BlackBerry Gateway White Paper

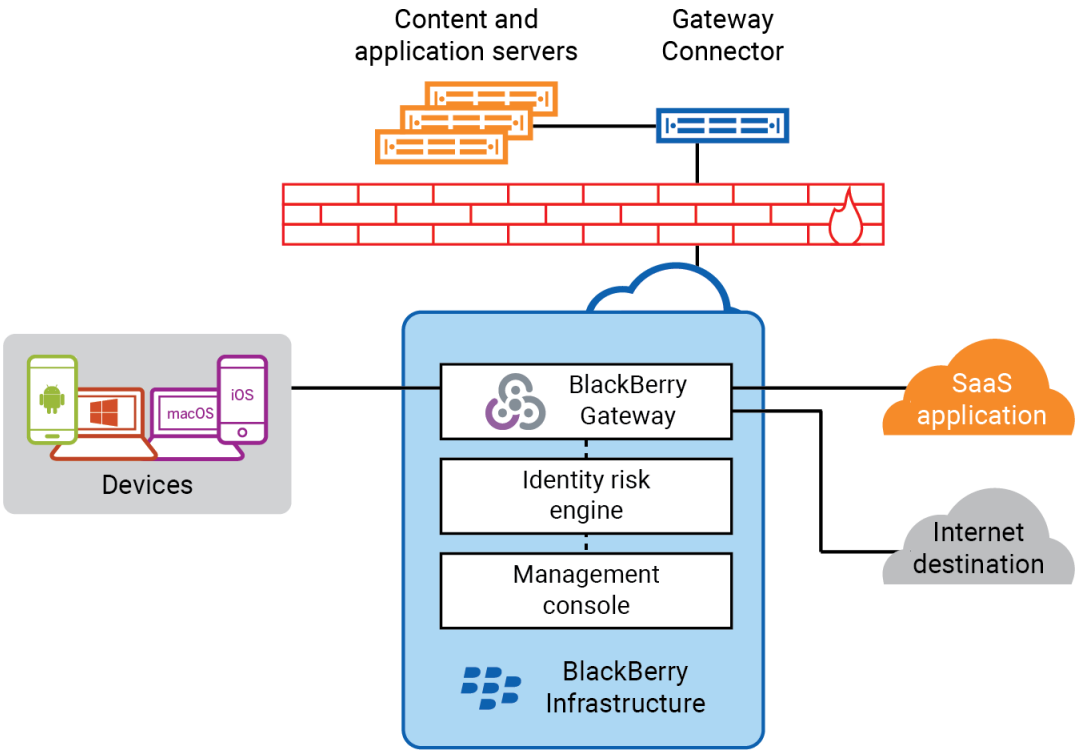
Zero Trust Network Access

BlackBerry Limited

www.blackberry.com

BlackBerry Gateway

Providing Zero Trust Network Access



Organizations today face a challenging environment as cybersecurity threats become more sophisticated and pervasive while the numbers of connected enterprise endpoints and the amount of data stored in the cloud grows exponentially. To maintain network security in your organization, a comprehensive security approach to both endpoint security and securing access to data in the cloud is essential to protect against and remediate cyberthreats.

Many organizations are embracing Software-as-a-Service as part of their current digital transformation and are increasingly relying on cloud-based services to provide critical business functions. Securing connections between users and business systems that lie beyond your firewall is essential and presents several challenges, particularly when users are working remotely and their devices connect to networks beyond your organization's control.

Until recently, many organizations have relied on a traditional "castle-and-moat" approach to network security where defenses surround the perimeter of the network, but once someone

has crossed the threshold or tunneled in, they are completely trusted. Network security experts now understand that this method is not sufficient for several reasons:

- Use of cloud-based services and SaaS applications is increasing, resulting in an extended and dynamic network perimeter where much of your proprietary data is stored outside of your physical location and more of your critical IT services reside in the cloud.
- Sophisticated phishing and social-engineering attacks can exploit users already inside the network.
- Using public Wi-Fi access points exposes various types of man-in-the-middle attacks, even for TLS traffic.
- Business partners, contractors, and large numbers of remote employees need access to your organization's tools and data to do their jobs, even when they are connected to networks outside of your perimeter.
- Performance deteriorates when you send traffic destined for cloud and SaaS services through your organization’s firewall and network.

Security-conscious organizations are moving to a Zero Trust approach to modernize network security while simultaneously enhancing and improving the network experience for end users. The Zero Trust security model trusts nothing and no one by default, including users inside the network perimeter. Every user, endpoint, and network are assumed to be potentially hostile. In Zero Trust security, no user can access anything until they prove who they are, that their access is authorized, that they’re not acting maliciously, and that the Wi-Fi or cellular network they are connected to is not compromised.

The question for organizations is how to implement a Zero Trust Network Access model that is continuously secure but still allows users to access all of the resources they need without losing productivity though frequent authentication prompts and reduced connection speeds. BlackBerry’s answer to this question is BlackBerry Spark.

BlackBerry Spark

BlackBerry Spark enables a Zero Trust security environment focused on earning trust across any endpoint, including desktop, mobile, server, and IoT. It continuously validates that trust at every event or transaction to deliver a Zero Touch experience for both IT and end users that improves security with no user interruption.

BlackBerry Spark offers suites of products that, together, provide a total solution for Zero Trust with full coverage across the full spectrum of devices, network, apps and people. BlackBerry Spark has these advantages:

- Provides a path from Zero Trust architecture to Zero Touch experience powered by strong AI
- Works across all endpoint types for complete coverage and better insight into trusted behavior

- Works with any Unified Endpoint Management (UEM) platform
- Provides continuous monitoring and threat detection to facilitate data and AI integrity
- Provides contextual and continuous authentication that spans endpoints, networks, apps, and people
- Builds on open standards to enable seamless integration with existing solutions
- Simplifies administration, reduces costs, and eliminates unnecessary friction

BlackBerry Gateway is the latest addition to BlackBerry Spark, designed to provide network security as a service from all of your endpoints to all of your access points.

Adopting a ZTNA framework for network security

Perimeter-based network security relies heavily on firewalls and VPNs to block untrusted traffic and protect trusted traffic moving in and out of the network. While they remain vital tools in your overall security solution, firewalls and legacy VPNs aren't enough to protect your network. Firewalls can't block all threats from trusted users or devices that may have been stolen or infected with a malicious app. VPNs provide encryption for trusted connections to prevent data from being compromised in-transit but don't protect your network from malware infecting a trusted device or prevent attacks from malicious apps or disgruntled insiders once a connection is trusted.

When users are connected to your network, you can block them from connecting to web sites that are known to contain malicious code or that violate your corporate use policy, but once your employees leave the building with their work laptops and mobile devices and connect to another network, your perimeter security can't block them or malicious apps on their devices from visiting those same web sites.

Legacy VPNs are also a less than ideal solution for connecting to SaaS applications. VPNs often won't connect through hotspots and hotel or airport Wi-Fi networks, they can be slow or disconnect easily over mobile networks, and they introduce latency for users who must tunnel into your network only to connect back out to a SaaS application, especially if those SaaS applications have secured access through restricted IP ranges.

If your organization is transitioning to a cloud-based model for many of your vital resources, your digital transformation needs to consider a Zero Trust Network Access (ZTNA) framework.

ZTNA combines secure web gateways and cloud access security brokers (CASB) to provide network security-as-a-service that both gives your users access to your extended network perimeter and protects your extended network from threats.

Secure web gateways use malware detection, URL filtering, machine learning, and other mechanisms to block users, processes, and apps from accessing Internet destinations, software, or data that could harm endpoints or your organization's IT infrastructure, and they can stand in the way of unauthorized access to SaaS applications.

CASBs act as a go-between for devices and other endpoints that access SaaS applications and other cloud services. They evaluate all traffic between endpoints and SaaS applications and allow organizations to set and enforce data protection and access control policies.

A ZTNA framework that combines a secure web gateway with a CASB and uses AI to continuously validate trust for all endpoints is a powerful tool for managing network security. You must consider several important factors when you implement ZNTA for your organization.

Protecting users out of the office

In today's business environment, users are working more and more outside of the office, whether they are working from home every day, travelling to meetings, or just keeping up with email after hours. Organizations need a solution that provides user-centric access control policies to protect every device used by every authorized user while they are connected to any work, home, or public network.

Compatibility with in-market apps

Organizations put a significant amount of money, time, and effort into choosing, deploying, and maintaining the apps employees use to do their jobs. A solution that works with the existing in-market apps employees are already using and doesn't require those apps to be reconfigured or redeployed has a lower total-cost-of-ownership than solutions that are more complex to implement or that only route traffic from a small number of apps.

Preserving battery and bandwidth

Mobile users need their battery to last them many hours, particularly when travelling, and they are not always able to connect to fast networks. If a significant portion of your employees are working at home, you need a solution that doesn't overload your VPN, strain your organization's network resources, and make slow connections even slower. To preserve battery and bandwidth, you need a solution that has a lightweight footprint on mobile devices and doesn't need to send traffic through your network before connecting to a SaaS application or another web site.

Protecting your privacy

Organizations want to keep their private data private, even from those they trust to secure it. To maintain your organization's privacy, you need a solution that can reliably detect threats in TLS traffic without decrypting it and compromising your privacy.

Malware detection

Secure web gateways analyze traffic moving in and out of endpoints to detect threats. To keep your users and networks safe, you need to detect far more than just known virus signatures. A solution that analyzes traffic using proven AI and machine learning techniques can detect new threats and zero-day attacks in real time. Machine learning techniques can also detect Internet

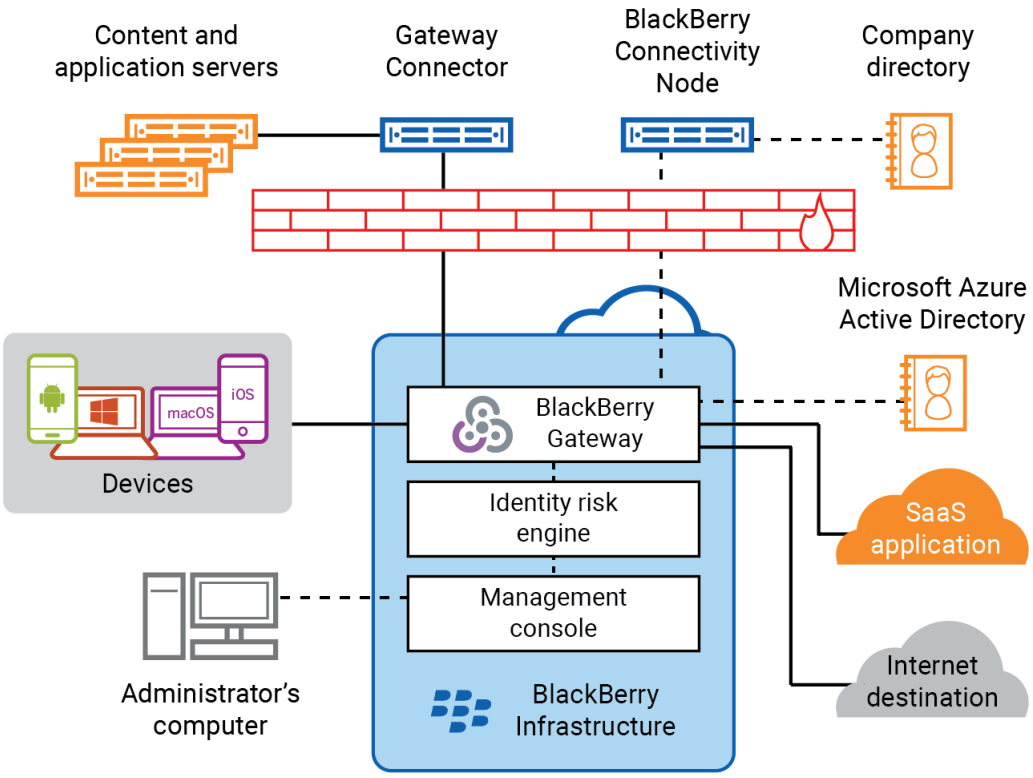
destinations that disperse malware and block users from connecting to the destination without relying on administrators to manually maintain lists of blocked addresses.

Application access control

You need to make sure that only trusted users can access your SaaS applications. At the same time, you need to make it easy for users to connect to services without requiring them to respond to multiple authentication prompts and enter multiple passwords on their devices throughout the day. A solution that analyzes user activity to identify risk levels and require additional authentication or deny access under anomalous conditions can help you satisfy the competing needs of Zero Trust and seamless access.

BlackBerry Gateway

BlackBerry Gateway answers the need for a secure, trusted, and lightweight solution by providing adding ZTNA to BlackBerry Spark. It uses a lightweight app or agent installed on users' devices, the established and trusted BlackBerry Infrastructure, and the BlackBerry AI and Machine Learning powered risk engine to provide Zero Trust network access from any app on any device used for work to any on-premises or cloud-based location inside or outside of your firewall.



How does BlackBerry Gateway work?

BlackBerry Gateway acts as both a secure web gateway and an inline CASB to provide several features that protect your organization's endpoints, data, and extended network. BlackBerry Gateway protects users' devices and other endpoints by allowing you to block access to Internet destinations with malicious content and web sites that don't meet your organization's acceptable use policy, even when users aren't directly connected to your organization's network. BlackBerry Gateway protects your data using network access control policies, and its AI and machine learning capabilities to provide Zero Trust access to your private network, SaaS applications, and other cloud-based resources.

Administrators manage BlackBerry Gateway using the cloud-based management console shared by many BlackBerry Spark products. Administrators can rely almost entirely on the robust BlackBerry AI to determine whether their users' connections are safe, or they can actively set network access control policies and block users' connections to sites that contravene your acceptable use policy. You can define policies and access rules at the organization, group, and user level.

An app installed on an iOS, Android, Windows 10, or macOS device communicates with BlackBerry Gateway in the BlackBerry Infrastructure. When any other app attempts to make a connection, BlackBerry Gateway uses automated and administrator-managed policies to determine whether to block the connection or route it to its destination.

Blocking unsafe and malicious connections

The first level of network security that BlackBerry Gateway provides blocks connections to Internet destinations that you don't want devices to reach. For example, if the user taps a link in an email message that goes to a site that BlackBerry Gateway knows to be malicious, BlackBerry Gateway blocks the connection to that destination.

The BlackBerry risk engine uses AI, machine learning, and many factors, including IP reputation, continuously updates an ever-growing list of unsafe Internet destinations that it can block endpoints from connecting to. Your administrators no longer need to manually maintain a list of blocked Internet destinations that contain threats.

If your organization wants to block users from visiting specific sites that violate your corporate use policy, you can create access control policies to specify additional destinations that all users or specific users or groups can't access, even when they are logged into an external network.

Securing connections to SaaS services

In addition to protecting devices, BlackBerry Gateway protects access to your organization's cloud-based applications according to the Zero Trust model and analyzes in real time whether each requested connection should be allowed. For example, a user opens their calendar app and attempts to get their schedule from Office 365. The BlackBerry Gateway app establishes a secure tunnel to the BlackBerry Infrastructure. If the BlackBerry Gateway AI has not detected

recent anomalous behavior, BlackBerry Gateway allows the connection to continue over the Internet

BlackBerry Gateway also supports using source IP pinning when forwarding connections to your cloud services. If your SaaS application can be configured to accept connections only from specific IP addresses, you can configure it to accept connections from BlackBerry Gateway source IP addresses dedicated to your organization. Devices that try to connect from addresses you haven't specified are denied access.

Securing connections to your private network

If you install the optional BlackBerry Gateway Connector, behind your firewall or in private cloud networks you can use BlackBerry Gateway to provide access control for your private network. BlackBerry Gateway establishes a secure tunnel between the BlackBerry Infrastructure and your private network. The Gateway Connector allows users to communicate with content and application servers behind your firewall using BlackBerry Gateway instead of a traditional VPN.

Integrating with BlackBerry Protect

BlackBerry Gateway integrates with BlackBerry Protect, which continuously evaluates the device security posture and detects and blocks malware before it can affect a device. BlackBerry Protect and uses machine learning techniques to detect malware and render new malware, viruses, bots, and future variants useless.

How BlackBerry Gateway uses AI to protect devices

BlackBerry Spark resides in the network data path and uses artificial intelligence and machine learning to create models that help determine user risk levels based on behavioral factors. BlackBerry Gateway uses these models to help uncover potential threats and apply appropriate remediation in real-time when needed.

Behavioral factors

Behavioral factors consider common behavior for the user and normal behavior for other users in similar roles and locations. For example: has user connected to this network before? Is this a normal time of the day and day of week for the user to be working? Is the behavior consistent with the user's own past behavior? Is the behavior consistent with many other users' past behavior?

Identifying anomalies

The BlackBerry AI uses machine learning techniques to find anomalies. Because BlackBerry Gateway is in the data path, it can examine usage patterns to identify anomalies that may be potential threats. The BlackBerry AI examines patterns holistically and relationally and considers multiple parameters. Using these techniques, BlackBerry Gateway can identify

intruders, malicious insiders, and bots, and other forms of malware that may be exfiltrating data or engaging in a command-and-control attack with anomalous external hosts.

Risk scores

Based on various factors, BlackBerry Gateway continually calculates risk scores for users. If the risk score is normal, BlackBerry Gateway allows users to connect to Internet destinations and authenticate with your cloud-based resources using your organization's normal access controls for SaaS applications. If a condition changes that increases the risk score, BlackBerry Gateway evaluates the change and acts according to your established policies. For example, BlackBerry Gateway may notify administrators of anomalous activity, limit or deny access to the resource, or request additional authentication beyond what is normally required to access your private network or the SaaS application.

Protect your organization with BlackBerry Spark and BlackBerry Gateway

BlackBerry Gateway protects your network both inside and outside your firewall. BlackBerry Gateway blocks intruders and malicious insiders from accessing information, and it stops bots and other forms of malware that have found their way onto an endpoint from reaching command and control servers.

BlackBerry Spark provides comprehensive Unified Endpoint Security (UES) to deliver Zero Trust security with a Zero Touch user experience. BlackBerry Gateway adds network security-as-a-service to BlackBerry Spark. Together, they offer visibility and protection across all endpoints and for connections to all of your cloud and network resources, and use AI, machine learning, and automation to provide improved cyberthreat prevention.

For more information on BlackBerry Gateway and BlackBerry Spark, visit www.blackberry.com.

Glossary of terms

AI/ML – Artificial Intelligence and Machine Learning

Artificial intelligence (AI) is a system that has been taught or has learned how to carry out specific tasks without being explicitly programmed how to do so. Today, most of the fruitful research and advancements have come from the sub-discipline of AI called machine learning (ML), which focuses on teaching machines to learn by applying algorithms to data.

NSaaS –Network Security as a Service

A security model where access to SaaS applications and other resources are protect by cloud-based network security tools.

Digital transformation

The process of updating business practices and implementing new technologies that help your organization to take advantage of and adapt to the rapidly and continuously evolving online world.

EMM – Enterprise Mobility Management

A comprehensive solution for managing mobile users, including mobile device management (MDM), mobile application management, identity and access management, and mobile content management.

Man-in-the-middle attack

A man-in-the-middle attack is a cybersecurity threat where a third-party inserts themselves in the middle of a connection between two parties for the purpose of eavesdropping or altering or disrupting communications. Attempted man-in-the-middle attacks are common on unsecured networks such as public Wi-Fi networks.

MTD – Mobile Threat Defense

A class of mobile security capabilities designed to counteract mobile malware and cyberattacks. These capabilities go beyond traditional EMM solutions and offer an extra layer of security by preventing, detecting, remediating, and improving overall security hygiene for an organization's entire mobile fleet and applications.

SaaS – Software-as-a-Service

A software delivery model where applications are hosted on cloud-based servers and users subscribe, individually or through their organization, to use the software through client app or web browser.

VPN – Virtual Private Network

Technology that allows a device to connect to a private network over the Internet and behave is if it were directly connected to the private network. Organizations often use VPNs to provide a secure tunnel between their network and remote users so that employees can securely access network resources while they are off-site.

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 150M 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.

BlackBerry. Intelligent Security. Everywhere.

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