BlackBerry | Cybersecurity

CylanceGATEWAY

AI-Empowered, Cloud-Native Zero Trust Network Access

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 expansion of remote work has blurred the traditional network perimeter, resulting in a significant increase in the organization's attack surface. Each new device, application, and user connecting with business resources introduces additional security risks. When remote workers connect a wide variety of unmanaged devices to the business network, these risks quickly multiply.

Recent estimates by Gartner indicate 74% of companies intend to permanently shift employees to a more remote work environment post COVID-19.[1] This workforce transformation 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.

CylanceGATEWAY™ 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 no longer viable. By implementing an AI-empowered Zero Trust framework, CylanceGATEWAY uses continuous authorization 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 its trustworthiness to receive access.

CylanceGATEWAY CAPABILITIES

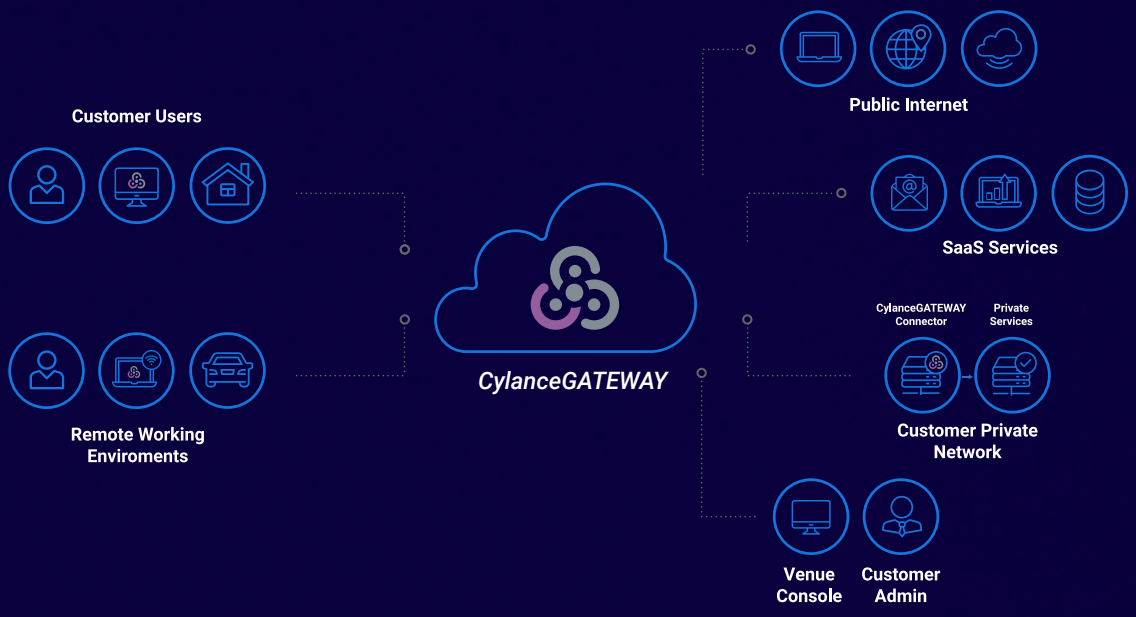
CylanceGATEWAY™ brings several advanced technologies together to keep network environments secure. It is built upon a robust TCP/IP stack, optimized for mobile and remote devices, and can detect threats in encrypted packets. It uses AI to detect suspicious behavior and anomalies throughout the environment, adjust access in real-time, and correlates and contextualizes threat information often overlooked by legacy solutions. CylanceGATEWAY protects networks, applications, and data without disrupting user productivity and without sacrificing privacy. Segmentation capabilities hide applications from public visibility, reducing the risk of DDoS attacks and preventing lateral movement. Source IP Pinning limits SaaS app connectivity to only trusted and known IPs, and the power to use customizable private IPs offers the flexibility to avoid errors in routing with other endpoints. CylanceGATEWAY enables precise, identity-aware, access provisioning to on-premises and cloud resources.

AI-EMPOWERED, ADAPTIVE, SECURE ACCESS

CylanceGATEWAY uses cloud AI to continuously analyze a number of factors when determining remote participants' trustworthiness and access privileges. 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 the user's IP address trusted?
- Is the participant who they say they are?
- Is the participant behaving normally?

CylanceGATEWAY at a Glance
AI-Assisted Zero Trust Network Access



CLOUD AI

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

- 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 user's trust score changes, the cloud AI can inform dynamic policy on the fly to take various actions. For positive changes in trust, a user may inherit modified or upgraded access privileges. Negative trust changes may result in restricted access, a request to re-authenticate, or trigger security alerts and remediation procedures.

FULL/SPLIT TUNNEL NETWORK SERVICES

CylanceGATEWAY™ 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 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. CylanceGATEWAY can also be configured in a per-app tunnel mode to manage application access further.

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 communicating with service providers without bypassing security measures.

Organizations can also use Source IP Pinning to hide internal resources from outside agitators looking to penetrate and move laterally through the network.

APP ACCESS, NOT NETWORK ACCESS

CylanceGATEWAY™ 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. CylanceGATEWAY grants segmented access to authorized applications via outbound-only connections stitched together at the service edge, ensuring users are never placed on the network. This segmentation hides applications from public visibility, prevents lateral movement, and drastically reduces the attack surface. It also offers network administrators greater visibility into user activity and traffic on the network.

The continuous authentication capabilities of CylanceGATEWAY also differentiate it from VPNs, which 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. CylanceGATEWAY continuously authenticates every network participant, eliminating excessive implicit trust. It looks at multiple factors, including user behavior, device trustworthiness, and network and app access patterns over an engagement. When the cloud AI senses an anomaly, it immediately takes measured steps to protect the environment based on the severity of the detection. CylanceGATEWAY can even detect DNS tunneling attacks to prevent adversaries from communicating using DNS protocol.

STRONG TCP/IP SECURITY

CylanceGATEWAY is built upon a robust TCP/IP stack with an IP security layer to enable secure connectivity via Windows®, macOS®, iOS®, and Android™ devices. It offers extensive protocol support, including VoIP, a cloud-native architecture, and full/split-tunnel access modes. Organizations relying on CylanceGATEWAY can use SaaS app identification to keep services like O365 from erroring out. CylanceGATEWAY protects against dangerous domains and addresses by using IP and URL reputation and classification features, preventing users from intentionally or unintentionally accessing them.

NETWORK THREAT DETECTION

CylanceGATEWAY 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 CylanceGATEWAY to identify complex and multi-stage threats invisible to other forms of analysis. The CylanceGATEWAY approach is high performance, requiring no packet decryption/re-encryption, and is therefore less demanding on network resources. By detecting threats within encrypted packets, CylanceGATEWAY protects the environment without compromising the privacy of participants on the network.

COMMON CylanceGATEWAY USE CASES

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

ZERO TRUST ADOPTION

Improve your overall risk posture by implementing a dynamic least-privilege network access model and adaptive identity-based controls, critical components of a Zero Trust architecture.

SECURE ACCESS FOR ALL USERS

Secure your hybrid business model and remote workforce with flexible access to critical resources on-premises or in the cloud.

ENDPOINT AND NETWORK SECURITY

Ensure protection across all endpoints and networks with integrated solutions that work smarter, not harder, providing enhanced visibility and safety against current and future cyberthreats.

IMPROVED COLLABORATION

Enable faster, more secure access beyond your FTEs. Contractors, vendors, and strategic partners can safely access resources to promote productivity on both managed and unmanaged devices.

VPN REPLACEMENT

Eliminate excessive implicit trust and latent risk by migrating away from antiquated perimeter defense solutions that expose your business to credential misuse and abuse.

MERGERS, ACQUISITIONS, AND DIVESTITURES

Improve the speed and agility of transformative events without the need to integrate networks to enable productivity. Deliver a more unified, stable, and secure experience with ease.

REAL-TIME VISIBILITY

Network administrators and security personnel can access detailed user activity information and use application discovery to make informed networking risk decisions.

GRANULAR POLICY MANAGEMENT

Take control of your networks and applications with outbound-only secure access and adaptive least-privilege policy management, enforced by a cloud-AI risk engine.

WHY CHOOSE CylanceGATEWAY

Adoption and Configuration

One-click configuration for many of the most popular SaaS apps streamlines operations for network administrators. Quick implementation improves the end-user experience.

Network Risk Reduction

Prevent unauthorized users from accessing your network with source IP Pinning technology. The use of customizable private IPs offers the flexibility to avoid errors in routing with other endpoints.

Network and Activity Visibility

Access insights at a glance with a user-friendly dashboard and real-time visibility into network traffic, security events, and indicators of compromise. View statuses, access histories, and top destinations.

Anywhere, Any-Device Connectivity

Enable your distributed workforce to work from home or from anywhere on both managed and unmanaged devices. Available for macOS, Windows, iPhone, and Android.

LEARN MORE

CylanceGATEWAY™ 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 cyberattacks.

Discover:

BlackBerry® Cyber Suite

BlackBerry Spark® Suite

[1] https://www.gartner.com/en/newsroom/press-releases/2020-04-03-gartner-cfo-surey-reveals-74-percent-of-organizations-to-shift-some-employees-to-remote-work-permanently2

Fast and Reliable Performance

Leverage the edge accelerator to optimize network paths, improving performance and speeds. Robust and resilient tunnel technology enables high-fidelity connections for any app and VoIP.

Integrated Threat Detection

CylanceGATEWAY conducts AI-assisted network threat detection by analyzing network telemetry without decryption. CylanceGATEWAY native integration with BlackBerry Spark® Unified Endpoint Security Suite ensures only healthy devices receive network access.

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 195M 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.

BlackBerry. Intelligent Security. Everywhere.

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

BB23 | 220627