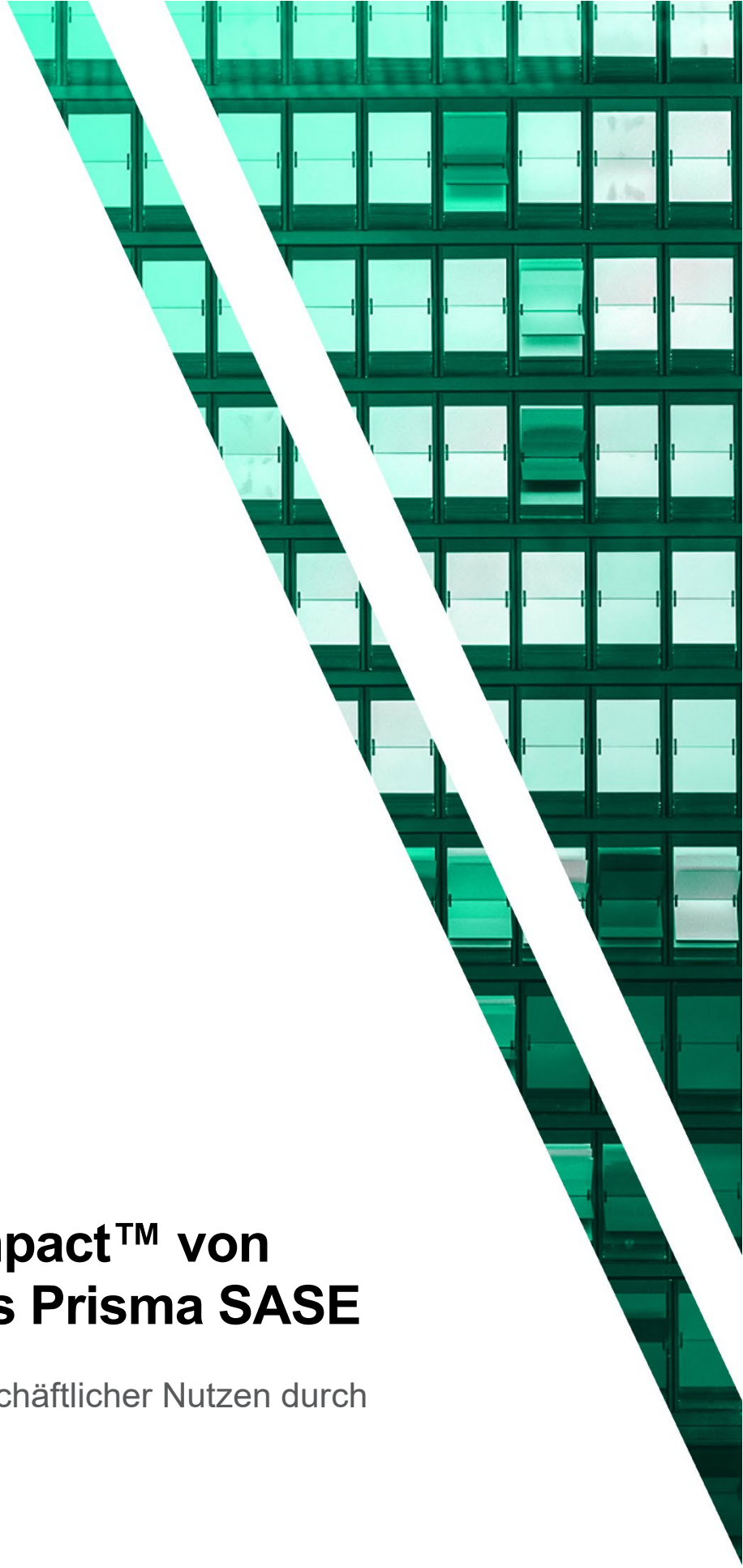
FORRESTER®



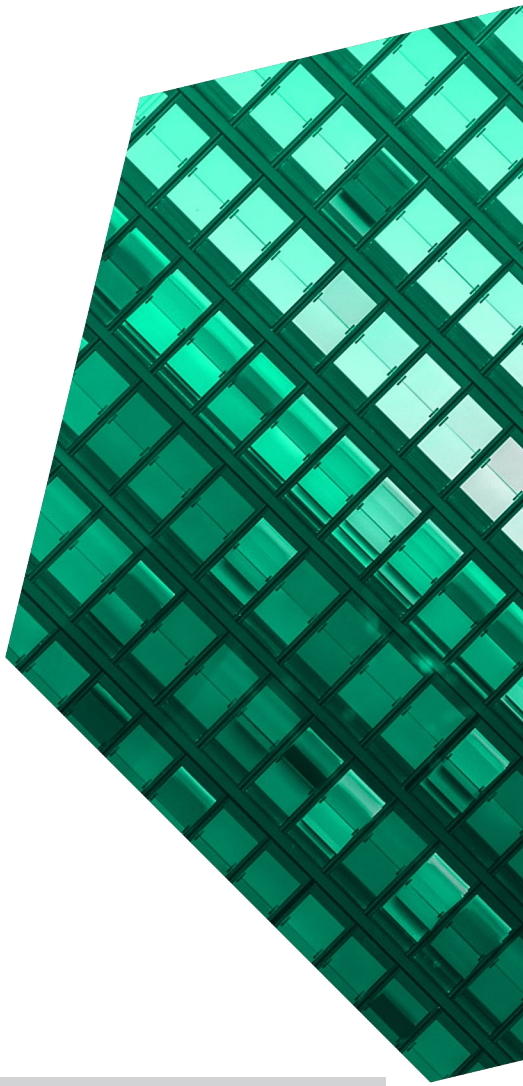
Total Economic Impact™ von Palo Alto Networks Prisma SASE

Kosteneinsparungen und geschäftlicher Nutzen durch Palo Alto Networks

DEZEMBER 2023

Inhaltsverzeichnis

Beraterteam: *Adi Sarosa*
Isabel Carey



ÜBER FORRESTER CONSULTING

Forrester bietet unabhängige, objektive und auf Forschungsergebnisse gestützte Beratungsdienstleistungen und unterstützt Führungskräfte so bei ihrer erfolgreichen Arbeit. Auf der Grundlage unserer kundenorientierten Studien arbeiten die erfahrenen Berater von Forrester gemeinsam mit Führungskräften daran, deren spezifische Prioritäten umzusetzen. Dabei kommt ein spezielles Kooperationsmodell zum Einsatz, das eine nachhaltige Wirkung sicherstellt. Weitere Informationen finden Sie auf unserer Website unter forrester.com/consulting.

Zusammenfassung

Unternehmen mit einer hochgradig verteilten Organisation – also solche mit vielen Standorten und/oder einem hohen Anteil an Mitarbeitern im Homeoffice – entscheiden sich häufig für eine SASE-Architektur (Secure Access Service Edge). Eine solche Architektur eignet sich vor allem für die Authentifizierung und Autorisierung von Anwendern, die sich mit der und über die Plattform verbinden. Allerdings handelt es sich bei SASE um eine transformative Technologie, die mehrere Netzwerk- und Sicherheitsfunktionen zu einer einheitlichen Lösung mit einer zentralen Oberfläche und einem Data Lake zusammenführt. Die Auswahl des richtigen Lösungsanbieters kann sich mitunter als risikoreich, aber auch als gewinnbringend erweisen.

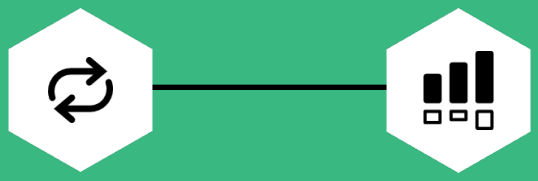
Prisma SASE vereint Netzwerksicherheit, SD-WAN und Autonomous Digital Experience Management (ADEM) in der Cloud. Dadurch wird unabhängig vom Standort des Anwenders die Sicherheit aller im Unternehmen genutzten Anwendungen gewährleistet.

Palo Alto Networks hat Forrester Consulting mit der Durchführung einer Studie zum Total Economic Impact™ (TEI) sowie mit der Untersuchung des potenziellen Return on Investment (ROI) beauftragt, den Unternehmen durch den Einsatz von Prisma SASE erzielen können.[1] Ziel dieser Studie ist es, den Lesern einen Bezugsrahmen zur Analyse der potenziellen finanziellen Effekte von Prisma SASE auf ihr Unternehmen an die Hand zu geben.

Zum besseren Verständnis der mit dieser Investition verbundenen Vorteile, Kosten und Risiken hat Forrester vier Unternehmensvertreter zu ihren Erfahrungen mit Prisma SASE befragt. Die Erfahrungen der Befragungsteilnehmer wurden daraufhin von Forrester für diese Studie zusammengefasst und als Grundlage zur Entwicklung eines entsprechenden Modellunternehmens genutzt. Es handelt sich hierbei um ein Unternehmen mit 50.000 Mitarbeitern, von denen 33 % im Homeoffice oder hybrid arbeiten, und einem jährlichen Umsatz von $7 Mrd.

Vor dem Einsatz von Prisma SASE kämpften die befragten Unternehmen gewöhnlich mit einer inkonsistenten und unvollständigen Sicherheit, einer unzureichenden Anwendererfahrung aufgrund der Art und Weise, wie der Datenverkehr an die Rechenzentren weitergeleitet wurde, und einer ungenügenden Skalierbarkeit, welche durch die Zunahme hybrider Arbeitsformen und den verstärkten Einsatz der Cloud bedingt war. Darüber hinaus erforderte die Verwaltung des Zugangsservices, dass sie verschiedene Punktlösungen zur Sicherung ihrer Umgebungen installieren mussten. Es fehlte ihnen an moderner Sicherheitstechnologie, während Sicherheits- und IT-Teams versuchten, mit den sich entwickelnden Geschäftsanforderungen Schritt zu halten. Im Zuge der digitalen Transformation wurden immer mehr Daten, Anwendungen und Prozesse in die Cloud verlagert, andere geschäftliche Kernfunktionen wurden jedoch weiterhin lokal betrieben. Dieser kleinteilige Ansatz führte jedoch dazu, dass die befragten Unternehmen Lösungen vieler verschiedener Anbieter in ihren Sicherheitssystemen einsetzten. Das erschwerte den Security Operations Teams (SecOps-Teams) die Integration von Technologien, die gewinnbringende Nutzung von Analysen, die Umsetzung konsistenter

WICHTIGE KENNZAHLEN



Return on Investment (ROI)
107 %

Kapitalwert
$9,49 Mio.

Richtlinien und die Bereitstellung einer konsistenten Erfahrung für die Endanwender.

Nach der Investition in Prisma SASE waren die betreffenden Unternehmen dagegen in der Lage, einen Großteil ihrer Zeit für bestimmte Verwaltungstätigkeiten und Ausgaben für Anbieter zu konsolidieren und so die betriebliche Effizienz zu steigern. Dabei stieg die Endanwenderproduktivität, insbesondere bei den Mitarbeitern, die nicht in den Büros vor Ort tätig sind. Sie stellten außerdem fest, dass die Kombination aus Prisma SASE und anderen in ihrer Umgebung installierten Lösungen von Palo Alto Networks die Wahrscheinlichkeit einer Datenpanne deutlich senkt.

Effizienzsteigerungen bei der Verwaltung von SASE und der Umsetzung von Richtlinienänderungen

75 %

WESENTLICHE ERKENNTNISSE

Quantifizierbarer Nutzen. Für das Modellunternehmen setzt sich der risikobereinigte barwertige Nutzen über den dreijährigen Analysezeitraum folgendermaßen zusammen:

- **75 % Mehreffizienz bei der SASE-Verwaltung und der Umsetzung von Richtlinienänderungen sowie bei der Reaktion auf Sicherheitsvorfälle sowie 80 % Zeitersparnis beim Skalieren und Einrichten neuer Standorte.** Während das Modellunternehmen früher mehrere Teams mit der Verwaltung seiner SASE-Lösung einsetzen musste, erzielt es durch den Einsatz von Prisma SASE Zeiteinsparungen und Effizienzsteigerungen bei zahlreichen Tätigkeiten sowohl seiner Security Operations Teams (SecOps-Teams) und NetOps-Teams (Netzwerkbetriebsteams). Über einen Zeitraum von drei Jahren summiert sich der Effizienzgewinn für das Modellunternehmen auf einen Wert von $2,2 Mio.
- **Produktivitätssteigerung bei den Endanwendern durch bessere Systemverfügbarkeit und weniger Eingriffe in ihr Netzwerk im Gesamtwert von $12,2 Mio. über drei Jahre.** Das Modellunternehmen profitiert ferner von einer höheren Produktivität der Endanwender und insbesondere derjenigen, die im Homeoffice bzw. nicht in ihrem Firmenbüro arbeiten, da die laufenden Sicherheitsaktivitäten weniger Störungen verursachen und sich die Systemverfügbarkeit ihrer Arbeitsumgebung insgesamt verbessert. Dies ist das Ergebnis einer besseren Integration und Kompatibilität der verschiedenen Lösungen von Palo Alto Networks untereinander sowie einer höheren Gesamtleistung. Über einen Zeitraum von drei Jahren hinweg entspricht diese Steigerung der Endanwenderproduktivität einem Wert von knapp $12,2 Mio. für das Modellunternehmen.
- **Verringerung der Wahrscheinlichkeit einer Datenpanne um 50 % nach drei Jahren.** Prisma SASE ersetzt mehrere unzusammenhängende Sicherheitslösungen durch eine einzige, integrierte Lösung und schließt so beim Modellunternehmen bestehende Sicherheitslücken. Dadurch sinkt die Wahrscheinlichkeit einer schwerwiegenden Datenpanne. Über einen Zeitraum von drei Jahren hinweg spart das Modellunternehmen durch das geringere Risiko einer Datenpanne knapp $3 Mio. ein.
- **Einsparung in einer Größenordnung von $846.000 über drei Jahre durch vermiedene Anschaffung und Rationalisierung der Sicherheits- und Netzwerkinfrastruktur.** Durch den Einsatz von Prisma SASE kann das

Modellunternehmen ebenfalls seine Ausgaben für Sicherheitstechnologien konsolidieren. Über einen Zeitraum von drei Jahren belaufen sich die durch die Anbieterkonsolidierung ergebenden Kosteneinsparungen für das Modellunternehmen auf insgesamt $846.000.

Nicht quantifizierbarer Nutzen. Die folgenden Vorteile generieren zwar einen Mehrwert für das Modellunternehmen, wurden aber in der vorliegenden Studie nicht quantifiziert:

- **Mehr Transparenz in der Sicherheitsumgebung.** Mit Prisma SASE kann das Modellunternehmen den Datenverkehr besser überwachen und weiß so jederzeit, was in seinem Netzwerk vor sich geht.
- **Bessere Mitarbeitererfahrung.** Mitarbeiter des Modellunternehmens – und zwar sowohl Angehörige der Sicherheitsorganisation als auch allgemeine Endanwender – schätzen außerdem die einfache und bequeme Nutzung von Prisma SASE sowie die Gewissheit, vor potenziellen Angriffen und Bedrohungen gut geschützt zu sein. Dies bewirkt nicht nur die bereits erwähnte Produktivitätssteigerung, sondern hat potenziell auch Einfluss auf die Bindung an das Unternehmen und dessen Marke, sowohl aus Sicht der internen als auch der externen Stakeholder.

Kosten: Für das Modellunternehmen setzen sich die risikobereinigten barwertigen Kosten über drei Jahre wie folgt zusammen:

- **Installations- und Bereitstellungskosten in Höhe von insgesamt $436.000 über drei Jahre.** Für die Bereitstellung und Installation der Lösung von Palo Alto Networks im gesamten Modellunternehmen ist ein gewisser Zeit- und Arbeitsaufwand erforderlich. Für die Implementierung von Prisma SASE im Vergleich zu anderen Lösungen von Palo Alto Networks (d. h. NGFW und CDSS) wird ein Zeitaufwand von 20 % der Arbeitszeit der mit der Implementierung beauftragten Mitarbeiter angenommen.
- **Schulungskosten und Zeitaufwand für die laufende Verwaltung in Höhe von insgesamt $63.000 über drei Jahre.** Die Lösung von Palo Alto Networks erfordert weniger Schulungsaufwand als herkömmliche Lösungen. Zudem berichteten die Befragungsteilnehmer, dass die angebotenen Schulungen effektiver und effizienter seien, sodass sich die Mitarbeiter schneller einarbeiten und ihre Kompetenzen erweitern konnten. Nach Abschluss der Schulung wendet das Team eine gewisse Zeit für die laufende Wartung und Verwaltung des Systems auf.

[1] Der Total Economic Impact™ (TEI) ist eine von Forrester Research entwickelte Methode, die die

Die Forrester-Perspektive: Zusammenführung von Sicherheits- und Netzwerkteams

Obwohl die Bereiche Netzwerk und Sicherheit eine lange und komplizierte Geschichte aufweisen, ist ein getrennter Ansatz nicht vertretbar,
da er die Vorteile digitaler Initiativen oft zunichtemacht.

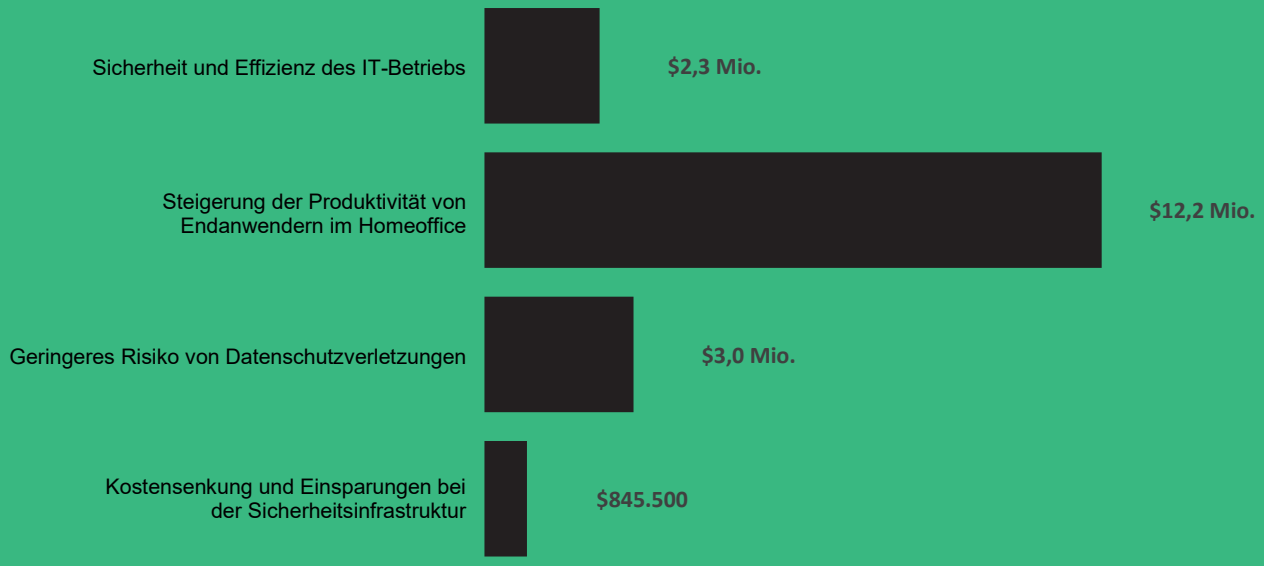
Heutzutage verwebt eine unternehmensweite Netzwerkstruktur Unternehmensressourcen, Kunden, Partner und digitale Assets, die alle Teile des Unternehmensumfelds zusammenzuführen. Dies ist jedoch nur möglich, wenn die Sicherheit in die Netzwerk-DNA eingebettet ist.

Quelle: „Introducing The Zero Trust Edge Architecture for Security and Network Services“, Forrester Research, Inc., 2. August 2021.

Kommunikation des Leistungsversprechens ihrer Produkte und Dienstleistungen gegenüber Kunden unterstützt. Die TEI-Methode hilft Unternehmen, den konkreten Mehrwert von IT-Initiativen gegenüber der Geschäftsleitung und anderen wichtigen Stakeholdern zu belegen, zu rechtfertigen und zu veranschaulichen.

ROI	NUTZEN	KW	AMORTISATION
107 %	**$18,34 Mio.**	**$9,49 Mio.**	**< 6 Monate**

Nutzen (über drei Jahre)



„Die von den Anwendern erreichbare Produktivität – auch und gerade von denen, die im Homeoffice arbeiten – ohne sich um die Integration mit anderen Systemen kümmern zu müssen, und das Maß an Sicherheit, das wir erreichen – all das wäre ohne Prisma SASE nicht möglich.“

– Chefarchitekt, Gesundheitswesen

TEI-BEZUGSRAHMEN UND -METHODIK

Aus den in den Befragungen erfassten Daten hat Forrester einen Bezugsrahmen zum Total Economic Impact™ für Unternehmen erstellt, die eine Investition in Prisma SASE erwägen.

Dieser Bezugsrahmen dient dazu, Kosten, Nutzen, Flexibilität und Risikofaktoren zu ermitteln, die für eine solche Investitionsentscheidung von Bedeutung sind. Zur Analyse der möglichen Effekte von Prisma SASE auf ein Unternehmen folgte Forrester einem mehrstufigen Ansatz.

Hierzu führte Forrester Consulting eine Online-Umfrage unter 351 Führungskräften im Bereich Cybersicherheit in internationalen Firmen in den USA, Großbritannien, Kanada, Deutschland und Australien durch. Zu den Umfrageteilnehmern gehörten Manager, Direktoren, Vizepräsidenten und leitende Angestellte, die für die Entscheidungsfindung, den Betrieb und die Berichterstattung im Bereich Cybersicherheit verantwortlich sind. Die Fragen an die Teilnehmer zielten darauf ab, die Cybersicherheitsstrategien der Führungskräfte und etwaige Datenpannen in ihrem Unternehmen auszuwerten. Die Probanden nahmen an der Umfrage über ein externes Forschungspanel teil, das die Umfrage im November 2020 im Auftrag von Forrester durchführte.

HINWEISE

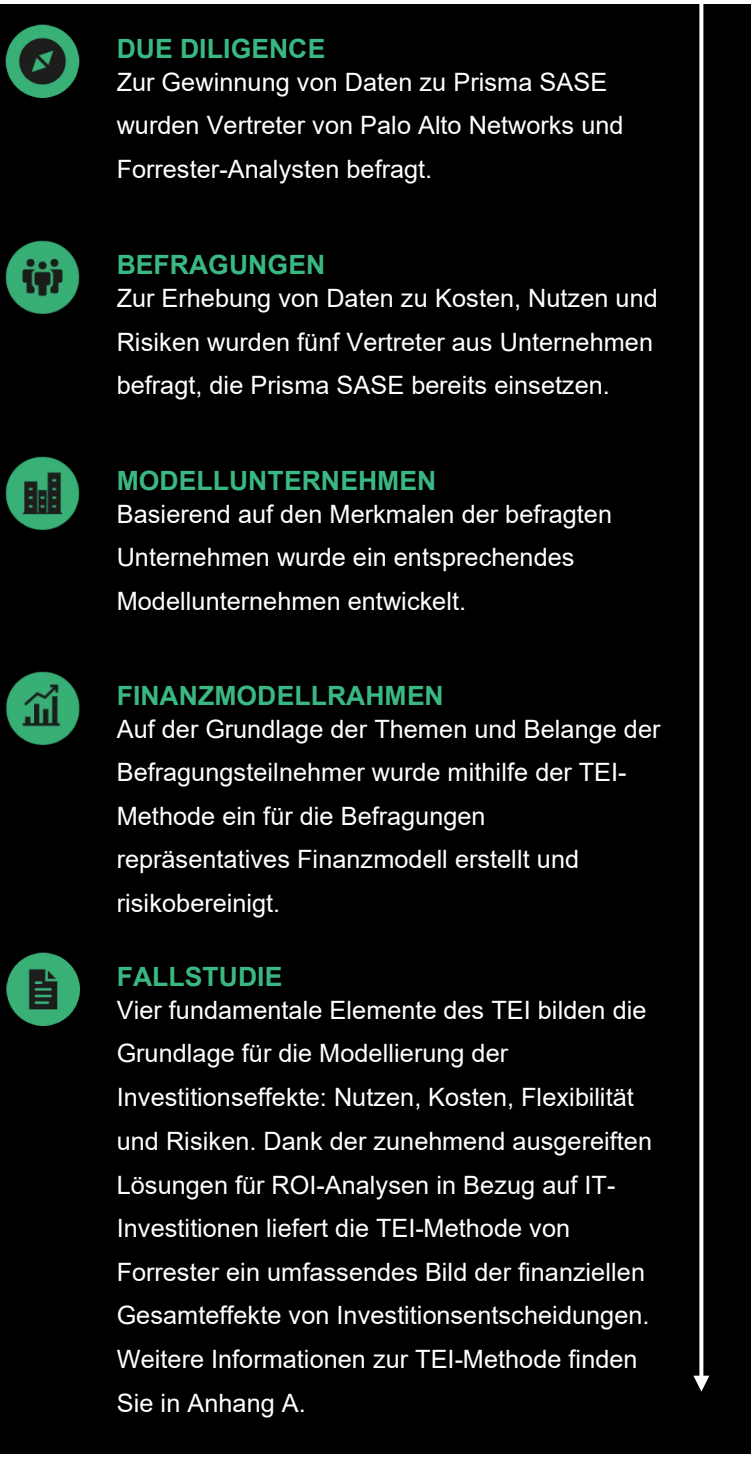
Unsere Leser werden auf Folgendes hingewiesen:

Diese Studie wurde von Palo Alto Networks in Auftrag gegeben und von Forrester Consulting durchgeführt. Sie ist nicht als Wettbewerbsanalyse aufzufassen.

Forrester trifft hierin keinerlei Annahmen über den potenziellen ROI, den andere Unternehmen und Organisationen erzielen werden oder können. Forrester empfiehlt seinen Lesern deshalb ausdrücklich, mithilfe des in der Studie dargelegten Bezugsrahmens eigene Prognosen zu erstellen, um die Angemessenheit einer Investition in Prisma SASE zu ermitteln.

Palo Alto Networks hat die Studieninhalte zwar geprüft und Forrester dazu Feedback gegeben, Forrester behält sich jedoch die redaktionelle Kontrolle über die Studie und ihre Ergebnisse vor und akzeptiert keine Änderungen an der Studie, die den Erkenntnissen von Forrester widersprechen oder die Bedeutung der Studie verfälschen würden.

Palo Alto Networks hat die Kundennamen für die Befragungen bereitgestellt, jedoch nicht selbst an den Befragungen teilgenommen.



Die Palo Alto Networks Prisma SASE Customer Journey

Beweggründe für die Investition in Prisma SASE

Befragungen

Funktion	Branche	Umsatz	Anz. Mitarbeiter
Chefarchitekt	Gesundheitswesen	$30 Mrd.	15.000
Direktor für Sicherheitsarchitektur und -engineering	Verarbeitendes Gewerbe	$17 Mrd.	160.000
SVP IT	Finanzdienstleistungen	$3 Mrd.	3.000
Senior Director	Gastgewerbe	$20 Mrd.	380.000

ZENTRALE HERAUSFORDERUNGEN

Vor der Einführung von Prisma SASE arbeiteten die Befragten nach eigener Aussage gegenüber Forrester in der Regel in einer Umgebung mit inkonsistenter und unvollständiger Sicherheit. Zur Umsetzung der Sicherheitsrichtlinien mussten sie ihren Netzwerkverkehr oft an ihre Rechenzentren weiterleiten, was zu einer negativen Erfahrung für die Endanwender führte. Darüber hinaus stellte die Erweiterung um neue Standorte und die Bereitstellung von Sicherheitsfunktionen für Mitarbeiter in Hybridarbeit und im Homeoffice eine enorme Herausforderung dar.

Die befragten Unternehmensvertreter beschrieben die folgenden typischen Herausforderungen, mit denen ihr Unternehmen zu kämpfen habe:

- **Bedarf an der Aktualisierung von Sicherheitssystemen für eine moderne Arbeitsumgebung.** Die Befragungsteilnehmer gaben an, dass die Kombination von Faktoren wie die Zunahme von Homeoffice- und Hybridarbeit, die Einführung von Cloud-Technologien und immer raffiniertere Cybersicherheitsangriffe zur Aufdeckung bisher nicht erkannter Sicherheitslücken in ihrer derzeitigen Umgebung geführt hätte. Ein modernes und umfassendes Sicherheitssystem für ihre Arbeitsumgebung zu finden, sei von entscheidender Bedeutung gewesen. Der Chefarchitekt aus dem Gesundheitswesen sagte: „Wir haben kaum jemanden, der Vollzeit im Büro arbeitet. Daher sind wir relativ stark auf die Prisma SASE-Lösungen von Palo Alto Networks angewiesen.“

„Eines der größten Risiken, vor denen wir heute stehen, ist die Geschwindigkeit, mit der Technologien in Unternehmen eingeführt und weiterentwickelt werden. Immer mehr Menschen arbeiten von außerhalb. Früher wurde Sicherheit dadurch gewährleistet, dass alle Mitarbeiter am selben Ort mit demselben Netzwerk verbunden waren. Aber das funktioniert heute nicht mehr.“

Direktor für Sicherheitsarchitektur und -engineering, verarbeitendes Gewerbe

- **Inkonsistenzen in der Anwendererfahrung mit Auswirkungen auf die Produktivität.** Die Interviewpartner stellten ferner fest, dass es in ihrer vorherigen Umgebung zu zahlreichen Störungen gekommen sei, die entweder durch Cybersicherheitsbedrohungen oder durch eine Sicherheitsmaßnahme als Reaktion auf eine potenzielle Bedrohung verursacht worden seien, die schließlich das gesamte System beeinträchtigte. Infolgedessen sei die Arbeit zahlreicher Geschäfts- und Endanwender für eine gewisse Zeit unterbrochen worden, was bei den Betroffenen oftmals schnell zu Frustrationen geführt hätte. Der SVP IT des befragten Finanzdienstleistungsunternehmens sagte hierzu weiter: „Für einen Anwender sind der Einsatz seines Laptops im Homeoffice und die Verwendung im Büro am Folgetag zwei völlig unterschiedliche Vorgänge, bei denen im Backend jeweils andere Technologien eingesetzt werden. Dies führt unter Umständen zu einer Unterbrechung des Arbeitsablaufs, sodass der Anwender z. B. Tickets erstellen oder unser Betriebsteam bitten muss, den Vorfall zu untersuchen. Bei Richtlinieninkonsistenzen oder wenn die anbieterseitige Unterstützung für eine Funktion fehlt, die der Anwender benötigt, entstehen so erhebliche Produktivitätsausfallkosten.“

„Vor dem Umstieg auf Prisma Access hatten wir viele Zuverlässigkeitsprobleme mit unserem alten VPN. Ständige Verbindungsunterbrechungen, langsame Konnektivität, hohe Latenzzeiten – all das bedeutet für den Endanwender erhebliche Zeitverluste und Produktivitätseinbußen.“

SVP IT, Finanzdienstleistungen

- **Schwierigkeiten bei der Skalierung der bestehenden Sicherheitsumgebung.** Schließlich wiesen die Teilnehmer der Befragung darauf hin, dass ihr existierendes Sicherheitssystem nicht mit dem Wachstum ihres Unternehmens habe Schritt halten können. Der Senior Director aus dem Gastgewerbe erklärte: „Unser Unternehmen ist enorm gewachsen. Dadurch ist die individuelle Verwaltung der Router für uns zu einem echten Albtraum geworden. Das galt vor allem, wenn wir die Richtlinien ändern wollten. Früher mussten wir dafür jeden einzelnen Router in der Umgebung anpassen.“

INVESTITIONSZIELE

Die befragten Unternehmen suchten nach einer Lösung mit folgendem Leistungsspektrum:

- **Steigerung der betrieblichen Effizienz ihrer Sicherheitsumgebung.** Die Befragten wünschten sich eine Lösung, die Zeit oder Geld – und im Optimalfall beides – spart. Hierdurch würden mehr Ressourcen freigestellt, die stärker strategisch ausgerichtet werden könnten. Der Chefarchitekt aus dem Gesundheitswesen äußerte sich wie folgt: „Einer der Gründe, warum wir uns für Prisma SASE entschieden haben, war, dass die Konfiguration zu 100 % in der Cloud erfolgt. Wir waren so nicht mehr auf Rechenzentren oder Hardware angewiesen, um die wir uns kümmern mussten.“

  Der Senior Director aus dem Gastgewerbe ergänzte: „Für uns waren die zentrale Verwaltung und die Integration mit anderen Lösungen der entscheidende [Faktor] dafür, dass wir uns [für Palo Alto Networks entschieden haben].“

- **Umfassendes Leistungsprofil und Zuverlässigkeit.** Die Befragten hoben zudem die Leistung der Lösung als weiteren wichtigen

Faktor für ihre Entscheidung hervor. Der Betriebsleiter aus dem verarbeitenden Gewerbe sagte: „Wir haben uns für Palo Alto Networks entschieden, weil das Unternehmen die wohl beste Firewalltechnologie anbietet. Außerdem wollten wir den Endanwendern ein erstklassiges Erlebnis bei gleichzeitig maximaler Sicherheit bieten.“

MODELLUNTERNEHMEN

Basierend auf den Befragungen erstellte Forrester einen TEI-Bezugsrahmen, ein Modellunternehmen und eine ROI-Analyse zur Veranschaulichung der finanziellen Effekte. Das Modellunternehmen bildet einen repräsentativen Querschnitt der vier befragten Unternehmen und wird für die Darstellung der aggregierten Finanzanalyse im nächsten Abschnitt verwendet. Das Modellunternehmen weist die nachfolgenden Eigenschaften auf:

Beschreibung des Modellunternehmens. Das Modellunternehmen ist ein dezentral operierendes Unternehmen mit 50.000 Beschäftigten und einem Jahresumsatz von $7 Mrd. 33 % der Beschäftigten arbeiten im Homeoffice oder hybrid. Das Unternehmen verfügt über 400 Standorte. Dazu gehören der Hauptsitz, das Rechenzentrum, die Cloud, Filialen sowie Verkaufs- und Produktionsstandorte. Im Schnitt bearbeitet das Sicherheitsteam des Modellunternehmens 1.200 Vorfälle pro Woche, d. h. 62.400 im ersten Jahr. Dabei dauert die Behebung eines Vorfalls durchschnittlich 2 Stunden.

Merkmale der Bereitstellung. Das Unternehmen nutzt Palo Alto Networks Prisma SASE, um Remotenetzwerke an seine Verkaufsstellen und Niederlassungen sowie seine Homeoffice- und Hybridmitarbeiter anzubinden. Dabei macht sich das Unternehmen End-of-Life-Zyklen zunutze und investiert Zeit zum Testen der bereitgestellten Lösung, wodurch sich zwar der Zeitrahmen verlängert, aber auch ein reibungsloser Übergang von der alten Lösung gewährleistet wird. An der Bereitstellung ist unter anderem das Netzwerksicherheitsteam beteiligt.

Grundlegende Annahmen

- **$7 Mrd. Jahresumsatz**
- **50.000 Mitarbeiter**
- **33 % der Beschäftigten arbeiten im Homeoffice oder in Hybridarbeit**
- **400 Standorte**
- **4 Rechenzentren**

Nutzenanalyse

Daten zum quantifizierten Nutzen, angewendet auf das Modellunternehmen

Gesamtnutzen						
Ref.	**Nutzen**	**Jahr 1**	**Jahr 2**	**Jahr 3**	**Gesamt**	**Barwert**
Atr	Sicherheit und Effizienz des IT-Betriebs	$911.250	$920.363	$929.475	$2.761.088	$2.287.368
Btr	Steigerung der Endanwenderproduktivität	$4.925.580	$4.925.580	$4.925.580	$14.776.740	$12.249.188
Ctr	Geringeres Risiko von Datenpannen	$1.189.320	$1.189.320	$1.189.320	$3.567.960	$2.957.663
Dtr	Kostensenkung und Einsparungen bei der Sicherheitsinfrastruktur	$340.000	$340.000	$340.000	$1.020.000	$845.530
	Gesamtnutzen (risikobereinigt)	$7.366.150	$7.375.263	$7.384.375	$22.125.788	$18.339.749

SICHERHEIT UND EFFIZIENZ DES IT-BETRIEBS

Daten und Fakten. Die Befragten merkten an, dass die Angehörigen der SecOps- und NetOps-Teams durch den Umstieg auf Prisma SASE entlastet werden konnten. Dies ist auf den Managed-Service-Aspekt der Lösung sowie auf verschiedene Automatisierungen von Aktivitäten zurückzuführen, die im Prozess implementiert werden können.

- Der Chefarchitekt aus dem Gesundheitswesen stellte fest: „Früher waren bei uns mehrere Teams mit SecOps befasst. Es gab einen Software-, einen Hardware- und einen Anwendungs-Layer. Heute sind diese drei Strukturen nicht mehr vorhanden. Wir beschäftigen nur noch Anwendungsexperten. So kommen wir also statt mit vorher fünf bis zehn mit nur noch ein oder zwei Mitarbeitern aus.“
- Weiterhin betonte er gegenüber Forrester die problemlose Skalierung: „Das Skalieren ist wesentlich einfacher geworden. Dabei kommen dieselben Richtlinien zur Anwendung. Die Skalierung erfolgt automatisch. Ohne PANW müssten wir selbst neue Gateways hinzufügen. Wir müssten zudem die für die Datenbankverarbeitung zuständigen Backend-Systeme und alle damit einhergehenden Backoffice-Prozesse erweitern.“
- Der Betriebsleiter aus dem verarbeitenden Gewerbe berichtete: „Was die Änderung von Richtlinien betrifft, brauchen wir statt vier Werktagen jetzt noch nicht einmal mehr 1 Stunde dafür. Dabei nehmen wir etwa 120 Änderungen pro Tag vor (80 % der Zeit).“

> **„Prisma SASE ist im Wesentlichen ein Managed Service. Daher müssen wir die Lösung nicht tagtäglich im Auge behalten. Wir müssen uns keine Gedanken über das System, die Gateways oder die Netzwerklatenz machen. Das alles ist nicht mehr unsere Sache.“**
>
> *Chefarchitekt, Gesundheitswesen*

- Er wies ausdrücklich auf den Nutzen hin, den sein Unternehmen aus der Verwendung von ADEM gezogen habe: „Unser Netzwerkteam nutzt ADEM jedes Mal, wenn es vom Helpdesk oder vom Servicedesk ein Ticket zum Thema Netzwerklatenz erhält. Mit ADEM ist es in der Lage nachzuvollziehen, wo das Problem liegt.“
- Der Senior Director eines Unternehmens aus dem Gastgewerbe sagte: „Mit SD-WAN ist die Einrichtung in einem einzigen Schritt erledigt. Wir brauchen nicht mehr mehrere Wochen und jede Menge Mitarbeiter. Der Vorgang ist innerhalb weniger Stunden, manchmal sogar innerhalb von Minuten erledigt. Früher waren es oft fünf oder sechs Mitarbeiter, die zwei Wochen lang an solchen Änderungen gearbeitet haben. Wir führen zwei bis drei Änderungszyklen pro Quartal durch.“

Modellierung und Annahmen. Forrester geht beim Modellunternehmen von den folgenden Annahmen aus:

- Das Unternehmen hat 20 Mitarbeiter, die der SecOps-Organisation angehören, sowie ein NetOps-Team mit zwölf Beschäftigten.
- Der durchschnittliche SecOps-Mitarbeiter verbringt im Schnitt 80 % seiner Zeit (im Verhältnis zu seiner sonstigen Arbeit) mit der Verwaltung von Tools und der Durchführung von Richtlinienänderungen. Weitere 10 % seiner Zeit verbringt er mit der Bearbeitung von Sicherheitsvorfällen.
- Durch den Einsatz der Prisma SASE-Lösung erzielt das SecOps-Teams bei seiner Arbeit eine Effizienzsteigerung, die eine Zeitersparnis von 75 % ausmacht.
- Der durchschnittliche NetOps-Mitarbeiter verbringt im Durchschnitt 25 % seiner Zeit (im Verhältnis zu seiner sonstigen Arbeit) mit der Skalierung und Einrichtung neuer Standorte.
- Durch den Einsatz der Prisma SASE-Lösung spart das NetOps-Team 80 % seiner Arbeitszeit im 1. Jahr. Dieser Wert steigt im 2. Jahr auf 85 % und im 3. Jahr auf 90 %.
- Das durchschnittliche Jahresgehalt eines SecOps-Mitarbeiters (inkl. Nebenkosten) beträgt $121.500, das eines NetOps-Mitarbeiters $135.000.
- Die Quote der zurückgewonnenen Produktivität beläuft sich auf 50 %, da davon ausgegangen wird, dass vom Beschäftigten nicht die gesamte eingesparte Zeit als zusätzliche Produktivität eingebracht wird.

Risiken. Der genaue Nutzen, den ein Unternehmen hierbei erzielt, hängt von den folgenden Faktoren ab:

- Der Größe und Qualifikation des Sicherheitsmanagementteams im Unternehmen
- Den bereits vor der Bereitstellung von Prisma SASE vorhandenen Kompetenzen und Systemen
- Der Komplexität der Sicherheitsumgebung
- Der Anzahl der Sicherheitsvorfälle, die vor der Implementierung von Prisma SASE ein manuelles Eingreifen erforderten
- Den weiteren Tools und Lösungen, die zur Unterstützung der Arbeit der SecOps- und IT-Ops-Teams implementiert wurden
- Dem Durchschnittsgehalt der Angehörigen der SecOps- und NetOps-Teams

Ergebnisse. Zur Berücksichtigung dieser Risiken hat Forrester den genannten Nutzen um 10 % nach unten korrigiert, wodurch sich über drei Jahre ein risikobereinigter Gesamtbarwert von $2,3 Mio. ergibt.

Sicherheit und Effizienz des IT-Betriebs

Ref.	Messgröße	Quelle	Jahr 1	Jahr 2	Jahr 3
A1	Größe der SecOps-Organisation (Mitarbeiter)	Modellunterneh-men	20	20	20
A2	Prozentsatz der Zeit, die für die Verwaltung von Tools und die Durchführung von Richtlinienänderungen aufgewendet wird	Modellunterneh-men	80 %	80 %	80 %
A3	Prozentuale Effizienzsteigerung durch Prisma SASE	Befragungen	75 %	75 %	75 %
A4	Zwischensumme: Gesamte Zeitersparnis bei der Bearbeitung von Sicherheitsvorfällen (Mitarbeiter)	A1*A2*A3	12	12	12
A5	Prozentualer Zeitaufwand für die Bearbeitung von Sicherheitsvorfällen	Modellunterneh-men	10 %	10 %	10 %
A6	Prozentuale Effizienzsteigerung durch Prisma SASE	Befragungen	75 %	75 %	75 %
A7	Zwischensumme: Gesamte Zeitersparnis bei der Toolverwaltung und der Durchführung von Richtlinienänderungen (Mitarbeiter)	A1*A5*A6	2	2	2
A8	Durchschnittliches Jahresgehalt (inkl. Nebenkosten) eines SecOps-Mitarbeiters	TEI-Standard	$121.500	$121.500	$121.500
A9	Zwischensumme: Gesamtwert der Effizienzsteigerung der SecOps-Organisation	(A4+A7)*A8	$1.701.000	$1.701.000	$1.701.000
A10	Größe der NetOps-Organisation (Mitarbeiter)	Modellunterneh-men	12	12	12
A11	Prozentsatz der für die Skalierung und Einrichtung neuer Standorte aufgewendeten Zeit	Modellunterneh-men	25 %	25 %	25 %
A12	Prozentuale Effizienzsteigerung durch Prisma SASE	Befragungen	80 %	85 %	90 %
A13	Durchschnittliches Jahresgehalt (inkl. Nebenkosten) eines NetOps-Mitarbeiters	TEI-Standard	$135.000	$135.000	$135.000
A14	Zwischensumme: Gesamtwert der Effizienzsteigerung der NetOps-Organisation	A10*A11*A12*A13	$324.000	$344.250	$364.500
A15	Produktivitätsrückgewinnung	TEI-Standard	50 %	50 %	50 %
At	Sicherheit und Effizienz des IT-Betriebs	(A9+A14)*A15	$1.012.500	$1.022.625	$1.032.750
	Risikobereinigung	↓10 %			
Atr	Sicherheit und Effizienz des IT-Betriebs (risikobereinigt)		$911.250	$920.363	$929.475
	Gesamt über drei Jahre: $2.761.088			**Barwert über drei Jahre: $2.287.368**	

STEIGERUNG DER ENDANWENDERPRODUKTIVITÄT

Daten und Fakten. Die Befragten merkten an, dass die vor der Umstellung auf Prisma SASE genutzte Sicherheitsumgebung gelegentlich Störungen bei Arbeiten der Geschäfts- und Endanwender verursacht hätte. Manchmal sei dies auch durch besonders störende Prüfverfahren verursacht worden. In anderen Fällen hätten Sicherheitslücken in der alten Umgebung Cybersicherheitsangriffe provoziert, die zu einer erheblichen Beeinträchtigung der Produktivität der Mitarbeiter geführt hätten, insbesondere derjenigen, die im Homeoffice arbeiteten.

- Der SVP IT des Finanzdienstleistungsunternehmens sagte zu Forrester: „Ich arbeite zu 100 % remote bzw. hybrid, und es gibt immer noch einen Prozentsatz von Mitarbeitern, die im Homeoffice arbeiten. Dieselbe Infrastruktur muss also auch heute noch funktionieren, wenn man drei Tage im Büro und zwei Tage zu Hause arbeitet. An diesen beiden Tagen muss alles nahtlos funktionieren: Wenn sie von zu Hause aus arbeiten, kommt eine andere Infrastruktur zum Einsatz als die im Büro verwendete Hardwarefirewall.“
- Der Chefarchitekt aus dem Gesundheitswesen ergänzte: „Wenn [unsere Mitarbeiter] angegriffen werden, können sie ihre Arbeit nicht mehr erledigen. Einmal hatten wir einen Ausfall an einem Wochenende zu verzeichnen, weil [unser früherer Anbieter] ein Upgrade durchgeführt hat, das nicht vollständig getestet worden war. Daher konnten wir uns nicht mehr mit unserem Netzwerk verbinden. Sage und schreibe 8 Stunden lang stand hier alles still.“

Modellierung und Annahmen. Forrester geht beim Modellunternehmen von den folgenden Annahmen aus:

- Es gibt 50.000 Mitarbeiter.
- 33 % der Mitarbeiter arbeiten im Homeoffice oder hybrid.
- 50 % der Mitarbeiter arbeiten direkt mit Cloud-Produkten, wobei davon ausgegangen wird, dass diese am meisten von den Lösungen von Palo Alto Networks profitieren.
- Bei jedem Systemausfall wird die Produktivität von 20 % der Mitarbeiter, die direkt mit Cloud-Produkten arbeiten, hiervon beeinträchtigt.
- Dank der Lösungen von Palo Alto Networks werden 8 % der durch Systemausfälle entstandenen Zeit- und Produktivitätsverluste wieder wettgemacht.
- Das durchschnittliche Jahresgehalt (inkl. Nebenkosten) eines Endanwenders beträgt $87.750.
- 50 % der Effizienzsteigerung werden in produktive Arbeit umgesetzt.

Risiken. Der genaue Nutzen, den ein Unternehmen hierbei erzielt, hängt von den folgenden Faktoren ab:

- Der Größe des Unternehmens und dem Anteil der Endanwender, deren Produktivität durch die Ausfallzeiten der Sicherheitslösung potenziell beeinträchtigt wird
- Der Komplexität der IT-Umgebung, die sich potenziell auf den Umfang und das Ausmaß der Ausfallzeiten auswirkt, die aufgrund von Untersuchungen und Geräte-Reimaging entstehen
- Dem geografischen Standort und der Branche, in denen das implementierende Unternehmen tätig ist, denn diese Faktoren haben einen Einfluss auf das durchschnittliche Jahresgehalt (inkl. Nebenkosten) der Endanwender

Ergebnisse. Zur Berücksichtigung dieser Risiken hat Forrester den genannten Nutzen um 15 % nach unten korrigiert, was über drei Jahre einen

Steigerung der Endanwenderproduktivität					
Ref.	**Messgröße**	**Quelle**	**Jahr 1**	**Jahr 2**	**Jahr 3**
B1	Gesamtzahl der Mitarbeiter	Modellunternehmen	50.000	50.000	50.000
B2	Prozentualer Anteil von Mitarbeitern im Homeoffice oder mit hybridem Arbeitsplatzmodell	Modellunternehmen	33 %	33 %	33 %
B3	Prozentsatz der in der Cloud erledigten Arbeit	Modellunternehmen	50 %	50 %	50 %
B4	Prozentsatz der von Systemausfällen betroffenen Endanwender	Modellunternehmen	20 %	20 %	20 %
B5	Prozentsatz der durch bessere Verfügbarkeit/geringere Ausfallzeiten wiedergewonnenen Zeit	Befragungen	8 %	8 %	8 %
B6	Durchschnittliches Jahresgehalt (inkl. Nebenkosten) eines geschäftlichen Anwenders	TEI-Standard	$87.750	$87.750	$87.750
B7	Produktivitätsrückgewinnung	TEI-Standard	50 %	50 %	50 %
Bt	Steigerung der Endanwenderproduktivität	B1*B2*B3*B4*B5*B6*B7	$5.794.800	$5.794.800	$5.794.800
	Risikobereinigung	↓15 %			
Btr	Steigerung der Endanwenderproduktivität (risikobereinigt)		$4.925.580	$4.925.580	$4.925.580
	Gesamt über drei Jahre: $14.776.740			**Barwert über drei Jahre: $12.249.188**	

risikobereinigten Gesamtbarwert von $12,2 Mio. ergibt.

GERINGERES RISIKO VON DATENPANNEN

Daten und Fakten. Die geringere Komplexität der Sicherheitsumgebung hat auch ein geringeres Sicherheitsrisiko zur Folge. Während in der vorherigen Umgebung die verschiedenen Einzellösungen nicht gut integriert gewesen wären bzw. nicht miteinander kommuniziert hätten, was zu potenziellen Sicherheitslücken und damit zu einem erhöhten Risiko von Datenpannen geführt hätte, sei dieses Risiko durch den Einsatz von Prisma SASE erheblich reduziert worden. Dieser Vorteil kam vor allem bei Unternehmen mit Mitarbeitern zum Tragen, die die Möglichkeit zum Homeoffice und/oder zur Hybridarbeit nutzten.

- Der Chefarchitekt aus dem Gesundheitswesen sagte zu Forrester: „Wir sind in der Lage, unsere Dienste in einer sicheren Umgebung anzubieten, da wir volle Transparenz über die Benutzeraktivitäten haben.“
- Der Direktor aus dem verarbeitenden Gewerbe merkte an: „Wenn der Sicherheitsperimeter den einzelnen Anwender umschließt und nicht einen geschlossenen Ort, verringert sich das Risiko.“
- Der SVP IT des befragten Finanzdienstleisters erklärte: „Einer der wichtigsten Aspekte ist die erhöhte Sicherheit und die Möglichkeit zu erkennen, welcher Datenverkehr nach draußen geht. Wir sind problemlos in der Lage, den Internetverkehr zu überwachen und festzustellen, was in unserem Netzwerk vor sich geht.“

Modellierung und Annahmen. Forrester geht beim Modellunternehmen von den folgenden Annahmen aus:

- Den Daten von Forrester zufolge muss das Modellunternehmen beim Einsatz von Punktlösungen mit durchschnittlich 3,2 Datenpannen pro Jahr rechnen.[2]
- Forrester modelliert die Kosten einer Datenpanne nach der Anzahl der Mitarbeiter im betroffenen Unternehmen. Diese Kosten belaufen sich beim Modellunternehmen auf $53 pro Mitarbeiter, wobei der Produktivitätsverlust der Mitarbeiter noch gar nicht berücksichtigt ist.[3] Sie umfassen:
  - Bußgelder
  - Rückerstattungen an Kunden, Kosten für Rechtsstreitigkeiten
  - Reaktion auf Vorfälle und Abhilfemaßnahmen
  - Entgangene Umsätze
  - Kosten für die Wiederherstellung des Markenwerts
  - Kosten für die Wiedergewinnung von Kunden
- Mit Prisma SASE verringert sich die Wahrscheinlichkeit einer Datenpanne für Unternehmen innerhalb von drei Jahren um bis zu 50 %.

„Ohne PANW wären wir unterschiedlichsten Angriffen ausgesetzt. Mitarbeiter, die in unseren geschäftlichen Räumen arbeiten, befinden sich hinter einer Firewall. Jetzt, wo die Mitarbeiter im Homeoffice oder im Ausland arbeiten, geht das verloren. Mit Tools wie Prisma SASE verfügt man weiterhin über das gleiche Maß an Transparenz, Kontrolle und Schutz.“

Chefarchitekt, Gesundheitswesen

- Die Zuschreibung zu Prisma SASE entspricht dem Prozentsatz der mobilen Mitarbeiter im Unternehmen, der 33 % beträgt.

Risiken. Der genaue Nutzen, den ein Unternehmen hierbei erzielt, hängt von den folgenden Faktoren ab:

- Den Auswirkungen von Palo Alto Networks auf den allgemeinen Sicherheitsstatus des Unternehmens im Vergleich zur vorherigen Lösung
- Dem Prozentsatz der Mitarbeiter, die von einer Datenpanne betroffen sind, und die Dauer der damit verbundenen Ausfallzeiten
- Den Durchschnittsgehältern der geschäftlichen Anwender

Ergebnisse. Zur Berücksichtigung dieser Risiken hat Forrester den genannten Nutzen um 15 % nach unten korrigiert, was über drei Jahre einen risikobereinigten Gesamtbarwert von $3 Mio. ergibt.

Geringeres Risiko von Datenpannen

Ref.	Messgröße	Quelle	Jahr 1	Jahr 2	Jahr 3
C1	Durchschnittliche Anzahl von Datenpannen pro Jahr	Forrester Research	3,2	3,2	3,2
C2	Gesamtzahl der Mitarbeiter	B1	50.000	50.000	50.000
C3	Durchschnittliche potenzielle Kosten einer Datenpanne je Mitarbeiter ohne Berücksichtigung der Ausfallzeiten für interne Nutzer	Forrester Research	$53	$53	$53
C4	Geringere Wahrscheinlichkeit von Datenpannen	Befragungen	50 %	50 %	50 %
C5	Prisma SASE zugeschrieben	B2	33 %	33 %	33 %
Ct	Geringeres Risiko von Datenpannen	C1*C2*C3*C4*C5	$1.399.200	$1.399.200	$1.399.200
	Risikobereinigung	↓15 %			
Ctr	Geringeres Risiko von Datenpannen (risikobereinigt)		$1.189.320	$1.189.320	$1.189.320
	Gesamt über drei Jahre: $3.567.960			**Barwert über drei Jahre: $2.957.663**	

[2] Quelle: Forrester Consulting, „Cost Of A Cybersecurity Breach Survey“, Q1 2021.

[3] Ebd.

KOSTENSENKUNG UND EINSPARUNGEN BEI DER SICHERHEITS- UND NETZWERKINFRASTRUKTUR

Daten und Fakten. Die Befragten merkten an, dass sie durch die verschiedenen Lösungen und Funktionen, die sie als Ergebnis ihrer Investition in Prisma SASE zur Verfügung gestellt bekommen hätten, einen bestimmten Prozentsatz ihrer jährlichen Ausgaben für Sicherheits- und Netzwerktechnologien haben reduzieren oder aufgeben können.

- Der Chefarchitekt aus dem Gesundheitswesen erläuterte Forrester, welche Lösungen man alle aus der Altumgebung seines Unternehmens durch die Investition in Prisma SASE habe ausmustern können: „Wir hatten ein spezielles Produkt für den Fernzugang. Dann hatten wir das, was wir H-Security nennen, oder das sichere Gateway. Das ist die Absicherung für Fernanwender. Und dann gab es noch das DLP (Data Loss Prevention), ein separates System zum Schutz vor Datenverlust. Es gab also drei separate Lösungen, die unterschiedliches Fachwissen und verschiedene Teams erforderten. Jetzt dagegen ist alles miteinander vereint.“
- Der Direktor aus dem verarbeitenden Gewerbe fügte hinzu: „Wir konnten unter anderem unserem Web-Proxy-Anbieter kündigen. Diese Einsparung geht jährlich in die Millionen.“

Modellierung und Annahmen. Forrester geht beim Modellunternehmen von den folgenden Annahmen aus:

- Die jährlichen Ausgaben des Unternehmens für Sicherheitstechnik belaufen sich auf $8 Mio.
- Die mit der Nutzung von Prisma SASE von Palo Alto Networks einhergehende Anbieterkonsolidierung entspricht 5 % der jährlichen Ausgaben für Sicherheitstechnik.

Risiken. Der genaue Nutzen, den ein Unternehmen hierbei erzielt, hängt von den folgenden Faktoren ab:

- Den jährlich anfallenden Kosten für die jeweilige zu ersetzende Technologie
- Dem Tempo, mit dem ein Unternehmen diese Technologie aufgrund von Lizenzvereinbarungen/Bedingungen und Netzwerkkonfigurationen ersetzen kann

Ergebnisse. Zur Berücksichtigung dieser Risiken hat Forrester den genannten Nutzen um 15 % nach unten korrigiert, was über einen Zeitraum von drei Jahren einen risikobereinigten Gesamtbarwert von $846.000 ergibt.

Kostensenkung und Einsparungen bei der Sicherheits- und Netzwerkinfrastruktur

Ref.	Messgröße	Quelle	Jahr 1	Jahr 2	Jahr 3
D1	Jährliche Ausgaben für Sicherheitstechnologien	Modellunternehmen	$8.000.000	$8.000.000	$8.000.000
D2	Prozentsatz der Einsparungen aus der Anbieterkonsolidierung durch Prisma SASE und SD-WAN	Befragungen	5 %	5 %	5 %
Dt	Kostensenkung und Einsparungen bei der Sicherheits- und Netzwerkinfrastruktur	D1*D2	$400.000	$400.000	$400.000
	Risikobereinigung	↓15 %			
Dtr	Kostensenkung und Einsparungen bei der Sicherheits- und Netzwerkinfrastruktur (risikobereinigt)		$340.000	$340.000	$340.000
	Gesamt über drei Jahre: $1.020.000			**Barwert über drei Jahre: $845.530**	

„Mit Prisma SASE erhält man eine Plattform, die mehrere Aufgaben gleichzeitig erfüllt. Wir waren in der Lage, drei separate Lösungen in einer einzigen zusammenzuführen. Unterm Strich bedeutet das eine erhebliche Kostenersparnis.“

Chefarchitekt, Gesundheitswesen

NICHT QUANTIFIZIERTER NUTZEN

Die Befragten nannten weitere Vorteile für ihr Unternehmen, die jedoch nicht quantifiziert werden konnten:

- **Bessere Transparenz für die Sicherheitsumgebung.** Die Befragten stellten fest, dass einer der größten Vorteile von Prisma SASE darin bestehe, dass sie nun einen besseren Einblick in den Zustand, die Leistung und die Nutzung der verschiedenen Teile der Sicherheitsorganisation erhielten. Der Chefarchitekt aus dem Gesundheitswesen sagte: „Wir sind nun in der Lage, den Datenverkehr ganz leicht im Auge zu behalten und zu sehen, was tatsächlich in unserem Netzwerk passiert.“

  Der SVP IT aus dem Finanzdienstleistungssektor ergänzte: „Das Attraktive an Palo Alto Networks waren die Schnittstelle und die gegebene Transparenz. Die Berichterstattung war für uns das Beste, was die Benutzeroberfläche angeht. Sie hat auf Anhieb besser funktioniert als unsere eigens entwickelte Berichtssoftware, die zudem sehr wartungsintensiv war.“

- **Besseres Mitarbeitererlebnis sowohl in puncto Nutzung der verschiedenen Lösungen als auch in Bezug auf die robustere, weniger intrusive Sicherheitsumgebung.** Die Befragungsteilnehmer stellten fest, dass die Kombination aller oben genannten Vorteile das Mitarbeitererlebnis in ihren Unternehmen optimiert habe. Der Direktor aus dem verarbeitenden Gewerbe merkte an: „Palo Alto Networks hat auf Anhieb perfekt funktioniert. Wir haben, was die Erlebnisqualität angeht, ein ausgezeichnetes Feedback von den Mitarbeitern erhalten.“

„PANW bereitet einem den weiteren Weg, nämlich die Integration weiterer Funktionen wie Remotenetzwerke, Zweigstellen und CASB.“

Direktor für Sicherheitsarchitektur und -engineering, verarbeitendes Gewerbe

FLEXIBILITÄT

Flexibilität hat für jedes Unternehmen einen anderen Stellenwert. Es sind mehrere Szenarien denkbar, in denen ein Kunde sich für die Implementierung von Prisma SASE entscheidet und zusätzliche Anwendungen und Geschäftsmöglichkeiten erst später erkennt, z. B.:

- **Langfristige positive Auswirkungen einer umfassenden Sicherheitslösung in der Umgebung.** Langfristig kann der Einsatz einer effizienten und umfassenden Sicherheitsumgebung die Leistungsfähigkeit eines Unternehmens, seine Marke und den Umgang mit neuartigen und künftigen Bedrohungen nachhaltig beeinflussen. Der Direktor aus dem verarbeitenden Gewerbe erläuterte das folgendermaßen: „Die Nutzung der Lösung von Palo Alto Networks bereitet einen auf den Rest des Weges vor. Dieser besteht darin, weitere Funktionen zu integrieren, z. B. Remotenetzwerke, Zweigstellen, CASB usw. Die nächste Generation von Tools und Funktionen von Palo Alto Networks wird es uns ermöglichen, die Abläufe bei der Entwicklung von Sicherheitsdesigns und Firewallrichtlinien noch weiter zu vereinfachen."

Flexibilität wird ebenfalls bei der Evaluierung im Rahmen eines spezifischen Projekts quantifiziert. Eine ausführlichere Beschreibung dazu befindet sich in Anhang A.

Die Forrester-Perspektive: Die wichtigsten Cybersicherheitsrisiken 2023 umfassen etablierte wie auch neuartige Bedrohungen

Noch bis vor kurzer Zeit war die Verteidigung gegen Angriffe auf maschinelles Lernen und künstliche Intelligenz eine Nischendisziplin, aber damit ist es jetzt vorbei. Umgekehrt setzen Angreifer ihrerseits verstärkt KI ein, was das Schadenspotenzial in einem Maße steigert, wie es vor dem Aufkommen dieser Technologien nicht möglich war.

Das Cloud Computing stellt angesichts der Reichweite der Cloud und der Komplexität von Cloud-Umgebungen ebenfalls eine sicherheitstechnische Herausforderung dar. Sicherheitsbedrohungen nehmen durch die wachsende Vielfalt der Rechen- und Speicherinfrastrukturen in der Cloud sowie durch das Unvermögen der IaaS-Anbieter zur Einbeziehung dieser neuen Varianten noch weiter zu.

Quelle: „The Future Of Cybersecurity And Privacy", Forrester Research, Inc., 3. August 2023

Kostenanalyse

Daten zu quantifizierbaren Kosten, angewandt auf das Modellunternehmen

Gesamtkosten							
Ref.	**Kosten**	**Jahr 0**	**Jahr 1**	**Jahr 2**	**Jahr 3**	**Gesamt**	**Barwert**
Etr	Interner Zeitaufwand für Installation und Bereitstellung	$248.400	$124.200	$62.100	$31.050	$465.750	$435.960
Ftr	Interner Zeitaufwand für Anwenderschulungen und fortlaufende Verwaltung	$950	$24.948	$24.948	$24.948	$75.794	$62.992
Gtr	Kosten für Prisma SASE	$162.068	$3.291.750	$3.291.750	$3.291.750	$10.037.318	$8.348.163
	Gesamtkosten (risikobereinigt)	$411.418	$3.440.898	$3.378.798	$3.347.748	$10.578.862	$8.847.115

INTERNER ZEITAUFWAND FÜR INSTALLATION UND BEREITSTELLUNG

Daten und Fakten. Die Befragten merkten an, dass die Implementierung von Prisma SASE ein komplexer Prozess gewesen sei, der die Zusammenarbeit verschiedener Teams in ihrem Unternehmen (IT, SecOps und NetOps) mit dem Team von Palo Alto Networks erfordert habe.

- Der Chefarchitekt eines Unternehmens aus dem Gesundheitswesen berichtete Forrester von dessen Einrichtungsprozess: „Nachdem wir verschiedene Anbieter evaluiert und uns für Palo Alto Networks entschieden hatten, haben wir die gesamte Lösung innerhalb eines Jahres eingerichtet. Hierbei waren mehrere Teams aus den Bereichen IT-Sicherheit, Compliance und Netzwerke beteiligt. Für die Bereitstellung des Agenten haben wir außerdem das Desktop-Support-Team mit einbezogen. Insgesamt haben also zwischen 10 und 20 Personen etwa 50 % ihrer Zeit [für die Implementierung] eingesetzt."
- Der Direktor aus dem verarbeitenden Gewerbe fügte hinzu: „Wir hatten sowohl einen Mitarbeiter aus meinem Netzwerkteam und einen aus dem IT-Team dabei. In den ersten Tagen wurden sie nur zu 50 % in Anspruch genommen, da der Großteil der Arbeit von den Mitarbeitern von Palo Alto Networks erledigt wurde. Als dann aber der Mandant in der Cloud einsatzbereit war, hat mein Team zu 100 % übernommen."
- In Bezug auf die Bereitstellung von Prisma SD-WAN äußerte sich der Senior Director des Gastgewerbeunternehmens wie folgt: „Eine ganze Reihe von Mitarbeitern konzentrierte sich voll und ganz auf die Bereitstellung. Wenn diese Aufgabe effizient durchgeführt wird, kann sie von 16 bis 18 Personen erledigt werden, die aktiv an dem Projekt beteiligt sind. Die meisten von ihnen bestehen in der Regel aus Netzwerkspezialisten und einige aus Ingenieuren."

Modellierung und Annahmen. Forrester geht beim Modellunternehmen von den folgenden Annahmen aus:

- Für die gesamte Bereitstellung von Palo Alto Networks wenden zehn NetOps-Mitarbeiter in der Anfangsphase insgesamt neun Monate für das Upgrade der Firewalls und die Anpassung der Richtlinien auf und verbringen im ersten Jahr fast fünf Monate mit der Feinabstimmung. Das Unternehmen macht sich End-of-Life-Zyklen zunutze und investiert die nötige Zeit zum Testen der Installation. Dies verlängert zwar den

Zeitrahmen, gewährleistet aber auch einen reibungslosen Übergang von der alten Lösung.

- Die beteiligten Mitarbeiter verbringen anfangs 80 % ihrer Zeit mit der Bereitstellung. Dieser Wert verringert sich in den Folgejahren allmählich.
- Das durchschnittliche Jahresgehalt eines NetOps-Mitarbeiters (inkl. Nebenkosten) beträgt $135.000.
- Da Unternehmen Prisma SASE in der Regel in Kombination mit anderen Lösungen von Palo Alto Networks einsetzen, wird davon ausgegangen, dass das Modellunternehmen 20 % der gesamten Installations- und Bereitstellungszeit für Prisma SASE aufwendet.

Risiken. Welche Kosten einem Unternehmen aus diesen Gründen genau entstehen, hängt von den folgenden Faktoren ab:

- Den Kompetenzen der betroffenen internen Mitarbeiter
- Der Komplexität der alten Umgebung
- Dem Jahresgehalt der betroffenen internen Mitarbeiter

Ergebnisse. Zur Berücksichtigung dieser Risiken hat Forrester die genannten Kosten um 15 % nach oben korrigiert, was über drei Jahre einen risikobereinigten Gesamtbarwert von $436.000 ergibt.

Interner Zeitaufwand für Installation und Bereitstellung

Ref.	Messgröße	Quelle	Jahr 0	Jahr 1	Jahr 2	Jahr 3
E1	Mit der PAN-Installation beauftragtes Netzwerkteam	Modellunterneh men	10	10	10	10
E2	Zeitaufwand pro Mitglied des Netzwerkteams	Befragung	80 %	40 %	20 %	10 %
E3	Jahresgehalt: NetOps-Mitarbeiter	TEI-Standard	$135.000	$135.000	$135.000	$135.000
E4	Prozentuale Zuschreibung zu Prisma SASE	Befragungen	20 %	20 %	20 %	20 %
Et	Interner Zeitaufwand für Installation und Bereitstellung	E1*E2*E3*E4	$216.000	$108.000	$54.000	$27.000
	Risikobereinigung	↑15 %				
Etr	Interner Zeitaufwand für Installation und Bereitstellung (risikobereinigt)		$248.400	$124.200	$62.100	$31.050
	Gesamt über drei Jahre: $465.750			**Barwert über drei Jahre: $435.960**		

INTERNER ZEITAUFWAND FÜR ANWENDERSCHULUNGEN UND FORTLAUFENDE VERWALTUNG

Daten und Fakten. Nach Abschluss der Einrichtung stellten die Befragten fest, dass die laufende Verwaltung von Prisma SASE unterschiedlich gut funktionierte. Für einige stellte es eine einfach zu überwachende Plattform dar, während andere zusätzliche Zeit und Investitionen aufgewendet hätten, um die Möglichkeiten der Lösung für ihr Unternehmen auch wirklich voll auszuschöpfen.

- Der befragte Chefarchitekt merkte an: „Wir haben ein oder zwei Personen, die das Tool bedienen, um Anfragen zu Richtlinienänderungen zu bearbeiten und Warnmeldungen zu überwachen. Vieles davon ist Arbeit auf der Ebene der Sicherheitsanwendungen.“
- Der Direktor aus dem verarbeitenden Gewerbe ergänzte: „Für die laufende Verwaltung von Prisma SASE benötigt mein Team schätzungsweise 10 % der Arbeitszeit. Die Bedienung ist wirklich kinderleicht.“
- Zu Prisma SD-WAN äußerte sich der Senior Director eines Unternehmens aus dem Gastgewerbe gegenüber Forrester wie folgt: „Wir treffen uns regelmäßig mit dem Team von Palo Alto Networks, um zu verstehen, wie sich die Plattform weiterentwickelt. Wir tauschen uns über Erfahrungen und bei Bedarf über Herausforderungen aus. Für die Wartung und die Optimierung der Plattform sind bei uns jeweils unterschiedliche Teams zuständig.“

Modellierung und Annahmen. Forrester geht beim Modellunternehmen von den folgenden Annahmen aus:

- Für Mitarbeiter, die keine Erfahrung mit Palo Alto Networks haben, sind insgesamt 20 Schulungsstunden erforderlich. In den Folgejahren sind jeweils 8 weitere Schulungsstunden nötig, um alle neuen Funktionen, Aktualisierungen und Erweiterungen zu vermitteln.
- Der Stundensatz inkl. Nebenkosten beträgt für die gesamte IT-Organisation durchschnittlich $54.
- Nach Abschluss der Schulung wird vorausgesetzt, dass die zehn Personen, die pro Jahr geschult werden, für die laufende Verwaltung zuständig sind. Sie wenden 10 % ihrer Arbeitszeit für die Verwaltung von Prisma SASE auf.
- Da Unternehmen NGFW und CDSS in der Regel gleichzeitig verwalten, wird im Modell davon ausgegangen, dass 20 % des gesamten Zeitaufwands für die laufende Verwaltung auf Prisma SASE entfallen.

Risiken. Welche Kosten einem Unternehmen aus diesen Gründen genau entstehen, hängt von den folgenden Faktoren ab:

- Der Größe der IT-Organisation und ihrer Erfahrung mit den Lösungen von Palo Alto Networks
- Dem durchschnittlichen Gehalt der IT-Mitarbeiter

Ergebnisse. Zur Berücksichtigung dieser Risiken hat Forrester die genannten Kosten um 10 % nach oben korrigiert, was über drei Jahre einen risikobereinigten Gesamtbarwert von $63.000 ergibt.

Interner Zeitaufwand für Anwenderschulungen und fortlaufende Verwaltung						
Ref.	**Messgröße**	**Quelle**	**Jahr 0**	**Jahr 1**	**Jahr 2**	**Jahr 3**
F1	Anzahl der Mitarbeiter, die eine Schulung zur laufenden Verwaltung erhalten	Modellunterneh men	10	10	10	10
F2	Stunden pro Schulungseinheit	Befragungen	8	2	2	2
F3	Durchschnittlicher Stundensatz inkl. Nebenkosten je IT-Organisationsmitarbeiter (SecOps, NetOps, IT-Betrieb)	TEI-Standard	$54	$54	$54	$54
F4	Interner Zeitaufwand für Anwenderschulungen	F1*F2*F3	$4.320	$1.080	$1.080	$1.080
F5	Prozentsatz der für die laufende Verwaltung aufgewendeten Zeit	Befragungen		10 %	10 %	10 %
F6	Wert des internen Zeitaufwands für die fortlaufende Verwaltung	F1*F3*2.080*F5		$112.320	$112.320	$112.320
F7	Prisma SASE zugeschrieben	Befragungen	$0	20 %	20 %	20 %
Ft	Interner Zeitaufwand für Anwenderschulungen und fortlaufende Verwaltung	(F4+F6)*F7	$864	$22.680	$22.680	$22.680
	Risikobereinigung	↑10 %				
Ftr	Interner Zeitaufwand für Anwenderschulungen und fortlaufende Verwaltung (risikobereinigt)		$950	$24.948	$24.948	$24.948
	Gesamt über drei Jahre: $75.794			**Barwert über drei Jahre: $62.992**		

KOSTEN FÜR PRISMA SASE

Daten und Fakten. Die Befragten erwarben die Hardware vorab und konnten die Abonnementkosten über die dreijährige Vertragslaufzeit abschreiben. So waren die jährlichen Kosten vorhersehbar.

Modellierung und Annahmen. Forrester geht beim Modellunternehmen von den folgenden Annahmen aus:

- Die jährlichen Kosten umfassen sowohl die anzuschaffende Hardware als auch die Abonnementgebühren für die Lösung.
- Abonnementverträge werden über die Laufzeit von drei Jahren abgeschrieben.
- Die Preise können variieren. Genaue Preisinformationen erhalten Sie von Palo Alto Networks.

Risiken. Welche Kosten einem Unternehmen aus diesen Gründen genau entstehen, hängt von den folgenden Faktoren ab:

- Der Anzahl der Anwender und Standorte, für die die Lösung implementiert werden soll
- Den speziellen Add-Ons, die zur weiteren Leistungsverbesserung implementiert werden sollen

Ergebnisse. Zur Berücksichtigung dieser Risiken hat Forrester die genannten Kosten um 5 % nach oben korrigiert, was über drei Jahre einen risikobereinigten Gesamtbarwert von $8,3 Mio. ergibt.

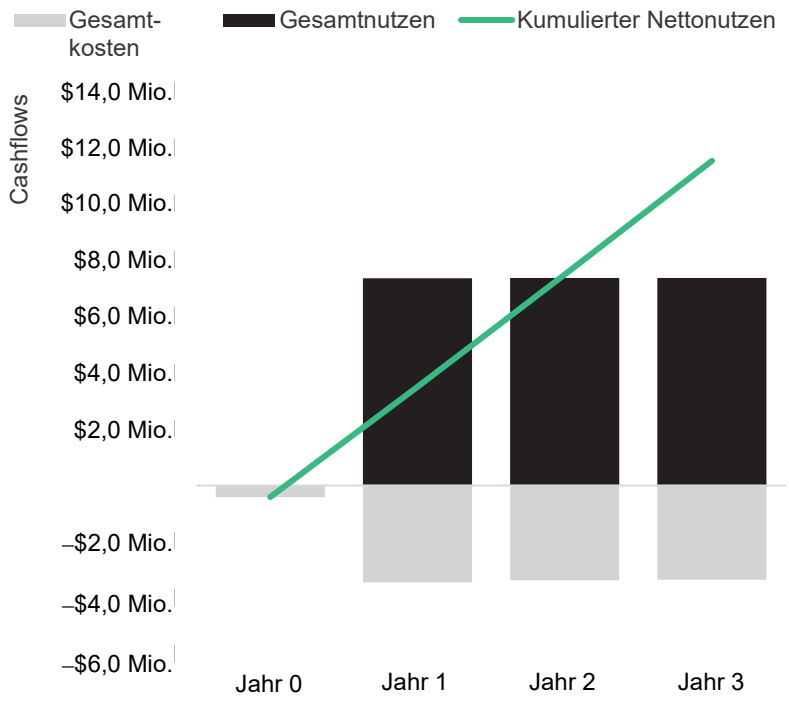
Kosten für Prisma SASE

Ref.	Messgröße	Quelle	Jahr 0	Jahr 1	Jahr 2	Jahr 3
G1	Jährliche Kosten für Prisma SASE	Modellunter-nehmen	$154.350	$3.135.000	$3.135.000	$3.135.000
Gt	Kosten für Prisma SASE	G1	$154.350	$3.135.000	$3.135.000	$3.135.000
	Risikobereinigung	↑5 %				
Gtr	Kosten für Prisma SASE (risikobereinigt)		$162.068	$3.291.750	$3.291.750	$3.291.750
	Gesamt über drei Jahre: $10.037.318			**Barwert über drei Jahre: $8.348.163**		

Zusammenfassung der Finanzergebnisse

KONSOLIDIERTE RISIKOBEREINIGTE MESSGRÖSSEN FÜR EINEN ZEITRAUM VON DREI JAHREN

Cashflowdiagramm (risikobereinigt)



Die in den Nutzen- und Kostenabschnitten berechneten finanziellen Ergebnisse können zur Bestimmung des ROI, des Kapitalwerts und des Amortisationszeitraums für die Investition des Modellunternehmens verwendet werden. Forrester hat dieser Analyse einen jährlichen Diskontierungssatz von zehn Prozent zugrunde gelegt.

Zur Ermittlung der risikobereinigten Werte für den ROI, den Kapitalwert und den Amortisationszeitraum wurden Risikoanpassungsfaktoren auf die unbereinigten Ergebnisse der einzelnen Nutzen- und Kostenpositionen angewendet.

Cashflowanalyse (risikobereinigte Schätzungen)

	Jahr 0	Jahr 1	Jahr 2	Jahr 3	Gesamt	Barwert
Gesamtkosten	($411.418)	($3.440.898)	($3.378.798)	($3.347.748)	($10.578.862)	($8.847.115)
Gesamtnutzen	$0	$7.366.150	$7.375.263	$7.384.375	$22.125.788	$18.339.749
Nettonutzen	($411.418)	$3.925.252	$3.996.465	$4.036.627	$11.546.926	$9.492.634
ROI						107 %
Amortisationszeitraum						< 6 Monate

Anhang A: Total Economic Impact

Der Total Economic Impact ist eine von Forrester Research entwickelte Methode, die die technologiebezogenen Entscheidungsprozesse eines Unternehmens optimiert und Anbieter bei der Kommunikation des Leistungsversprechens ihrer Produkte und Dienstleistungen gegenüber ihren Kunden unterstützt. Die TEI-Methode hilft Unternehmen, den konkreten Mehrwert von IT-Initiativen gegenüber der Geschäftsleitung und anderen wichtigen Stakeholdern zu belegen, zu rechtfertigen und zu veranschaulichen.

KONZEPT DES TOTAL ECONOMIC IMPACT

Nutzen stellt den Wert dar, der dem Unternehmen durch das betreffende Produkt entsteht. Bei der TEI-Methode werden der Nutzen und die Kosten gleich gewichtet. Dadurch wird eine umfassende Untersuchung der Effekte einer bestimmten Technologie auf das gesamte Unternehmen ermöglicht.

Kosten berücksichtigen alle Ausgaben, die zur Schaffung des angestrebten Mehrwerts oder Nutzens durch das betreffende Produkt erforderlich sind. Die Kostenkategorie innerhalb des TEI erfasst die über das gegenwärtige Geschäftsumfeld hinausgehenden Mehrkosten für die mit der Lösung verbundenen laufenden Kosten.

Flexibilität ist ein strategischer Wert, der bei zukünftigen Investitionen erzielt werden kann, sofern diese auf bereits getätigten Investitionen aufbauen. Die Möglichkeit, diesen Nutzen zu realisieren, stellt bereits einen Barwert dar, der prognostiziert werden kann.

Risiken messen die Unsicherheit von Nutzen- und Kostenschätzungen angesichts 1) der Wahrscheinlichkeit, dass die Schätzungen den ursprünglichen Prognosen entsprechen, und 2) der Wahrscheinlichkeit, dass die Schätzungen im Laufe der Zeit mit den tatsächlichen Werten abgeglichen werden. Die Risikofaktoren der TEI-Methode basieren auf einer „Dreiecksverteilung“.

Die Spalte mit den Anfangsinvestitionen enthält Kosten, die zum „Zeitpunkt 0“ oder zu Beginn von Jahr 1 anfallen und nicht abgezinst werden. Alle anderen Cashflows werden mit dem Kalkulationszinssatz zum Jahresende abgezinst. Für jede Gesamtkosten- und Gesamtnutzenschätzung werden Barwertberechnungen vorgenommen. Die Berechnungen des Kapitalwerts in den Übersichtstabellen entsprechen der Summe der Anfangsinvestition und des abgezinsten Cashflows für die einzelnen Jahre. Die Summen und Barwertberechnungen in den Tabellen für Gesamtnutzen, Gesamtkosten und Cashflow ergeben möglicherweise nicht den exakten Gesamtwert, da einige Beträge eventuell gerundet sind.

BARWERT

Der Barwert oder aktuelle Wert der (abgezinsten) Kosten- und Nutzenschätzungen zu einem gegebenen Zinssatz (dem Diskontierungssatz). Der Barwert für Kosten und Nutzen fließt in den Gesamtkapitalwert des Cashflows ein.

KAPITALWERT

Der Barwert oder aktuelle Wert des (abgezinsten) zukünftigen Nettocashflows zu einem gegebenen Zinssatz (dem Diskontierungssatz). Ein positiver Projektkapitalwert bedeutet in der Regel, dass die betreffende Investition vorgenommen werden sollte, sofern nicht andere Projekte höhere Kapitalwerte aufweisen.

RETURN ON INVESTMENT (ROI)

Die erwartete Rendite eines Projekts in Prozent. Zur Berechnung des ROI wird der Nettonutzen (Nutzen abzgl. Kosten) durch die Kosten dividiert.

DISKONTIERUNGSSATZ

Der in der Cashflowanalyse verwendete Zinssatz, mit dem der Zeitwert des Geldes berechnet wird. Unternehmen verwenden in der Regel Diskontierungssätze zwischen acht Prozent und 16 Prozent.

AMORTISATIONSZEITRAUM

Die Gewinnschwelle einer Investition. Dies ist der Zeitpunkt, an dem der Nettonutzen (Nutzen abzgl. Kosten) den Anfangsinvestitionen bzw. -kosten entspricht.

Anhang B: Ergänzendes Material

Themenverwandte Studien von Forrester

„The Future Of Cybersecurity and Privacy“, Forrester Research, Inc., 3. August 2023

„Top Cybersecurity Threats in 2023“, Forrester Research, Inc., 17. April 2023

„Introducing the Zero Trust Edge Architecture for Security and Network Services“, Forrester Research, Inc., 2. August 2023

Anhang C: Schlussbemerkungen


FORRESTER®