BlackBerry Intelligent Security. Everywhere.

BLACKBERRY GATEWAY

Zero Trust Network Access (ZTNA): Damit moderne Remote-Belegschaften von überall aus sicher und produktiv tätig sein können

SOLUTION BRIEF

Der Trend zum Homeoffice und zu BYOD-Richtlinien ist eine echte Herausforderung für alle, die für die Absicherung der Technologien am Arbeitsplatz zuständig sind. Denn Mitarbeiter, die von zu Hause aus arbeiten, nutzen häufig geschäftliche und private Technologien ganz nach Belieben. Diese Sorglosigkeit eröffnet erfahrenen Bedrohungsakteuren viele neue Möglichkeiten. Jedes neue Gerät, jede neue Anwendung und jeder neue Anwender, der sich mit Unternehmensressourcen verbindet, ist eine potenzielle Gefahr für sensible Daten. Und je mehr Personen von außen zugreifen und je vielfältiger die genutzten Geräte sind, desto größer das Risiko.

Hybride Mitarbeitermodelle vergrößern die Angriffsfläche exponentiell und stellen damit vor allem Unternehmen mit begrenzten Ressourcen vor große Herausforderungen. Jetzt gilt es, eine effektive Lösung zu finden, mit der Sie die Cybersicherheit gewährleisten und eine wachsende Anzahl von Geräten, Apps und Verbindungen managen können. Dafür brauchen Sie eine Lösung, die Ihren Mitarbeitern zuverlässig Zugriff gewährt, ohne Unbefugten Tür und Tor zu öffnen. Vor allem aber brauchen Sie eine Lösung, die Ihre wertvollen Unternehmensressourcen kontinuierlich vor bekannten und unbekannten Bedrohungen schützt und sich nicht negativ auf die Produktivität auswirkt.

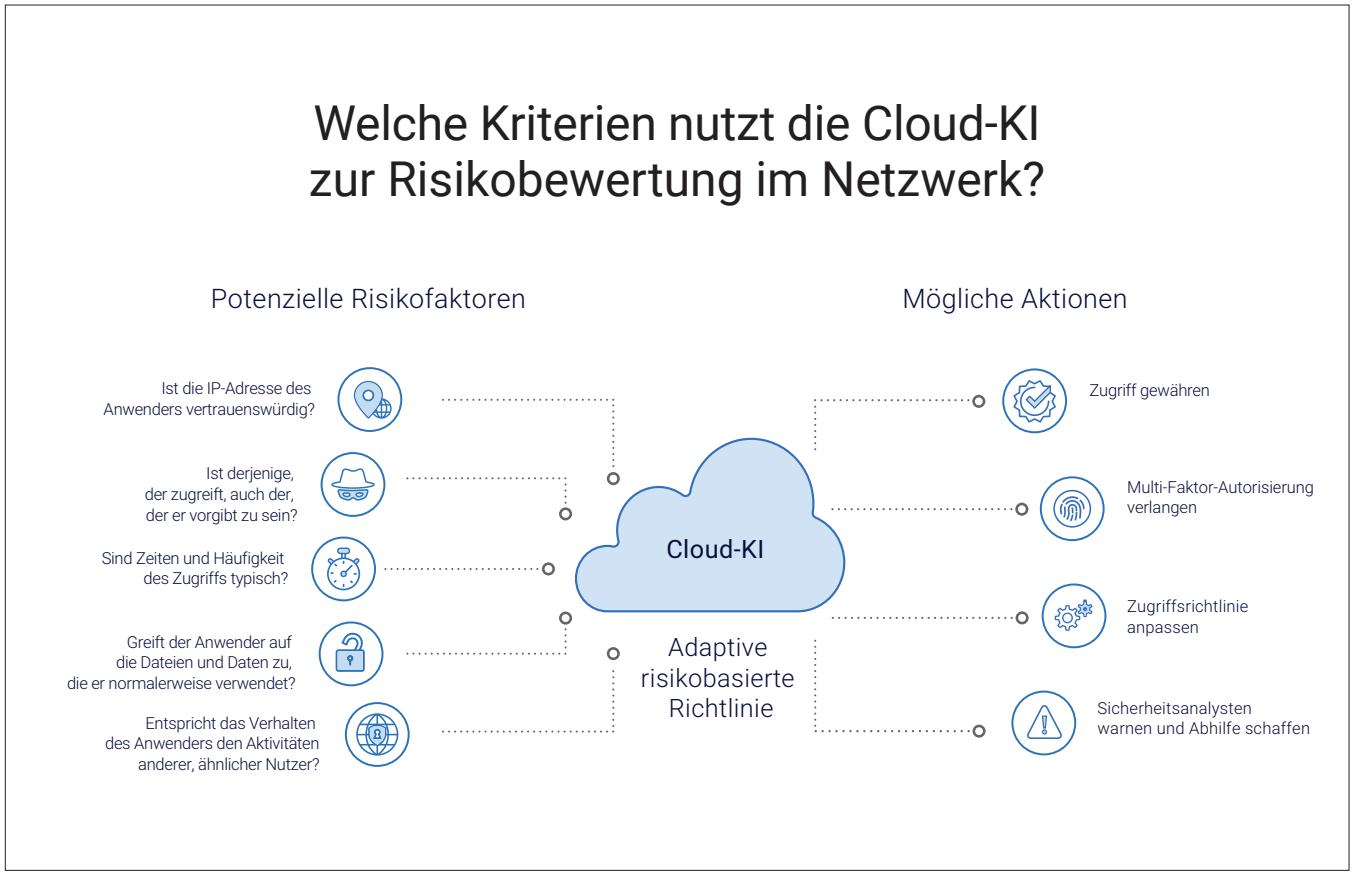
Diesen intelligenten und flexiblen Schutz bietet Ihnen BlackBerry® Gateway.

DIE VORTEILE VON BLACKBERRY GATEWAY

SICHERER ZUGRIFF AUF PRIVATE ANWENDUNGEN, DIE VOR ORT ODER IN DER ÖFFENTLICHEN CLOUD GEHOSTET WERDEN

BlackBerry Gateway ist eine Zero Trust Network Access (ZTNA)-Lösung. Bei einem Zero-Trust-Sicherheitsansatz wird alles standardmäßig als nicht vertrauenswürdig behandelt. Dank BlackBerry Gateway müssen Sie nicht unzählige Geräte einzeln verifizieren, authentifizieren und sichern. Denn alle Interaktionen werden kontinuierlich überwacht. In einer Zero-Trust-Architektur müssen alle Anwender, Geräte und Apps kontinuierlich vertrauenswürdig handeln, um weiterhin Zugriff auf interne Ressourcen zu bekommen. Durch das kontinuierliche Monitoring der Interaktionen führen Änderungen bei der Sicherheitseinschätzung direkt zu Änderungen bei den Zugriffsrechten und anderen Maßnahmen in Echtzeit. Darüber hinaus sorgt BlackBerry Gateway durch die Integration mit den BlackBerry® Endpoint Solutions dafür, dass nur vertrauenswürdige und fehlerfreie Geräte auf firmeneigene Anwendungen zugreifen dürfen.

BlackBerry Gateway bietet Ihnen einen sicheren, vereinfachten und segmentierten Zugriff auf private Applikationen, die vor Ort oder in einer öffentlichen Cloud gehostet werden. Sie profitieren von der One-Click-Konfiguration für die beliebtesten SaaS-Anwendungen. Zudem arbeitet BlackBerry Gateway mit einer fortschrittlichen KI-Netzwerkrisiko-Engine, um Ihre Remote-Belegschaft mit freigegebenen Ressourcen durch einen sicheren Tunnel zu verbinden. Die Cloud-KI analysiert kontinuierlich verschiedene Faktoren, die zuverlässig die Vertrauenswürdigkeit und die Zugriffsberechtigungen der Remote-Nutzung belegen.



Beispielsweise passt die Cloud-KI dann, basierend auf den folgenden Variablen, die Vertrauensstufe an:

- Ist die IP-Adresse des Anwenders vertrauenswürdig?
- Ist derjenige, der zugreift, auch der, der er vorgibt zu sein?
- Ist das Verhalten typisch?
- Wird auf die üblichen Ressourcen zugegriffen?
- Entspricht das Verhalten eines Anwenders seinen früheren Aktivitäten oder Anwendern mit ähnlichen Rollen?

Ändert sich ein Wert signifikant, kann die Cloud-KI dynamische Richtlinien aktivieren und eine Reihe von Maßnahmen ergreifen. Bei positiven Änderungen kann der Teilnehmer mit einem veränderten oder verbesserten Zugriff rechnen. Negative Vertrauensveränderungen führen zu verringertem Zugriff, einer Aufforderung zur erneuten Authentifizierung und im schlimmsten Fall zu Sicherheitswarnungen und Wiederherstellungsmaßnahmen.

Die präventive Prüfung und der Schutz aller möglichen und unmöglichen Kombinationen privater Technologien vor einem Zugriff ist schlicht nicht umsetzbar. BlackBerry Gateway löst dieses Problem, indem es alles, was mit firmeneigenen Ressourcen in Berührung kommt, kontinuierlich authentifiziert und nur vertrauenswürdigen Anwendern Zugriff gewährt. Dieses Vorgehen ist weniger umständlich als der Versuch, die gesamte Remote-Technologie zu sichern, und weniger riskant als die einmalige Authentifizierung von Geräten vor dem permanenten Zugriff.

REDUZIERUNG DES NETZWERKRISIKOS

Der Erfolg von BlackBerry Gateway beruht auf einem robusten TCP/IP-Stack mit einer IP-Sicherheitsschicht, die eigens für mobile und stromsparende Geräte optimiert ist. BlackBerry Gateway bietet Ihnen eine umfangreiche Protokollunterstützung, einschließlich VOIP, einer Cloud-nativen Architektur sowie Full- und Split-Tunnel-Zugangsmodi. Mit BlackBerry Gateway können Sie außerdem die SaaS-App-Identifikation nutzen und so dafür sorgen, dass Dienste wie Office 365 nicht ausfallen.

Dank der Fähigkeit, Bedrohungsinformationen im gesamten Netzwerk zu analysieren und zu korrelieren, kann BlackBerry Gateway Endpunkte isolieren und Netzwerkregeln modifizieren. Zudem bietet Ihnen die TCP/IP-Schicht Sicherheit beim Cloud-Zugriff durch die Analyse auch verschlüsselter Pakete. So gelingt es, Anomalien zu erkennen und die Unternehmensumgebung zu sichern, ohne die Privatsphäre der Kommunikation zu gefährden. Außerdem identifiziert BlackBerry Gateway bösartige Domains und Adressen mithilfe von IP- und URL-Reputationsfunktionen, um zu verhindern, dass Anwender darauf zugreifen.

LEISTUNGSSTARKE PLATTFORM

BlackBerry Gateway lässt sich problemlos mit fortschrittlichen, KI-gestützten Endpoint Solutions wie BlackBerry® Protect integrieren. Diese Cybersicherheitslösungen sorgen im Verbund für umfassenden Schutz vor Bedrohungen, die es auf Ihre Geräte, Netzwerke und Anwenderidentitäten abgesehen haben. Dank modernster KI verhindern die Endpunktlösungen bekannte, unbekannte und Zero-Day-Bedrohungen. Gleichzeitig stellt BlackBerry Gateway sicher, dass nur vertrauenswürdige und fehlerfreie Geräte auf Ihr Unternehmensnetzwerk zugreifen können.

ANWENDUNGSFÄLLE

BlackBerry Gateway löst zahlreiche Probleme. Vor allem die folgenden Konzepte und Verfahren haben sich in der Praxis bewährt:

Entscheiden Sie sich für Zero Trust

Verringern Sie Ihr Risiko durch die Implementierung eines dynamischen Netzwerkzugriffsmodells mit Least-Privilege-Ansatz und adaptiven identitätsbasierten Kontrollen. Denn dies sind die entscheidenden Bestandteile einer Zero-Trust-Architektur .

Sicherer Zugang für alle Anwender

Schützen Sie Ihr hybrides Geschäftsmodell und Ihre Remote-Belegschaft durch dynamische Zugriffsberechtigungen auf wichtige Ressourcen vor Ort oder in der Cloud.

Endpunkt- und Netzwerksicherheit

Schützen Sie Ihre Endgeräte und Netzwerke mit integrierten Lösungen, die nicht mehr, sondern intelligenter arbeiten. Gewinnen Sie einen besseren Überblick über Ihre Bedrohungslage und schützen Sie sich vor aktuellen und zukünftigen Cyberangriffen.

Verbesserte Zusammenarbeit

Bieten Sie nicht nur Ihren Festangestellten einen schnellen und sicheren Zugriff, sondern auch Auftragnehmern, Zulieferern und strategischen Partnern. Damit alle mit verwalteten und nicht verwalteten Geräten sicher auf freigegebene Ressourcen zugreifen können.

VPN-Ersatz

Verabschieden Sie sich von veralteten Perimeter-Verteidigungslösungen. Denn Sie bergen ein latentes Risiko und implizieren ein Vertrauen, das dazu führen kann, dass Anmeldeinformationen kompromittiert oder unberechtigt eingesetzt werden.

Fusionen, Zukäufe und Verkäufe

Verbessern Sie ohne großen Aufwand die Geschwindigkeit und Agilität Ihrer transformativen Vorhaben. Um die Produktivität zu steigern, müssen Sie keine Netzwerke integrieren. Bieten Sie allen ein einheitliches, stabiles und sicheres Arbeiten.

Transparenz in Echtzeit

Dank detaillierter Informationen zu Anwenderaktivitäten und der Nutzung von Anwendungen können Sie fundierte Netzwerk- und Risikoentscheidungen treffen.

Differenzierte Richtlinienverwaltung

Übernehmen Sie die Kontrolle über Ihre Netzwerke und Anwendungen. Gewähren Sie nur sicheren Zugriff nach außen und verfolgen sie einen adaptivem Least-Privilege-Ansatz bei Ihren Richtlinien, der von einer KI-gesteuerten Cloud-Risiko-Engine durchgesetzt wird.

VORTEILE GEGENÜBER VPN

BlackBerry Gateway unterscheidet sich von einem VPN durch einen anderen Zugriff auf die Unternehmensressourcen. Gelingt es einem Angreifer, sich über VPN zu authentifizieren, hat er breiten Zugriff auf die Umgebung. BlackBerry Gateway gewährt segmentierten Zugriff auf freigegebene Anwendungen. Diese Segmentierung schränkt die öffentliche Sichtbarkeit ein, verhindert Lateral Movement und reduziert dadurch die Angriffsfläche signifikant. Außerdem bietet es Ihnen einen besseren Einblick in die Anwenderaktivitäten und den Datenverkehr in Ihrem Netzwerk.

VPNs verfolgen einen statischen Ansatz zur Authentifizierung und Autorisierung. Wurde der Verifizierungsprozess erfolgreich durchgeführt, erklären sie den Anwender für die Dauer der Verbindung für sicher. BlackBerry Gateway hingegen authentifiziert jeden Netzwerknutzer kontinuierlich und beseitigt damit das implizierte Vertrauen. Dafür berücksichtigt es mehrere Faktoren. Darunter das Anwenderverhalten, die Vertrauenswürdigkeit des Geräts sowie Netzwerk- und App-Zugriffsmuster im Verlauf einer Verbindung. Erkennt die Cloud-KI einen verdächtigen Vorgang, leitet sie sofort Maßnahmen zum Schutz der Umgebung ein, die sich nach dem Schweregrad des Vorfalls richten.

BlackBerry Gateway ist eine Cloud-native Lösung und leicht zu skalieren, damit es den Anforderungen einer sich ändernden Organisation gerecht wird. Zudem bietet es verwalteten und nicht verwalteten Geräten direkten und sicheren Zugriff auf SaaS-Apps. Wachsenden Unternehmen, die noch mit VPN arbeiten, entstehen oft unnötige Kosten, wenn sie den Remote-Zugriff für neue Mitarbeiter einrichten. Die Absicherung von SaaS-Anwendungen mit einem VPN kann ein Backhauling des internetgebundenen Datenverkehrs von Remote-Anwendern erfordern, was wiederum den Bedienkomfort beeinträchtigt.

MIT BLACKBERRY GATEWAY SICHER IN DIE ZUKUNFT

BlackBerry Gateway nutzt fortschrittliche Cloud-KI, kontinuierliche Authentifizierung und einen robusten TCP/IP-Stack, um Interaktionen über Geräte mit Windows®, macOS®, iOS®, and Android™ zu sichern. Es reduziert die Angriffsfläche erheblich, indem es nur den Zugriff auf Apps gewährt und nicht auf das gesamte Netzwerk. Außerdem interagiert es nur mit vertrauenswürdigen Einheiten und Geräten. Durch seine Analyse- und Korrelationsfähigkeiten kann BlackBerry Gateway Bedrohungen besser kontextualisieren und erkennen. So deckt es bösartige Aktivitäten auf, die bei anderen Analysemethoden unsichtbar bleiben.

BlackBerry verfügt über jahrzehntelange Erfahrung bei der Absicherung von mobilen und Remote-Mitarbeitern und schützt über 500 Millionen Endpunkte weltweit. Wenn Sie mehr darüber erfahren möchten, wie BlackBerry Gateway Ihr Unternehmen schützen kann, besuchen Sie uns unter BlackBerry.com.

BlackBerry Intelligent Security. Everywhere.

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 195 Millionen Fahrzeuge. 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 Endpoint Security, Endpoint Management, Verschlüsselung und eingebettete Systeme führend. Die Vision von BlackBerry ist klar – das Sichern einer vernetzten Zukunft, der Sie vertrauen können.

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