FORRESTER®

TEI-Spotlight:

Sicherer Remote-Zugriff und sorgenfreies Arbeiten dank Prisma Access von Palo Alto Networks

Forrester sprach kürzlich im Rahmen einer Total Economic Impact™ (TEI)-Studie mit mehreren Palo Alto Networks-Kunden über ihre Investition in Prisma Access.[1] Im Rahmen dieser Interviews ermittelte Forrester verschiedene Vorteile der der kundenseitigen Einführung von Prisma Access, einer Cloud-basierten Netzwerksicherheitslösung, die Teil der Secure Access Services Edge Plattform (SASE) von Palo Alto Networks ist. Prisma Access wird hauptsächlich für die Verbindung und den sicheren Zugriff für Remote-Benutzer, Zweigstellen/Standorte und andere Remote-Netzwerke verwendet.

Da immer mehr Anwendungen, Server und Services Cloud-basiert sind und Remote-Arbeit zum weltweiten Standard wird, prüfen Unternehmen von Neuem, ob alte Punktlösungen angemessen skaliert werden können und ihren Benutzern und Standorten einen sicheren, zuverlässigen Zugriff bieten können. Mitarbeiter setzen in der Regel auf Remote Access VPN oder ähnliche Dienste, um auf kritische Daten zuzugreifen oder wichtige, zeitkritische Aufgaben auszuführen. Das bedeutet, dass der sichere Zugriff seitens der Benutzer eine tatsächliche Auswirkung auf das Geschäftsergebnis eines Unternehmens haben kann. Angesichts der zunehmenden Komplexität und Raffinesse von Cyberangriffen ist es zudem von entscheidender Bedeutung, dass Unternehmen Protokolldaten aller Dienstleistungen zentralisieren und nutzen können, um Sicherheitslücken zu schließen und potenzielle Bedrohungen für die Netzwerksicherheit zu erkennen und zu mindern.

Palo Alto Networks stellt eine integrierte Plattform bereit, die den umfassenden Netzwerk- und Sicherheitsanforderungen von Unternehmen gerecht wird. Prisma Access, eine Cloud-native Lösung, bietet konsistente Netzwerksicherheitsdienste und Zugriff auf alle Arten von Cloud-Anwendungen für Remote-Benutzer sowie auf Remote-Standorte. Dank Prisma Access müssen sich Unternehmen nicht mehr auf mehrere Punkt- und On-Premise-Lösungen verlassen, wodurch sowohl Kosten als auch Komplexität reduziert werden und gleichzeitig die allgemeine Sicherheitslage verbessert wird.

Return on investment (ROI)
247 %

Net Present Value (NPV, Nettobarwert)
28,5 Mio. USD

Um die Vorteile, Kosten und Risiken im Zusammenhang mit Prisma Access besser zu verstehen, beauftragte Palo Alto Networks Forrester Consulting damit, Stakeholder in zehn ausgesuchten Unternehmen zu befragen und Umfragen bei 133 weiteren Kunden durchzuführen, um eine Total Economic Impact™-Studie (TEI) durchzuführen. Für dieses Prisma Access Spotlight nutzte Forrester Daten von neun interviewten Unternehmen, die alle Erfahrung mit der Nutzung von Prisma Access zur Bereitstellung eines sicheren Remote-Zugriffs für kritische Anwendungen und Dienstleistungen für weltweit verbreitete Unternehmen haben.

In dieser Zusammenfassung liegt der Fokus darauf, wie die interviewten Unternehmen Prisma Access und dessen Wert für ihr Unternehmen nutzen.

Verringerung der Wahrscheinlichkeit eines Datenlecks

45 %

INVESTITIONSFAKTOREN

Unternehmen nannten die folgenden Faktoren für ihre Investition in Prisma Access von Palo Alto Networks:

- **Bereitstellen einer sicheren, zuverlässigen Verbindung für alle Benutzer von überall aus.** Alte Lösungen wie On-Premise VPNs oder Web Proxy-Services boten nicht die Transparenz, die Unternehmen für die zuverlässige Sicherung ihrer Netzwerke benötigen, und waren bekanntermaßen unzuverlässig, da Benutzer sich über häufige Trennungen der Verbindung und Zugriffsprobleme beschwerten. Ein leitender VP in der Finanzdienstleistungsbranche erklärte: „Bei unserer vorherigen Remote-Zugriffslösung beklagten sich unsere Benutzer oft über langsame Geschwindigkeiten, insbesondere wenn sie international unterwegs waren. Außerdem müssen wir uns jetzt keine Sorgen mehr um Betriebszeit und Verfügbarkeit machen, da Palo Alto Networks als Teil der Dienstleistung im Rahmen einer SLA eine hohe Betriebszeit gewährleistet."

> **„Einer der Vorteile von Prisma Access ist, dass wir dabei gar nichts machen müssen. Wir müssen uns nicht die ganze Zeit mit Patching und Überwachung der Portale und der Gateways befassen."**
>
> *Leiter der Netzwerk- und Überwachungsdienste, Bildung*

- **Skalierung zur Deckung der steigenden Nachfrage für Remote-Zugriff vor und nach der Pandemie.** Noch bevor COVID-19 die meisten Unternehmen dazu zwang, flexiblere Remote-Arbeit zu ermöglichen, hatten Unternehmen Schwierigkeiten, ihre alten Lösungen zu skalieren, um der steigenden Nachfrage für Remote-Zugriff gerecht zu werden. Die interviewten Unternehmen hatten sich vor der COVID-19-Pandemie für die Bereitstellung von Prisma Access entschieden und stellten fest, dass die verbesserte Skalierbarkeit ein entscheidender Faktor für die Aufrechterhaltung des Geschäftsbetriebs war, während die Belegschaft zunehmend auf Remote-Arbeit umgestellt wurde. Ein leitender VP in der Finanzdienstleistungsbranche erklärte: „Prisma Access hat es unseren Nutzern ermöglicht, auf die Anwendungen und Daten zuzugreifen, die sie benötigen, und zwar auf sichere Weise, unabhängig davon, wo sie sich befinden. Dies war während der gesamten Pandemie von entscheidender Bedeutung, da unser Unternehmen zu 100 % auf Remote-Arbeit umgestellt hat. Unsere bisherige Remote-Zugriffslösung hätte keinesfalls effektiv skaliert werden können, um diese Umstellung auf Remote-Arbeit zu unterstützen."

  Darüber hinaus möchten Unternehmen, dass alle Benutzer Prisma Access nutzen, um sicherzustellen, dass sie vor Bedrohungen geschützt sind, insbesondere beim Zugriff auf Apps oder Daten von riskanten Standorten aus. Ein Leiter der Netzwerk- und Überwachungsdienste in der Bildungsbranche sagte: „Wir haben zwei primäre Anwendungsfälle, die wir vorher mit VPN und jetzt mit Prisma Access unterstützen. Einer besteht darin, den Remote-Zugriff für Remote-Benutzer bereitzustellen, die auf sicherere Anwendungen im Campus-Netzwerk zugreifen müssen. Der andere Anwendungsfall besteht darin, unseren Benutzern eine sichere Internetverbindung bereitzustellen, während sie sich in einem unsicheren Netzwerk befinden. Benutzer melden sich häufig von öffentlichen Hotspots, Hotels, Cafés usw. aus an. Deshalb ermutigen wir alle Benutzer dazu, diese Dienste zu nutzen, um ihre eigenen Geräte zu sichern."

- **Verbesserung der Leistung während gleichzeitig Wartung und Support reduziert werden.** Die beiden Hauptprobleme, mit denen Unternehmen bei alten Lösungen konfrontiert waren, waren Zuverlässigkeit und Leistung. Benutzer beschwerten sich über häufige Trennungen der Verbindung und langsame Geschwindigkeiten, überlastete Helpdesk-Ressourcen und negative Auswirkungen auf Produktivität und Benutzererfahrung. Abgesehen von den benutzerbezogenen Problemen erforderten alte Lösungen häufige Updates, Patches und Überwachungsmechanismen, um sicherzustellen, dass das Netzwerk sicher und ordnungsgemäß funktioniert. Ein Leiter der Netzwerk- und Überwachungsdienste in

LESEN SIE DIE VOLLSTÄNDIGE STUDIE HIER

der Bildungsbranche sagte: „Wir hatten [mit einer alten VPN-Lösung] allein schon in Bezug darauf Probleme, dass wir den VPN-Server neu starten und überwachen mussten. Drei Jahre lang musste mein Team ständig auf den Server aufpassen. Das ist einer der Vorteile von Prisma Access: Wir müssen überhaupt nichts machen. Wir müssen uns nicht die ganze Zeit mit Patching und Überwachung befassen."

WARUM PALO ALTO NETWORKS PRISMA ACCESS?

Unternehmen gaben die folgenden Hauptgründe für eine Investition in Prisma Access an:

- **Cloud-basierte und skalierbare Lösung.** Ein Leiter der Netzwerk- und Überwachungsdienste in der Bildungsbranche sagte: „Früher erhielten wir bei unserer alten Lösung von unseren Benutzern viele Beschwerden über langsame Geschwindigkeiten, insbesondere von internationalen Benutzern, weil wir ein VPN mit Full-Tunneling bereitstellen. Bei Prisma Access finden wir es gut, dass die Lösung eine Full-Tunnel-Konfiguration unterstützt und die Gateways den Datenverkehr zum Internet ordnungsgemäß verarbeiten können. Das war einer der wichtigen Faktoren, und als wir unseren Proof-of-Concept machten, ließen wir Benutzer und Lehrkräfte die Lösung aus der ganzen Welt testen, um uns bei der Bewertung zu helfen, und wir erhielten großartiges Feedback."
- **Verbesserte Leistung, Zuverlässigkeit und Sicherheit.** Ein leitender VP in der Finanzdienstleistungsbranche sagte: „Sicherheitsinvestitionen werden oft auf Grund der Tatsache gerechtfertigt, um wie viel sie Risiken reduzieren können, und Prisma Access reduziert definitiv das Risiko für uns. Aber es ist auch eines der wenigen Sicherheitsprodukte, die es unserem Unternehmen ermöglichen, produktiver zu sein und die Effizienz unserer Benutzer zu verbessern."
- **Erhöhung der Unternehmenssicherheit durch Integration mit dem Rest des Ökosystems von Palo Alto Networks.** Ein Leiter der Netzwerk- und Überwachungsdienste im Bildungswesen sagte: „Uns gefällt es, dass Prisma Access in alle unsere internen Protokollierungsmechanismen wie unser SIEM und das Helpdesk-System integriert ist. Unsere alte Lösung war in Bezug auf Protokolle und Integrationen sehr begrenzt, aber mit Palo Alto Networks und Prisma Access haben wir eine bessere Transparenz und können sehen, woher der Datenverkehr in unseren Netzwerken kommt."

DIE WICHTIGSTEN ERGEBNISSE

Prisma Access spielte eine Rolle bei einigen der wichtigsten messbaren Vorteile der umfassenderen TEI-Studie über das Netzwerk-Sicherheitsportfolio von Palo Alto Networks. Zu den wichtigsten Vorteilen und Auswirkungen von Prisma Access auf die Gesamtlösung gehörten:

Die Einsparungen von 9,2 Millionen USD durch eine Reduzierung des Risikos von Sicherheitsverletzungen um 45 %. Obwohl Prisma Access nicht allein dafür verantwortlich ist, spielte es eine wichtige Rolle bei der Reduzierung der Wahrscheinlichkeit von und der Auswirkungen einer Sicherheitsverletzung für Unternehmen.

- **Geringere Wahrscheinlichkeit eines Datenlecks.** Anwendungen und schützen sowohl das Netzwerk als auch das Endbenutzergerät vor Malware und internetbasierten Angriffen, während sie verbunden sind." To „Anwendungen, wodurch sowohl das Netzwerk als auch das Endgerät bei einer aktiven Verbindung vor Malware und internetbasierten Angriffen geschützt werden.
- **Geringere Auswirkungen bei einem Sicherheitsvorfall.** Alle Sicherheitsprotokolle lassen sich problemlos in vorhandene SIEM-Sicherheitslösungen und andere Sicherheitslösungen von Palo Alto Networks integrieren. Dadurch werden Transparenz und Erkennungsfunktionen verbessert und Sicherheitsteams können Bedrohungen schneller erkennen und beheben.

Einsparungen von 9,9 Millionen USD in drei Jahren durch Straffung der Sicherheitsinfrastruktur. Prisma Access konnte Unternehmen dabei unterstützen, ihre alte Sicherheitsinfrastruktur zu rationalisieren und redundante Technologien wie VPN-Dienste und On Premise-Infrastrukturen zu entfernen.

- **Kosteneinsparungen, verminderte Komplexität und stärkere Sicherheit.** Mit Prisma Access konnten Unternehmen redundante Punktlösungen entfernen, die Komplexität ihrer Umgebung verringern, die Zahl der genutzten Anbieter reduzieren und Sicherheitslücken schließen.

Effizientere Verwaltung der Sicherheitsinfrastruktur reduziert die Arbeitsbelastung um knapp 50 % und führt zu Einsparungen von 1,9 Millionen USD. Durch die Einführung von Prisma Access sind Unternehmen nicht mehr für die Wartung alter Lösungen verantwortlich, wodurch die Arbeitskosten gesenkt werden und Unternehmen wertvolle Ressourcen höherwertigeren Aufgaben zuweisen können.

- **Reduzierter Wartungsaufwand und bessere Leistung erhöhen die Benutzerzufriedenheit.** Unternehmen berichteten, dass sie mit Prisma Access nicht mehr ständig Portale und Gateways patchen und überwachen mussten. Endbenutzer berichteten von einer verbesserten Leistung in Bezug auf Konnektivität und Geschwindigkeit und konnten Prisma Access in der Regel mühelos installieren und ausführen.

Reduzierung der Zeit bis zum Erreichen einer angemessenen Sicherheitslage um 30 %. Mit Prisma Access können Unternehmen konsistente Sicherheitsrichtlinien und -kontrollen auf den gesamten eingehenden Datenverkehr anwenden, wodurch der Aufwand für die Bereitstellung und Feinabstimmung im Vergleich zu Punktlösungen.

- **Zentralisierte Verwaltung über die zentrale Konsole Panorama.** Prisma Access lässt sich mit anderen Sicherheitsprodukten von Palo Alto Networks integrieren, einschließlich der Sicherheits-managementlösung Panorama. Panorama ermöglicht die Verwaltung der Sicherheitsrichtlinien und die Überwachung von Diensten von einem zentralen Ort aus, wobei jede Anwendung oder jeder Dienst ein ähnliches Erscheinungsbild hat. Dies verkürzt die Schulungszeiten und verbessert die Erfahrung für Sicherheits- und IT-Teams. Darüber hinaus bietet Prisma Access eine spezielle Cloud-basierte Management-Konsole für Kunden, die Panorama nicht nutzen.

ZUSÄTZLICHE RESSOURCEN

Forrester entwickelte zusätzliche Ressourcen, um die Auswirkungen und Vorteile der in dieser Studie genannten Lösungen genauer zu analysieren. Weitere Informationen und Zugang zu diesen zusätzlichen Ressourcen finden Sie hier:

- The Total Economic Impact™ von Palo Alto Networks für Netzwerksicherheit und SD-WAN
- Zusammenfassung:TEI™ von Palo Alto Networks für Netzwerksicherheit und SD-WAN
- TEI-Spotlight: CloudGenix SD-WAN
- TEI-Spotlight: Über die Cloud bereitgestellte Sicherheitsdienste

TOTAL ECONOMIC IMPACT-ANALYSE

Für weitere Informationen laden Sie den vollständigen Bericht „The Total Economic Impact™ von Palo Alto Networks für Netzwerksicherheit und SD-WAN“ herunter, der von Palo Alto Networks in Auftrag gegeben und von Forrester Consulting bereitgestellt wurde.

UNTERSUCHUNGSERGEBNISSE

Forrester hat Stakeholder in zehn Unternehmen sowie 133 Kunden befragt, die neben anderen Cloud-basierten Sicherheitsdiensten, SD-WAN und NGFWs von Palo Alto Networks bereits Prisma Access nutzen, und anhand dieser Daten eine auf drei Jahre ausgelegte Finanzanalyse erstellt. Auf der Basis des ermittelten Risikobarwerts wurden dabei folgende Vorteile identifiziert:

- Einsparungen von insgesamt 11,7 Millionen US-Dollar durch Kostenvermeidung und effizientere Verwaltung der Sicherheitsinfrastruktur.
- Einsparungen durch Effizienzsteigerungen für Sicherheit, IT-Betrieb und Endbenutzer in Höhe von insgesamt 6,0 Millionen USD.
- Geringeres Risiko eines Datenlecks, wodurch 9,2 Millionen USD gespart werden.
- Lesen Sie die Studie für weitere Vorteile und Informationen.

Return on investment (ROI)

247 %

Net Present Value (NPV, Nettobarwert)

28,5 Millionen USD

Anhang A: Fußnoten

[1] Total Economic Impact ist eine von Forrester Research, Inc. entwickelte Methodik, die die technologiebezogenen Entscheidungsprozesse von Unternehmen optimieren und Anbieter dabei unterstützen soll, Kunden das Nutzenversprechen ihrer Produkte und Dienstleistungen zu vermitteln. Die TEI-Methodik unterstützt Unternehmen darin, den materiellen Wert von IT-Initiativen gegenüber der Geschäftsführung und anderen wichtigen Entscheidungsträgern im Unternehmen aufzuzeigen, zu begründen und zu veranschaulichen.


FORRESTER®