BlackBerry
Intelligent Security. Everywhere.

Lösungsprofil

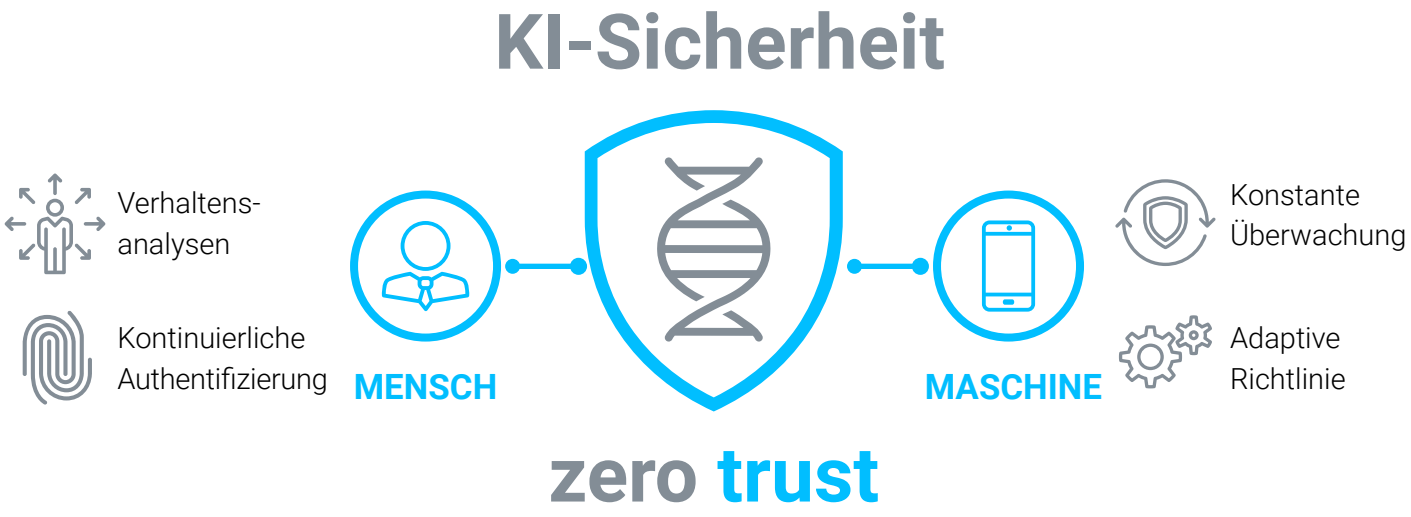
BlackBerry Cyber Suite

Brückenschlag zwischen Zero Trust und Zero Touch

Die Herausforderung, Daten und Endpunkte zu sichern und zu schützen, ist keine neue Anforderung, aber heute wichtiger denn je. Da sich die Angriffsfläche durch die Verbreitung neuer Arten von Endpunkten – von Mobiltelefonen bis hin zum Internet der Dinge (IoT) – in Verbindung mit einer Welle von Remote-Arbeitnehmern rund um den Globus in rasantem Tempo vergrößert, entsteht ein perfekter Sturm. Das Konzept und die Umsetzung eines Zero-Trust-Rahmens war noch nie so wichtig wie heute, da die Sicherung und der Schutz von Endpunkten und Daten mit dem Zero Trust-Ansatz Hand in Hand gehen.

Zero Trust wurde entwickelt, um der De-Perimeterisierung bzw. der Auflösung der Perimeter von Unternehmensnetzwerken entgegenzuwirken. Mit der zunehmenden Konsumerisierung von Technologie und dem Aufstieg von Cloud-basierten Anwendungen mussten CISOs ihren Ansatz ändern und davon ausgehen, dass Datenverkehr innerhalb eines Unternehmensnetzwerks nicht unbedingt vertrauenswürdiger ist als Datenverkehr, der von außen eingeht. Bei Zero Trust geht es darum, Vertrauen zu schaffen und den Zugang einzuschränken. Es geht darum, sicherzustellen, dass man einen vertrauenswürdigen Benutzer auf einem vertrauenswürdigen Gerät hat, während gleichzeitig der Zugriff auf diejenigen Daten und Anwendungen beschränkt wird, die diese Person für ihre Arbeit benötigt. Ein Gleichgewicht zwischen den Anforderungen des Zero Trust-Konzepts und der Produktivität der Arbeitnehmer zu finden, war für sich alleine schon schwierig genug, noch bevor Unternehmen im März 2020 ihre globale Belegschaft über Nacht auf ein Heimarbeitsmodell umstellten. Hierdurch sind Zero Trust und Geschäftskontinuität in der Prioritätsliste der Herausforderungen, für die eine Lösung gefunden werden muss, ganz nach oben gerutscht.

Die Bestandteile von BlackBerry Cyber Suite bilden gemeinsam die Grundlage für eine Zero Trust-Sicherheitsarchitektur für Unternehmen.



Wie BlackBerry diese Probleme angeht:

Die BlackBerry® Cyber Suite ist ein gezielt entwickeltes Set von Sicherheitskontrollen, die ein minimal invasives (Zero Touch) und daher benutzerfreundliches Zero-Trust-Framework bieten. Bei der BlackBerry Cyber Suite handelt es sich um integrierte hochmoderne Sicherheitskontrollen und -prozesse, welche die Grundlage für eine Zero Trust-Sicherheitsarchitektur bilden, die von traditionellen Endpunkten über mobile Geräte bis hin zu IoT-Geräten reichen.

Die Module von BlackBerry Cyber Suite bilden gemeinsam die Grundlage für eine Zero Trust-Sicherheitsarchitektur. Fortgeschrittene Zero-Trust-Praktiker in allen Segmenten haben festgestellt, dass die Umsetzung dieser Architektur mehrere Vorteile mit sich gebracht hat, darunter:

- Verbessertes Sicherheitsniveau mit erhöhter Übersicht und größerer Kontrolle für eine effektivere Risikominderung
- Sicherung und Verwaltung aller Angriffsflächen, von Laptops und Servern über mobile Geräte bis hin zu IoT-Geräten
- Zeit- und Kostenersparnis durch eine einheitliche Plattform, die sich leicht bereitstellen und verwalten lässt
- BlackBerry Cyber Suite erhöht die Geschwindigkeit und Agilität des Sicherheitsteams und bietet gleichzeitig einen besseren Überblick über eine heterogene IT-Infrastruktur.

BlackBerry Cyber Suite

KOMPONENTE	BESCHREIBUNG
Endpunktschutz	Durch den Einsatz von künstlicher Intelligenz (KI) und maschinellen Lernfunktionen bietet BlackBerry® Protect automatisierte Malware-Prävention, Anwendungs- und Skriptkontrolle, Speicherschutz und eine Durchsetzung von Geräterichtlinien. Es sagt Cyber-Angriffe voraus und verhindert sie mit beispielloser Wirksamkeit, Benutzerfreundlichkeit und minimaler Beeinträchtigung des Systems.
Erkennung und Bekämpfung von Bedrohungen auf Endpunkten	BlackBerry® Optics erweitert die von BlackBerry® Protect gebotene Bedrohungsabwehr durch den Einsatz künstlicher Intelligenz zur Verhinderung von Sicherheitsvorfällen. Es bietet eine echte KI-basierte Verhinderung von Vorfällen, Ursachenanalysen, eine intelligente Jagd auf Bedrohungen und automatisierte Funktionen zur Erkennung und Bekämpfung von Bedrohungen.
Mobile Bedrohungsabwehr	BlackBerry Protect Mobile erkennt und behebt hochentwickelte Bedrohungen auf Geräte- und Anwendungsebene. Es stoppt mittels KI-gesteuerten Bedrohungsschutzes Cyberattacken auf allen Mobilgeräten.
Verhaltensanalysen für Benutzer und Organisationen	BlackBerry® Persona schafft Vertrauen auf der Grundlage biometrischer Daten, der Nutzung von Anwendungen sowie von Netzwerk- und Prozessaufrufmustern. Es verwendet eine adaptive Risikobewertung und dynamische Richtlinienanpassung über mobile Geräte hinweg, um eine kontinuierliche Authentifizierung zu ermöglichen.

Endpunktschutz

BlackBerry® Protect verhindert mittels eines automatisierten, präventiven Ansatzes die Ausführung von Malware auf den Endpunkten eines Unternehmens. Es verhindert Sicherheitsverletzungen, u.a. durch polymorphe Ransomware, Zero-Day-Angriffe und andere Malware und umfasst Sicherheitsvorkehrungen zur Verhinderung skriptbasierter, dateiloser, speicherbasierter und auf externen Geräten beruhender Angriffe. BlackBerry Protect erreicht dies ohne Eingriffe von Benutzern oder Administratoren, sowie ohne Cloud-Verbindung, Signaturen, Heuristiken oder Sandboxes.

Funktionsumfang

Malware-Ausführungskontrolle

- Die zentrale Schutztechnologie, die künstliche Intelligenz und maschinelles Lernen nutzt, um Malware zu erkennen und zu verhindern
- Schützt Microsoft® Windows®-, macOS®- und Linux®-Umgebungen

Durchsetzung von Richtlinien für die Nutzung von Geräten

- Kontrolle der Verwendung von USB-Massenspeichergeräten
- Verhinderung von Datendiebstahl über Wechselmedien

Anwendungskontrolle

- Sperrung von Geräten mit fester Funktion und Einschränkung von Änderungen
- Verhinderung des Hinzufügens neuer Anwendungen

Speicherschutz

- Proaktives Erkennen und Stoppen von speicherbasierten Angriffen
- Ermöglicht detaillierte Ausschlüsse und erweiterte Fehlerbehebung und Berichterstattung

Skriptkontrolle

- Verhinderung der Ausführung unbefugter Skripts
- Effektivere administrative Kontrolle mit detaillierten Whitelist- und Safelist-Funktionen
- Enthält übergeordnete Steuerelemente, mit denen Skripts wie PowerShell blockiert werden können, wenn sie nicht in einer bestimmten Anwendung ausgeführt werden.

Erkennung und Bekämpfung von Bedrohungen auf Endpunkten

BlackBerry® Optics ist eine EDR-Lösung, die den von BlackBerry Protect gebotenen Schutz vor Bedrohungen durch den Einsatz künstlicher Intelligenz zur Verhinderung von Sicherheitsvorfällen erweitert. BlackBerry Optics bietet eine echte KI-basierte Verhinderung von Vorfällen, Ursachenanalysen, eine intelligente Jagd auf Bedrohungen und automatisierte Funktionen zur Erkennung und Bekämpfung von Bedrohungen sowie zur Behebung der gegebenenfalls angerichteten Schäden. Im Gegensatz zu anderen EDR-Produkten erfordert BlackBerry Optics keine umfangreichen Investitionen in die Infrastruktur vor Ort. Daten müssen nicht zur Speicherung und Analyse kontinuierlich in eine Cloud-Umgebung gestreamt werden, und für den Betrieb wird kein technisches Fachwissen benötigt. BlackBerry Optics und seine echten KI-basierten Funktionen zur Verhinderung von Vorfällen sind so konzipiert, dass sie auf dem Endpunkt ausgeführt werden können. Dank dieser schlanken Architektur können Unternehmen EDR-Funktionen mit einer einfachen Benutzeroberfläche und automatisierten Reaktions- und Abhilfemaßnahmen kostengünstig umsetzen.

Funktionsumfang

Dezentrale Suche und Erfassung

Unser einzigartiger Ansatz zur Datenerfassung optimiert die Sammlung, Suche und Analyse von Daten.

Durchgängige plattformübergreifende Transparenz

Dank der Unterstützung von Microsoft Windows-, MacOS- und Linux-Endpunkten können Unternehmen über eine einzige Lösung den Überblick über die Situation in ihrer gesamten Umgebung behalten.

Ursachenanalyse

Webbasierte On-Demand-Ursachenanalyse von Angriffen, die von BlackBerry Protect blockiert werden, sowie von anderen interessanten Artefakten, die auf Endpunkten identifiziert wurden.

Unternehmensweite Jagd auf Bedrohungen

Sofortige Durchsuchung von Endpunktdaten, um versteckte potenzielle Bedrohungen auf Endpunkten aufzuspüren.

Schnelle Reaktion auf Vorfälle

Schnelle Umsetzung von Gegenmaßnahmen, Quarantäne und Abruf verdächtiger Dateien und/oder Isolierung kompromittierter Endpunkte gegenüber dem Netzwerk.

Dynamische Erkennung von Bedrohungen

Automatisiert die Erkennung potenzieller Bedrohungen in Echtzeit mithilfe benutzerdefinierter und speziell entwickelter Erkennungsregeln.

Für die Cloud geeignet aber nicht von der Cloud abhängig

Stellt Daten lokal auf jedem Endpunkt zur Verfügung, so dass Sie nicht auf Konnektivität oder manuelle Eingriffe angewiesen sind.

Remote-Reaktion

Bietet eine Schnittstelle zur intuitiven und interaktiven Ausführung von Skripts sowie zur Ausführung traditioneller oder nativer Befehle auf Systemen, um diese schnell zu prüfen und die Ergebnisse dieser Befehle nahezu in Echtzeit zu sehen.

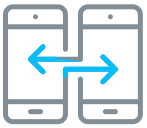
Automatisierte Reaktion

Automatisiert die Behebung von schädlichen Ereignissen in Ihrer gesamten Infrastruktur

Benutzerdefinierte Reaktion

Individuelle Anpassung automatisierter Reaktionsmaßnahmen in Verbindung mit Regelsätzen zur Eliminierung der Verweildauer.

Mobile Bedrohungsabwehr



Auf mobilen Endgeräten dient BlackBerry Protect als mobile Bedrohungsabwehrlösung (MTD), die die von BlackBerry® UEM gebotene Grundsicherung erweitert. Es verhindert, erkennt und behebt bösartige Bedrohungen auf Geräte- und Anwendungsebene. Es kombiniert die mobilen Endpunktverwaltungsfunktionen von BlackBerry® UEM mit fortschrittlichem, KI-gesteuertem Bedrohungsschutz. Mit BlackBerry Protect können mobile Geräte gefährlichen Cyberattacken in einer Zero Trust-Umgebung einen Schritt vorausbleiben.

Funktionsumfang:

Erkennung von Sideloaded iOS®-Anwendungen
Sideloaded-Anwendungen werden sofort erkannt und durchsucht.

Android™-Malware-Scan

BlackBerry UEM App Store mit Android- und APK-Malware-Scan
Alle Anwendungen im BlackBerry UEM App Store, einschließlich benutzerdefinierter Partner- und Kundenanwendungen, werden durchsucht und vor Malware geschützt.

Erkennung von Phishing und gefährlichen URLs
Die KI von BlackBerry Protect arbeitet ständig daran, zu verstehen, wie Malware oder gefährliche URLs aussehen und welche von ihnen möglicherweise eingebettete Phishing-Elemente enthalten.

Offline-Schutz für Android und iOS

Prüfung der Integrität von iOS-Apps für BlackBerry® Dynamics™ SDK Apps:
BlackBerry Protect gewährleistet die Integrität von Anwendungen, die auf der BlackBerry Dynamics SDK-Plattform basieren, und stellt sicher, dass nur sichere Anwendungen auf die Geräte gelangen. Zudem verhindert es jegliche Manipulation von BlackBerry®-Anwendungen.

Integriertes Dashboard-Berichtswesen
Die Überwachung und Alarmierung von Endbenutzern über das BlackBerry UEM-Dashboard sowie entsprechende Benachrichtigungen ermöglicht es Analysten, Malware und Hacker-Ereignisse schnell und in Echtzeit zu beheben.

Verhaltensanalysen für Benutzer und Organisationen

BlackBerry® Persona bietet eine kontinuierliche Authentifizierung mit maschinellem Lernen und prädiktiver KI zur dynamischen Anpassung von Sicherheitsrichtlinien auf der Grundlage von Benutzerstandort, Gerät und anderen Faktoren. BlackBerry Persona verwendet außerdem eine adaptive Risikobewertung und dynamische Richtlinienanpassung über mobile Geräte hinweg, um eine kontinuierliche Authentifizierung für Benutzer zu ermöglichen. Durch die Verbesserung der Erfahrung bei der Verifizierung von Benutzern schützt BlackBerry Persona die Umgebung vor menschlichen Fehlern und gut gemeinten Umgehungslösungen.

Funktionsumfang:

Adaptive Risikobewertung

- Verhaltensort: Betrachtet die Häufigkeit und die Muster von Benutzern, basierend auf der prädiktiven Analyse anonymisierter Standortdaten zur Bestimmung eines standortbasierten Risikowertes.
- Netzwerk: Bestimmt die Häufigkeit der Netzwerknutzung und passt die Sicherheit auf der Grundlage dieses Profils dynamisch an. Der erstmalige Zugriff auf ein öffentliches Wi-Fi würde beispielsweise eine entsprechende Anpassung der Risikobewertung nach sich ziehen.
- Zeit- und Nutzungsanomalien: Nahtlose Integration mit anderen Identitätsanbietern und Systemen. Die bewährte Sicherheitsinfrastruktur von BlackBerry ermöglicht eine sichere und einfache gemeinsame Nutzung sämtlicher Daten.
- Geräte- und App-DNA: Die Fähigkeit zur Bestimmung, ob das Gerät und die Apps konform und auf dem neuesten Stand sind. BlackBerry Persona kann die Sicherheitsrichtlinie auf Grundlage des DNA-Profils des Geräts und der Anwendung anpassen.

Dynamische Richtlinienübernahme

- Zugang gewähren
- Eine Richtlinie verabschieden
- Zur Authentifizierung auffordern
- Warnen und Gegenmaßnahmen einleiten

Kontinuierliche Authentifizierung

- Nutzt passive Biometrie und andere nutzungsbasierte Muster, um die Benutzeridentität kontinuierlich und unaufdringlich zu überprüfen.
- Ein böswilliger Benutzer wird automatisch daran gehindert, auf Anwendungen zuzugreifen, wenn er ein anormales Verhalten an den Tag legt.
- Verstärkt das Sicherheitsniveau und verbessert gleichzeitig die Endbenutzererfahrung gegenüber einer statischen Zeitüberschreitung.

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 über 175 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 eine sichere vernetzte Zukunft, der man vertrauen kann.

BlackBerry. Intelligente Sicherheit. Überall.

Für weitere Informationen besuchen Sie BlackBerry.com und folgen Sie @BlackBerry.

BlackBerry
Intelligent Security. Everywhere.

BB 20-0140 | 201125