BlackBerry | Cybersecurity

CylanceGATEWAY

KI-gestützte, Cloud-native Zero-Trust-Lösung zum Schutz sensibler Daten

DATENBLATT

Zuverlässiger Netzwerkschutz ist in Zeiten, in denen hybrides Arbeiten und BYOD hoch im Kurs stehen, unerlässlich. Jedes neue Gerät, jede neue Anwendung und jeder neue Anwender, der sich mit Unternehmensressourcen verbindet, ist eine potenzielle Gefahr für sensible Daten. Denn je mehr Personen von außen zugreifen und je vielfältiger die genutzten Geräte sind, desto größer ist die Angriffsfläche und damit auch das Risiko.

Laut aktuellen Schätzungen von Gartner[1] wollen 74 % der Unternehmen auch nach der Pandemie dezentrales Arbeiten ermöglichen. Doch der Trend zum hybriden Arbeiten ist eine echte Herausforderung für die Netzwerksicherheit. Ressourcen, die bisher von traditionellen Netzwerkgrenzen geschützt wurden, werden von außen erreichbar sein müssen. Außerdem werden Mitarbeiter immer häufiger mit den verschiedensten Geräten auf arbeitsbezogene SaaS-Angebote und Unternehmensdaten zugreifen und dadurch neue Sicherheitsrisiken erzeugen.

Die Schwachstellen, die durch Remote-Arbeit entstehen, entschärft die Cloud-native Zero Trust Network Access (ZTNA)-Lösung CylanceGATEWAY™ für Sie. Eine präventive Prüfung und der Schutz aller möglichen und unmöglichen Kombinationen privater Technologien vor einem Zugriff ist zwar wünschenswert, aber schlicht nicht umsetzbar. Deshalb verwendet CylanceGATEWAY ein KI-gestütztes Zero-Trust-Framework zur kontinuierlichen Authentifizierung und sorgt dafür, dass nur sichere und vertrauenswürdige Geräte auf Unternehmensressourcen zugreifen dürfen. Denn nicht jedes private Gerät und nicht jede private App ist sicher. Aber jedes Gerät, das auf sensible Daten zugreifen möchte, muss seine Vertrauenswürdigkeit beweisen.

CylanceGATEWAY FÄHIGKEITEN

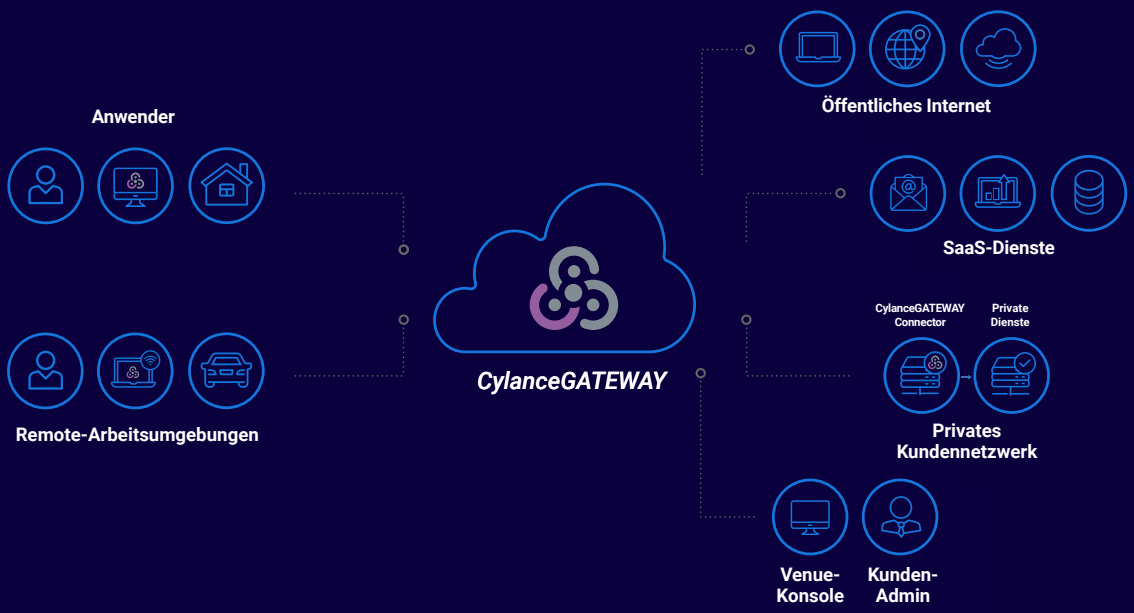
Zum Schutz der Netzwerkumgebungen verwendet CylanceGATEWAY™ mehrere fortschrittliche Technologien. Es basiert auf einem robusten TCP/IP-Stack, ist für mobile und Remote-Geräte optimiert und entdeckt Bedrohungen in verschlüsselten Paketen. Mithilfe fortschrittlicher KI kann es verdächtiges Verhalten und Anomalien in der gesamten Umgebung erkennen, den Zugriff in Echtzeit anpassen und Bedrohungsinformationen, die von herkömmlichen Lösungen oft übersehen werden, korrelieren und kontextualisieren. CylanceGATEWAY bietet zuverlässigen Schutz für Ihre Netzwerke, Apps und Daten, ohne die Produktivität Ihrer Anwender zu beeinträchtigen. Mit den Segmentierungsfunktionen können Sie Anwendungen vor allzu neugierigen Augen verbergen, was das Risiko für DDoS-Angriffe reduziert und Lateral Movement verhindert. Zudem können Sie durch das Source IP Pinning die Konnektivität von SaaS-Anwendungen auf vertrauenswürdige und bekannte IPs beschränken. Fazit: Mit CylanceGATEWAY können Sie Ihren Anwendern präzise und identitätsbewusst Zugriff auf lokale und Cloud-Ressourcen gewähren.

KI-GESTÜTZTER, ADAPTIVER UND SICHERER ZUGRIFF

CylanceGATEWAY nutzt Cloud-KI, um kontinuierlich wichtige Faktoren zu analysieren, die zuverlässig die Vertrauenswürdigkeit und die Zugriffsberechtigungen der Remote-Nutzung belegen. Nicht nur Anwender werden einer Prüfung unterzogen, sondern auch Anwendungen und Bots, die auf die Umgebung zugreifen möchten. Die Cloud-KI passt dann, basierend auf den folgenden Variablen, die Vertrauensstufe an:

- Ist die IP-Adresse des Anwenders vertrauenswürdig?
- Ist der derjenige, der zugreift, auch der, der er vorgibt zu sein?

CylanceGATEWAY im Überblick
KI-gestützter Zero-Trust-Netzwerkzugriff



CLOUD-KI

CylanceGATEWAY Cloud-KI analysiert kontinuierlich die Netzwerkrisikofaktoren für jede verbundene Einheit und ändert die Zugriffsebenen dynamisch. Je nach Vertrauenswert.

- 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 Vertrauensfaktor signifikant, kann die Cloud-KI je nach Schwere des Verdachts eine Reihe von Maßnahmen ergreifen. Bei positivem Verhalten kann der Anwender mit fortgesetztem und verbessertem Zugriff rechnen. Negative Vertrauensveränderungen führen zu verringertem Zugriff, einer Aufforderung zur erneuten Authentifizierung und im schlimmsten Fall zu Sicherheitswarnungen und Wiederherstellungsmaßnahmen.

NETZWERKDIENSTE MIT FULL/SPLIT-TUNNEL

CylanceGATEWAY™ bietet Ihnen einen sicheren Kommunikationstunnel zwischen Remote- oder mobilen Anwendern und der Unternehmensumgebung. Der sichere Tunnel arbeitet in einem Full- oder Split-Access-Modus. Ganz nach Ihren Anforderungen. Der Full-Modus sichert die gesamte Kommunikation zwischen dem Anwender und dem Unternehmensnetzwerk. Beim Split-Tunnel-Verfahren werden nur bestimmte Ressourcen durch den Tunnel transportiert – das spart Bandbreite. Der Split-Tunnel-Ansatz ist vor allem beim Einsatz von BYOD- und Homeoffice-Geräten sinnvoll, denn er trennt strikt den beruflichen Datenverkehr von der privaten Nutzung.

SOURCE IP PINNING

Einige Webdienste und Cloud-Anwendungen lehnen Netzwerkverkehr ab, der nicht von explizit registrierten IP-Adressen stammt. Das führt dazu, dass einige Unternehmen diese Sicherheitsmaßnahmen umgehen, indem sie die IP-Adressen ändern oder verbergen. Den Datenverkehr senden sie dann direkt an die Dienstanbieter und generieren so eine unnötige Sicherheitslücke.

Mit Source IP Pinning können Sie die IP-Adressen von Geräten kontrollieren, die mit Service Providern kommunizieren, ohne Sicherheitsmaßnahmen zu umgehen. Außerdem können Sie so auch interne Ressourcen vor externen Agitatoren verbergen, die nach Möglichkeiten suchen, tiefer in Ihr Netzwerk vorzudringen und einen Lateral-Movement-Angriff durchzuführen.

ZUGRIFF ÜBER EINE APP STATT ÜBER DAS NETZWERK

CylanceGATEWAY™ unterscheidet sich von einem VPN durch einen anderen Zugriff auf die Unternehmensressourcen. Gelingt es einem Angreifer, sich über VPN zu authentifizieren, hat er weitreichenden Zugriff auf die Umgebung. Mit CylanceGATEWAY können Sie segmentiert Zugriff auf autorisierte Anwendungen über ausgehende Verbindungen gewähren, die am Service-Edge zusammengefügt werden. Dadurch stellen Sie sicher, dass Anwender nicht irgendwo im Netzwerk platziert werden. Mit der Segmentierung können Sie auch Anwendungen verbergen, Lateral Movement verhindern und Ihre Angriffsfläche erheblich reduzieren. Zudem gewinnen Sie durch Gateway einen besseren Überblick über die Aktivitäten und den Datenverkehr in Ihrem Netzwerk.

Eine weitere Besonderheit ist die kontinuierliche Authentifizierung durch CylanceGATEWAY. Anders VPNs, die einen statischen Ansatz zur Authentifizierung und Autorisierung verfolgen. Wurde der Verifizierungsprozess erfolgreich durchgeführt, erklären sie den Anwender für die Dauer der Verbindung als sicher. Um ein übermäßiges implizites Vertrauen zu verhindern, authentifiziert CylanceGATEWAY jeden Netzwerkteilnehmer kontinuierlich anhand verschiedener Faktoren. Darunter das Anwenderverhalten, die Vertrauenswürdigkeit des Geräts sowie Netzwerk- und App-Zugriffsmuster im Verlauf einer Verbindung. Erkennt die Cloud-KI eine Anomalie, leitet sie sofort Maßnahmen zum Schutz der Umgebung ein, die sich nach der Schwere des Vorfalls richten.

STARKE TCP/IP-SICHERHEIT

Der Erfolg von CylanceGATEWAY beruht auf einem robusten TCP/IP-Stack mit einer IP-Sicherheitsschicht, die eigens für Windows®-, macOS®-, iOS®- und Android™-Geräte optimiert ist. CylanceGATEWAY bietet Ihnen eine umfangreiche Protokollunterstützung, einschließlich VOIP, einer Cloud-nativen Architektur sowie Full- und Split-Tunnel-Zugangsmodi. Mit CylanceGATEWAY können Sie außerdem die SaaS-App-Identifikation nutzen und so dafür sorgen, dass Dienste wie Office 365 nicht ausfallen. Darüber hinaus können die IP-Reputationsfunktionen von CylanceGATEWAY bösartige Domains und gefährliche Standorte identifizieren und Ihre Mitarbeiter vor der Interaktion mit gefährlichen Netzwerkeinheiten schützen.

NETZWERKBEDROHUNG ERKENNEN

CylanceGATEWAY entdeckt und kontextualisiert Bedrohungen im gesamten Netzwerkverkehr. Auch innerhalb verschlüsselter Pakete. Durch seine Analyse- und Korrelationsfähigkeiten kann CylanceGATEWAY komplexe und mehrstufige Bedrohungen identifizieren, die für andere Analyseformen unsichtbar bleiben. CylanceGATEWAY verzichtet auf die Ent-/Wiederverschlüsselung von Paketen. Das Ergebnis ist eine hoch performante Lösung, die weniger Netzwerkressourcen beansprucht. Denn die Identifizierung von Bedrohungen innerhalb verschlüsselter Pakete schützt Ihre Umgebung, ohne die Privatsphäre der Anwender im Netzwerk zu gefährden.

HÄUFIGE CylanceGATEWAY ANWENDUNGSFÄLLE

CylanceGATEWAY löst durch seinen KI-gestützten Zero-Trust-Ansatz zahlreiche Probleme. Vor allem die folgenden Konzepte und Verfahren von CylanceGATEWAY haben sich in der Praxis bewährt:

ENTSCHEIDEN SIE SICH FÜR ZERO TRUST

Verringern Sie Ihr Gesamtrisiko durch die Implementierung eines dynamischen Netzwerkzugriffs 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 privaten Geräten sicher auf freigegebene Ressourcen zugreifen können.

VPN-ERSATZ

Verabschieden Sie sich von veralteten Lösungen, die Ihr Unternehmen nur an den Netzwerkgrenzen verteidigen. 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 adaptiven Least-Privilege-Ansatz bei Ihren Richtlinien, der von einer KI-gesteuerten Cloud-Risiko-Engine durchgesetzt wird.

GUTE GRÜNDE FÜR CylanceGATEWAY

Konfiguration und Akzeptanz

Durch die One-Click-Konfiguration für viele beliebte SaaS-Anwendungen entlasten Sie Ihre Netzwerkadministratoren und verbessern durch die schnelle Implementierung die Akzeptanz bei den Anwendern.

Reduziertes Netzwerkrisiko

Verhindern Sie mit Source IP Pinning, dass nicht autorisierte Personen auf Ihr Netzwerk zugreifen. Und durch Segmentierung verbergen Sie Anwendungen vor allzu neugierigen Augen und eliminieren unerwünschtes Lateral Movement.

Netzwerk- und Aktivitätstransparenz

Das anwenderfreundliche Dashboard bietet Ihnen einen Überblick über Ihren Netzwerkverkehr, Sicherheitsereignisse und Indikatoren für eine Gefährdung. Hier können Sie sich auch den Status, die Zugriffshistorie und die wichtigsten Netzwerkziele anzeigen lassen.

Mit jedem Gerät von überall aus sicher zugreifen

Ermöglichen Sie es Ihrer Remote-Belegschaft, von zu Hause oder von jedem beliebigen Ort aus zu arbeiten. Und zwar sowohl mit verwalteten als auch mit nicht verwalteten Geräten. Verfügbar für macOS, Windows, iPhone und Android.

MEHR ERFAHREN

CylanceGATEWAY™ ist nur eine von zahlreichen KI-gestützten, präventiven Sicherheitslösungen von BlackBerry. Überzeugen Sie sich selbst von unserem erstklassigen Angebot, mit dem Sie sich bestmöglich auf Cybervorfälle vorbereiten sowie Angriffe rechtzeitig entdecken und stoppen können.

Entdecken Sie:

BlackBerry® Cyber Suite

BlackBerry Spark® Suite

[1] https://www.gartner.com/en/newsroom/press-releases/2020-04-03-gartner-cfo-surey-reveals-74-percent-of-organizations-to-shift-some-employees-to-remote-work-permanently2

Schnelle und zuverlässige Performance

Mit dem Edge Accelerator können Sie die Netzwerkpfade optimieren, um die Leistung und die Geschwindigkeit zu verbessern. Die robuste und widerstandsfähige Tunneltechnologie sorgt für zuverlässige Verbindungen für alle Anwendungen und ermöglicht VoIP.

Integrierte Bedrohungssuche

CylanceGATEWAY bietet Ihnen eine KI-gestützte Erkennung von Netzwerkbedrohungen, indem es zuverlässig Netzwerktelemetrie auch ohne Entschlüsselung analysiert. Die native Integration von CylanceGATEWAY in die BlackBerry Spark® Unified Endpoint Security Suite stellt sicher, dass nur vertrauenswürdige und fehlerfreie Geräte Zugang zum Netzwerk erhalten.

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 215 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.

BlackBerry. Intelligent Security. Everywhere.

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

BB23 | 220721