FORRESTER®

Zusammenfassung:

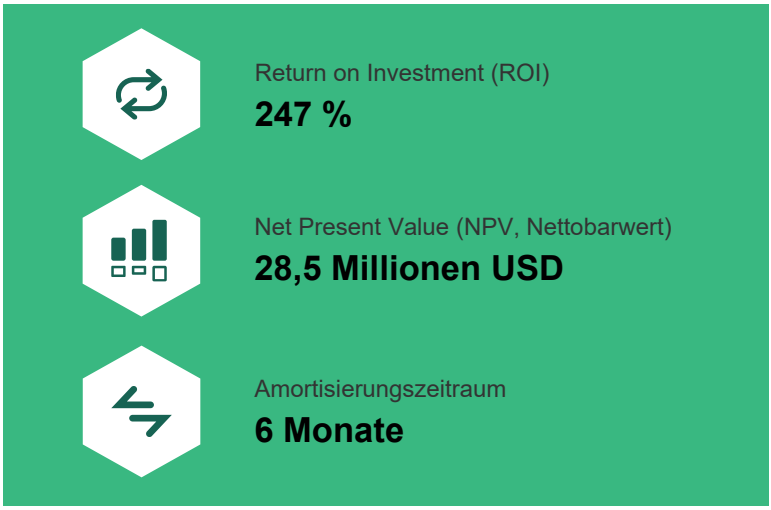
Der Total Economic Impact™ von Palo Alto Networks für Netzwerksicherheit und SD-WAN

Palo Alto Networks beauftragte Forrester Consulting mit der Durchführung einer objektiven Total Economic Impact™-Studie (TEI) und der Untersuchung des ROI, den Unternehmen bei der Bereitstellung von Palo Alto Networks-Lösungen für Netzwerksicherheit und SD-WAN erzielen.g von Palo Alto Networks für Netzwerksicherheit und SD-WANerzielen. Der Zweck dieser Studie ist es, Lesern einen Bezugsrahmen zur Evaluierung der potenziellen finanziellen Auswirkungen der Palo Alto Networks Produkte auf ihre Unternehmen zu liefern. Zu diesen Produkten gehören Next-Generation Firewalls (NGFWs), Palo Alto Networks Prisma SD-WAN und über die Cloud bereitgestellte Sicherheitsdienste wie IPS (Intrusion Prevention Systems), SWG (Secure Web Gateway),
URL-Filtering, Malwareanalyse, Sandboxing, DNS Security und Sicherheitsfeatures für IoT-Anwendungen.

Die Netzwerksicherheits- und SD-WAN-Lösungen von Palo Alto Networks umfassen wichtige Sicherheitskontrollen und unterstützen Unternehmen bei der Zentralisierung der Verwaltung, der Aufrechterhaltung optimaler Konnektivität und der Ausweitung von Sicherheitsrichtlinien und -kontrollen auf alle Benutzer, Anwendungen und Geräte.

Um die mit dieser Investition verbundenen Vorteile, Kosten und Risiken besser zu verstehen, hat Forrester Stakeholder in neun Unternehmen befragt und 133 Kunden mit Erfahrung in der Nutzung der Palo Alto Networks Lösung an einer Umfrage teilnehmen lassen. Für die Zwecke dieser Studie fasste Forrester die Erfahrungen der befragten Kunden zusammen und kombinierte die Ergebnisse zu einem Modellunternehmen.

Vor der Bereitstellung der Netzwerksicherheitslösung von Palo Alto Networks nutzten die Kunden herkömmliche Firewalls mit mehreren Punktlösungen, um ihre Umgebungen zu sichern. Dies war ein Nebeneffekt der Bemühungen zur digitalen Transformation. Sicherheits- und IT-Teams versuchten, mit den wandelnden Geschäftsanforderungen Schritt zu halten, doch den Unternehmen fehlte es an moderner Sicherheits-



technologie und effizienten Prozessen. Durch Initiativen zur digitalen Transformation wurde ein Teil der Daten, Anwendungen und Prozesse in die Cloud verlagert, während andere Kerngeschäftsfunktionen weiterhin in On-Premises-Umgebungen ausgeführt wurden.

Die Netzwerksicherheitslösung von Palo Alto Networks bot den Kunden eine gemeinsame Plattform mit zentralisierter Datenverwaltung: Panorama – die Sicherheits-management-Lösung von Palo Alto Networks. Dadurch wurde der Untersuchungsaufwand erheblich reduziert und es wurden wertvolle Ressourcen freigesetzt, sodass sich die verantwortlichen Teams mehr auf die Optimierung und die flächendeckendere Absicherung des Netzwerks konzentrieren konnten. Die Unternehmen der Befragten haben einige oder alle diese Netzwerksicherheits- und SD-WAN-Lösungen von Palo Alto Networks bereitgestellt.

Die getätigten Investitionen haben unter anderem zu den folgenden Vorteilen geführt: Effizienzsteigerungen für IT-, Sicherheits- und Netzwerkbetriebsteams, geschäftliche Endbenutzer und Mitarbeiter in Ladengeschäften; eine deutlich geringere Wahrscheinlichkeit einer Sicherheits-verletzung; geringere Kosten im Zusammenhang mit der Lizenzierung und dem Management der vorhandenen Punktlösungen; umfassendere Schutzfunktionen und

Verbesserungen bei IoT-Sicherheit, Zero Trust und SD-WAN-Funktionen.

DIE WICHTIGSTEN ERGEBNISSE

Auf der Basis des ermittelten Risikobarwerts wurden folgende Vorteile identifiziert:

Gemindertes Risiko von Datenlecks

- **Die Wahrscheinlichkeit eines Datenlecks verringerte sich nach drei Jahren um 45 %.** Mit den Lösungen von Palo Alto Network konnten die Unternehmen Sicherheitslücken schließen, die Transparenz erhöhen, ein Zero-Trust-Sicherheitsmodell umsetzen und konsistente Sicherheitsrichtlinien im gesamten Unternehmen anwenden. Über die Cloud bereitgestellte Sicherheitsservices unterstützten das SecOps-Team mit Rund-um-die-Uhr-Support sowie dem Schutz vor Schwachstellen und allen bekannten und unbekannten Bedrohungen.

Effiziente Sicherheits- und IT-Prozesse

- **SOC-Teams konnten die Anzahl der erweiterten Untersuchungen um 35 % reduzieren, die durchschnittliche Zeit bis zur Abwehr einer Bedrohung um 20 % verkürzen und die Anzahl der Geräte, auf die saubere Images aufgespielt werden müssen, um die Hälfte reduzieren, was in drei Jahren zu Einsparungen von 5,1 Millionen USD führte.** Durch die Bereitstellung von Sicherheitslösungen von Palo Alto Networks wurde die Transparenz in den Netzwerken der Unternehmen deutlich verbessert und es wurden Automatisierungsfunktionen eingeführt, durch welche die Anzahl der kritischen Warnungen, einschließlich Fehlalarme, im Laufe der Zeit gesenkt wurde. Außerdem konnten die Unternehmen die durchschnittliche Zeit bis zur Abwehr einer Bedrohung reduzieren, da den Analysten die benötigten Daten nun jederzeit zur Verfügung standen. Infolgedessen gab es weniger Malware-Infektionen und andere Probleme mit Endgeräten, was den Arbeitsaufwand für das IT-Betriebsteam reduzierte.

Geringerer Aufwand für die Verwaltung der Sicherheitsinfrastruktur

50 %

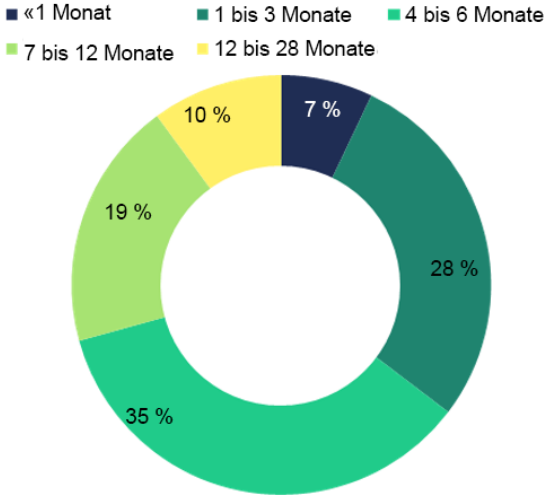
Verbesserung der Endbenutzerproduktivität

- **Verbesserte Endbenutzerproduktivität sowie weniger Sicherheitsvorfälle und Untersuchungen führten in drei Jahren zu Einsparungen in einer Höhe von insgesamt 865.226 USD.** Dank der Sicherheitslösungen von Palo Alto Networks verbringen Endbenutzer weniger Zeit mit der Interaktion mit den Sicherheits- und IT-Betriebsteams und können sich stattdessen auf ihre eigentlichen Aufgaben und den Wertzuwachs für ihr Unternehmen konzentrieren.

Senkung und Vermeidung der Kosten für

„Wie lange hat Ihr Unternehmen mit NGFW im Vergleich zu Punktlösungen ungefähr gebraucht, um eine stabile Sicherheitslage zu erreichen?“

(Es werden nur die fünf meistgenannten Ergebnisse angezeigt.)



Grundlage: 83 Benutzer von Palo Alto Networks-Lösungen, die ein „geringeres Cybersicherheitsrisiko im Unternehmen“ als Vorteil angaben
Quelle: Eine von Palo Alto Networks in Auftrag gegebene und von Forrester Consulting durchgeführte Studie, Oktober 2020

Erreichen einer stabilen Sicherheitslage innerhalb von 6 Monaten nach dem Wechsel zu Palo Alto Networks

70 % der Kunden

Sicherheitsinfrastruktur

- **Das Straffen der Sicherheitsinfrastruktur führte zu Einsparungen von 9,9 Millionen USD in drei Jahren.** Nach der Implementierung von Palo Alto Networks-Lösungen entfernten die Unternehmen ältere Sicherheitssysteme und -produkte. Angesichts der Tatsache, dass die Unternehmen Sicherheitslösungen von bis zu 17 Anbietern nutzten, hatten die Vereinfachung der Umgebung und die Reduzierung der Anzahl der Anbieter Priorität, und die Lösung von Palo Alto Networks bot überlegenen Schutz bei geringeren Kosten. Zu den Technologien, die von den Cloud-basierten Sicherheitsservices von Palo Alto Networks abgelöst wurden, gehören Intrusion Prevention (IPS/IDS), Secure Web Gateway (SWG), Web Proxy, VPN-Malware-Analyse (z. B. Sandboxing), DNS und Software-as-a-Service (SaaS)-Anwendungssicherheit.

Effiziente Verwaltung der Sicherheitsinfrastruktur über eine gemeinsame Plattform

- **Aufgrund effizienterer Verwaltungsabläufe konnten rund 50 % der Vollzeit-Sicherheitsexperten für die Arbeit an höherwertigen Initiativen eingesetzt werden, was innerhalb von drei Jahren zu Einsparungen von 1,9 Millionen USD führte.** Durch das Wegfallen alter Anbieter und die Konsolidierung auf eine gemeinsame Plattform waren weniger Mitarbeiter erforderlich, um die gleichen Aufgaben auszuführen, sodass die Unternehmen die Anzahl der mit der Verwaltung beauftragten Teams um etwa die Hälfte reduzieren konnten. Darüber hinaus ermöglichte die gemeinsame Plattform den Unternehmen die schnelle Implementierung von Updates, Patches und Sicherheitsrichtlinien auf der gesamten Plattform von einem zentralen Ort aus, anstatt jedes Sicherheitsgerät manuell und über mehrere Anbieter hinweg zu aktualisieren.

Zeit zum Erreichen der angemessenen Sicherheitslage

30 % schneller

Reduzierung von Kosten und Risiken in Bezug auf IoT-Sicherheit

- **Einsparung von 1,4 Millionen USD beim IoT durch geringeren Managementaufwand und eine Reduzierung der Anzahl der neu erworbenen IoT-Geräte.** Mit IoT Security konnten die Unternehmen alle ihre IoT-Geräte von einer zentralen Plattform aus identifizieren und sichern, den Zustand und Standort jedes einzelnen Geräts schnell verstehen und den Wert und die Auslastung jedes Geräts mit den erweiterten Berichtsfunktionen maximieren. Dadurch konnten Neukäufe um 10 % reduziert werden.

Verringerte Wahrscheinlichkeit einer Sicherheitsverletzung nach 3 Jahren

45 %

Dauer bis zum Erreichen der Sicherheitslage

- **Reduzierung der Zeit um 30 %, um eine angemessene Sicherheitslage zu erreichen, und Einsparungen von 812.860 USD über drei Jahre hinweg.** Durch die Nutzung der NGFWs und Cloud-basierten Sicherheitsservices von Palo Alto Networks konnten die Unternehmen ihre Sicherheitslösungen schneller einrichten und schneller einen stabilen Zustand erreichen. Dies gab den Sicherheitsteams einen Vorsprung bei der Optimierung der Lösung und dem Erreichen von Zero Trust Standards im Vergleich zur Verwendung von Punktlösungen.

Reduzierung der WAN-Hardware- und Konnektivitätskosten

- **Senkung der Kosten für WAN-Hardware und Konnektivität an Remote-Standorten um über 90 %, was 6,04 Millionen USD über drei Jahre entspricht.** Durch den Wechsel von Multiprotocol Label Switching (MPLS) zu Prisma SD-WAN konnten die Unternehmen die monatlichen Betriebs-kosten an ihren Standorten deutlich senken und gleichzeitig die Transparenz und Kontrolle des Netzwerkverkehrs verbessern.

LESEN SIE DIE VOLLSTÄNDIGE STUDIE HIER

Effizientes SD-WAN-Management

- **Reduzierung des Managementaufwands für IT-Teams um die Hälfte und Verbesserung der Effizienz von Zweigstellen und Einzelhandelsunternehmen um 12 % mit Prisma SD-WAN, wodurch über drei Jahre 4,9 Millionen USD eingespart werden konnten.** Durch eine intuitive Benutzeroberfläche und speziell entwickelte Hardware ermöglichte Prisma SD-WAN die zentrale Verwaltung des SD-WAN für IT-Teams. Darüber hinaus konnten Unternehmen dank der verbesserten Bandbreite, Netzwerkleistung und Sicherheitskontrollen Telearbeitern bessere Technologien bereitstellen und so die Produktivität und das Kundenerlebnis verbessern.

MODELLUNTERNEHMEN

Anhand der Befragungen und Umfragen hat Forrester einen TEI-Bezugsrahmen erstellt, ein Modellunternehmen entworfen und eine ROI-Analyse durchgeführt, mit der die finanziell betroffenen Bereiche aufgezeigt werden können. Das Modellunternehmen ist repräsentativ für die neun Unternehmen, die an Forrester-Umfragen teilgenommen haben und die 133 Unternehmen, die von Forrester befragt wurden, und dient als Basis für die Finanzanalyse im nächsten Abschnitt. Das Modellunternehmen hat folgende Merkmale:

- **Beschreibung des Modellunternehmens.** Das Modellunternehmen ist ein dezentrales Unternehmen mit 50.000 Mitarbeitern und einem Jahresumsatz von 7 Milliarden USD. Das Unternehmen verfügt über 400 Standorte, darunter Hauptsitz, Rechenzentrum, Cloud, Zweigstelle sowie Einzelhandels- und Produktionsstandorte. Das Sicherheitsteam des Modellunternehmens reagiert auf 1.200 Vorfälle pro Woche, oder 62.400 im ersten Jahr, wobei es durchschnittlich 2 Stunden dauerte, um jeden Vorfall zu lösen.

INVESTITIONSFAKTOREN

Die befragten und interviewten Unternehmen taten sich mit häufig auftretenden Herausforderungen wie den folgenden schwer:

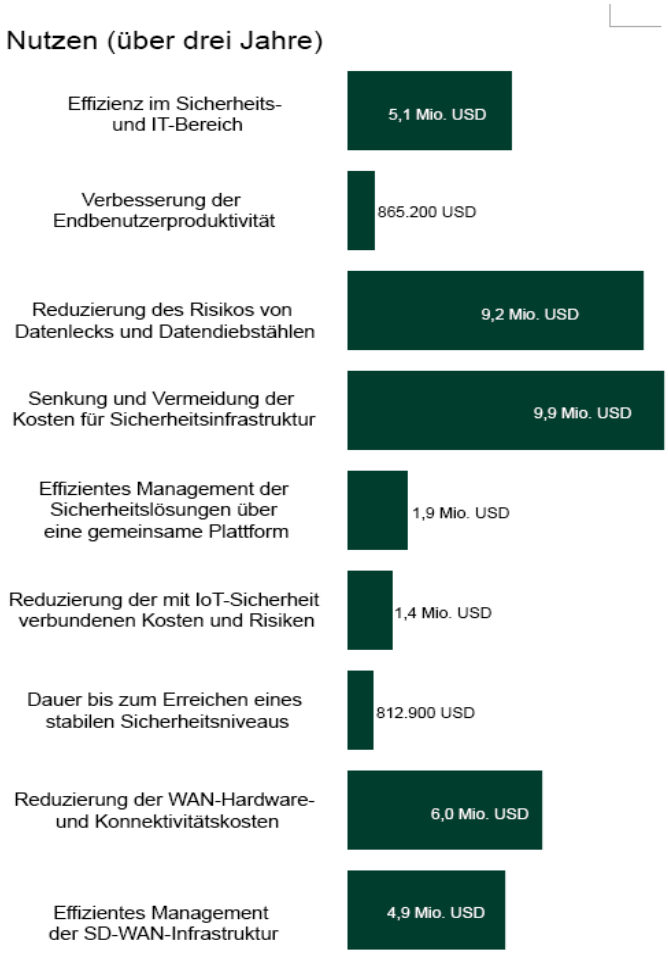
- **Leistungsschwächere, alte Cybersicherheits-Punktlösungen.** Die Befragten gaben an, dass ihre Unternehmen alte Punktlösungen einsetzen, die die Erwartungen in Bezug auf Geschwindigkeit, Leistung, Kundensupport des Anbieters nicht erfüllen konnten und eine mangelnde Ausrichtung an Zero-Trust-Strategien vorwiesen. Früher bereitgestellte Produkte ließen sich nur langsam aktualisieren, erforderten erhebliche Kapitalinvestitionen bei der Wartung der erforderlichen Hardware und verursachten erhebliche Betriebsinvestitionen, um die Lösungen am Laufen zu halten.
- **Segmentierte, dezentrale Sicherheitsfunktionen und -plattformen.** Mehrere Befragte gaben an, dass ihre Unternehmen vor der Bereitstellung verschiedener NGFW-Varianten von Palo Alto Networks und Cloud-basierten Sicherheitsdiensten für On-Premise- und Cloud-Infrastrukturen unterschiedliche Sicherheitslösungen verwendeten, die für die Durchführung einfacher Aufgaben mehrere Fähigkeiten erforderten. Sicherheitsteams hatten Probleme mit der Transparenz über mehrere Technologien hinweg, konnten Erkenntnisse und Einblicke nicht schnell genug übertragen, verfügten über keine zusammenhängende Suite zur Überwachung ihrer Netzwerke und konnten Risiken aufgrund von Lücken in den Infrastrukturen nicht quantifizieren.
- **Schutz vor immer ausgefeilteren Angriffen und der Wunsch nach Transparenz und Kontrolle auf Layer 7.** Da Cybersicherheitsbedrohungen immer ausgefeilter werden, gaben die Befragten an, dass ihre Unternehmen versuchen, ihre alternden Sicherheitsinfrastrukturen zu aktualisieren und von On-Premise Punktlösungen wegzukommen. Sie suchten nach umfassenderer Layer-7-Transparenz für die Netzwerkumgebung und benötigten Einblicke auf Anwendungsebene. Ihre alten Lösungen konnten nicht die erforderliche Transparenz, Entschlüsselung oder Leistung bieten.

WARUM PALO ALTO NETWORKS?

Die Unternehmen suchten nach einer Lösung, die Folgendes ermöglicht:

- **Vereinheitlichung von Sicherheit, Richtlinien und Management für alle Netzwerk- und Cloud-Umgebungen über eine einzige zentrale Plattform.** Ein Leiter der IT-Architektur in der Technologiebranche sagte: „Ich habe jetzt eine einheitlichere Sicherheitspolitik in meiner gesamten Infrastruktur weltweit. Anstelle von verschiedenen Anbietern mit unterschiedlichen Richtlinien und separaten Updates habe ich nun einen konsistenten Sicherheitsansatz für alle Umgebungen Das lässt sich auf eine zentrale Ansicht zurückführen, aber auch ohne diese habe ich eine Sicherheitsrichtlinie, die ich nur einmal definieren muss und dann überall verwenden kann."

- **Bereitstellung einer zentralen Ansicht und verbesserter Transparenz während der Cloud-Transformation.** Ein CISO in einem Einzelhandelsunternehmen sieht die konkreten Vorteile einer integrierten und vernetzten Lösung: „Das schöne an dieser Technologie ist, dass sich alles in Panorama integrieren lässt.“ In Panorama können wir alles von einer Konsole aus steuern. Statt dass 600 Firewalls einzeln verwaltet werden, kann ich meinen Bedrohungsverkehr über eine Konsole ansehen. Das spricht für sich.“
- **Gute Integration mit vorhandenen Plattformen zur Automatisierung.** Über die Cloud bereitgestellte Sicherheitsservices nutzen Netzwerkeffekte, um die Analyse einer Bedrohung für einen Kunden zu automatisieren und ähnliche Bedrohungen für alle Kunden in Sekunden oder weniger zu vermeiden. Ein Leiter der IT-Architektur in der Computerindustrie sagte: „Wir wollten sofort einsetzbare Automatisier-ungsfunktionen.“ Wir wollten nicht alle Produkte kaufen müssen und dann eine weitere Million Dollar ausgeben, um zusätzlich die Automatisierung zu entwickeln. Wir wollten eine gute Integration mit den bereits vorhandenen Plattformen, und wir mussten in andere Bereiche expandieren können, in die wir noch nicht unbedingt investiert haben.“



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
- TEI-Spotlight: Prisma SD-WAN
- TEI-Spotlight: Über die Cloud bereitgestellte Sicherheitsdienste
- TEI-Spotlight: Prisma-Zugriff


FORRESTER®