the IT skills shortage** – One difficulty with innovation is that there is often a shortage of experts available to help understand and implement it. This can cause existing personnel to also fear for their job and make a point to actually slow the adoption of new technology. The simplicity of ZTNA - all cloud-hosted, all software, no hardware—makes it easy to set up without the need to hire new specialists. This simplicity allows IT leaders to adopt technology that can secure access to applications moving to cloud, even from unmanaged mobile devices, while maximizing the productivity of the IT staff. Existing staff learns a new technology and gains skills that will make them more marketable as well.
- 2. Provides a superior user experience** – Users are no longer working only in the office, but from home and on the road too. These users include a mix of employees and third-party users as well, and they all expect an Amazon-like experience when accessing apps. ZTNA ensures that each have a fast and completely seamless user experience when accessing private applications. There is no VPN to login to, they don't have to think about whether or not they need to use VPN, and it supports all device types. For third-party users and BYOD devices, there is no need to deploy an endpoint agent. ZTNA browser access features allow for policy-based access to private apps in those scenarios as well. Productivity goes up as a result of being able to connect to apps from anywhere, on any device.
- 3. Delivers agility and scale** – The number of employees, user devices, applications, and amount of traffic continues to grow. Cloud-delivered ZTNA services are hosted by the vendor, so increasing scale is no longer the concern of the IT team. As demand goes up, the ZTNA service handles the additional load automatically. There is no need to deploy additional HW appliances or virtualized firewalls, which will slow down public cloud adoption projects. More agility and more scale are critical to an IT leaders success, and are delivered through ZTNA.



**4. Reduces risk** – Security is often the largest barrier to cloud adoption and allowance of mobile 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 (i.e VPN, virtual DMZs, firewalls etc.) are inherently trusting and should be avoided. They place remote users 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 might have lateral access across the network. This is the case with both employees as well as third parties, who could have weaker security practices. ZTNA services use policies to provide only authorized users (based on identity and device posture) connectivity to specific private apps running in public cloud, private cloud or datacenter. With ZTNA, IT leaders can embrace cloud and mobility, without the typical risks associated with doing so.

**5. Accelerates adoption of cloud and mobility** – Cloud and mobility are priorities for the majority of enterprise teams today, but it can take months or even years to implement securely and 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 use software to reduce complexity, thereby reducing implementation time from months or years to just hours. With ZTNA organizations can more quickly reap the benefits of cloud and 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.”<sup>2</sup>**

**– Alex Philips, Chief Information Officer, National Oilwell & Varco**

<sup>2</sup> Software Defined Perimeter for Infrastructure as a Service, The SDP Working Group, Cloud Security Alliance, 2017. (<https://cloudsecurityalliance.org/group/software-defined-perimeter>)

Learn about  
ZTNA, offered  
as a service  
from Zscaler

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 services 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.

Learn more about ZPA by visiting  
[zscaler.com/products/zscaler-private-access](https://zscaler.com/products/zscaler-private-access)  
or by contacting sales at [sales@zscaler.com](mailto:sales@zscaler.com)

