Goodbye VPN.

WILLKOMMEN ZTNA.

VPNs sind oft langsam, umständlich und unsicher.
Dieser Leitfaden verrät Ihnen, warum ZTNA (Zero Trust Network Access) die überlegene Alternative für Ihre hybride Belegschaft ist.

BlackBerry® | Cybersecurity

Effektive Cybersicherheit ist schon lange kein Nice-to-have mehr, sondern ein Muss. Allerdings fällt es vielen Unternehmen immer noch schwer, ihre Daten und Anwendungen angemessen vor Cyberangriffen zu schützen. Und mit dem Trend zu Remote- und Hybrid-Arbeit steigt die Gefahr: Bis Ende 2023 werden laut einer Gartner-Studie 71 % der Knowledge Worker in den USA zumindest teilweise remote arbeiten.[1] Schon heute gewähren 95 % der Unternehmen ihren Beschäftigten den Remote-Zugriff auf Unternehmensdaten.[2]

Noch ist VPN in vielen Unternehmen das Mittel der Wahl, um die User mit Arbeitsressourcen hinter der Firewall zu verbinden. Doch dieser Ansatz ist veraltet und riskant. VPN ist den unerbittlichen und immer raffinierter werdenden Cyberangriffen nicht gewachsen. User klagen über die umständliche Bedienung und IT-Administratoren über den Zeitaufwand und die mangelhafte Performance.

Daher überrascht es kaum, dass

63 % der Unternehmen, die noch mit VPN arbeiten, in naher Zukunft auf eine Zero-Trust-Lösung wechseln wollen.[2]

Wechseln auch Sie rechtzeitig zu ZTNA.

Dieser Leitfaden verrät Ihnen die vier wichtigsten Gründe, warum Sie sich von VPN verabschieden und sich für ZTNA entscheiden sollten.

Sie erfahren, wie ZTNA:

- die Latenzzeit und Komplexität für User verringert
- die Sicherheit stärkt und Ihre Angriffsfläche für Cyberkriminelle minimiert
- das Management vereinfacht und den administrativen Aufwand verringert
- mehr Skalierbarkeit und Flexibilität bietet
- VPNs in jedem Fall überlegen ist

Was ist Zero Trust Network Access?

ZTNA arbeitet mit den Prinzipien von Zero Trust, um alle Sitzungs- und Ressourcenanfragen kontinuierlich zu authentifizieren und zu autorisieren. Und zwar bevor der Zugriff auf Anwendungen, Dateien oder andere sensible Informationen gewährt wird. Es verzichtet auf implizites Vertrauen und verweigert den Zugriff standardmäßig. Zudem stärkt ZTNA die Sicherheit im gesamten Unternehmen, da es mithilfe adaptiver Zugriffskontrollen, die auf identitäts- und kontextabhängigen Richtlinien basieren, den Least-Privilege-Ansatz umsetzt.

VPN gewährt breiten Netzwerkzugriff. ZTNA hingegen arbeitet nach dem Prinzip „Nie vertrauen, immer überprüfen“ und gewährt nur den minimal erforderlichen Zugriff auf Basis der User-Identität und kontextbezogener Informationen. Dies verringert das Risiko für einen unbefugten Zugriff – durch Externe und durch Insider. Außerdem minimiert es die Auswirkungen potenzieller Sicherheitsverletzungen.

Zero Trust Security überzeugt durch:

- Least-Privilege-Zugriff
- Kontinuierliche Überprüfung der User-Identität
- Segmentierung von Anwendungen
- Verschlüsselte Übertragungen zwischen Usern und Anwendungen
- Verbesserte Transparenz im Unternehmen

Die vier wichtigsten Gründe für einen Wechsel zu ZTNA

(... verabschieden Sie sich von Ihrem VPN)

1 Verbessern Sie die User Experience

50 % *der Belegschaft arbeiten remote oder in einem Hybridmodell.*[3]

ZTNA bietet – im Gegensatz zu VPNs – eine nahtlose und anwenderfreundliche User Experience, indem es sicheren Zugriff auf Ressourcen von jedem Ort, zu jeder Zeit und mit jedem Gerät ermöglicht.

ZTNA-User können sich mit Authentifizierungsmethoden wie Multi-Faktor-Authentifizierung (MFA) und Single Sign-on (SSO) authentifizieren. Der Vorteil: Die Notwendigkeit für VPNs entfällt, der neue Ansatz ist nutzerzentriert, fördert die Produktivität und ermöglicht der remote und mobil arbeitenden Belegschaft sicheren Zugriff auf Ressourcen, ohne den Bedienkomfort einzuschränken.

Für VPN-Verbindungen sind die Latenzzeiten typisch und nervend zugleich. Bei ZTNA hingegen können sich die authentifizierten User direkt mit den Anwendungen verbinden, ob über ein Rechenzentrum oder die Cloud. Wer vom Trust Broker verifiziert wurde, kann dann direkt auf die genehmigten Ressourcen zugreifen, ohne alle Daten über ein VPN übertragen zu müssen.

Hoher Bedienkomfort:

- Schnelle Verbindungen
- Hohe Verfügbarkeit
- Support für jedes Endgerät
- Optimierte Authentifizierung

Problem:

VPN leitet den Backhaul-Traffic durch das Rechenzentrum. Das führt häufig zu einer Überlastung der Netzwerke und zu nervenden, langsamen Verbindungen. Ist die Authentifizierung dann auch noch umständlich, schadet das der User Experience.

Lösung:

Cloud-native ZTNA-Lösungen bieten Usern einen optimierten Zugriff auf Anwendungen auf globaler Ebene. Backhaul-Traffic fällt dabei nicht an. Das Resultat: schnellere Verbindungen, die sich positiv auf die Zufriedenheit und Produktivität der Anwender auswirken können. Zudem erleichtert ZTNA die Remote-Arbeit und BYO-Bereitstellungen durch eine vereinfachte User-Verwaltung. Darüber hinaus ermöglicht es einen sicheren Zugriff von jedem Gerät und von jedem Standort auf jede genehmigte Anwendung.

Die vier wichtigsten Gründe für einen Wechsel zu ZTNA

(... verabschieden Sie sich von Ihrem VPN)

2 Stärken Sie die Sicherheit durch Minimierung der Angriffsfläche

Das VPN- und Firewall-Sicherheitsmodell bringt Usern in aller Regel ein übermäßiges, implizites Vertrauen entgegen und bietet je nach Rolle und Netzwerkstandort breiten Zugriff auf Netzwerkressourcen. ZTNA hingegen setzt das Least-Privilege-Prinzip um.

Authentifizierte User können nur mit verifiziert fehlerfreien Geräten auf genehmigte Ressourcen zugreifen, die sie für die Arbeit benötigen. Dies reduziert das Risiko für unbefugten Zugriff und Lateral Movement durch Angreifer signifikant. Und es minimiert den Schaden, falls Angreifer doch ins Netzwerk eindringen sollten.

Außerdem segmentieren ZTNA-Lösungen Anwendungen und verbergen sie vor der Öffentlichkeit.

80 %

der Technologie-Führungskräfte sehen VPN noch als Teil ihrer Cybersicherheitsstrategie. Doch 74 % geben zu, dass sie nicht wissen, ob VPN ausreicht, um ihr Unternehmen vor Cyberangriffen zu schützen.[4]

Problem:

VPNs geben IP-Adressen preis und erhöhen dadurch die Angriffsfläche. Haben sich Bedrohungsakteure einmal Zugang zum Netzwerk verschafft, können sie sich seitlich bewegen und weitere User, Geräte und Daten gefährden.

Lösung:

ZTNA arbeitet mit Anwendungssegmentierung, um Anwendungen vor der Öffentlichkeit zu verbergen und so die Angriffsfläche zu verkleinern. Der Anwendungszugriff erfolgt nach dem Least-Privilege-Prinzip pro Sitzung.

Die vier wichtigsten Gründe für einen Wechsel zu ZTNA

(... verabschieden Sie sich von Ihrem VPN)

3 Zentralisieren und vereinfachen Sie die Administration

ZTNA erleichtert die Administration durch die Zentralisierung von Zugriffsrichtlinien und Authentifizierungsmechanismen. Bei herkömmlichen Ansätzen ist die Verwaltung der Regeln komplex und zeitaufwendig. Außerdem erfordern VPNs zahlreiche physische Geräte vor Ort. Diese müssen zudem noch alle überwacht und gewartet werden. Bei den Geräten handelt es sich um VPN-Gateways, Load Balancer und Firewalls, die manuell konfiguriert und gewartet werden müssen. Dies beschränkt die Skalierbarkeit eines VPNs.

ZTNA hingegen bietet:

- eine einheitliche Ansicht der User-Aktivitäten und Zugriffsberechtigungen
- Sichtbarkeit und Kontrolle über Netzwerkressourcen
- vereinfachtes Access Management und reduzierten Verwaltungsaufwand durch einen zentralisierten Ansatz

Darüber hinaus unterstützt ZTNA die nahtlose Integration mit Identity and Access Management (IAM) Systemen, wodurch die Verwaltung von User-Identitäten und Zugriffsberechtigungen von einem einzigen Kontrollpunkt aus erleichtert wird. Diese Vereinfachung der Verwaltungsprozesse ermöglicht es Unternehmen, Sicherheitsrichtlinien durchzusetzen, User-Aktivitäten zu verfolgen sowie schnell und effizient auf Sicherheitsvorfälle zu reagieren.

22 % *der Unternehmen hadern mit den Wartungskosten für herkömmliche VPN-Infrastrukturen.*[5]

Problem:

VPNs erfordern den Einsatz von Appliances in Rechenzentren. Diese brauchen manuelle Konfigurationen und Wartung, was mit Kosten, Zeit und Komplexität verbunden ist.

Lösung:

ZTNA konsolidiert die Verwaltung und Konfiguration. Es vereinfacht die Bereitstellung und die Netzwerksicherheitsprogramme, während es zugleich die Zugriffskontrolle und die Richtlinienverwaltung optimiert.

Die vier wichtigsten Gründe für einen Wechsel zu ZTNA

(... verabschieden Sie sich von Ihrem VPN)

4 Profitieren Sie von mehr Skalierbarkeit und Flexibilität

Cloudbasierte ZTNA-Lösungen bieten Skalierbarkeit und Flexibilität. Immer mehr Unternehmen arbeiten mit Cloud-Services, genehmigen Remote-Arbeit und erweitern ihren digitalen Fußabdruck. Dafür brauchen sie sicheren Zugriff auf Ressourcen – und diesen bietet ZTNA. Mit ZTNA können Sie sicherstellen, dass User und Geräte vor dem Zugriff auf wichtige Systeme und Daten authentifiziert und autorisiert werden. Und zwar unabhängig davon, ob sich die Ressourcen in der Cloud oder vor Ort befinden.

Um den dynamischen Anforderungen der heutigen Geschäftswelt gerecht zu werden, brauchen Unternehmen Skalierbarkeit und Flexibilität. ZTNA bietet einen sicheren Rahmen für Initiativen zur digitalen Transformation. Es ermöglicht Unternehmen, verteilte Ressourcen sicher zu verbinden, Beschäftigte an entfernten Standorten zu unterstützen und neue Technologien nahtlos zu integrieren.

Leichte Skalierbarkeit:

- Cloud-nativ
- Keine wartungsintensive Infrastruktur
- Unterstützt Initiativen zur digitalen Transformation

37 % *der Unternehmen berichten über eine bessere organisatorische Flexibilität.*[6]

Problem:

VPNs sind auf den Einsatz von Appliances in Rechenzentren angewiesen. Bei einer Skalierung brauchen Sie zusätzliche Ressourcen und weitere Hardware. Dies schränkt Ihre Flexibilität ein und macht die Bereitstellung eines sicheren Zugangs bei einer größeren Personenzahl zu einem teuren Vergnügen.

Lösung:

Mit ZTNA ersparen Sie sich die Anschaffungs- und Wartungskosten für VPN-Geräte und die Infrastruktur. Alles, was Sie brauchen, befindet sich in der Cloud. So können Sie bei Bedarf Prozesse besser skalieren und sind gleichzeitig flexibler, um Anpassungen während des Betriebs vorzunehmen.

ZTNA ist VPNs überlegen – in jedem Fall

	ZTNA	VPN
VERBESSERTE SICHERHEIT		
Adaptiver Zugriff nach dem Least-Privilege-Prinzip	✓	X
Minimierte Angriffsfläche	✓	X
Kontinuierliche Auswertung	✓	X
Segmentierung von Anwendungen	✓	X
Zufriedene, produktive User		
Mehr Transparenz für User	✓	X
Schnellere Verbindungen zu SaaS-Anwendungen	✓	X
Kein Backhaul-Traffic	✓	X
Verbesserte User Experience	✓	X
Verbesserter Remote-Zugriff mit hoher Verfügbarkeit	✓	X
Optimierte Authentifizierung	✓	X
Vereinfachte Verwaltung		
Vereinfachte Administration	✓	X
Leicht zu skalieren	✓	X
Cloud-nativ	✓	X
Integrierter Security-Stack	✓	X
Kein teurer Security-Stack und keine teure Infrastruktur nötig	✓	X
Schnelle Bereitstellung	✓	X
Verbesserte Agilität	✓	X
Budgetfreundlich	✓	X
Support für verwaltete und nicht verwaltete Geräte	✓	X
Optimierte Einrichtung von SaaS-Anwendungen und Konnektivität	✓	X
Unterstützt die digitale Transformation	✓	X

Entscheiden Sie sich für ZTNA

77 % *der Unternehmen berichten, dass Zero Trust sowohl Sicherheits- als auch Geschäftsvorteile bietet.*[6]

Mit ZTNA können Sie unbesorgt moderne Arbeitsweisen erlauben und neue Technologien einführen. Denn Sie können darauf vertrauen, dass der sichere Zugriff unabhängig von der Netzwerkumgebung oder dem Standort der Ressourcen gewährleistet ist.

Wenn Sie zu ZTNA wechseln, können Sie Ihre Sicherheit erhöhen, Ihre Angriffsfläche minimieren, die User Experience verbessern, die Administration vereinfachen sowie Ihre Skalierbarkeit und Flexibilität erhöhen.

Ersetzen Sie Ihr VPN durch CylanceEDGE

CylanceEDGE™ von BlackBerry kann Ihr VPN ersetzen. Es bietet Ihnen Datensicherheit und sicheren Zugriff auf private und SaaS-Apps – überall und jederzeit. Diese moderne, Cloud-native Lösung ermöglicht es Ihnen, das zu schützen, was am wichtigsten ist. CylanceEDGE ist so flexibel, dass es verwaltete und nicht verwaltete Geräte unterstützen kann. Es ist ausgelegt für eine kontinuierliche Authentifizierung und Autorisierung. Zudem kann es sensible Daten im Ruhezustand und bei der Übertragung identifizieren. Dadurch verbessert es die Transparenz und kann eine Exfiltration verhindern. Weitere Informationen finden Sie auf unserer Website.

[1] Gartner Pressemitteilung: 1. März 2023, Gartner prognostiziert, dass 39 % der weltweiten Knowledge Worker bis Ende 2023 hybrid arbeiten werden.
[2] Gartner Peer Insights, ZTNA for Hybrid Work Environments survey
[3] Enterprise Strategy Group Complete Survey Results, 2023 SASE Series: SSE Leads the Way Towards SASE, August 2023
[4] Gartner Peer Insights, ZTNA for Hybrid Work Environments survey
[5] Enterprise Strategy Group Research Report, Transitioning Network Security Controls to the Cloud, August 2020
[6] Enterprise Strategy Group Survey Results, The State of Zero Trust Security Strategies, May 2021

BlackBerry | Cybersecurity

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 235 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****.*

BB23 | 231018