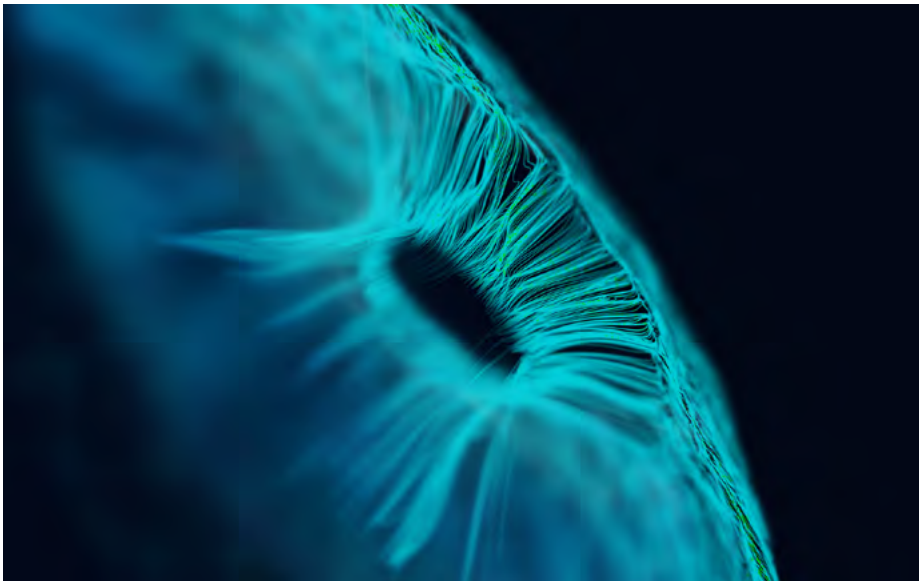
BlackBerry
Intelligent Security. Everywhere.

Datenblatt

# BlackBerry Optics

Erkennung und Bekämpfung von Bedrohungen auf Endpunkten auf der Basis von KI



## Präventionsorientierte EDR

Präventionsprodukte, die sich auf Signaturen verlassen, können mit modernen Angriffen nicht mehr mithalten, da sich diese blitzschnell verändern. Die Folge: Sicherheitsteams müssen sich durch Unmengen täglicher Warnmeldungen kämpfen. Da ist es nahezu unmöglich, kritische Sicherheitsprobleme aufzuspüren, sodass sich Angreifer ungestört im Unternehmen ausbreiten können.

Präventionsorientierte Sicherheit kann die Anzahl der durch die Sicherheitsinfrastruktur erzeugten Warnungen deutlich verringern. Dies verringert die Belastung und die Frustration, die mit endlosen, fruchtlosen Untersuchungen von Warnmeldungen einhergehen.

Während BlackBerry® Protect Malware, schädliche Skripts, unseriöse Anwendungen und dateilose Angriffe daran hindert, dem Unternehmen Schaden zuzufügen, bietet BlackBerry® Optics auf der Basis von künstlicher Intelligenz (KI) die EDR-Funktionen, die Sie benötigen, um Daten und Unternehmen zu schützen.

## Auf der Basis von KI

BlackBerry Optics ist eine EDR-Lösung, die den von BlackBerry Protect gebotenen Schutz vor Bedrohungen ausweitet. Sie setzt auf KI, um weitläufige Sicherheitsvorfälle zu identifizieren und zu verhindern.

BlackBerry Optics bietet Folgendes:

- KI-basierte Verhinderung von Vorfällen
- Kontextorientierte Erkennung von Bedrohungen
- Erkennung von Bedrohungen durch maschinelles Lernen
- Ursachenanalyse
- Intelligente Jagd auf Bedrohungen
- Automatisierte Remote-Untersuchungen
- Dynamische Reaktionsmöglichkeiten auf der Basis vorgegebener Abläufe

## Vorteile

- Verringerung der Verweilzeit und der Auswirkungen potenzieller Sicherheitsverletzungen
- Erzielung eines konstanten Sicherheitsniveaus, unabhängig vom Kompetenzniveau der Sicherheitsfachkräfte
- Einsparung erheblicher zeitlicher und finanzieller Ressourcen in Verbindung mit der Erholung von einem erfolgreichen Angriff

BlackBerry. Optics

BlackBerry Optics ist eine Lösung zur Erkennung und Bekämpfung von Bedrohungen auf Endpunkten (Endpoint Detection and Response, EDR), die darauf ausgelegt ist, den von BlackBerry Protect gebotenen Schutz vor Bedrohungen auszuweiten. Sie setzt zur Identifikation und Vermeidung von Sicherheitsvorfällen auf KI.

BlackBerry Optics unterscheidet sich in einigen wichtigen Punkten von anderen EDR-Produkten, die sich nur mit viel Aufwand implementieren lassen, einen hohen Wartungsaufwand mit sich bringen und noch schwerer zu verwenden sind:

- BlackBerry Optics lässt sich innerhalb von Minuten auf Endpunkten installieren und erfordert dazu weder zusätzliche Hardware noch kostspieliges Datenstreaming.
- Es ermöglicht latenzfreie Erkennung und Reaktion durch lokale Speicherung und Analyse von Daten auf dem Endpunkt, ohne dass laufend Updates erforderlich sind.
- Es bietet eigenständige, automatisierte Module zur Erkennung von Bedrohungen durch maschinelles Lernen, die darauf ausgelegt sind, Bedrohungen aufzudecken, die sich anhand statischer Verhaltensregeln nur schwerlich erkennen lassen würden.

In Kombination mit BlackBerry Protect bietet BlackBerry Optics die Erkennungs- und Präventionsfunktionen, die Sie benötigen, um Angreifern stets einen Schritt voraus zu sein, sodass Ihr Unternehmen geschützt bleibt.

Das Release 2.4 der BlackBerry EDR-Lösung bietet mehrere Verbesserungen an InstaQuery, FocusView und der Logik der Context Analysis Engine (CAE) von BlackBerry Optics, und bietet so noch mehr Transparenz. Zu diesen Verbesserungsschwerpunkten zählen:

- Verbesserungen an der Untersuchung von Registereinträgen
- DNS-Transparenz
- Übersicht über Windows®-Anmeldeereignisse
- Übersicht über RFC 1918 Adressbereich
- Verbesserte WMI-Untersuchung über Windows-API
- Verbesserte PowerShell-Untersuchung über Windows-API

Das Release 2.4 von BlackBerry Optics bietet mehrere Produktverbesserungen, die sowohl die Breite als auch in die Tiefe der EDR-Suchparameter erhöhen. Diese Verbesserungen, die auf dem grundlegenden KI-basierten Schutz von BlackBerry Protect sowie auf lokal gespeicherten Daten aufbauen, bieten in Echtzeit die Gewissheit, die Sie benötigen, um Untersuchungen sowie Triage- und Gegenmaßnahmen anzustoßen, wenn eine CAE-Regel ausgelöst wird. Dies bietet Sicherheitsexperten die Möglichkeit, sich bei ihrer Suche und der Ergreifung von Gegenmaßnahmen an die hohe Geschwindigkeit der Bedrohungslandschaft anzupassen, ohne dass sie durch Cloud-Abfragen, langwierige forensische Analysen oder andere zeitraubende Prozesse aufgehalten werden. Das Computer Security Incident Response Team kann sämtliche Artefakte nachvollziehen, die vor und nach dem auslösenden Ereignis eingetreten sind. Das Ergebnis:

- Erhöhte Suchparameter-Flexibilität bei InstaQuery-, FocusView- und CAE-Regeln
- Schnellere Reaktion auf Vorfälle
- Ausrichtung nach dem MITRE ATT&CK-Framework
- Erweiterte automatisierte Reaktionen über CAE-Regeln

## *EDR-Lösung BlackBerry Optics*

| Für den Einsatz in Großunternehmen geeignet | Erkennung | Untersuchung und Reaktion |
|---|---|---|
| • Dezentrale Suche und Erfassung<br>• Plattformübergreifende Transparenz<br>• API-Zugriffsmöglichkeiten<br>• Syslog-Integration | • Kontextorientierte Erkennung<br>• Auf maschinellem Lernen beruhende Module<br>• MITRE ATT&CK-Framework | • Zweite Generation<br>• Durch die Cloud erweiterte Modelle |

## Erkennung und Bekämpfung von Bedrohungen auf Endpunkten – verbreitete Anwendungsfälle

- **Verhinderung schädlicher Aktivitäten:** BlackBerry Protect, die Basis von BlackBerry Optics, ist speziell darauf ausgelegt, erfolgreiche Angriffe auf Endpunkte zu verhindern. Hierzu zählen:
  - Erkennung und Blockierung schädlicher ausführbarer Dateien und Datei-Identifikation mittels KI
  - Kontrolle, wer wo und wie Skripts ausführen darf
  - Verwaltung der Verwendung von USB-Geräten, Verhinderung unbefugter Geräte
  - Eliminierung der Möglichkeit für Angreifer, dateilose Malware-Angriffstechniken einzusetzen
  - Verhinderung der Auslieferung schädlicher Nutzdaten in E-Mail-Anhängen
- **Untersuchung von Angriffs- und Warnungsdaten:** Benutzer können Warnungen anderer Sicherheitskontrollen, etwa von BlackBerry Protect, mit leicht verständlichen Visualisierungen aller damit verbundenen Aktivitäten untersuchen und nützliche Informationen vom Endpunkt abrufen.
- **Unternehmensweite Suche nach Bedrohungen:** Benutzer können auf sämtlichen Endpunkten des Netzwerks schnell nach Dateien, ausführbaren Programmen, Hash-Werten und anderen Anzeichen auf eine Kompromittierung suchen, um versteckte Bedrohungen aufzuspüren.
- **Erkennung von Bedrohungen auf Endpunkten:** Verdächtiges Verhalten und andere Anzeichen auf eine mögliche Kompromittierung von Endpunkten werden automatisch aufgedeckt.
- **Schnelle, automatisierte Reaktion auf Vorfälle auf der Basis vorgegebener Abläufe:** Benutzer können kritische forensische Daten automatisch von betroffenen Endpunkten abrufen und automatisch Gegenmaßnahmen ergreifen, wenn ein schädlicher Endpunkt entdeckt wird.

## Mehr erfahren

BlackBerry Optics ist nur eine aus einer ganzen Reihe von Sicherheitslösungen der Spitzenklasse, die BlackBerry anbietet. Erfahren Sie mehr über unsere vollständige Auswahl an Sicherheitssuiten, die Ihrem Unternehmen überall intelligente Sicherheit bieten können.

**Informationen zu unseren Lösungen:**

BlackBerry Spark® Suite:

BlackBerry® Unified Endpoint Security Suite

BlackBerry® Unified Endpoint Management Suite

## Über BlackBerry

BlackBerry (NYSE: BB; TSX: BB) bietet intelligente Sicherheitssoftware und -dienste für Unternehmen und Regierungen weltweit. Das Unternehmen sichert mehr als 500 Millionen Endpunkte ab, darunter 150 Millionen Autos, die heute auf unseren Straßen unterwegs sind. Das Unternehmen mit Sitz in Waterloo, Ontario, setzt KI und maschinelles Lernen ein, um innovative Lösungen in den Bereichen Cybersicherheit, Sicherheit und Datenschutz zu liefern, und ist in den Bereichen Endpunkt-Sicherheitsmanagement, Verschlüsselung und eingebettete Systeme führend. Die Vision von BlackBerry ist klar – eine vernetzte Zukunft zu sichern, der Sie vertrauen können.

***BlackBerry. Intelligent Security. Everywhere.***

Besuchen Sie für weitere Informationen BlackBerry.com und folgen Sie @BlackBerry.

BlackBerry
Intelligent Security. Everywhere.



BB20-0223DACH | 200713