BlackBerry Intelligent Security. Everywhere.

BLACKBERRY GATEWAY.

AI-Empowered and Privacy-Friendly Zero Trust Network Access Solution.

DATA SHEET

Strong network security is critical in an era where work-from-home and bring-your-own-device (BYOD) policies are gaining broad acceptance. The convenience of remote work comes with a significant increase to the attack surface of the organization. Each new device, application, and user connecting with business resources introduces additional security risks. When remote workers connect a wide variety of home office technology to the business network, these risks quickly multiply.

Recent estimates[1] predict the number of remote workers to double in 2021, and 70% of workers to be partially remote by 2025. This transformation of the workforce means more business resources will both move to, and be accessed from, outside of the traditional network perimeter. Remote workers will increasingly try to access work-related software-as-a-service (SaaS) offerings and organizational data from various devices, creating security risks.

[1] https://www.forbes.com/sites/carolinecastrillon/2021/12/27/this-is-the-future-of-remote-work-in-2021/?sh=5d30aff11e1d

BlackBerry® Gateway is a Zero Trust Network Access (ZTNA) solution that mitigates the additional security vulnerabilities created by supporting mobile and remote workers. Trying to preemptively verify and protect all possible combinations of home office technology before allowing it on the business network is not viable. By implementing an AI-empowered Zero Trust framework, BlackBerry Gateway uses continuous authentication to ensure only secure and trusted devices access business resources. Every home office device or app may not be secure, but each one connecting to the business environment must prove their trustworthiness to receive access.

BLACKBERRY GATEWAY CAPABILITIES

BlackBerry Gateway brings several advanced technologies together to keep network environments secure. It is built upon a robust TCP/IP stack, optimized for mobile and remote devices, and can detect threats in encrypted packets. It uses AI to detect suspicious behavior throughout the environment, adjust access in real-time, and correlate and contextualize threat information often overlooked by legacy solutions. BlackBerry Gateway

protects workers without disrupting their productivity by limiting access to apps, not the network, and allowing IP pinning.

AI-Empowered, Trust-Based, Adaptive, Secure Access

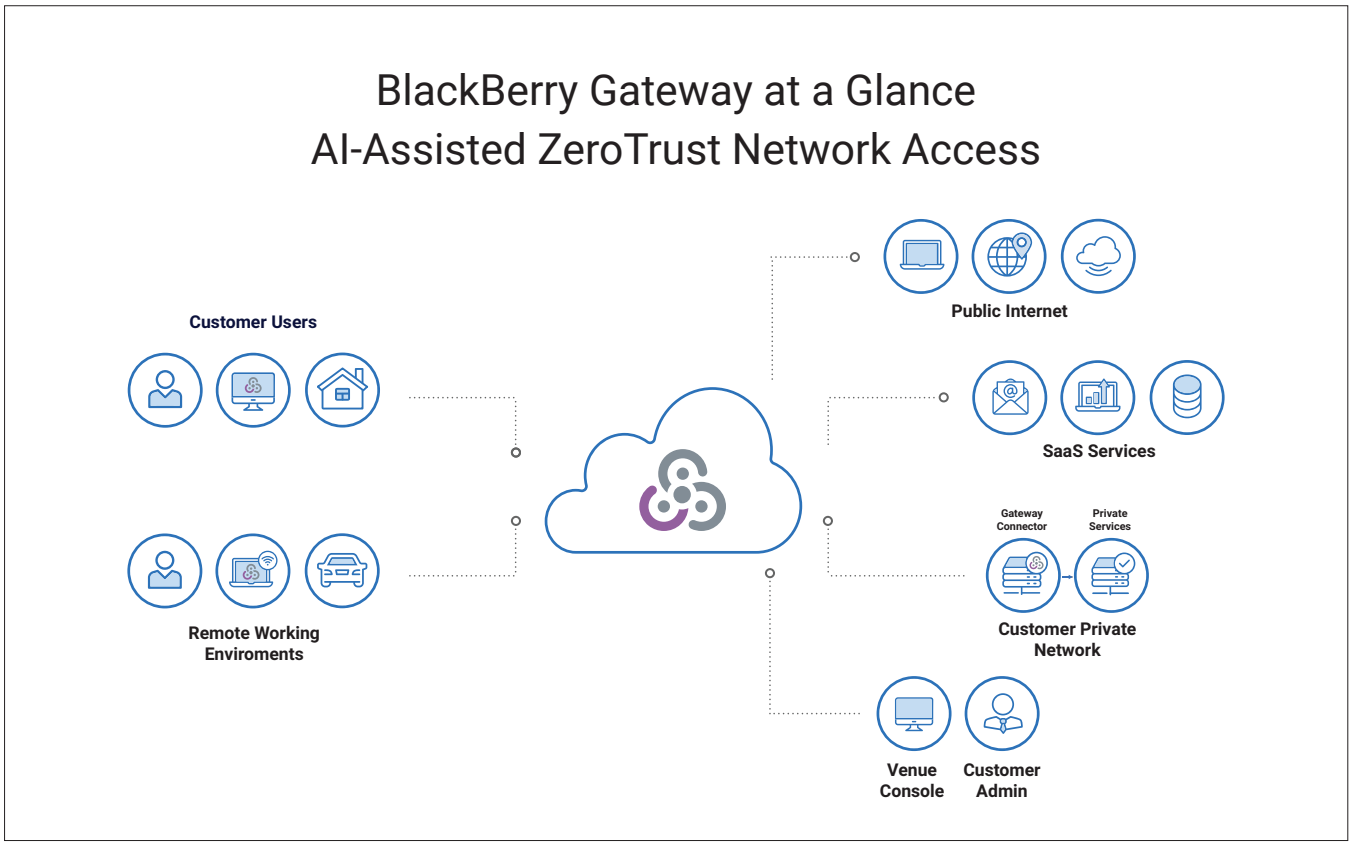
BlackBerry Gateway uses Cloud AI to continuously analyze a number of factors when determining the trustworthiness and access privileges of remote participants. Participants are not limited to users, but could be applications or bots seeking access to the environment as well. When evaluating access, the Cloud AI may adjust trust levels based upon the following variables:

- Is a participant operating from a high-risk location?
- Is the participant who they say they are?
- Is the participant behaving normally?
- Is the participant accessing the expected resources?
- Does a user's behavior align with their past activity, or other users performing similar roles?

When a trust score significantly changes, the Cloud AI can take various actions. For positive changes in trust, a participant may be rewarded with continued or upgraded access. Negative trust changes may result in less access, a request to re-authenticate, or trigger security alerts and remediation procedures.

Full/Split Tunnel Network Services

BlackBerry Gateway provides a secure communications tunnel between remote or mobile users and the business environment. The secure tunnel operates in a full or split access mode depending on the needs of the organization. Full mode secures all communication between the user



CLOUD AI

BlackBerry Gateway Cloud AI continuously analyzes network risk factors for each connected entity and dynamically changes access levels according to their trustworthiness.

and the business network. Split mode allows admins to designate particular resources for secure communication while leaving other traffic open. The split tunnel approach is useful for separating work apps from personal ones being accessed on the same BYOD or home office device.

Source IP Pinning

Some web services and cloud applications will reject network traffic originating from anywhere other than the IP addresses explicitly registered by an organization. Some organizations respond to this restriction by simply bypassing cybersecurity measures that modify or hide IP addresses. They send traffic directly to the service providers, which creates a security vulnerability.

Source IP Pinning allows organizations to control the IP addresses of devices sending data to service providers without bypassing security measures. Organizations can also use Source IP Pinning to hide internal resources from outside agitators looking for ways to penetrate and move laterally through the network.

App Access, Not Network Access

BlackBerry Gateway differs from a VPN in the way it grants access to business resources. A VPN authenticates to a network, offering successful attackers broad access to the environment. Instead, BlackBerry Gateway grants access to an app and offers no greater visibility into the network, drastically reducing the attack surface.

The continuous authentication capabilities of BlackBerry Gateway also differentiate it from the VPN approach. VPNs take a static approach to authentication and authorization. Once an entity passes the initial verification process, VPNs declare them safe for the duration of their connection. BlackBerry Gateway continuously authenticates external actors. It looks at multiple factors, including user behavior, device trustworthiness, and

network and app access patterns over the course of an engagement. When the Cloud AI senses something suspicious, it immediately takes measured steps to protect the environment based on the severity of the detection.

Strong TCP/IP Security

BlackBerry Gateway is built upon a robust TCP/IP stack with an IP security layer optimized for mobile and low-power devices. It offers extensive protocol support, including VOIP, a cloud-native architecture, and full-tunnel/split-tunnel access modes. Organizations relying on BlackBerry Gateway can use SaaS app identification to ensure services like O365 never error out. Malicious domains and locations can be identified using Gateway's IP reputation features and protect employees from interacting with dangerous network entities.

Network Threat Detection

BlackBerry Gateway detects threats existing in network traffic, including within encrypted packets, and contextualizes threat information identified throughout the network. The ability to analyze and correlate information across environments allows BlackBerry Gateway to identify complex and multi-stage threats invisible to other forms of analysis. The BlackBerry Gateway approach is high performance, requiring no packet decryption/re-encryption, and is therefore less demanding on network resources. Detecting threats within encrypted packets protects the environment without compromising the privacy of participants on the network.

COMMON BLACKBERRY GATEWAY USE CASES

By using an AI-empowered, Zero Trust approach to network security, BlackBerry Gateway solves many real-world problems facing organizations today. Examples of BlackBerry Gateway's features improving the business environment include:

AI-Empowered ZTNA

Secure access to the public Internet, and SaaS and on-premises applications, from anywhere. Enable high-fidelity VVoIP and safe browsing without a VPN.

Dynamic Network Access Controls

Network access controls are modulated with a real-time network risk score based on user or group behavior analytics.

AI-Empowered Network Threat Detection

Detect network threats and anomalies using AI without the need of network packet decryption.

Source IP Pinning

Limit unauthorized users from gaining access to business and network resources. Source IP Pinning allows organizations to control the IP addresses of devices sending data to SaaS providers without using techniques that bypass security measures.

One-Click Configuration

Configurable access for Microsoft 365 and other major SaaS apps.

Customizable Dashboards

SecOps can analyze network traffic patterns, compromises, and alerts. NetOps can analyze connector status, access histories, and top destinations.

LEARN MORE

BlackBerry Gateway is just one of the AI-empowered, preventative, world-class security solutions BlackBerry offers. Learn more about our full selection of security

suites designed to help your organization prepare for, prevent, detect, and respond to cyber attacks.

Discover:

BlackBerry® Cyber Suite

BlackBerry Spark® Suite

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 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**.*