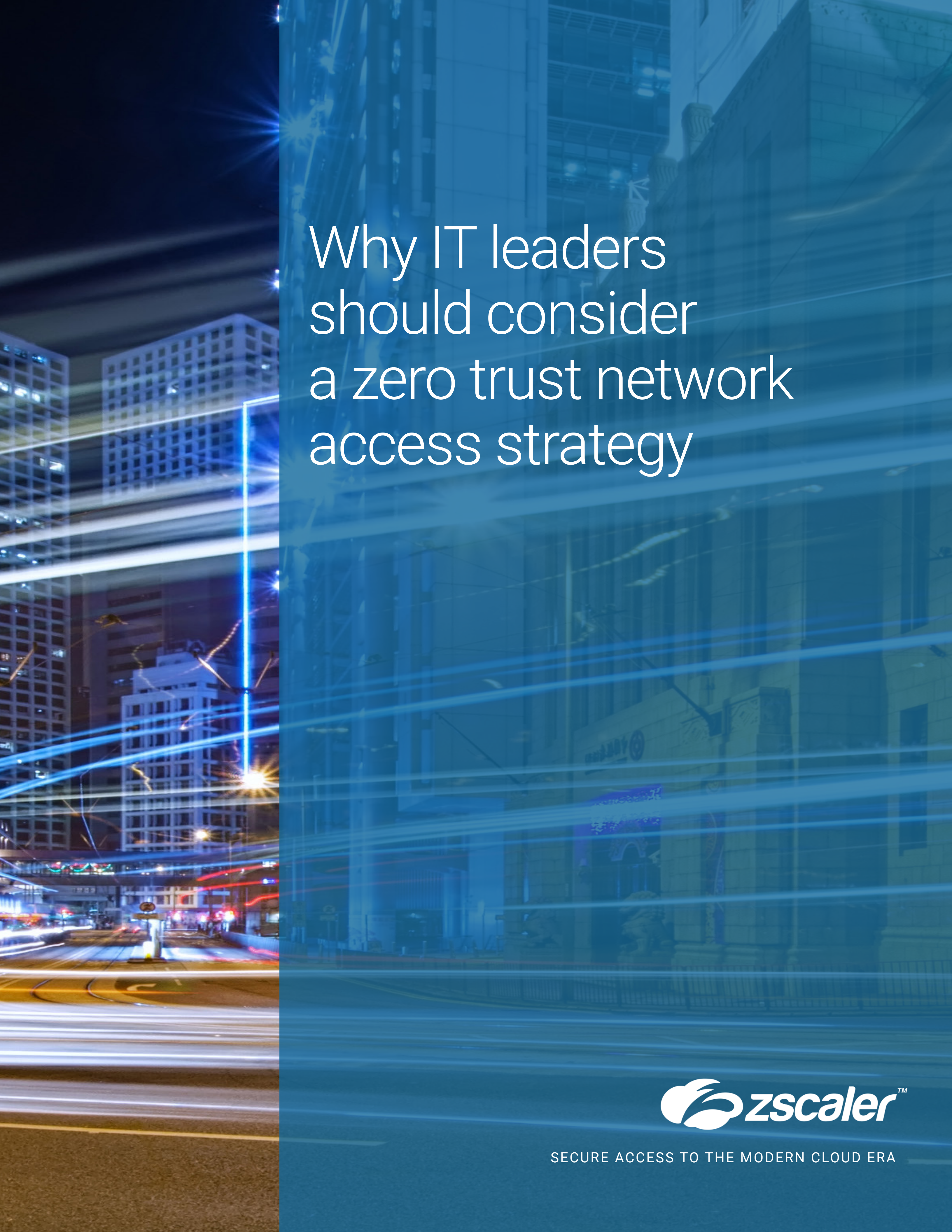

Why IT leaders should consider a zero trust network access strategy

SECURE ACCESS TO THE MODERN CLOUD ERA

A solution for a changing IT environment

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 opportunities previously out of reach for most enterprises. 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 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.

The time has come for security to evolve, moving protections closer to the user and bringing a new emphasis on convenience, flexibility, and reliability.

> **"By 2023, 60% of enterprises will phase out most of their remote access virtual private networks (VPNs) in favor of ZTNA."[1]**
>
> **– Gartner**

[1] Riley, Steve; MacDonald, Neil; and Orans, Lawrence, "Market Guide for Zero Trust Network Access," Gartner, April 2019.

Challenges that technology leaders must overcome

To advance business initiatives and bridge the gap between business needs and IT capabilities, IT leaders must choose technology that 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 adoptiof 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."** [1]

[1] Riley, Steve; MacDonald, Neil; and Young, Greg, "It's Time to Isolate Your Services From the Internet Cesspool," Gartner, September 2016.

ZTNA enables business success

ZTNA, which is also known as a software-defined perimeter (SDP), creates 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 identity, context and policy adherence of the specified participants before allowing access. This removes the application assets from public visibility and significantly reduces the surface area for attack.

Earlier we discussed the five key factors that IT leaders must consider when adopting new technologies. Let's take a look at how ZTNASDP 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. The simplicity of ZTNA - all software, no hardware—makes it easy to implement 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.
2. **Provides a superior user experience** – Users are playing an increasingly large role when it comes choosing enterprise technology. Providing a positive user experience is one of the most important benefits of the ZTNA. It allows users to access applications seamlessly, regardless of whether that application is running in a cloud or data center. A cloud-like user experience has become the new standard, and ZTNA delivers it.
3. **Delivers agility and scale** – The number of enterprise applications, users, and user devices is constantly changing, along with the needs of the business. By leveraging the internet and cloud to provide users with access to applications, ZTNA offers offer a level of agility and scale unmatched by any legacy technology. Just think how difficult it would be to scale the number of hardware stacks across multiple data centers around the world. Now compare this to the scale of the internet. The internet wins by a long shot.

4. **Reduces risk** – Security is often one of largest barriers to cloud adoption and the allowance of personal mobile devices, as these technologies can mean increased risks to the business. ZTNA provides provide secure, policy-based remote access to applications and check both device posture and identity prior to allowing access. Only authorized users can access an application. With ZTNA, IT leaders can ensure that even as applications move to third-party IaaS platforms they remain secure. Additionally, users may leverage their own device for work without having their device serve as a conduit for nefarious activity or being responsible for the spread of malware across the corporate network. After all, with ZTNA, users are never placed on the network to begin with.

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 SDP, organizations can keep cloud resources completely dark to unauthorized users. This completely eliminates many attack vectors including brute-force attacks; network flood attacks, as well as TLS vulnerabilities such as Heartbleed and Poodle.**[2]

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

Learn about ZTNA, offered as a service from Zscaler

The zero trust network access is a valuable tool to enterprise IT leaders. At Zscaler we have developed an ZTNA service called Zscaler Private Access (ZPA™). The service uses the cloud to provide secure and seamless remote access to internal applications.

Learn more about ZPA by visiting **zscaler.com/products/zscaler-private-access** or by contacting sales at **sales@zscaler.com**

zscaler™