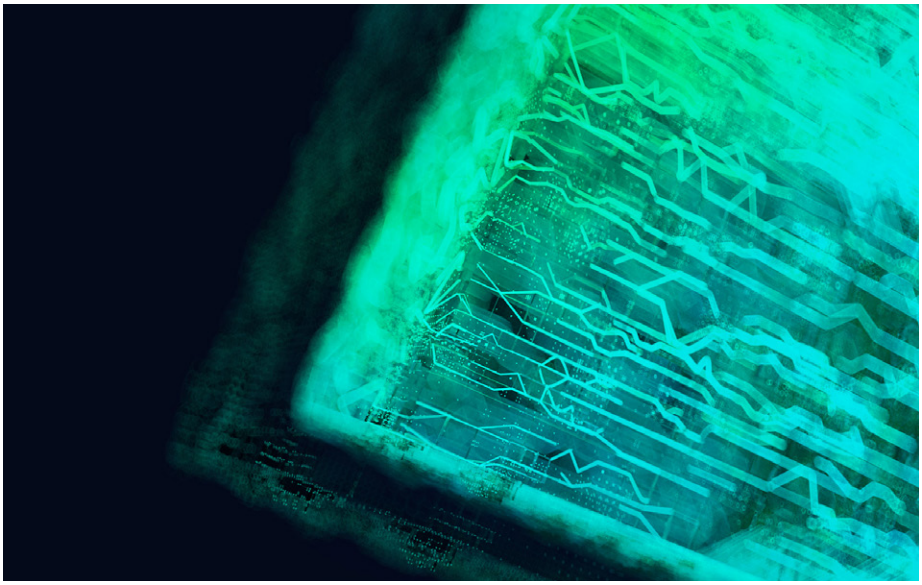
BlackBerry
Intelligent Security. Everywhere.

Datenblatt

BlackBerry Protect

Zukunftssichere Endgerätesicherheit



Jahrelang basierte der Bedrohungsschutz für Endpoint Security Lösungen in erster Linie auf Signaturen, die erstellt wurden, nachdem es erste Attacken und der Schaden bereits angerichtet war. Wenn man davon ausgeht, dass alle möglichen Angriffe bereits einmal beobachtet wurden, ist der Einsatz von Signaturen sinnvoll. Heutzutage mutiert Malware täglich, ja sogar stündlich, signaturbasierte Präventionstools sind daher überholt. Es ist ein stärker präventiv ausgerichteter Ansatz für die Endpunktsicherheit erforderlich.

Durch den automatisierten Ansatz, bei dem die Prävention an erster Stelle steht, hat BlackBerry neu definiert, was eine Endpoint Security Software für Unternehmen leisten kann und soll. Es ist eine genaue, effiziente und effektive Lösung zur Verhinderung der Ausführung von Advanced Persistent Threats und Malware an den Endpunkten eines Unternehmens. BlackBerry® Protect verhindert Sicherheitsverletzungen und bietet zusätzliche Sicherheitskontrollen zum Schutz vor skriptbasierten, dateilosen, speicher- und gerätebasierten Angriffen von außen. BlackBerry Protect erreicht dies ohne Eingriffe von Benutzern oder Administratoren, sowie ohne Cloud-Verbindung, Signaturen, Heuristiken oder Sandboxen.

Funktionsumfang

Durchsetzung von Richtlinien für die Nutzung von Geräten

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

Rollenbasierte Zugriffssteuerung (Role-Based Access Controls, RBAC)

- Risikominimierung durch differenzierte Rollenverwaltung mit benutzerdefinierter RBAC
- Verbesserung der Beschränkungen des Netzwerkzugangs über die Rollen der einzelnen Benutzer
- Einschränkung der Mitarbeiter-Zugriffsrechte auf die für ihre Arbeit benötigten Informationen
- Keine Auswirkungen auf vorhandene Benutzer

Anwendungskontrolle

- Sperren von Geräten mit festgelegter Funktion
- Unterbinden schädlicher Binärdateien und der Modifikation von Binärdateien
- Sperren bestimmter Systeme und Beschränken von Änderungen

BlackBerry Protect for Desktop

Das in BlackBerry Protect verwendete algorithmische Modell bedeutet, dass es, weil die Sicherheitslösung auf den Endpunkten läuft, keine Signaturen, Patches, System-Scans oder langsame Endpunkte gibt. Kunden, die von reaktiven, signaturbasierten Legacy-Antivirenprodukten umgestiegen sind, konnten eine Investitionsrendite von bis zu 99 %, eine 97%ige Reduzierung des Reimaging von Rechnern, eine bessere Hardware- und Akkuleistung und eine 90%ige Reduzierung der für die Verwaltung der Lösung erforderlichen Arbeitsstunden verzeichnen.[1]

Die BlackBerry Protect-Architektur besteht aus einem einzigen Lightweight-Agent, der über die BlackBerry-eigene SaaS-basierte Cloud-Konsole verwaltet wird. Die Cloud-Konsole lässt sich problemlos in vorhandene Softwareverwaltungssysteme und Sicherheitstools integrieren. Für Umgebungen mit „Luftschranken" besteht die Möglichkeit hybrider und lokaler Verwaltung. Der Endpunkt-Agent erkennt und unterbindet Malware auf dem Host, und zwar unabhängig von einer Cloud-Verbindung und ohne die Notwendigkeit laufender Updates. BlackBerry Protect ist in der Lage, Malware in offenen, isolierten und virtuellen Netzwerken zu erkennen und unter Quarantäne zu stellen. Der auf maschinellem Lernen basierende Ansatz von BlackBerry stoppt die Ausführung von schädlichem Code, unabhängig davon, ob dieser bereits bekannt ist, und auch dann, wenn eine unbekannte Obfuskationstechnik eingesetzt wird. Kein anderes Anti-Malware-Produkt kommt an die Genauigkeit, Einfachheit der Verwaltung und Wirksamkeit von BlackBerry Protect heran.

BlackBerry Protect – Merkmale

Echte Verhinderung von Zero-Day-Angriffen

Belastbares KI-Modell verhindert die Ausführung von Zero-Day-Nutzlasten.

Durchsetzung von Richtlinien für die Nutzung von Geräten

Kontrolliert, welche Geräte in der Umgebung verwendet werden, und eliminiert externe Geräte als mögliche Angriffsvektoren.

KI-basierte Verhinderung von Malware

Praxiserprobte künstliche Intelligenz untersucht jede Anwendung, die versucht, eigenständig zu starten - und zwar noch vor deren Ausführung.

Erkennung und Unterbindung von Memory Exploitation

Identifiziert proaktiv Versuche zur bösartigen Nutzung des Speichers (dateilose Angriffe) mit sofortigen, automatisierten Gegenmaßnahmen.

Script-Verwaltung

Wahrt volle Kontrolle darüber, wann und wo Scripts in der Umgebung ausgeführt werden.

Anwendungskontrolle für Geräte mit festgelegter Funktion

Stellt sicher, dass sich Geräte mit fester Funktion immer in einem optimalen Zustand befinden, und eliminiert damit die bei nicht verwalteten Geräten auftretenden schleichenden Veränderungen.

Funktionsumfang

Speicherschutz

- Proaktives Erkennen und Stoppen bösartiger Arbeitsspeichernutzung
- Verhindern von Angriffen, die nur den Arbeitsspeicher betreffen, wie etwa die Rechteausweitung
- Differenzierte Ausschlüsse sowie erweiterte Fehlerbehebung und Berichterstattung

Skriptkontrolle

- Verhinderung der Ausführung unbefugter Skripts
- Differenzierte Whitelist- und Safelist-Funktionen
- Unterstützung von MacOS®, Microsoft® und Linux®
- Verhindern der Ausführung von PowerShell-Einzeilern

Erkennung von Sideloaded iOS®-Anwendungen

- Sideloaded-Anwendungen werden sofort gescannt und erfasst

BlackBerry Protect for Mobile

Mehr denn je setzen Unternehmen heute Mobilgeräte ein, um in einem agilen, wachsenden Markt konkurrenzfähig zu sein und die Verbindung unter ihren Mitarbeitern zu gewährleisten. Erstmals ist mehr als die Hälfte aller mit dem Internet verbundenen Geräte mobil.[2] Gleichzeitig ist Malware für Mobilgeräte so weit verbreitet wie nie zuvor. Die Zahl der Angriffe ist allein im letzten Jahr um 50 % gestiegen.[3] Während der Schwerpunkt von Sicherheitslösungen für Unternehmen in der Vergangenheit auf Desktop-Geräten lag, entdecken immer mehr Unternehmen die wachsende Bedrohung durch Malware-Phishing-Angriffe auf Mobilgeräte, insbesondere im Rahmen von Anwendungen.

Der durch solche Angriffe verursachte Schaden kann beträchtlich sein, da personenbezogene Daten (Personally Identifiable Information, PII) und andere kritische Daten öfter als früher kompromittiert werden. Dies führt dazu, dass immer mehr Unternehmen Deep Packet Inspection (DPI) und andere Möglichkeiten zum Schutz vor bösartigen Angriffen einführen.

Es überrascht daher nicht, dass der Markt für Mobile Threat Defense (MTD) rasch wächst. MTD bietet eine zusätzliche Sicherheitsebene durch Prävention, Erkennung, Behebung und Verbesserung der allgemeinen Sicherheitshygiene für alle Ebenen der Mobilgerät-Flotte und der mobilen Anwendungen eines Unternehmens.

Unsere BlackBerry Protect MTD-Lösung erweitert die von BlackBerry® UEM gebotene Sicherheitsbasis, indem sie hochentwickelte bösartige Bedrohungen auf mobilen Geräten bekämpft. BlackBerry Protect überwacht Angriffe auf Geräte- und Anwendungsebene und geht über die Sicherheit der Standard-Anwendungscontainer von BlackBerry hinaus.

- Auf Geräteebene identifiziert BlackBerry Protect for Mobile Sicherheitslücken und potenzielle bösartige Aktivitäten durch die Überwachung von Betriebssystem-Updates, Systemparametern, Gerätekonfigurationen und Systembibliotheken.
- Auf der Anwendungsebene verwendet BlackBerry Protect for Mobile Anwendungs-Sandboxing und Code-Analyse sowie Anwendungstests zur Identifizierung von Malware und Grayware.

Darüber hinaus identifiziert BlackBerry Protect for Mobile jede Malware, die über Sideloaded-Anwendungen, einzigartige signaturbasierte Malware oder Simulationen hereinkommen könnte, und bildet eine zusätzliche Sicherheitsebene zur BlackBerry Dynamics SDK-Plattform. Dadurch können Partner und Kunden eigene sichere Anwendungen für mobile Geräte erstellen, auf welche die Mitarbeiter von ihren Geräten aus zugreifen können.

Funktionsumfang

Durchsuchung nach Android™-Malware

Suche nach Android- und APK-Malware im UEM App Store

- Scannen aller Anwendungen im UEM-App-Store von BlackBerry, einschließlich Kunden- und Kundenpartneranwendungen, zum Schutz vor Malware

Erkennung von Phishing und gefährlichen URLs

- Nutzt KI, um bösartige URLs, einschließlich solcher mit eingebetteten Phishing-Elementen, auszumachen und zu stoppen.

Sichere Anwendungserstellung

- Partner und Unternehmen können angepasste, sichere Anwendungen für Geräte erstellen, auf die im Unternehmen zugegriffen werden kann.

Prüfung der Integrität von iOS-Apps für BlackBerry® Dynamics SDK Apps

- Gewährleistet die Integrität der auf der BlackBerry® Dynamics™ SDK-Plattform erstellten Anwendungen
- Ausschließlich sichere Anwendungen können auf Geräte geladen werden, Manipulation von BlackBerry® wird unterbunden

Mögliche Anwendungsszenarien für BlackBerry Protect

BlackBerry Protect bietet umfassende Bedrohungsprävention, die Sicherheitsverletzungen auf Endpunkten durch folgende Funktionen stoppt:

- Identifizieren und Blockieren bösartiger ausführbarer Dateien ohne die Notwendigkeit laufender Updates oder einer Cloud-Verbindung
- Identifizieren von Sicherheitsschwachstellen und potenziell böswilligen Aktivitäten durch Überwachung von Betriebssystem-Updates, Systemparametern, Gerätekonfigurationen und Systembibliotheken
- Kontrollieren, wer wo Skripts wie ausführen darf
- Verwalten der USB-Geräte-Nutzung, Verhindern der Verwendung nicht autorisierter Geräte
- Stoppen von dateilosen Malware-Angriffen
- Sperren von Geräten mit festgelegter Funktion, etwa Kiosken oder POS-Terminals
- Unterbinden von Zero-Day- und Ransomware-Angriffen
- Stoppen arbeitsspeicherbasierter Angriffe und Exploits
- Verwenden von Anwendungs-Sandboxing und Code-Analyse sowie Anwendungssicherheitstests zur Identifikation von Malware und Grayware
- Identifizieren aller Malware, die über Sideloaded-Anwendungen, signaturbasierte unique Malware oder Simulationen hereinkommen könnte
- Schutz für Endpunkte bei Online- und Offline-Nutzung

1 https://www.cylance.com/en-us/company/about-us/our-customers/2019-forrester-tei-report.html#form-anchor

2 https://gs.statcounter.com/platform-market-share/desktop-mobile-tablet

3 https://research.checkpoint.com/cyber-attack-trends-2019-mid-year-report/

Mehr erfahren

BlackBerry Protect ist nur eine aus einer ganzen Reihe erstklassiger Sicherheitslösungen, die BlackBerry anbietet. Erfahren Sie mehr über unser Sortiment an Sicherheitssuiten, die Ihrem Unternehmen überall intelligente Sicherheit bieten können.

Informationen zu unseren Lösungen:

BlackBerry Spark® Suite

BlackBerry Spark® Unified Endpoint Security Suite

BlackBerry Spark® 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.

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

BlackBerry
Intelligent Security. Everywhere.

BB20-0250 | 200709