BlackBerry. Intelligent Security. Everywhere.

TOP 5 REASONS TO ADOPT ZERO TRUST NETWORK ACCESS

Secure access to enterprise resources has never been more essential to enable productivity, remain competitive, and protect critical assets. For the modern enterprise, supporting a hybrid workforce model is a necessity. It adds complexity to operations and a need to secure network connections and data hosted both on-premises or in the cloud. Digital business transformation requires anywhere, anytime access to critical systems, services, and data over the Internet, which expands the surface area for attack and exposes your operations to threat actors. That's why security leaders need to develop adaptive trust frameworks delivered via the cloud and built on the principles of Zero Trust.

Zero Trust Network Access (ZTNA) is a highly secure and adaptive framework that protects organizations from countless known and emerging cyberthreats. It relies on the strong principles of Zero Trust to restrict organizational resources to known entities and trustworthy actors.

There are many compelling reasons to adopt ZTNA powered by AI. Here are the top 5:

1 IMPROVE SECURITY POSTURE AND REDUCE ATTACK SURFACE

- ZTNA offers a clear advantage over VPNs to support a distributed workforce. It continuously authenticates users and devices and the context in which they access data and apps on networks. On the other hand, VPNs offer static authentication, granting access to the entire network.
- ZTNA is inherently secure and grants access to segmented applications with no visibility to the network. This dramatically reduces the attack surface by preventing lateral movement within the network.
- With source-IP pinning, limit unauthorized users from gaining access to network resources.
- Restrict access to malicious sites with IP and URL reputation and classification technology.
- ZTNA enables organizations to begin migrating their security posture from endpoint detection and response (EDR) toward an extended detection and response (XDR) model.

2 SUPPORTS DIGITAL BUSINESS TRANSFORMATION AND HYBRID WORKFORCE

- Simple for network administrators to implement, manage and monitor. Its cloud-based architecture scales well to accommodate hybrid and mobile workforces.
- ZTNA provides the ability to monitor traffic to SaaS apps.
- Fully functional in an on-premises or connected environment.
- For end-users, ZTNA offers the ability to support BYOD and WFH programs, enabling anytime, anywhere secure connectivity from their favorite devices.
- ZTNA integration with strong endpoint security ensures only healthy and trusted devices access workplace apps.

3 ACCELERATE THE ADOPTION OF ZERO-TRUST ARCHITECTURE

- AI-empowered ZTNA may perform predictive threat detection, a critical component for achieving a prevention-first security posture.
- ZTNA can use an AI modulated risk score to detect threat indicators based on user behavior, access patterns, network flows, and other data. This allows ZTNA to identify and stop threats beyond malware, including fileless and insider attacks.
- AI-driven ZTNA may detect and stop both traditional and zero-day malware pre-execution, preventing damage to systems, networks, data, and business resources.
- Trained AI threat detection models deployed directly on endpoints continuously monitor and protect devices with access to business resources regardless of connectivity.

4 INCREASED SPEEDS AND IMPROVED END-USER EXPERIENCE

- ZTNA enables better speed and performance with direct access to SaaS apps from corporate or personal devices with less network congestion. Users can securely use networks at home, the office, or on the road at a coffee shop or hotel.
- With full-tunnel and split-tunnel access modes, end-user privacy remains protected while network bandwidth is freed to improve the end-user experience.
- VPNs can create the issue of backhauling network traffic and degrade SaaS app connectivity and the user experience. ZTNA with a secure gateway can protect remote connectivity to SaaS apps without severely impacting productivity.

5 EXTENSIVE SCALABILITY TO ACCOMMODATE DYNAMIC WORK ENVIRONMENTS

- Cloud-native solutions grow with you. ZTNA offers improved scalability with no need for additional hardware.
- Leverage devices your business and employees already have.
- Continuously secure all endpoints and connections with business resources without adding significant operational friction or disruption to employee workflow.
- Correlate device and user context to create a big-picture view of security risks before granting network access.

BLACKBERRY: THE SECURE PATH FORWARD

BlackBerry offers integrated solutions that support secure access for the evolving enterprise from the endpoint to the network. BlackBerry® Gateway and BlackBerry® Protect enable secure productivity from anywhere and seamless connectivity for all your devices.

To learn more about securing your organization, visit us at BlackBerry.com.

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 175M cars on the road today. 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 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.

BlackBerry. Intelligent Security. Everywhere.

MKTG-17907 | 221301