Goodbye VPN,
MEET ZTNA

VPNs are often slow, hard to manage, and insecure. This guide shows how Zero Trust Network Access is the superior alternative for your hybrid workforce.

BlackBerry® | Cybersecurity

Effective cybersecurity is more than a nice-to-have—it is mission-critical. Yet organizations struggle to adequately protect their data and applications from relentless cyberattacks, a task that is made even harder by the distributed nature of today's remote and hybrid workforces. According to Gartner research, 71% of U.S. knowledge workers will work remotely at least part time by the end of 2023.[1] And 95% of organizations say their employees may access corporate data from off-site.[2]

The outdated, but still common, model for remote access—a virtual private network (VPN) connecting the user to work resources behind a firewall—is failing to hold up against relentless and increasingly sophisticated cyberattacks. In addition, VPNs are often difficult for end-users to use, time-consuming for IT administrators and sluggish in performance.

So, it's no surprise that

63% of the organizations using a VPN plan to replace it with a Zero Trust solution in the near future.[2]

It’s time to replace your VPNs with ZTNA.

In this guide, we explore the top four reasons why organizations should ditch their VPNs and adopt Zero Trust Network Access (ZTNA) to protect their users, apps and sensitive data.

You’ll learn how ZTNA:

- Reduces latency and complexity for end-users
- Strengthens security by minimizing the attack surface available to cybercriminals
- Simplifies management and reduces administrative overhead
- Provides scalability and flexibility
- Beats VPNs every time

What is Zero Trust Network Access?

ZTNA utilizes Zero Trust principles to continuously authenticate and authorize every session and resource request before granting access to applications, files, or other sensitive information. It removes excessive, implicit trust and instead denies access by default. ZTNA strengthens security across the enterprise by granting access on a least privilege basis, using strict identity- and context-based access controls to grant or deny access.

While a VPN grants access to an entire network, ZTNA operates on the principle of "never trust, always verify" and grants the minimum access needed based on user identity and contextual information. This reduces the risk of unauthorized access—by either outside attackers or an insider data breach—and mitigates the impact of potential security breaches.

Zero Trust Security Provides:

- Least-privilege access
- Continuous verification of user identity
- Application segmentation
- Encrypted end-user-to-application transmissions
- Improved enterprise visibility

Top Four Reasons to Adopt ZTNA

(...say goodbye to your VPN)

50% *of employees work remotely or in a hybrid model.*[3]

1 Improve Your User Experience

Unlike VPNs, ZTNA provides a seamless and user-friendly experience by enabling secure access to resources from anywhere, anytime, and using any device.

ZTNA users can authenticate themselves using methods such as multifactor authentication (MFA) and single sign-on (SSO). This simplifies the authentication process while maintaining a high level of security. By eliminating the need for VPNs and implementing a user-centric approach, ZTNA enhances productivity and enables remote and mobile workers to access resources securely without sacrificing convenience.

Additionally, VPN connections can experience latency, frustrating users. ZTNA allows authenticated users to connect directly to applications, whether at a data center or in the cloud. Once a user is verified by the trust broker, then they're able to directly access the resources they need without having to transmit all data through a VPN.

User Friendly Experience

- Fast connection speeds
- High availability
- Supports any end-user device
- Streamlined authentication

Problem:

VPNs backhaul traffic to the data center, effectively creating a traffic jam that results in slower connection speeds. In combination with clunky, static authentication, VPNs create poor user experiences.

Solution:

Cloud-native ZTNA offers end-users optimized access to applications on a global scale without the need to backhaul traffic. This results in fast connection speeds, improving user satisfaction and productivity. ZTNA also improves remote work and BYO deployments with simplified user management, enabling secure access from any device and from any location to any application.

Top Four Reasons to Adopt ZTNA

(...say goodbye to your VPN)

2 Strengthen Security by Minimizing the Attack Surface

Unlike the VPN and firewall security model, which typically grants broad access to network resources based on a network location or user role, ZTNA enforces the principle of least privilege. By employing very granular access controls, ZTNA minimizes the possible attack surface and strengthens security.

Once users are authenticated and their devices verified as being uninfected, they can access only the resources they need for their jobs, reducing the potential for unauthorized access or lateral movement by attackers. This minimizes the damage that cyberattackers can do even if they successfully breach the network.

Additionally, ZTNA solutions segment applications, hiding them from public visibility, so the location of the app can't be discovered by threat actors.

80% *of tech leaders use a VPN as part of their cybersecurity strategy, yet 74% say they are not confident or don't know if a VPN is sufficient to protect their organization from cyberattacks.*[4]

Problem:

VPNs expose IP addresses, increasing your attack surface. Should a breach occur, threat actors have broad access to the network and can move laterally, compromising other users, devices, and data.

Solution:

ZTNA uses application segmentation to hide apps from public visibility, shrinking your attack surface. Application access is granted on a per-session, least-privilege basis.

Top Four Reasons to Adopt ZTNA

(...say goodbye to your VPN)

3 Centralize and Simplify Management

ZTNA simplifies administrative management by centralizing access policies and authentication mechanisms. In traditional network security models, managing access control rules across different systems and applications can be complex and time-consuming. And VPNs require stacks of on-premises physical appliances that must be monitored and maintained. This includes devices such as VPN gateways, load balancers and firewalls that require people to manually configure and maintain. This also limits the scalability of a VPN.

Alternatively, ZTNA provides:

- A unified view of user activity and access permissions
- Visibility and control over network resources
- Simplified access management and reduced administrative overhead with a centralized approach

In addition, ZTNA supports seamless integration with identity and access management (IAM) systems, making it easier to manage user identities and access privileges from a single control point. This simplification in management processes enables organizations to enforce security policies, track user activity, and respond to security incidents quickly and efficiently.

22% *of organizations say the cost associated with maintaining a traditional VPN infrastructure is problematic.*[5]

Problem:

VPNs require the deployment of appliances in data centers. This creates the need for manual configurations and maintenance, adding costs, time, and complexity.

Solution:

ZTNA consolidates management and configuration, simplifying deployment and network security programs while streamlining access control and policy management.

Top Four Reasons to Adopt ZTNA

(...say goodbye to your VPN)

4 Scalability and Flexibility

37% *of organizations report better organizational agility.*[6]

Cloud-based ZTNA offers scalability and flexibility to meet the needs of modern enterprises. As organizations increasingly adopt cloud services, embrace remote work, and expand their digital footprint, ZTNA allows secure access to resources regardless of location. With ZTNA, you can ensure that users and devices are authenticated and authorized before accessing critical systems and data, whether resources are located in the cloud or on-premises.

Scalability and flexibility are essential for accommodating the dynamic nature of today's business needs. ZTNA provides a secure framework for digital transformation initiatives, enabling organizations to securely connect distributed resources, support remote workers, and seamlessly integrate new technologies.

Simple to Scale

- Cloud-native
- No infrastructure to maintain
- Support digital business transformation

Problem:

Since VPNs require the deployment of appliances in data centers, scaling requires additional resources and more hardware. This reduces your agility and makes enabling secure access at scale more expensive.

Solution:

ZTNA removes the need to buy and maintain appliances and infrastructure to facilitate secure access. With ZTNA, everything you need is in the cloud, improving your ability to scale your operations when needed, while giving you added flexibility to make adjustments on-the-fly.

Why ZTNA Beats VPNs – Every Time

	ZTNA	VPN
Enhanced Security		
Adaptive, least-privilege access	✓	X
Minimizes attack surface	✓	X
Continuous evaluation	✓	X
Application segmentation	✓	X
Happy, Productive Users		
Transparent to end-users	✓	X
Fast connection speeds to SaaS apps	✓	X
Does not backhaul traffic	✓	X
Optimized to improve the end-user experience	✓	X
Optimizes remote access with high availability	✓	X
Streamlined authentication	✓	X
Simplified Management		
Simplified administration	✓	X
Easy to scale	✓	X
Cloud-native	✓	X
Integrated security stack	✓	X
No expensive security stack and infrastructure to maintain	✓	X
Fast deployment	✓	X
Improves agility	✓	X
Optimizes security budget	✓	X
Support for managed and unmanaged device	✓	X
Streamline SaaS app setup and connectivity	✓	X
Support for digital business transformation	✓	X

Make the Switch to ZTNA

77% *of businesses report seeing both security and business benefits from Zero Trust.*[6]

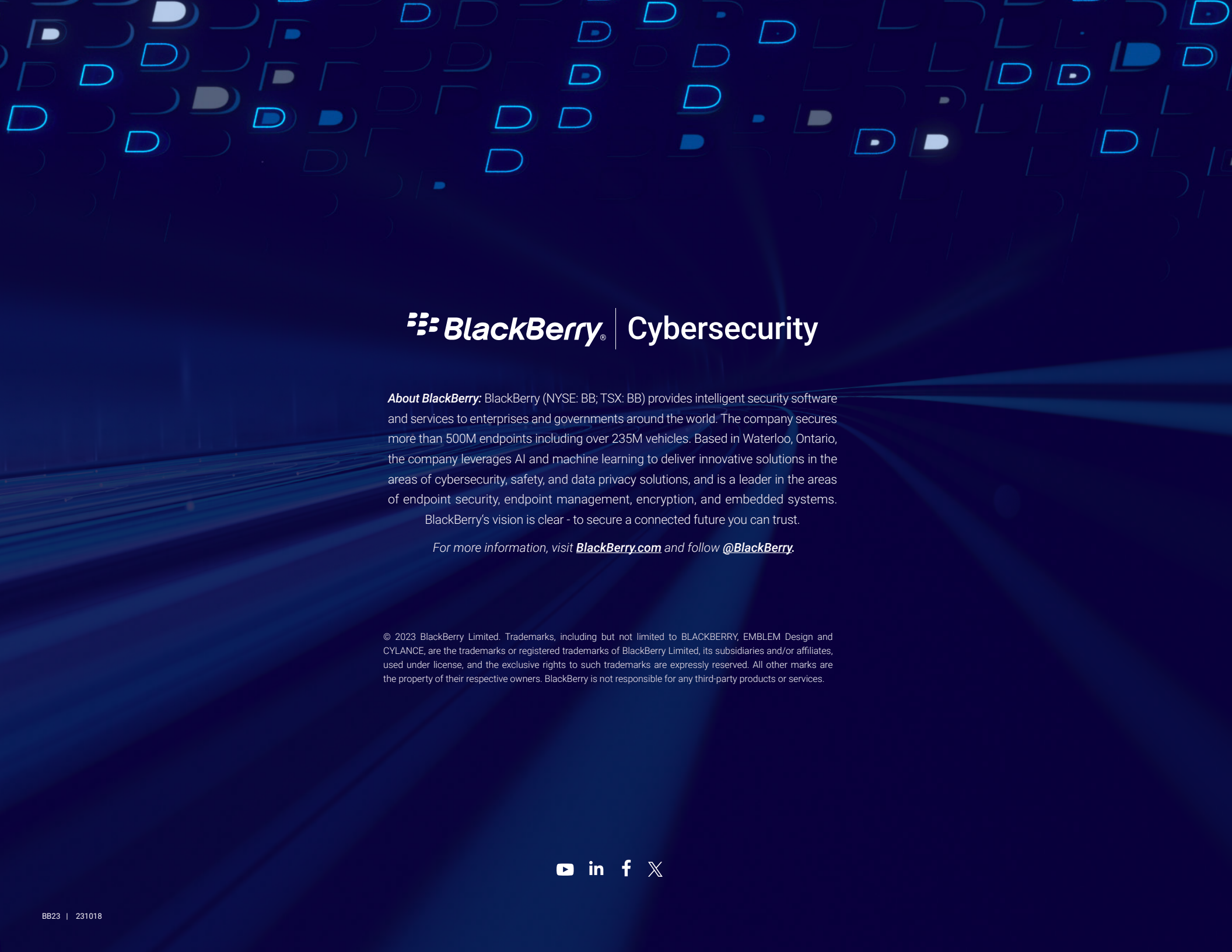
With ZTNA, organizations can confidently embrace modern workplace practices and technologies, knowing that secure access is maintained regardless of the network environment or resource location.

Organizations adopting ZTNA can enhance security, minimize the attack surface, improve end-user experiences, simplify management, and achieve scalability and flexibility. It's time to switch and embark on a safer digital journey with ZTNA.

Replace your VPN with CylanceEDGE.

CylanceEDGE™ from BlackBerry can replace your VPN and deliver secure access to private and SaaS apps anywhere, anytime, with data security. This modern, cloud-delivered solution empowers organizations to protect what matters most, is flexible enough to support managed and unmanaged devices, enables continuous authentication and authorization, and identifies sensitive data-at-rest and detection of data-in-motion to enhance visibility and prevent exfiltration. With CylanceEDGE, your users will thank you. To learn more, visit our website.

[1] Gartner Press Release: March 1, 2023, Gartner Forecasts 39% of Global Knowledge Workers Will Work Hybrid by the End of 2023
[2] Gartner Peer Insights, ZTNA for Hybrid Work Environments survey
[3] Enterprise Strategy Group Complete Survey Results, 2023 SASE Series: SSE Leads the Way Towards SASE, August 2023.
[4] Gartner Peer Insights, ZTNA for Hybrid Work Environments survey
[5] Enterprise Strategy Group Research Report, Transitioning Network Security Controls to the Cloud, August 2020
[6] Enterprise Strategy Group Survey Results, The State of Zero Trust Security Strategies, May 2021



About BlackBerry: BlackBerry (NYSE: BB; TSX: BB) provides intelligent security software and services to enterprises and governments around the world. The company secures more than 500M endpoints including over 235M vehicles. Based in Waterloo, Ontario, the company leverages AI and machine learning to deliver innovative solutions in the areas of cybersecurity, safety, and data privacy solutions, and is a leader in the areas of endpoint security, endpoint management, encryption, and embedded systems. BlackBerry's vision is clear - to secure a connected future you can trust.

*For more information, visit **BlackBerry.com** and follow **@BlackBerry**.*

BB23 | 231018