BlackBerry
Intelligent Security. Everywhere.

Lösungsprofil

KI-basierte Threat and Incident Prevention, Detection, and Response

Einleitung

Traditionelle Cybersicherheitsmethoden sind überholt Es ist nicht mehr ausreichend, sich auf Netzwerkparameter zu verlassen und einfach neue Sicherheitsebenen einzubauen. Das Netzwerk-Perimeter gibt es nicht mehr[1]. Mobile Technologien und immer neue Endpunkte, welche Daten austauschen und sich mit unterschiedlichsten Netzwerken verbinden, bieten ganz neue Angriffsflächen. Angriffsvektoren nehmen mit einem unglaublichen Tempo zu während traditionelle Sicherheitsbarrieren mehr und mehr versagen[2].

Sich vor bekannten Bedrohungen zu schützen, ist zweifellos wichtig. Innerhalb der heutigen Bedrohungslandschaft müssen Unternehmen jedoch auch die mehr als 350.000 neuen Malware-Varianten täglich abwehren-[3].

Viele Cybersicherheitsunternehmen versuchen, diese neuen Bedrohungen zu stoppen, indem sie bestehende Lösungen um zusätzliche Sicherheitsebenen erweitern. Dieser Ansatz macht die Sicherheitsinfrastruktur meist noch komplexer, so dass es für Analysten immer schwieriger wird, Bedrohungen schnell zu erkennen und effektiv darauf zu reagieren. Außerdem werden die Vorteile neuer Sicherheitsebenen schnell durch den Bedarf an weiteren Systemressourcen und eine Überlastung durch zu viele Warnmeldungen aufgehoben.

Der BlackBerry-Ansatz

BlackBerry Cylance vermeidet die Schwächen herkömmlicher AV-Lösungen durch den Einsatz künstlicher Intelligenz (KI) zur Erkennung von Bedrohungen. Unsere Cybersicherheits-KI wird von mehr als einer Milliarde sicherer und schädlicher Dateien ständig weitertrainiert. Damit sind unsere Sicherheitsexperten in der Lage, mehr als eine Million Dateimerkmale zu referenzieren und zu beurteilen, bevor bestimmt wird, ob ein Programm ausgeführt werden soll. Die von BlackBerry PROTECT® gebotenen Funktionen zur Ermittlung von Bedrohungsprofilen bieten Kunden einen prädiktiven Vorteil[4] von bis zu 33 Monaten gegenüber bekannter, unbekannter und Zero-Day-Malware.

BlackBerry Spark® Unified Endpoint Security Suite

BlackBerry® Optics, Teil der BlackBerry Spark® Unified Endpoint Security Suite, setzt geschulte Modelle zur Erkennung von Bedrohungen direkt am Endpunkt ein. Hierdurch sind geschützte Geräte in der Lage, als eigenständige Sicherheitszentren zu agieren, ohne auf eine Verbindung zur Cloud angewiesen zu sein. BlackBerry OPTICS umfasst eine konfigurierbare Context Analysis Engine (CAE), die Ereignisse auf Endpunkten nahezu in Echtzeit überwacht. Die CAE identifiziert verdächtiges Verhalten gemäß den Definitionen in Geräterichtlinien und Erkennungsregeln, die von Ihrem internen Sicherheitsteam vorgegeben werden. Beispielsweise können Client-Endpunkte Warnungen senden oder automatisierte Antworten aktivieren, je nachdem, wie PowerShell aufgerufen wird und wo es aufgerufen wird.

1 https://misti.com/infosec-insider/demistifying-infosec-network-perimeter

2 https://blogs.blackberry.com/en/2020/05/blackberry-spark-suites-bringing-order-to-the-chaos

3 https://www.av-test.org/en/statistics/malware/

4 https://threatvector.cylance.com/en_us/home/cylance-vs-future-threats-the-predictive-advantage.html.

BlackBerry hat die Übernahme von Cyclance im Februar 2019 abgeschlossen. Die CylancePROTECT® Lösung ist jetzt als BlackBerry Protect bekannt.

BlackBerry Spark UES Suite	Vorteile für Ihr Unternehmen
KI **identifiziert und blockiert schädliche Anwendungen** – einschließlich derjenigen, die noch nie zuvor gesehen wurden – und verhindert eine Ausführung auf Endpunkten	Die Wahrscheinlichkeit, dass ein Unternehmen durch einen **Zero-Day-Angriff in Mitleidenschaft gezogen wird, sinkt deutlich**
Statische, auf maschinellem Lernen aufbauende und benutzerdefinierte Regeln **identifizieren und blockieren komplexe Bedrohungen**	Unternehmen **verringern die Verweilzeit** und die Auswirkungen potenzieller Sicherheitsverletzungen
Playbook-gesteuerte Arbeitsabläufe automatisieren Untersuchung und Reaktion, so dass geeignete Maßnahmen ergriffen werden können	Unternehmen erzielen **konstante Sicherheitsniveaus**, unabhängig vom Kompetenzniveau ihrer Sicherheitsfachkräfte
Ein KI-basierter **präventionsorientierter EDR-Ansatz** wehrt die meisten Angriffe ab, noch bevor sie ausgeführt werden	Unternehmen **sparen erhebliche zeitliche und finanzielle Ressourcen** bei der Wiederaufnahme des Betriebs nach einem erfolgreichen Angriff
Ein erweitertes Toolset **erkennt und entschärft Insider-Bedrohungen**, dateilose Angriffe und verdächtige laterale Bewegungen innerhalb von Netzwerken	Unternehmen können **Bedrohungen schnell erkennen, verhindern und untersuchen und bekommen so einen umfassenden Einblick** in die Methoden und Motive von Angreifern

Erfüllung von Sicherheitsanforderungen - Anwendungsfälle

Die folgenden Anwendungsfälle veranschaulichen die Vorteile des von BlackBerry verfolgten präventionsorientierten Cybersicherheitsansatzes:

Malware (Ransomware, Trojaner, Adware, etc.)

Die Lösungen von BlackBerry® verwenden eine ständig trainierte KI, um Portable Executable-Dateien zu beurteilen, bevor sie einem Speicherplatz zugewiesen und ausgeführt werden. Das auf dem Endpunkt laufende Machine-Learning-Modell bestimmt innerhalb von Millisekunden, ob eine Datei schädlich oder sicher ist. Ist sie schädlich, wird die Ausführung verhindert und wehrt damit den Versuch des Angreifers ab, den Endpunkt zu infiltrieren

Dateilose Malware

Dateilose Angriffe treten immer häufiger auf[5], da Angreifer zunehmend darauf setzen, legitime Systemressourcen zu missbrauchen, um in ein Unternehmen einzudringen. Sicherheitsprodukte, die auf die Identifizierung schädlicher ausführbarer Dateien angewiesen sind, können diese Art von Angriffen nicht verhindern. Die von BlackBerry angebotenen Lösungen verhindern dateilose Angriffe auf mehrere Arten, unter anderem durch eine Verhinderung von Speicher-Exploits sowie durch Skript-Verwaltung und spezielle Module zur Erkennung dateiloser Bedrohungen. Wenn ein Angreifer versucht, Zugriffsrechte zu eskalieren, eine Prozess-Injektion vorzunehmen oder Systemspeicher zu missbrauchen, wird der Angriff schnell von BlackBerry-Lösungen erkannt und verhindert.

Unsere Lösungen bieten Analysetools zur Aufdeckung von Bedrohungen innerhalb der Windows-Registry, wo dateilose Angriffe üblicherweise Persistenzmechanismen einrichten. Endpunkte können damit Windows Management Instrumentation-Ereignisse (WMI-Ereignisse) – eine zentrale Komponente eingenisteter Angriffe –erkennen, analysieren und aufzeichnen. Geschützte Endpunkte überwachen und katalogisieren die Nutzung von PowerShell, einem kritischen Tool, das Bedrohungsakteure einsetzen, um Systemaufgaben und -prozesse schnell zu automatisieren.

5 https://securityboulevard.com/2019/10/fileless-malware-on-the-rise/

Schädliche Skripts

Skripts erfreuen sich unter Bedrohungsakteuren einer hohen Beliebtheit. Dafür gibt es mehrere Gründe: Zum einen sind schädliche Skripts, die eine beliebige Anzahl von Systemoperationen ausführen können, in der Cybercrime-Unterwelt für unerfahrene Angreifer problemlos erhältlich. Zum anderen tun sich viele Sicherheitsprodukte schwer, Skripts zu erkennen, da sie häufig auch für legitime Zwecke eingesetzt werden. Mit der BlackBerry Spark UES Suite können Unternehmen die integrierte Skriptverwaltung nutzen. Sicherheitsexperten können die volle Kontrolle darüber behalten, wann und wo Skripts ausgeführt werden. Dies macht es möglich, Skripts auch weiterhin für legitime Zwecke einzusetzen, Missbrauchsversuche durch Angreifer gleichzeitig jedoch stark einzudämmen.

Schädliche E-Mail-Anhänge

Phishing-Angriffe stellen für Angreifer eine der effektivsten Möglichkeiten dar, sich Zugang zu einem Endpunkt zu verschaffen. Mitarbeiter öffnen schädliche Anhänge, die sie für legitim halten, und erlauben so schädliche Angriffe. Mit den von BlackBerry angebotenen Lösungen werden gefährliche Anhänge identifiziert und automatisch blockiert. Wenn ein angehängtes Dokument beispielsweise ein VBA-Makro enthält, das für riskant gehalten wird, wird dessen Ausführung verhindert.

Externe Geräte

USB-Speichergeräte werden von vielen Unternehmen oft eingesetzt. Sie bergen jedoch erhebliche Risiken für Umgebungen, wenn sie mit Malware infiziert sind oder missbraucht werden, um vertrauliche Daten aus dem Unternehmen heraus zu übermitteln. Um auf dieses Risiko zu bekämpfen, bieten die Lösungen von BlackBerry entsprechende Richtlinien für die Nutzung externer Geräte. Wir begrenzen die Gefahren, die von USB-Sticks und anderen tragbaren Datenspeichern ausgehen, indem wir Administratoren die Kontrolle geben, welche Geräte verbunden werden können.

Systemadministratoren können mögliche Datenschutzverletzungen durch Insider-Bedrohungen untersuchen und eindämmen, indem sie unsere Übersichtsfunktion für Windows Logon Events verwenden. Diese ermöglicht es jedem Endpunkt, Detailinformationen zu Windows Logon Events zu erkennen und aufzuzeichnen, einschließlich IP-Adressen, Domänen und Zeitsignaturen. Sicherheitsadministratoren können Anmeldeinformationen analysieren, um ihre Berechtigungsprozesse zu optimieren, Benutzer über mehrere Systeme hinweg zu überwachen oder verdächtige Aktivitäten zu verfolgen.

Aufdeckung versteckter Bedrohungen

Die Erkennung schädlicher Aktivitäten ist für die Vermeidung von Sicherheitsverstößen von zentraler Bedeutung. Diese Aufgabe wird schwierig, wenn Hacker das Verhalten legitimer Benutzer nachahmen, indem sie auf dieselben Tools und Ressourcen zugreifen. Viele Cybersicherheitslösungen versenden Warnmeldungen an Systemadministratoren, wenn verdächtige Aktivitäten erkannt werden. Wird die Schwelle für das Auslösen einer Warnmeldung zu niedrig eingestellt, werden die IT-Mitarbeiter schnell von einer Fülle fehlerhafter Warnungen überrannt. Wird die Schwelle jedoch zu hoch angesetzt, droht Gefahr, dass Sicherheitsanalysten einen anstehenden Angriff komplett übersehen.

Die Lösungen von BlackBerry optimieren den Untersuchungsprozess, indem sie sofortigen Zugriff auf forensisch relevante Daten auf dem Endpunkt bieten. Sicherheitsanalysten können die mit einer Warnmeldung verbundenen kritischen Informationen einsehen und schnell ermitteln, ob ein Vorfall gefährlich oder harmlos ist. Für eine eingehende Untersuchung versetzen unsere Tools die Endpunkte in die Lage, genau zu erfassen, wie DNS-Abfragen eingetreten sind. Unter anderem können der Zeitpunkt, die Domäne und die IP-Adresse des Anforderers festgehalten werden. Darüber hinaus bieten wir Funktionen wie etwa eine Übersicht über den RFC 1918-Adressbereich, um die Verfolgung lateraler Bewegungen innerhalb von Netzwerken zu unterstützen.

Untersuchung von Angriffs- und Warnungsdaten

Informationen sind eine wichtige Voraussetzung für den Schutz der Infrastruktur und die Vermeidung von Verletzungen. Analysten, die die Taktiken, Techniken und Verfahren (TTPs) von Cyberangriffen verstehen, sind besser gerüstet, um sie zu stoppen. Die Sicherheitslösungen von BlackBerry decken versteckte Bedrohungen auf, indem sie die zurückgelassenen kritischen forensischen Daten erfassen. So erzeugt beispielsweise die Funktion Focus View in BlackBerry OPTICS eine Zeitleiste mit den Systemaktivitäten im Vorfeld eines Angriffs. Die Erfassung einzelner Endpunktdaten bietet einen zusätzlichen Kontext für verdächtige Aktivitäten und damit auch einen umfassenderen Überblick über einen Vorfall. Ihr Sicherheitsteam kann die erfassten Daten analysieren, um festzustellen, wie es möglich war, in Ihre Umgebung einzudringen. Noch offene Schwachstellen können dann entsprechend behoben werden.

Aufspürung von Bedrohungen durch den Einsatz von Indikatoren, die auf eine Kompromittierung hindeuten

Eine Jagd auf Bedrohungen ist im Kern eine Überprüfung von Hypothesen. Sicherheitsanalysten formulieren eine Hypothese und führen dann (unter Verwendung von IOCs oder anderen Bedingungen) eine Reihe von Untersuchungen durch, um ihre Theorie zu überprüfen oder zu widerlegen. BlackBerry erfasst sowohl aktuelle als auch historische Endpunktdaten und liefert Analysten damit wichtige Informationen zur Risikobeurteilung. Im Gegensatz zu anderen Tools, die sämtliche Daten eines Endpunkts speichern, bewahren BlackBerry-Lösungen nur die forensisch relevanten Daten auf. Dadurch kann sich Ihr Sicherheitsteam auf konkret nutzbare Daten konzentrieren, anstatt enorme Mengen irrelevanter Daten durchforsten zu müssen.

Statische, auf maschinellem Lernen aufbauende und benutzerdefinierte Regeln

BlackBerry OPTICS automatisiert die kritische Aufgabe der Suche nach verdächtigen Artefakten über Endpunkte und Unternehmen hinweg. Hierfür werden speziell trainierte KI-Modelle direkt auf dem Endpunkt eingesetzt, so dass jedes Gerät in der Lage ist, Erkennungs- und Reaktionsaktivitäten durchzuführen. Indem Endpunkte als unabhängige Sicherheitszentren agieren können, werden Latenzzeiten bei der Reaktion auf Bedrohungen eliminiert.

Die Context Analysis Engine (CAE) ist eine treibende Kraft hinter BlackBerry OPTICS. Sie erlaubt es Sicherheitsanalysten, eigene Sicherheitsregeln zu erstellen oder vorgefertigte Regeln auszuwählen, einschließlich derjenigen, die dem MITRE ATT&CK-Framework[6] entsprechen. Sicherheitsexperten können die CAE verwenden, um benutzerdefinierte Regeln für die Erkennung sowie für zu ergreifende Gegenmaßnahmen zu entwickeln und diese dann auf Endpunkten innerhalb der Umgebung implementieren.

Ergreifung von Gegenmaßnahmen

Für Unternehmen ist es wichtig, effektiv auf Bedrohungen reagieren zu können. Gegenmaßnahmen, die gleich zu Beginn eines Angriffs erfolgen, können die Auswirkungen einer Datenschutzverletzung deutlich minimieren. Mit BlackBerryOPTICS kann Ihr Sicherheitsteam automatisierte Ablaufpläne mit Maßnahmen für den Umgang mit Bedrohungen erstellen, die ausgelöst werden, wenn bestimmte Bedingungen erfüllt sind. Automatisierte Ablaufpläne eliminieren die Verweilzeit und gewährleisten, dass Ihr Unternehmen im Fall einer Bedrohung innerhalb der gesamten Umgebung einheitliche, schnelle und effektive Gegenmaßnahmen ergreift.

Beispielsweise können Sicherheitsanalysten Endpunkte, die automatisierte Gegenmaßnahmen auslösen, isolieren, um weitere Analysen vorzunehmen. Eine Untersuchung von Geräten, die verdächtige Aktivitäten melden, kann Einblicke in die TTPs von Angreifern bieten oder versteckte Schwachstellen der Umgebung aufdecken. Durch eine Fokussierung auf relevante Daten und die Ergreifung frühzeitiger Gegenmaßnahmen zur Bekämpfung von Bedrohungen direkt auf den Endpunkten wird Ihr Sicherheitsansatz nicht nur effizienter, sondern auch effektiver.

6 https://attack.mitre.org/

Die Vorteile der BlackBerry-Cybersicherheit

Unsere KI-basierten Lösungen sparen Zeit und Geld, indem sie Zero-Day-Bedrohungen, komplexe Angriffe und Datenschutzverletzungen vorhersehen und verhindern[7]. Weniger Verstöße bedeutet niedrigere Kosten für die Systemreparatur und seltenere Systemwiederherstellungsmaßnahmen. Eine Automatisierung de Endpunktsicherheit über unsere KI-basierten Lösungen bietet Ihnen die Möglichkeit, sich auf andere Aufgaben zu konzentrieren.

Die von BlackBerry bereitgestellten Sicherheitstools lassen sich leicht implementieren und liefern Vorteile, die sich direkt finanziell messen lassen. Beispielsweise erlebte ein Unternehmen nach einer Umstellung auf BlackBerry Folgendes[8]:

- **Erhöhte Produktivität des Cybersicherheitsteams:** Ein einziger Mitarbeiter nutzt BlackBerry PROTECT und BlackBerry OPTICS, um Probleme innerhalb der Umgebung zu überwachen und darauf zu reagieren – eine Aufgabe, für die zuvor das gesamte Team benötigt wurde. Heute konzentriert sich das Cybersicherheitsteam proaktiv auf die Jagd auf Bedrohungen und den Umgang mit anderen geschäftskritischen Anforderungen.
- **Verringerung der Ausfallzeiten um 95 % durch schnellere Untersuchung und Behebung:** Weniger Endbenutzer werden kompromittiert. Eine schnellere Untersuchung und Abwehr von Bedrohungen erlaubt es Anwendern, ihre eigentliche Arbeit schnell wieder aufzunehmen.
- **Reduzierung der Neuinstallationen von Geräten um 97 %:** Das Unternehmen nimmt weniger Rechner für ein Re-Imaging offline. Weniger Re-Imaging-Maßnahmen und kürzere Benutzer-Ausfallzeiten bedeuten, dass mehr IT-Ressourcen verfügbar sind, die anderweitig eingesetzt werden können.
- Das Unternehmen nahm nach dem Wechsel auf die Software-as-a-Service-Lösung (SaaS) von BlackBerry seine veraltete, vor Ort installierte Endpunktsicherheitslösung vollständig außer Betrieb.

Wechseln Sie noch heute auf intelligentere Sicherheit

BlackBerry kann bestehende Lösungen durch KI-basierte Präventionstechnologie ergänzen oder Cybersicherheitssysteme komplett ersetzen. Unsere Beratungsdienste vereinfachen die Umstellung auf BlackBerry Lösungen. Wir unterstützen Sie bei der Bereitstellung, Implementierung und Optimierung oder durch eine Verstärkung Ihres Sicherheitsteams.

Mit unseren KI-basierten präventionsorientierten Sicherheitslösungen schützen Sie Ihr Unternehmen und entlasten Ihre IT von sich ständig wiederholenden Aufgaben.

Weitere Informationen

Besuchen Sie uns unter: https://www.blackberry.com/us/en/products/blackberry-spark-suites

7 https://www.adapture.com/blog/cylance-forrester-report/

8 https://s7d2.scene7.com/is/content/cylance/prod/cylance-web/en-us/resources/knowledge-center/resource-library/reports/ForresterTEI-CylancePROTECTandCylanceOPTICS.pdf?kui=pz-UectBOAQ9Dbcsm1qPOQ

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 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.

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

BlackBerry
Intelligent Security. Everywhere.

MKTG20-0637 | 201216