Enterprise Strategy Group
by TechTarget

Overcoming Insecure VPNs and Modernizing Remote Access with ZTNA

VPNs can no longer support modern secure access needs. The increasing use of cloud applications, shift to remote and hybrid work, prevalence of unmanaged and mobile devices, and need to support third-party access have stressed traditional VPN architectures to the breaking point. Security teams should begin evaluating zero trust network access (ZTNA) solutions as a VPN replacement to more efficiently, effectively, and securely connect remote users with the resources they need to do their jobs.

VPNs Fail to Address Key Remote Access Challenges

Corporate resources are more distributed than ever before. Applications and data are increasingly cloud-resident, and users often work remotely. Yet most organizations continue to rely on VPNs that offer limited security, visibility, and scalability.

THE NATURE OF WORK HAS FUNDAMENTALLY CHANGED:

Organizations using public cloud infrastructure services[1]
75%

Employees working remotely or in a hybrid manner[2]
63%

Users accessing corporate resources are third parties[3]
34%

67%
of organizations are using VPN to support remote access.[4]

KEY CHALLENGES PROVIDING SECURE ACCESS:[5]

34%
of organizations report complexity with the increasing use of cloud-based resources.

25%
of companies indicate introduction of security and compliance issues from employees not following policy.

30%
of respondents cite difficulty addressing secure access from employee-owned devices.

22%
of organizations say the cost associated with maintaining a traditional VPN infrastructure is problematic.

26%
of companies say employees circumventing corporate security controls is a challenge.

20%
of organizations point to negative impacts to user experience and productivity.

Zero Trust Network Access Can Help Organizations Modernize Secure Access and Replace VPNs

Many organizations have begun to turn to ZTNA and explore VPN replacement to improve security, increase flexibility, and deliver a stronger user experience.

MANY THAT HAVE BEGUN TO USE ZTNA ARE EXPLORING VPN REPLACEMENT.[6]

We use ZTNA for specific use cases or applications and are planning to expand to move away from VPN
49%

We use ZTNA for specific use cases or applications and are actively expanding in order to move away from VPN
13%

We use ZTNA for most of our remote access needs in order to move away from VPN
7%

ZTNA Advantages over VPN:

1 Stronger security through zero trust

ZTNA supports stricter and more contextual access policies and continually monitors and assesses connections even after authentication.

2 A better user experience

Because ZTNA tools are cloud-delivered, they can directly connect remote users to cloud-based applications, without the need to backhaul traffic.

3 Flexibility and simplicity

ZTNA operates as-a-service, negating the need to deploy or maintain appliances and providing the ability to quickly scale capacity up or down as needs change.

Zero Trust Drives Both Security and Business Benefits

Zero trust is often viewed through the lens of cybersecurity modernization. Yet many organizations that have implemented zero trust have seen both security and business benefits. This makes zero trust a critical aspect of any digital transformation journey.

BENEFITS SEEN FROM ZERO TRUST ADOPTION:[7]

77%
report seeing both security and business benefits from zero trust.

SPECIFICALLY:

43%
report fewer cyber incidents.

37%
report better organizational agility.

36%
report increased productivity.

34%
report increased user satisfaction.

The Bigger Truth

Rather than continue to cope with VPNs' limitations, organizations are accelerating their adoption and the use of ZTNA solutions to align the growing need for secure remote access with the increased digitalization of how, where, and when employees work. ZTNA solutions offer the scalability, cost efficiency, security, and performance now essential to efficient operations, improved employee experience, and a more reliable cybersecurity framework.

LEARN MORE

BlackBerry Cybersecurity

1. Source: Enterprise Strategy Group Complete Survey Results, 2022 Technology Spending Intentions Survey, November 2021.
2. Source: Enterprise Strategy Group Complete Survey Results, 2021 SASE Trends: Plans Coalesce but Convergence Will Be Phased, December 2021.
3. Source: Enterprise Strategy Group Complete Survey Results, 2021 SASE Trends: Plans Coalesce but Convergence Will Be Phased, December 2021.
4. Source: Enterprise Strategy Group Survey Results, The State of Zero Trust Security Strategies, May 2021.
5. Source: Enterprise Strategy Group Research Report, Transitioning Network Security Controls to the Cloud, August 2020.
6. Source: Enterprise Strategy Group Complete Survey Results, 2021 SASE Trends: Plans Coalesce but Convergence Will Be Phased, December 2021.
7. Source: Enterprise Strategy Group Survey Results, The State of Zero Trust Security Strategies, May 2021.