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 is more critical than ever due to the sheer complexity of operations and the 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 in 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 endpoint to the network. BlackBerry® Gateway and BlackBerry® Protect enable secure productivity for the evolving enterprise from the cloud-native solutions to implement, manage, and monitor. Its cloud-based architecture scales well to accommodate hybrid and mobile workforces. BlackBerry provides the ability to monitor traffic to SaaS apps, enabling anytime, anywhere secure access to the network. FOR END-USER, ZTNA OFFERS THE ABILITY TO SUPPORT BYOD AND WFH PROGRAMS, ENABLING ANYTIME, ANYWHERE SECURE ACCESS TO BUSINESS RESOURCES REGARDLESS OF CONNECTIVITY. BlackBerry (NYSE: BB; TSX: BB) provides intelligent security software and services to protect devices with access to business resources regardless of connectivity. BlackBerry offers integrated solutions that support secure access for the evolving enterprise from the cloud to the network. BlackBerry is not responsible for any third-party products or services. BlackBerry is a trademark of BlackBerry Limited, and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners. BlackBerry’s vision is clear — to protect devices with access to business resources regardless of connectivity. BlackBerry offers integrated solutions that support secure access for the evolving enterprise from the cloud to the network. BlackBerry is not responsible for any third-party products or services. BlackBerry is a trademark of BlackBerry Limited, and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners. 

**TOP 5 REASONS TO ADOPT ZERO TRUST NETWORK ACCESS**

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 the network. ZTNA offers a stronger foundation, granting access to the entire network.
   - ZTNA is inherently secure and grants access to segmented applications with no visibility to the network. This drastically 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**
   - A comprehensive ZTNA may perform prediction threat detection, a critical component for achieving a prevention-first security posture.
   - ZTNA can use AI modulated risk scores to detect threats 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.
   - A driven ZTNA may detect and stop both traditional and zero-day malicious pre-execution, preventing damage to systems, networks, data, and business resources.
   - BlackBerry’s solution empowers deployed and managed contexts to continuously monitor and protect devices with access to business resources regardless of connectivity.

3. **ACCELERATE THE ADOPTION OF ZERO-TRUST ARCHITECTURE**
   - ZTNA enables better speed and performance with direct access to SaaS apps from corporate or personal devices with egalitarian access to the network connection. Users can securely user network at home, at the office, or at the cloud as a coffee shop on the train.
   - WIP Full-tunnel and split-tunnel access modes, exclusive proxy and firewall protection enabled to prevent the network bandwidth from being utilized to improve the end-user experience.
   - WIPs can create an environment of backhauling network traffic and degrade SaaS app connectivity and use experience. ZTNA with a secure gateway can provide transparent connectivity to SaaS apps without severely impacting productivity.

4. **INCREASED SPEEDS AND IMPROVED END-USER EXPERIENCE**
   - Cloud-native solutions grow with your ZTNA offers improved scalability with no need for additional hardware.
   - Leverage devices your business and employees already own.
   - Continuously secure all endpoints and connections with business resources without adding significant operational friction or discomfort to employees workloads.
   - Correlate device and user context to create a lifecycle view of security risks before granting network access.

5. **EXTENSIVE SCALABILITY TO ACCOMMODATE DYNAMIC WORK ENVIRONMENTS**
   - Cloud-native solutions grow with your ZTNA offers improved scalability with no need for additional hardware.

About BlackBerry

Blackberry Limited ( ticker: BB ) is a cybersecurity software and services company that makes software and experiences around the world. Its company makes more than 500M devices using BlackBerry 10 and Android platforms, including smartphones, feature phones, and embedded systems. BlackBerry’s solutions make mobile computing easier to use — and more secure and connected — everywhere. BlackBerry is headquartered in Waterloo, Ontario, Canada. For more information, visit BlackBerry.com, like us on Facebook, or follow us on Twitter and LinkedIn. © 2023 BlackBerry Limited and/or its subsidiaries. All rights reserved. SO2023-0628-RF

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 withstand continuous connectivity to your data. To learn more about securing your organization, visit us at BlackBerry.com.