BlackBerry | Cybersecurity

# BLACKBERRY CYBERSECURITY PRODUCT AND DATA SECURITY BRIEF

*Shared Under NDA Only*

SECURITY BRIEF

This document describes how the BlackBerry® endpoint cybersecurity product and software development lifecycle ensures the security of our products, our infrastructure, and our customers' data.

BlackBerry endpoint cybersecurity products extend protection across organizations by combining network and endpoint telemetry to provide full visibility, enabling preventative protection, instant response, and threat hunting fully managed by an expert team of BlackBerry analysts 24x7x365. This provides organizations with peace of mind and drastically reduces the costs associated with building a security operations center (SOC).

AI-powered BlackBerry endpoint cybersecurity products prevent threats such as zero-day threats and phishing attacks on Windows®, Mac®, Android™, iOS®, and Windows Server, both online and offline, while combatting against security gaps with full visibility and advanced threat hunting capabilities. An added layer of zero-trust network access provides a proactive approach and hardens defense with continuous network authentication, preventing both insider and external attacks.

The Cylance® management console and infrastructure services from BlackBerry are hosted on Amazon Web Services (AWS). AWS is a highly available, scalable, and secure cloud service that makes deploying BlackBerry endpoint security products less cumbersome than traditional security products.

The use of AWS allows BlackBerry to deliver the following benefits to customers:

- Lower operational costs as compared to traditional, on-premises solutions that require additional hardware
- Highly available endpoint security products with real-time monitoring of the services to ensure minimal service interruptions
- Low maintenance requirements given the cloud-based delivery of the endpoint security products
- Safeguarded endpoint security with encryption, authentication, audit logging, penetration testing, etc.

- Ability to scale the deployment of endpoint security products on an as-needed basis
- 24x7x365 data center and software support operations

## *How BlackBerry Endpoint Cybersecurity Products Use the Cloud*

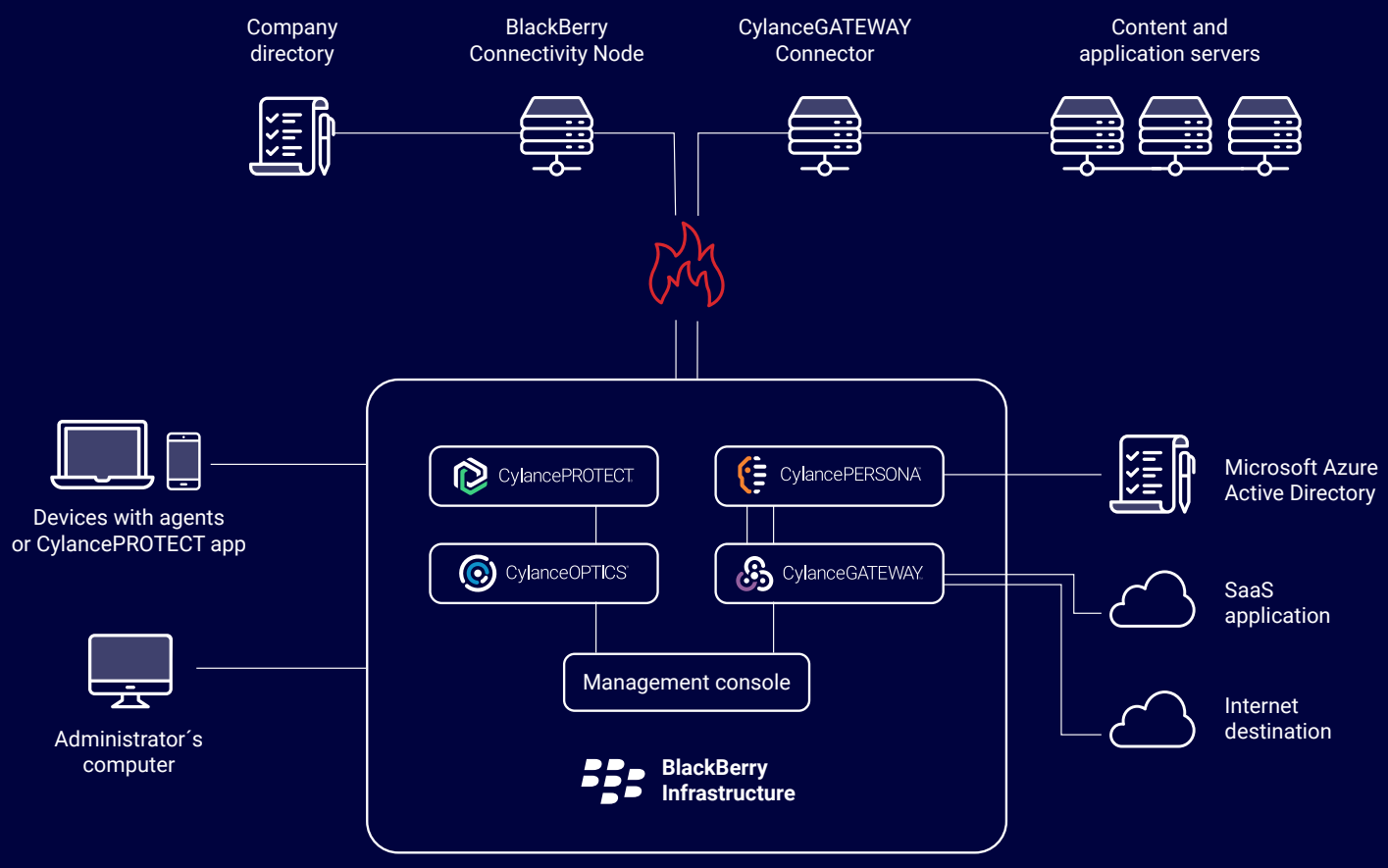
BlackBerry endpoint cybersecurity products use the cloud for data analysis and hosting the Cylance management console, which allows customers to interact with their security solution from any web browser. The AI-based Cylance data analysis system, known as CylanceINFINITY™, generates highly effective mathematical models designed to solve discreet security challenges.

CylanceINFINITY works by collecting and analyzing security-related data about portable executable (PE) files as well as system behaviors. Then, using machine learning, it calculates likely outcomes based on what the dataset illustrates. The results generated are constantly getting smarter from environmental feedback and a constant stream of new data from all around the world.

From this machine learning and data analysis, compressed artificial intelligence models are then created to be deployed and used locally on endpoints.

See Figure 1 for an overview of the architecture of BlackBerry endpoint cybersecurity products and their interactions with the cloud services.

*Figure 1 – BlackBerry Endpoint Cybersecurity Product Architecture*



**Cylance Agent/Service - Cloud Communications**

| URL | TYPE | DETAILS |
|---|---|---|
| *login.cylance.com* | **Device Registration** | • Register new devices<br>• Re-register new devices |
| *data.cylance.com* | **Status Calls (via REST Service): Communicates at randomized minute** | • Global quarantine<br>• Client status<br>• Policy<br>• Safe list<br>• Events<br>• System info report<br>• System threat list report |
| *update.cylance.com* | **Agent/Service Updates** | • Agent/Service gets update from agent update, not web console<br>• Simultaneous updates are throttled per organization<br>• Prevents network disruption<br>• Default throttle set at 1,000 agents<br>• Throttle can be changed by Cylance Support |
| *Api2.cylance.com/api.cylance.com* | **Threat Analysis** | • Performs threat analysis and cloud scoring (Cylance Score)<br>• Sends unknown files up to the cloud for analysis<br>• Domain is depreciated but is kept open to support older CylancePROTECT Desktop agents. Api2.cylance.com directs to the same destination as api.cylance.com for the purpose of threat analysis and risk scoring |
| *cement* | **Handling incoming client traffic and optimize outgoing resources** | • Handles incoming client traffic and optimizes outgoing resources on a global scale between endpoint agents and the cloud backend<br>• Policy distribution to endpoints<br>• Tenant content tailored such as black and white lists<br>• General content that applies to all users<br>• Updates for new agent versions, model updates, and other required content updates |

The CylancePROTECT® agent is lightweight and installed on endpoint devices, which communicates with the cloud service to:

- Pull down policy
- Send information about threats and hosts
- Receive commands sent out through the management console
- Upload potentially malicious file samples (configuration set by customer)
- Download agent updates

The agent uses Transport Layer Security (TLS) to secure customers' data and provide privacy and integrity of the data being transferred. The cloud connection also uses digitally signed certificates to authenticate the Amazon RDS as agents are locked to shards cryptographically.

In addition to the CylancePROTECT agent, the CylanceOPTICS® agent is installed on each endpoint to enable additional capabilities. The service communicates with the cloud service to:

- Pull down policy
- Transmit user-requested search results
- Transmit automated root cause analysis and telemetry data
- Download service updates
- Receive context analysis engine rules and updates
- Provide remote response

The CylanceGATEWAY™ agent is installed on each endpoint to enable Zero Trust Network Access (ZTNA). The service communicates with the cloud service to:

- Pull down policy
- Log all network activity for devices that have work mode enabled
- Provide access to the network from authorized endpoints

The CylancePERSONA™ agent is installed on each endpoint to enable the artificial-intelligence-based identity and access management (IAM) solution to enable continuous authentication. The service communicates with the cloud service to:

- Pull down policy
- Receive and update the user, event, and scoring model

BlackBerry endpoint cybersecurity products also support strong authentication via both SAML and OIDC, and local multi-factor authentication. The providers we support are: OneLogin, Okta, Active Directory Federation Services, Azure Active Directory, and PingID.

The steps taken to ensure data integrity, security, availability, and privacy of the BlackBerry endpoint cybersecurity products are discussed in the following sections.

BlackBerry has a dedicated Product Security Incident Response Team (PSIRT) responsible for managing vulnerabilities that are discovered in BlackBerry in-market products. This includes monitoring for new attack techniques in the industry, vulnerabilities in open-source libraries, and working with customers and researchers who may discover vulnerabilities in our products. We work collaboratively with customers and security researchers who discover and report vulnerabilities to BlackBerry to remediate those vulnerabilities. The BlackBerry PSIRT team has developed a coordinated vulnerability disclosure policy aligned with ISO29147.

## *Data Control, Privacy, and Portability*

**Multi-Tenancy** — Databases are run within Amazon's Relational Database Service (RDS). Amazon RDS automatically patches and backs up the database, enabling point-in-time recovery. Critical and private data is isolated with, and protected, using the encryption on RDS with both key management and rotation to ensure customer data is always protected. Using the multi-zone deployment option for mission-critical workloads ensures high availability and provides a built-in automated failover from the primary database to a synchronously replicated secondary database in case of a failure.

BlackBerry endpoint cybersecurity products support deployments in AWS GovCloud and can also provide dedicated databases for customers at an additional charge. BlackBerry uses a multi-tier architecture and never exposes RDS instances to the Internet.

**Data Security** — BlackBerry endpoint cybersecurity products are designed to collect and store minimal customer data. No data is shared among customers. BlackBerry utilizes OAuth for administrator authentication to limit exposure to sensitive customer login details, which means that no login credentials could be retrieved if somebody accessed our entire database. The only instance in which credentials are stored in the BlackBerry systems is when the customer chooses to use the BlackBerry Online Account system (a BlackBerry IDP) to authenticate administrators.

**Security Controls** — To ensure security in AWS, BlackBerry uses the following security controls:

| SECURITY CONTROL | PROTECTION PROVIDED |
|---|---|
| Strong Authentication | Prevent credential misuse |
| Virtual Private Network | Enable secure communications |
| Firewall | Prevent malicious network access |
| Intrusion Detection | Detect suspicious network or host activity |
| Log Monitoring and Analysis | Detect multi-facet attacks |
| CylancePROTECT | Prevent malware |
| CylanceOPTICS | Prevent and detect advanced attacks |

In addition to these security controls, BlackBerry regularly performs penetration testing of the AWS environments.

**Data Privacy** — Customers have the option of uploading portable executable files to the management console from CylancePROTECT, which generates additional evidence, such as threat indicators, by analyzing uploaded files. Uploaded samples are de-identified and information about the customer submitting the file is not tracked. BlackBerry de-identifies all API inputs.

BlackBerry aggregates data to calculate metrics and uses individualized API keys for accounting and abuse prevention, however individual submissions to API keys cannot be linked. As an example, BlackBerry can tell if a customer is using the service, and at what rate, but it is not possible to generate a report detailing the information customers have submitted. Enabling these policies will affect the data visible to company administrators and may make it more difficult to resolve detected issues.

BlackBerry endpoint cybersecurity products collect data from each device on which they are installed.

Below is a listing of the data that CylancePROTECT and CylanceOPTICS generates and transfers to the cloud servers, based on the customer's configuration.

**In-Region Hosting** — To help customers meet their data privacy requirements, BlackBerry infrastructure is deployed across multiple geographies to meet customers' requirements. Current locations include Australia, Brazil, Germany, Japan, and the United States.

**Data Portability** — BlackBerry allows the export of many pieces of information in the console. Users can

extract their threat and device data and take it with them or back it up locally. BlackBerry APIs let customers extract this information programmatically.

**Data Retention** — BlackBerry will contact the customer at the end-of-contract to facilitate data removal or data transfer. Data collected by the CylanceOPTICS process is stored on the endpoint and by default it is restricted to 1 GB. Alert data is stored in the cloud for 30 days by default.

**Data Items Collected by CylancePROTECT and Transmitted/Stored in the Management Console**

*signifies data can be suppressed by policy

| **USER ACCOUNT INFORMATION FOR EACH CYLANCEPROTECT ADMINISTRATOR LOGIN** | |
|---|---|
| Administrators | Email address<br>Level of access to zones |
| **DEVICE INFORMATION STORED FOR EVERY DEVICE PROTECTED BY CYLANCEPROTECT** | |
| Operating System, Version, and Service Pack | Windows Security settings enabled/disabled<br>Antivirus<br>Anti-malware Firewall<br>UAC<br>Windows Update<br>Network Access Protection |
| *Network* | **MAC address(es)***<br>**IP address(es)***<br>**Hostname and FQDN*** |
| *Agent* | **CylancePROTECT agent version**<br>**CylanceOPTICS agent version** |
| *Device Identity* | **Device's distinguished name***<br>**Device's group membership from Active Directory last logged in user account name*** |
| *Executables* | **SHA256, MD5 and SHA1 hash**<br>**File data uploaded to cloud (if and only if enabled in policy, or requested individually by an administrator)** |

| | |
|---|---|
| *Threats* | File owner*<br>File path*<br>Location on disk<br>Drive type (USB \| Internal \| Network, etc.) Created/Access/Modified date time<br>Code signing certificate information Cylance score |
| *Agent Logs* | Agent operational and debug logs, automatically when enabled in policy, or individually on an administrator's request |
| **OPERATIONAL METRICS ABOUT THE CYLANCEPROTECT SERVICE RUNNING ON EACH ENDPOINT** | |
| *CPU* | CPU user %<br>CPU priv %<br>CPU total % |
| *Agent Process* | Thread count<br>Handle count<br>Elapsed time |
| *Memory* | Paged memory size 64 (K)<br>Peak paged memory size 64 (K)<br>Paged system memory size 64 (K)<br>Nonpaged system memory size 64 (K)<br>Working set private memory 64 (K)<br>Working set 64 (K)<br>Peak working set 64 (K)<br>Private memory size 64 (K)<br>Page faults per sec<br>Virtual memory size 64 (K)<br>Peak virtual memory size 64 (K) |
| *I/O* | IO data bytes per sec |
| *Network* | Bandwidth usage |

**Data Items Collected by CylanceOPTICS and Transmitted/ Stored in the Management Console**

CylanceOPTICS captures endpoint data to assist in root cause analysis, threat hunting, and incident response to threats and outbreaks. CylanceOPTICS stores the data it collects into BlackBerry's AWS cloud instance. CylanceOPTICS caches the most recent events locally in an encrypted database on each endpoint to reduce security blind spots when a device is offline. CylanceOPTICS only collects data when it has been enabled by policy.

CylanceOPTICS also features several automated workflows that gather and correlate data from endpoints to reduce the amount of time required to investigate and respond to security incidents.

To create an accurate timeline of events or contextual analysis should a security incident or investigation occur, CylanceOPTICS records a large portion of all the security events that occur on an endpoint. These events are generally composed of any combination of eleven groups, known as artifacts: API Calls, DNS, Event, File, Network, PowerShell trace, Process, Registry, Users, Windows event, and WMI trace. While these artifacts are collected and cached locally, when an event occurs, the relevant subset for the event may be uploaded to BlackBerry cloud services. Not all of them may currently display in the management console.

The following CylanceOPTICS features will automatically upload different combinations and quantities of the above artifacts to BlackBerry cloud services depending on how an environment's device policies and features are configured.

For more information on data structures that CylanceOPTICS uses to identify threats, please access BlackBerry Docs: https://docs.blackberry.com/en/unified-endpoint-security/blackberry-ues/administration/administration/Analyzing-endpoint-data-collected-by-Optics/Data-structures-that-Optics-uses-to-identify-threats

**Data Items Collected by CylanceGATEWAY and Transmitted/Stored in the Management Console**

CylanceGATEWAY logs all network activity for devices that have work mode enabled. The network activity log records the user, device model and OS, destination, date and time, and other details about each attempted connection event.

If a connection is identified as a potential threat, the Anomaly column specifies the type of threat detected.

- **Behavioral risk** anomalies are potential threats based on unusual user behavior.
- **DNS Tunneling** anomalies are potential threats based on analysis of the DNS traffic from the client to the attacker's DNS server.
- **Reputation** anomalies are potential threats from addresses on the BlackBerry list of unsafe Internet destinations and are detected by destination reputation.
- **Signature detection** anomalies refer to potential threats detected by intrusion protection.

**Data Items Collected by CylancePERSONA and Transmitted/Stored in the Management Console**

CylancePERSONA retains alert data for 90 days in the management console which includes the following:

- **2FA Provisioning:** The user set up two-factor authentication on a device.
- **Alert Only:** An alert was triggered for the user. No mitigation action has been triggered.
- **Failed 2FA Logon:** The user failed to pass the 2FA logon.
- **Forced Step-Up Authentication (Mitigation Triggered):** The user was required to enter their username and password or to pass a 2FA challenge to continue using the device.
- **Lateral Movements:** The user's credentials are being used to log in to another device, which can be a sign of compromised user credentials.
- **User Failed Logon:** The user failed to enter the correct username and password when logging into the device.

## *Availability and Scalability*

Amazon runs one of the best-connected networks available. AWS datacenters are massively cross-connected to every major backbone provider. Details on the AWS global infrastructure can be found on Amazon's website. Additionally, AWS offers large interconnect points at nine global centers, with more than 100 edge connections, ensuring high likelihood of continued availability. BlackBerry can mirror the Cylance management console to any of the nine major centers with very little effort.

The BlackBerry DevOps team is responsible for uptime and currently tracks to 99.95% availability. Customers are notified about all planned maintenance. Unplanned outages trigger email notifications and are posted on the BlackBerry Customer Support Portal. Even in the event of an unexpected outage of the cloud service, all devices are fully protected. The CylancePROTECT agent can analyze and quarantine threats autonomously without a cloud connection. There is no loss of protected device logging data. Please note that each customer tenant can handle many hundreds of thousands of endpoints and where higher scalability is required, further provision can be made by the BlackBerry web operations team.

AWS is one of the most scalable cloud-based web services available today. A recent report found that one-third of Internet users access at least one site hosted on AWS on an average day. AWS receives around 1% of all Internet traffic. Many of the most popular sites use AWS exclusively, while many more use it in some capacity. AWS clients include the FDA, NASA/JPL, Centers for Disease Control and Prevention, Comcast, Unilever, Siemens, Novartis, Instagram, Netflix, Pinterest, and Salesforce.com.

**Product Certifications**

| CERTIFICATIONS | SCOPE | DATA OBTAINED |
|---|---|---|
| FedRAMP | CylancePROTECT<br>CylanceOPTICS | January 2017 |
| Unqualified SOC2 Type 2 | CylancePROTECT<br>CylanceOPTICS | July 1, 2017 through June 30, 2018 |
| StateRAMP | CylancePROTECT<br>CylanceOPTICS | January 10, 2022 |

BlackBerry maintains multiple certifications to demonstrate leadership in product security and to ensure the company follows a standardized approach to security assessment, data handling, and continuous monitoring.

In addition, BlackBerry used a third-party assessor to validate our adherence to the Privacy Shield Framework. BlackBerry also performs third-party validation for PCI and HIPPA/HITECH. CylancePROTECT has been certified compliant with HIPAA/HITECH malicious software protection, detection, and reporting requirements. The certification is made by DirectDefense, a leading provider of HIPAA/HITECH security assessment services to industries, such as healthcare and insurance, that process, store, or transmit electronic protected health information (ePHI).

CylancePROTECT also achieved PCI-DSS Requirement 5 compliance attestation which states that all organizations must run anti-malware solutions to protect payment card data. DirectDefense, a PCI Qualified Security Assessor company, certified the usage of CylancePROTECT to meet PCI-DSS anti-malware requirements.

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 | 220722