BlackBerry | Cybersecurity

TOP 9 SIGNS
IT'S TIME TO ADOPT A ZERO TRUST ACCESS SOLUTION

If your organization struggles to secure an expanding digital footprint without compromising user experience, Zero Trust Access (ZTA) may be the answer. ZTA enables work from anywhere while protecting users, applications, and data by reducing cyberattacks, increasing ROI, and promoting today's hybrid workforce. Here are some top signs that your organization is ready to adopt a ZTA solution.

1 YOU'RE STILL USING A VPN OR OTHER LEGACY SOLUTIONS

Problem: Designed to support old-fashioned business models where employees primarily work in offices, VPNs and legacy solutions can't meet today's distributed workforce needs for cybersecurity, scalability, and performance.

Solution: ZTA's modern approach to cybersecurity protects your infrastructure, empowers your workforce, and aligns IT with business objectives.

2 EMPLOYEES CAN'T SECURELY WORK FROM ANYWHERE

Problem: According to Gartner, remote workers are 53% of the total workforce[1], so helping them be securely productive is a priority: continuously entering login names and passwords for different resources is frustrating and time-consuming. Unfortunately, VPNs and other on-premises-based legacy solutions weren't designed to support remote workforces. Performance degrades when more people use them because traffic is backhauled through the corporate data center.

Solution: Cloud-delivered ZTA is designed to support today's distributed workforce, delivering secure and reliable access to the resources employees need to be productive, no matter where they are.

3 USERS CAN'T CONNECT FROM THE DEVICES THEY WANT TO USE

Problem: Remote workers aren't the only ones who require flexible access—campus-based employees also want the freedom to use personal devices in and out of the office. When employees can't use the tools and devices they prefer, they may attempt to circumvent security controls by turning to less secure systems like public file-sharing sites and personal email, increasing the risk of data breaches.

Solution: ZTA can authenticate an identity on any healthy device (both managed and unmanaged), increasing flexibility and productivity without compromising security.

4 INFORMATION AND RESOURCES AREN'T PROTECTED

Problem: VPNs can't detect and stop advanced threat tactics and new malicious behaviors or keep employees from connecting to suspicious websites or falling victim to phishing scams that may result in ransomware, data breaches, and more.

Solution: AI-based ZTA detects and stops suspicious activity to protect intellectual property, financial information, and other confidential data against both inside and outside threats.

5 YOUR ORGANIZATION DOESN'T HAVE VISIBILITY INTO DATA, APPLICATIONS, AND RESOURCES

Problem: Many VPNs and legacy solutions track when people enter and exit the network and not much else. Organizations may find it difficult to locate and consolidate sensitive information, understand high-risk endpoints and users, and develop a better understanding of at-rest and in-motion data with fewer resources.

Solution: ZTA manages and records all access requests to applications, data, and resources to inform risk management decisions. ZTA can also identify, classify, and inventory sensitive data to improve security.

6 ADMINISTRATION TASKS ARE COMPLEX AND TIME-CONSUMING

Problem: VPNs and legacy systems often call for hands-on configuration, requiring staff to spend time on manual administration instead of strategic projects. If your organization has multiple cybersecurity solutions and juggles many vendor relationships, administration time and costs can rise accordingly.

Solution: A well-thought-out ZTA solution protects all enterprise resources through a single, centralized interface that simplifies administration.

7 BENEFITS AREN'T KEEPING PACE WITH COSTS

Problem: VPNs and legacy solutions are expensive to maintain and scale, especially hardware-based systems. Organizations with a complicated security infrastructure need additional headcount, administration time, and funding to support growth.

Solution: A single, centralized ZTA solution delivers superior security and access while reducing complexity and costs.

8 CLOUD MIGRATION ISN'T SUPPORTED

Problem: Most organizations are currently undergoing some form of cloud migration, and many young organizations and startups were born in the cloud. Generally, cloud infrastructure is less expensive than buying and managing physical servers and offers superior flexibility, scalability, and performance. Unfortunately, old-fashioned VPNs and other legacy solutions can't secure remote cloud-based resources.

Solution: ZTA is designed to seamlessly protect and defend enterprises with increasingly blurred perimeters.

9 YOUR OPERATIONS AREN'T FLEXIBLE OR SCALABLE

Problem: Digital transformation isn't just a buzzword—when IT and operations are aligned, organizations can capture deeper insights, streamline workflows, and increase efficiency to deliver better products, services, and experiences. VPNs and legacy solutions simply can't secure that kind of growing digital footprint.

Solution: ZTA delivers powerful, flexible security that can scale and evolve with your organization.

If your organization faces one or more of these challenges, CylanceEDGE™ from BlackBerry is an effective, affordable ZTA solution that can help modernize your security operations. CylanceEDGE delivers ZTA and data security to private and SaaS apps to enable work from anywhere. This modern, cloud-delivered solution supports managed and unmanaged devices, enables continuous authentication and authorization, and identifies sensitive data at rest and detects data in motion to enhance visibility and prevent exfiltration.

For more information about CylanceEDGE, get started here.

[1] https://www.gartner.com/smarterwithgartner/hybrid-and-remote-workers-change-how-they-use-it-equipment

BlackBerry. Intelligent Security. Everywhere.

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 215M 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 | 230502