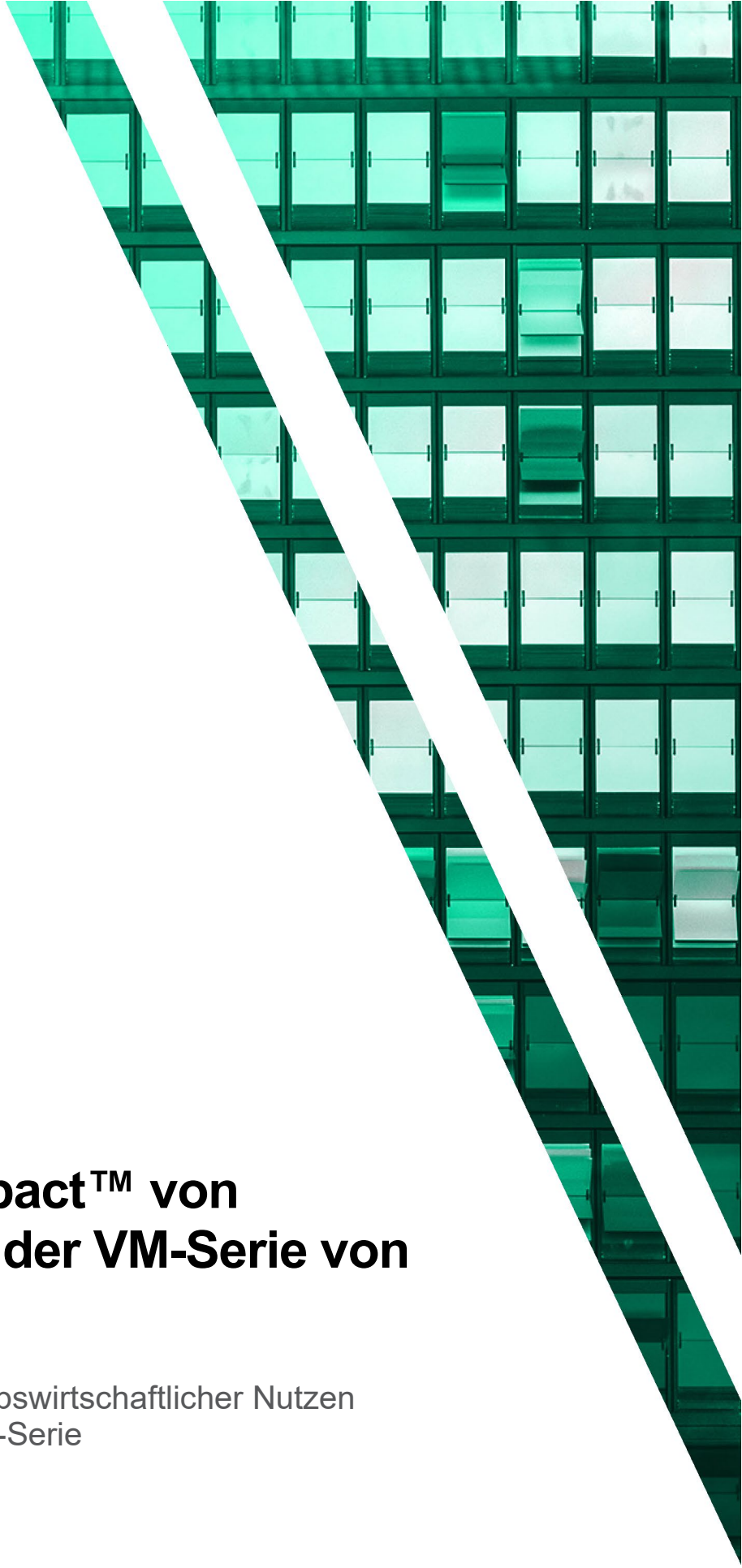
FORRESTER®



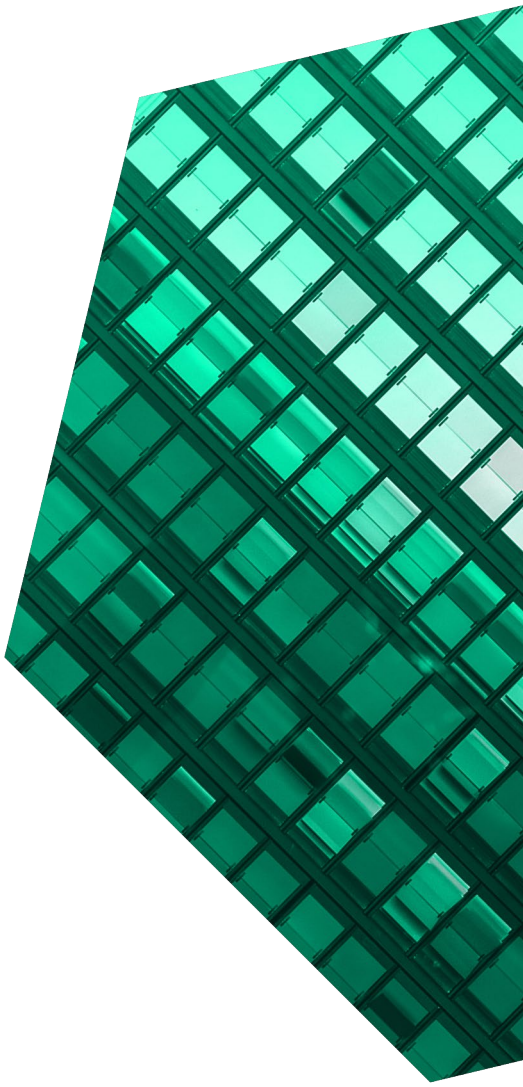
Total Economic Impact™ von virtuellen Firewalls der VM-Serie von Palo Alto Networks

Kosteneinsparungen und betriebswirtschaftlicher Nutzen durch virtuelle Firewalls der VM-Serie

SEPTEMBER 2021

Inhaltsverzeichnis

Beratungsteam: *Sam Conway*
Isabel Carey



INFORMATIONEN ZU FORRESTER CONSULTING

Forrester Consulting bietet unabhängige und objektive, forschungsbasierte Beratung, um Führungskräften in ihren Organisationen zum Erfolg zu verhelfen. Weitere Informationen erhalten Sie unter forrester.com/consulting.

Zusammenfassung

Unternehmen migrieren zunehmend in die Cloud und machen sich mit den Vorteilen von Hybrid-Cloud- und Multi-Cloud-Implementierungen vertraut. Daher müssen sich ihre Sicherheitsteams mit Schwachstellen und Netzwerkanforderungen neuen Typs auseinandersetzen. Firewalls gehören nach wie vor zu den zuverlässigsten Tools für Sicherheitsexperten, die für die On-Premises-Sicherheit sorgen. Gleichzeitig haben sich Next-Generation-Firewalls als Steuerungsebene für den Schutz von Datenpfaden in die verschiedenen Clouds etabliert. Die Firewalls der VM-Serie von Palo Alto Networks bieten flexible Sicherheitslösungen für agile

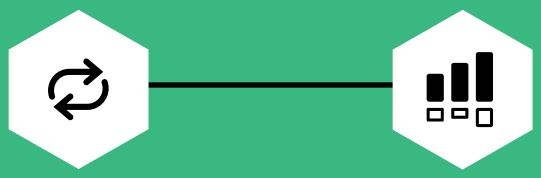
Palo Alto Networks beauftragte Forrester Consulting mit der Durchführung einer Studie zum Total Economic Impact™ (TEI) sowie mit der Untersuchung der potenziellen Kapitalrendite (ROI), die Unternehmen durch den Einsatz von virtuellen Firewalls der VM-Serie erzielen können.[1] Ziel dieser Studie ist es, den Lesern einen Bezugsrahmen zur Beurteilung der potenziellen finanziellen Auswirkungen von virtuellen Firewalls der VM-Serie von Palo Alto Networks auf ihr Unternehmen bereitzustellen.

Die Firewalls der VM-Serie von Palo Alto Networks bieten alle Funktionen der hardwarebasierten Next-Generation-Firewalls (NGFWs) von Palo Alto Networks, jedoch in Form von virtuellen Maschinen (VMs). Firewalls der VM-Serie umfassen ein breites Funktionsspektrum, um die aktuellen Herausforderungen an die Netzwerksicherheit in öffentlichen und privaten Clouds, virtualisierten Rechenzentren und softwaredefinierten Niederlassungen zu bewältigen. Unternehmen können ihre bestehenden Hardwareinfrastrukturen nutzen, um Firewalls zusammen mit anderen virtualisierten Netzwerken, Sicherheitsservices und sogar Anwendungen zu hosten.

Amortisierungsdauer:

< 6 Monate

WICHTIGE KENNZAHLEN



Kapitalrendite (ROI)
115 %

Kapitalwert (KW)
1,83 Mio. $

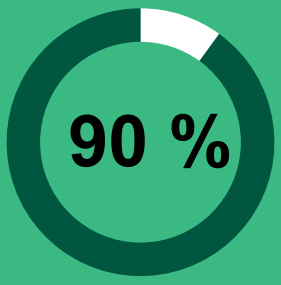
Um den Nutzen, die Kosten und die Risiken in Verbindung mit dieser Investition besser zu verstehen, befragte Forrester acht Entscheidungsträger und führte eine Umfrage mit 132 Entscheidungsträgern durch, die Erfahrung im Umgang mit virtuellen Firewalls hatten. Für diese Studie hat Forrester die Erfahrungen der befragten Personen aggregiert und die Ergebnisse in einem Modellunternehmen zusammengeführt.

Vor dem Einsatz virtueller Firewalls der VM-Serie setzten die befragten Unternehmen in erster Linie auf Hardware-Firewalls mit Punktlösungen. Als sie jedoch im Rahmen der digitalen Transformation größere Projekte in Angriff nahmen und sich auf eine unternehmensweite Virtualisierung zur Konsolidierung von Netzwerk- und Sicherheitsinfrastrukturen und öffentlichen Clouds zubewegten, erkannten sie, dass herkömmliche Firewalls nicht das benötigte Maß an Flexibilität boten. Die Unternehmen prüften, ob sie auf native Sicherheitsfunktionen von Cloud-Service-Anbietern hätten zurückgreifen können, stellten jedoch fest, dass diese nicht über die Fähigkeiten verfügten, die ein ausgereifter Sicherheitsanbieter wie Palo Alto Networks vermittelt. Ferner nutzten die Unternehmen im Schnitt vier öffentliche Clouds

und wollten ihre Sicherheits-Stacks nicht noch weiter verkomplizieren.

Nach der Investition in virtuelle Firewalls der VM-Serie bekamen die befragten Unternehmen die Sicherheitsprobleme ihrer Hybrid-Cloud- und Multi-Cloud-Umgebungen in den Griff. Ihre Sicherheitsteams konnten problemlos erweiterte Sicherheitskontrollen einrichten und konsistente Sicherheitsrichtlinien von einer zentralen Konsole aus definieren, durchsetzen und verwalten. Die erhöhte Transparenz gestattete eine präzise Steuerung des eingehenden, ausgehenden und internen Datenverkehrs (East-West-Traffic), wodurch die Angriffsflächen stark reduziert wurden. Dank des Formfaktors der VM-Serie konnten die Unternehmen außerdem die Implementierung und Bereitstellung von Firewalls flexibel automatisieren und bedarfsbasiert skalieren. So wurden Implementierungszeiten verkürzt und durch Überdimensionierung entstehende Kosten vermieden.

Verkürzung der Firewall-Implementierungs-zeit



WESENTLICHE ERGEBNISSE

Quantifizierter Nutzen. Der quantifizierte Nutzen, angegeben als risikobereinigter Barwert, umfasst Folgendes:

- **Verringerung des Zeitaufwands für die Implementierung von Firewalls um 90 % und Effizienzsteigerung bei den Netzwerk- und Sicherheitsteams um 80 %, wodurch innerhalb von drei Jahren 1,3 Mio. US-Dollar eingespart wurden.** Die Bereitstellung von Firewalls der VM-Serie nimmt deutlich weniger Zeit in Anspruch als bei herkömmlichen Firewalls, bei denen die Hardware angeliefert, installiert und konfiguriert werden muss. Darüber hinaus erkannten die befragten Unternehmen Effizienzgewinne durch die Konsolidierung der Firewall-Verwaltung in Palo Alto Networks Panorama (Tool zur zentralen Verwaltung der Netzwerksicherheit), die Pflege eines zentralen Richtliniensatzes für alle Clouds, das Zentralisieren von Patches und das Aufspielen von Upgrades.
- **Verringerung des Zeitaufwands für das Erreichen eines angemessenen Sicherheitsstatus um 30 %, wodurch innerhalb von drei Jahren 436.800 US-Dollar eingespart wurden.** Durch Nutzung der NGFWs von Palo Alto Networks und der über die Cloud implementierten Sicherheitsservices konnten die befragten Unternehmen ihre Sicherheitslösungen

Mit Palo Alto Networks konnten wir uns von verschiedenen Sicherheits- und Netzwerkkomponenten lösen und Sicherheit eher als Plattform betrachten. Es half uns, die Umgebung zu vereinfachen, und ermöglichte uns den Wechsel zur Cloud. Und genau deswegen haben wir uns am Ende für Palo Alto Networks entschieden. Die Alternative hätte darin bestanden, verschiedene Anbieter und Tools einzusetzen und diese dann zusammenzuführen.

– Global Head of IT Engineering, Getränkebranche

schneller einrichten und innerhalb von kürzerer Zeit einen stabilen Status erreichen. Dies verschaffte den Sicherheitsteams im Vergleich zum Einsatz von Punktlösungen einen Vorsprung bei der Optimierung der Lösung gemäß Zero-Trust-Standards.

- **Reduzierung der Sicherheitsvorfälle, die eine manuelle Untersuchung erforderten, um 18 % und Verkürzung der mittleren Lösungsdauer (Mean-Time-to-Resolution, MTTR) um 25 %, was Einsparungen von 240.100 US-Dollar über drei Jahre zur Folge hatte.** Durch den Einsatz der zentral verwalteten Firewalls der VM-Serie konnten die Fachkräfte für Netzwerksicherheit, IT und Security Operations (SecOps) zuvor manuell durchgeführte Prozesse automatisieren und den Einblick in den Netzwerk-Traffic verbessern. Dieses Mehr an Transparenz und die höhere Datenqualität führten zur schnelleren Lösung von Problemen.
- **Weniger Zwischenfälle und höhere Effizienz für die Endbenutzer, quantifiziert mit einem Mehrwert von 493.400 US-Dollar über drei Jahre.** Dank der besseren Bedrohungsabwehr und der geringeren Anzahl von Zwischenfällen mussten die Endbenutzer weniger Ausfallzeiten in Kauf nehmen und konnten sich auf ihre eigentlichen Aufgaben konzentrieren. Hierdurch entstand ein zusätzlicher Mehrwert für die Unternehmen der Befragten.
- **Senkung der Gesamtkosten für Sicherheits-Stacks durch Ausmusterung von Punktlösungen und vermiedene Überdimensionierung, wodurch innerhalb von drei Jahren fast 573.800 US-Dollar eingespart wurden.** Die Befragten gaben an, dass die Firewalls der VM-Serie es ihren Unternehmen ermöglichten, für ihre Multi-Cloud-Implementierungen ein konsistentes Toolset zu verwenden und die in der Cloud bereitgestellten Sicherheitsservices zu nutzen. So ließ sich ihrem Vernehmen nach der gesamte über Netzwerke oder Clouds laufende Traffic zuverlässig schützen und Punktlösungen konnten außer Betrieb gestellt werden. Darüber hinaus erzielten die Unternehmen durch die einfache Bereitstellung von Firewalls der VM-Serie ein Maß an Skalierbarkeit, das mit herkömmlichen Appliances nicht möglich gewesen wäre. Die Notwendigkeit einer Überdimensionierung aufgrund einer zu erwartenden Nutzungszunahme entfiel vollständig.

„Wenn Sie zwei verschiedene Firewall-Technologien verwalten, haben Sie beinahe den doppelten Aufwand.“
CISO, Hersteller medizinischer Geräte

Wir haben unsere Entscheidung für eine Investition in Palo Alto Networks mit Blick auf finanzielle Aspekte, die Sicherheit, mögliche Betriebskosteneinsparungen und den Funktionsumfang abgewogen … Wenn man Palo Alto Networks mit anderen Anbietern vergleicht, kann man nicht einfach die Preise gegeneinander aufrechnen.

– EVP of Engineering, IT-Dienstleistungen

- **Verringerung der Wahrscheinlichkeit einer Datenschutzverletzung um 20 % nach drei Jahren.** Mit Palo Alto Networks konnten die Unternehmen Zero-Trust-Sicherheitsmodelle implementieren und einheitliche Sicherheitsrichtlinien anwenden. Die VM-Serie ermöglichte es, die Angriffsflächen durch Segmentierung und Mikrosegmentierung, erweiterte Bedrohungsabwehr und Firewalls auf Anwendungsebene zu reduzieren.

Nicht quantifizierter Nutzen. Der für diese Studie nicht quantifizierte Nutzen umfasst die folgenden Elemente:

- **Ausnutzung bestehender Kompetenzen und dadurch Vermeidung von Schulungen und Neueinstellungen.** Die Unternehmen konnten die Firewalls der VM-Serie von Palo Alto Networks mit den vorhandenen Personalressourcen implementieren und verwalten. Da Palo Alto Networks zu den Branchenführern im Firewall-Bereich gehört, sind entsprechende Kompetenzen weit verbreitet, sodass keine zusätzlichen Ressourcen eingestellt und geschult werden müssen.
- **Steigerung von Skalierbarkeit und Flexibilität.** Dank der Ausführung als virtuelle Maschine lassen sich die Firewalls der VM-Serie bei Bedarf schnell einrichten oder auch entfernen. Dies gewährleistet, dass Unternehmen sich innerhalb kürzester Zeit an veränderte Anforderungen anpassen können und gleichzeitig die Kosten im Griff behalten.
- **Verbesserung der Wettbewerbsfähigkeit.** Einige der befragten Unternehmen sicherten sich dank Palo Alto Networks einen Wettbewerbsvorteil bei der Erbringung von Technologiedienstleistungen. Diese Unternehmen boten in der Cloud gehostete Services an und nutzten die mit der VM-Serie einhergehende Sicherheit als Alleinstellungsmerkmal, um Kunden zu gewinnen und zu binden.
- **Gewährleistung, dass Sicherheit kein Hindernis für die digitale Transformation darstellt.** Sicherheitsteams haben den Auftrag, den Betrieb so sicher wie möglich zu machen, sollten aber die digitale Transformation ihres Unternehmens nicht behindern. Die Firewalls der VM-Serie lassen sich im Handumdrehen implementieren, sodass der nötige Sicherheitsstatus schnell erreicht wird und das Unternehmen die Vorteile von Public-Cloud- und Hybrid-Cloud-Migrationen ausnutzen kann. Darüber hinaus konnten die Teams schnell auf neue Bedrohungsvektoren im Zuge der digitalen Transformation reagieren und Ressourcen am Netzwerk-Edge (z. B. Verkaufskioske) schützen.

Kosten. Die risikobereinigten barwertigen Kosten umfassen:

- **Firewall-Lizenzen in Höhe von insgesamt 1 Mio. US-Dollar über drei Jahre.** Die Unternehmen zahlten bislang jährliche Lizenzgebühren, um Firewalls der VM-Serie sowie über die Cloud erbrachte Sicherheitsservices (Cloud-Delivered Security Services, CDSS) nutzen zu können. Kürzlich jedoch hat Palo Alto Networks ein flexibles Verbrauchsmodell eingeführt, das eine dynamische Größenanpassung der Firewalls je nach aktuellem Bedarf und das Hinzufügen oder Ändern neuer CDSS-Optionen gestattet. Dieses flexible Preismodell (mit dem Kunden die Sicherheit besser an sich rasant ändernde Umstände anpassen können) soll sogar noch mehr Kosteneffizienz bieten als die jährlichen Lizenzgebühren, die Forrester für das Modellunternehmen errechnet hat.
- **Interner Bereitstellungsaufwand in Höhe von insgesamt 4.900 US-Dollar über drei Jahre.** Die Befragten gaben an, dass die Einrichtung von Firewalls der VM-Serie Zeit und Aufwand erforderte und weitere Firewalls in den Folgejahren installiert wurden.
- **Laufende Verwaltungskosten in Höhe von insgesamt knapp 441.000 US-Dollar über drei Jahre.** Die Befragten gaben an, dass in ihren Unternehmen interne Arbeitskosten für die laufende Verwaltung implementierter Firewalls der VM-Serie anfielen. Dies umfasste Kosten für Anpassungen, Aktualisierungen und das Einführen neuer Richtlinien.

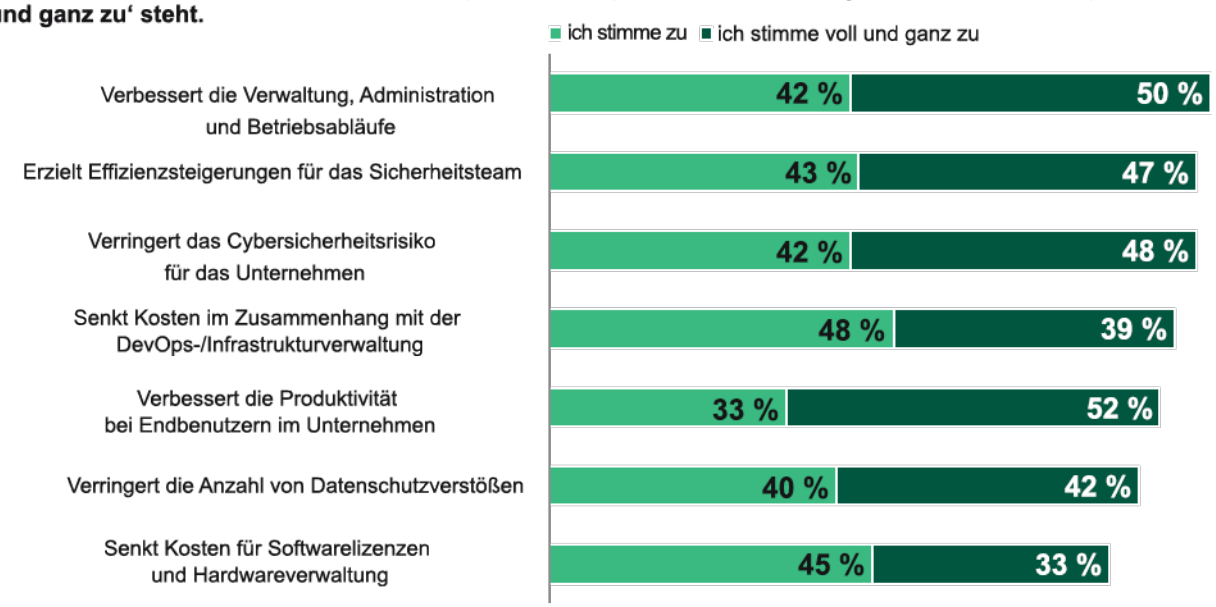
- **Kosten für Whitebox-Appliances in Höhe von 151.000 US-Dollar über drei Jahre.** Die Unternehmen implementierten ihre Firewalls der VM-Serie auf Standardhardware, weswegen gewisse zusätzliche Kosten für neue Appliances anfielen.

Geringere Wahrscheinlichkeit von Datenschutzverstößen

20 % Reduzierung bis Jahr 3

Die Kundenbefragungen und die Finanzanalyse ergaben, dass ein Modellunternehmen über einen Zeitraum von drei Jahren einen Nutzen von 3,43 Mio. US-Dollar gegenüber Kosten von 1,6 Mio. US-Dollar erzielt, was einen Kapitalwert (KW) von 1,83 Mio. US-Dollar und einen ROI von 115 % ergibt.

Abbildung 1: „Inwiefern stimmen Sie zu, dass die virtuellen Firewalls der VM-Serie von Palo Alto Networks (auch im gemeinsamen Einsatz mit einem beliebigen Sicherheitsservice) folgende Eigenschaften aufweisen? Verwenden Sie für Ihre Antwort eine Skala von 1 bis 5, wobei 1 für ‚ich stimme überhaupt nicht zu' und 5 für ‚ich stimme voll und ganz zu' steht.



Basis: 132 Entscheidungsträger aus dem Bereich Cloud-Sicherheit
Quelle: Studie im Auftrag von Palo Alto Networks, vorgelegt im Juni 2021 von Forrester Consulting

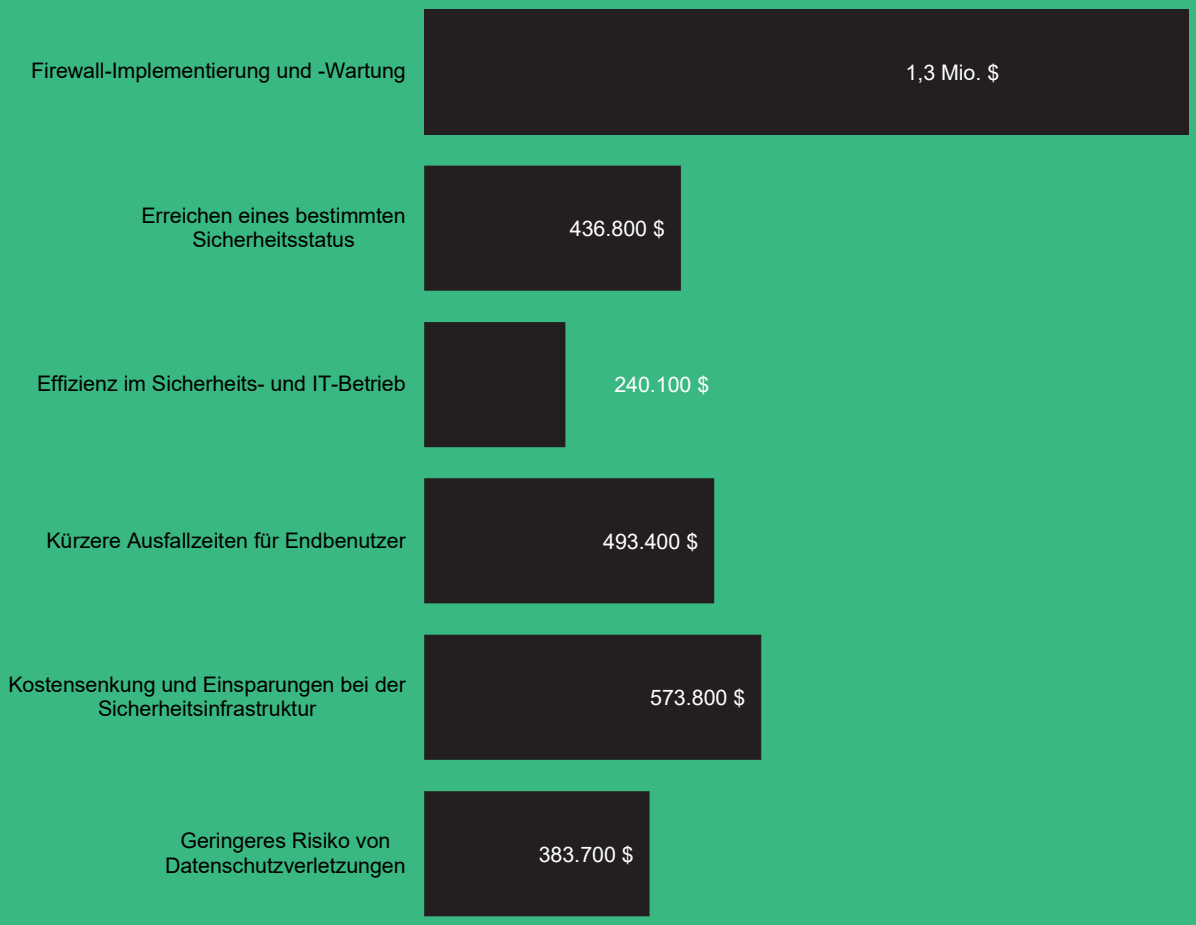
ROI
115 %

NUTZEN (BW)
3,43 Mio. $

KAPITALWERT
1,83 Mio. $

AMORTISIERUNG
< 6 Monate

Nutzen (über drei Jahre)



TEI-BEZUGSRAHMEN UND -METHODIK

Aus den in der Befragung erfassten Daten hat Forrester einen Bezugsrahmen zum Total Economic Impact™ für Unternehmen erstellt, die eine Investition in virtuelle Firewalls der VM-Serie von Palo Alto Networks in Erwägung ziehen.

Dieser Bezugsrahmen dient dazu, Kosten, Nutzen, Flexibilität und Risikofaktoren zu ermitteln, die für die Investitionsentscheidung von Bedeutung sind. Forrester verwendete ein mehrere Schritte umfassendes Verfahren, um die Auswirkungen zu bewerten, die virtuelle Firewalls der VM-Serie von Palo Alto Networks in einem Unternehmen haben können.

Forrester Consulting führte eine Onlineumfrage mit 351 Führungskräften im Bereich Cybersicherheit in globalen Unternehmen in den USA, Großbritannien, Kanada, Deutschland und Australien durch. Zu den Umfrageteilnehmern gehörten Manager, Abteilungsleiter, Vice Presidents und Führungskräfte auf Leitungsebene, die für Entscheidungen, Betrieb und Berichterstattung im Bereich Cybersicherheit verantwortlich sind. Die Fragen an die Teilnehmer zielten darauf ab, die Cybersicherheitsstrategien der Führungskräfte und etwaige Sicherheitslücken in ihren Organisationen zu bewerten. Die Befragten nahmen an der Umfrage über ein externes Forschungspanel teil, das die Umfrage im November 2020 im Auftrag von Forrester durchführte.

OFFENLEGUNGEN

Die Leser werden auf Folgendes hingewiesen:

Diese Studie wurde von Palo Alto Networks in Auftrag gegeben und von Forrester Consulting vorgelegt. Sie ist nicht als Wettbewerbsanalyse zu verstehen.

Forrester äußert hierin keine Vermutungen über den potenziellen ROI, den andere Unternehmen erzielen werden. Forrester empfiehlt den Lesern dringend, mithilfe des in der Studie dargelegten Bezugsrahmens eigene Prognosen zu erstellen, um die Angemessenheit einer Investition in virtuelle Firewalls der VM-Serie zu ermitteln.

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

Palo Alto Networks stellte die Kundennamen für die Befragungen bereit, nahm an den Befragungen jedoch nicht teil.

SORGFALTSPFLICHT

Es wurden Vertreter von Palo Alto Networks sowie Forrester-Analysten befragt, um Daten zu virtuellen Firewalls der VM-Serie zu erheben.

KUNDENBEFRAGUNGEN

Um Informationen zu Kosten, Nutzen und Risiken zu sammeln, wurden Interviews mit acht Entscheidungsträgern geführt und weitere 132 Entscheidungsträger befragt, deren Unternehmen virtuelle Firewalls der VM-Serie nutzen.

MODELLUNTERNEHMEN

Es wurde ein Modellunternehmen basierend auf den Eigenschaften der Unternehmen der Befragten erstellt.

FINANZMODELLRAHMEN

Auf der Grundlage der Themen und Belange der Entscheidungsträger wurde mithilfe der TEI-Methodik ein für die Befragungen repräsentatives Finanzmodell erstellt und risikobereinigt.

FALLSTUDIE

Vier fundamentale Elemente von TEI bilden die Grundlage für die Modellierung der Investitionsauswirkungen: Nutzen, Kosten, Flexibilität und Risiken. Dank der zunehmend ausgereiften Lösungen für ROI-Analysen in Bezug auf IT-Investitionen liefert die TEI-Methodik von Forrester ein umfassendes Bild der finanziellen Gesamtauswirkung von Kaufentscheidungen. Weitere Informationen zur TEI-Methodik finden Sie in Anhang A.

Customer Journey bei virtuellen Firewalls der VM-Serie von Palo Alto Networks

Beweggründe für die Investition in virtuelle Firewalls der VM-Serie

Befragte Entscheidungsträger

Befragte Person	Branche	Region	Umsatz
Lead Architect	IT-Services	Europa	80 Mio. $
Leitende Fachkraft aus der Netzwerktechnik	IT-Services	Europa	80 Mio. $
Network Engineer	Kommunikationsinfrastruktur	USA	6 Mrd. $
EVP of Engineering	IT-Services	USA	k. A.
Global Head of IT Engineering	Getränkeindustrie	Weltweit	37 Mrd. $
Information Security Engineer	Geschäftsdienstleistungen	Nordamerika	3 Mrd. $
Senior Security Engineer	Geschäftsdienstleistungen	Nordamerika	3 Mrd. $
CISO	Medizinische Geräte	Nordamerika	800 Mio. $

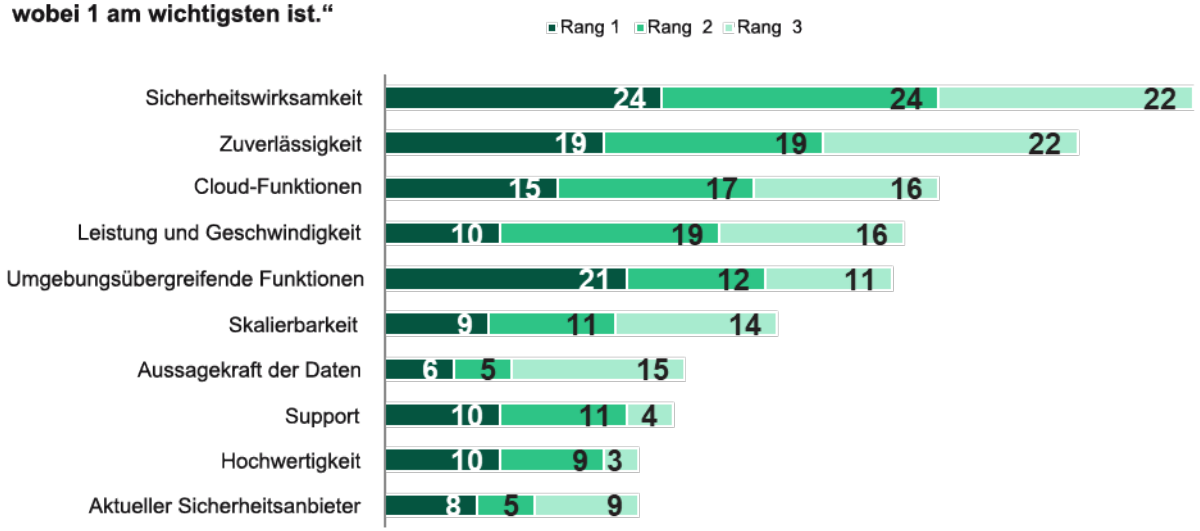
ZENTRALE HERAUSFORDERUNGEN

Die Befragten sprachen über die typischen Herausforderungen, mit denen ihr Unternehmen zu kämpfen hatte:

- **Leistungsschwache herkömmliche Punktlösungen.** Die Befragten gaben an, dass zuvor eingesetzte Punktlösungen die Erwartungen in Bezug auf Geschwindigkeit, Leistung und anbieterseitigen Kundensupport nicht erfüllen konnten. Upgrades solcher Produkte benötigten viel Zeit und einen erheblichen internen Aufwand für Bereitstellung und Wartung.
- **Dezentralisierte Sicherheitsplattformen und -funktionen.** Vor dem Einsatz von Firewalls der VM-Serie verzeichneten die befragten Unternehmen Probleme mit der Verwaltung dezentraler Sicherheitstools, was Transparenzlücken und redundante Arbeiten zur Folge hatte. Beispielsweise mussten Unternehmen, die mehrere Clouds nutzten, bei der Verwendung nativer Tools mehrere Versionen derselben Richtlinien entwickeln und implementieren.
- **Organisatorische Vorgaben für die Cloud-Migration.** Viele der Unternehmen arbeiteten in Umgebungen mit strikten Zeitvorgaben für Cloud-Migrationen. Sie benötigten daher

„Als wir uns von unserer Muttergesellschaft trennten, stand uns gerade einmal ein verlängertes Wochenende von vier Tagen zur Verfügung, um die Trennung lokal umzusetzen. Also richteten wir alles parallel ein, um den Schnitt in so kurzer Zeit machen zu können – auch die neuen Firewall-Systeme X, Y und Z. Für uns war vor allem wichtig, mit der Umstrukturierung voranzukommen.“
CISO, Hersteller medizinischer Geräte

Abbildung 2: „Wählen Sie aus der folgenden Liste die drei wichtigsten Kriterien für die Auswahl eines Netzwerksicherheitsanbieters aus und ordnen Sie diese in der Reihenfolge ihrer Wichtigkeit von 1 bis 3, wobei 1 am wichtigsten ist.“



Basis: Entscheidungsträger in unterschiedlicher Zahl aus dem Bereich Cloud-Sicherheit
Quelle: Studie im Auftrag von Palo Alto Networks, vorgelegt im Juni 2021 von Forrester Consulting

Sicherheitslösungen, die sich schnell implementieren ließen und zudem einen angemessenen Einblick erlaubten, um ihre neuen Cloud-Implementierungen zuverlässig schützen zu können.

WARUM PALO ALTO NETWORKS?

Die befragten Unternehmen evaluierten mehrere Lösungen, bevor sie sich am Ende für die virtuellen Firewalls der VM-Serie entschieden. Die folgenden zentralen Funktionen spielten bei den Investitionen eine wichtige Rolle:

- **Layer-7-Transparenz.** Die Firewalls der VM-Serie bieten portübergreifende Transparenz in der Anwendungsschicht und liefern für Richtlinienentscheidungen relevante Daten.
- **Anwendungssegmentierung.** Unternehmen können Firewalls der VM-Serie zur Segmentierung und Steuerung der Anwendungskommunikation einsetzen. Hinzu kommt eine fortschrittliche Bedrohungsabwehr, die laterale Bedrohungen für das Netzwerk erkennt und blockiert.
- **Fortschrittliche Sicherheit mit CDSS.** Sicherheitsabonnements von Palo Alto Networks können für die VM-Serie aktiviert werden, ohne zusätzliche Sensoren oder Appliances installieren oder implementieren zu müssen. Dadurch profitieren Unternehmen von zusätzlichem Schutz durch Services wie fortschrittliche IPS (Intrusion Prevention Systems), Sicherheit für DNS (Domain Name System), URL-Filter und Schutz vor Zero-Day-Bedrohungen sowie Sandboxing ohne zusätzlichen Overhead.
- **Benutzerbasierte Richtlinien.** Die Firewalls der VM-Serie bieten von Haus aus benutzerbasierte Richtlinien und sind mit einer großen Zahl von

„Eine der Eigenschaften, die Palo Alto in Sachen Sicherheit mitbringt, ist die zielgerichtete Wirkung. Basis der gesamten Lösung sind Identität sowie die Fähigkeit, Sicherheitsfunktionen in Echtzeit zu aktualisieren.“
Global Head of IT Engineering, Getränkebranche

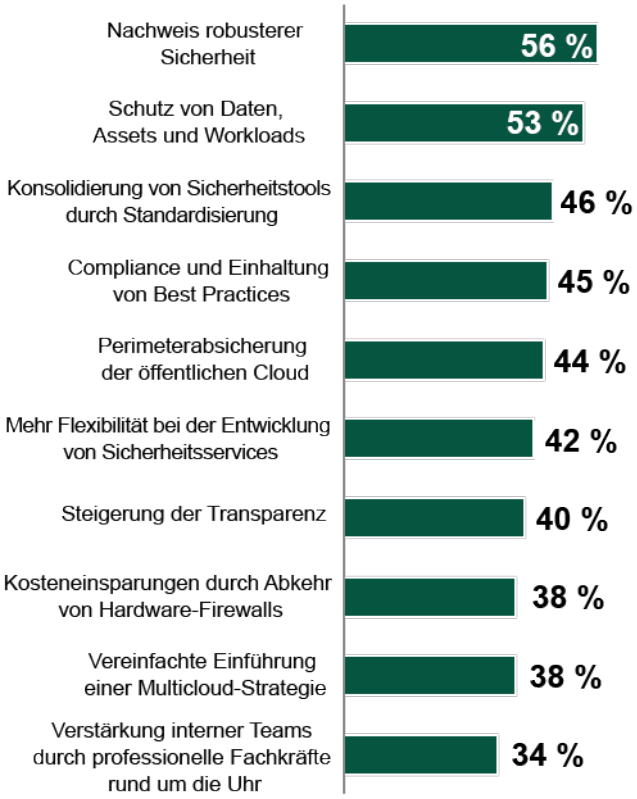
Benutzer-Repositorys integriert. Dies ermöglicht die Einrichtung dynamischer benutzerbasierter Richtlinien für die Zugriffssteuerung zusätzlich zu den anwendungsbasierten Richtlinien.

- **Zentralisierte Verwaltung für einheitliche Richtlinien und vereinfachte Verwaltung.** Die Firewalls der VM-Serie lassen sich zentral über Panorama verwalten, wodurch die übergreifende Richtlinienkonsistenz in vielen Cloud- und On-Premises-Bereitstellungen gewährleistet wird. Dank Panorama müssen Betreiber ihre Netzwerksicherheitsmaßnahmen nicht mehr über mehrere getrennte Konsolen verwalten.
- **Automatisierte Bereitstellung und Richtlinienaktualisierung.** Unternehmen können die Funktionen der VM-Serie nutzen, um Sicherheit in die Arbeitsabläufe der Anwendungsentwicklung zu integrieren. Dies umfasst etwa automatische Bereitstellungen und Richtlinien-Updates, den Einsatz nativer Vorlagen für bestimmte Cloud-Provider sowie die cloudnative Skalierbarkeit.

Grundlegende Annahmen

- **3 Mrd. $ Umsatz**
- **ansässig in den USA**
- **anfänglich 100 Firewalls der VM-Serie**
- **7.500 Angestellte**
- **12 SecOps-VZÄ**
- **8 NetOps-VZÄ**

Abbildung 3: „Welche Faktoren waren ausschlaggebend für die Entscheidung, in virtuelle Firewalls der VM-Serie von Palo Alto Networks zu investieren?“



Basis: 132 Entscheidungsträger aus dem Bereich Cloud-Sicherheit
Quelle: Studie im Auftrag von Palo Alto Networks, vorgelegt im Juni 2021 von Forrester Consulting

MODELLUNTERNEHMEN

Basierend auf den Befragungen hat Forrester einen TEI-Bezugsrahmen, ein Modellunternehmen und eine ROI-Analyse für die Bereiche erstellt, in denen finanzielle Auswirkungen zutage treten. Das Modellunternehmen ist repräsentativ für die acht von Forrester interviewten Entscheidungsträger sowie die 132 an der Umfrage beteiligten Unternehmen und dient zur Darstellung der zusammengefassten Finanzanalyse im nächsten Abschnitt. Die Eigenschaften des Modellunternehmens sind nachfolgend aufgelistet:

Beschreibung des Modellunternehmens. Das Modellunternehmen ist ein dezentral operierendes Unternehmen mit einem Jahresumsatz von 3 Mrd. US-Dollar und 7.500 Angestellten. Es hat seinen Sitz in den USA und ist weltweit tätig. Das Sicherheitsteam des Unternehmens bearbeitet 154 Zwischenfälle (Incidents) pro Woche.

Beschreibung des Smartsheet-Rollouts. Mithilfe von Firewalls der VM-Serie sichert das Modellunternehmen sowohl North-South- als auch East-West-Traffic übergreifend für mehrere Cloud-Bereitstellungen ab. Das

Unternehmen implementiert 156 virtuelle Firewalls bis zum Jahr 3. Diese werden auf Standard-Appliances bereitgestellt. Die Verwaltung der Firewalls der VM-Serie erfolgt mit Panorama. Palo Alto Networks CDSS erweitert jede NGFW-Implementierung um Inline-Schutz vor bekannten und unbekannten Bedrohungen (mittels Palo Alto Networks Threat Prevention und WildFire-Malware-Analyse) sowie vor sämtlichen Bedrohungen aus dem Internet (mittels Palo Alto Networks URL Filtering und DNS Security). Dies umfasst auch die Command-and-Control-Abwehr und den Schutz vor Datenverlust (Data Loss Prevention, DLP).

Nutzenanalyse

Daten zum quantifizierten Nutzen, angewendet auf das Modellunternehmen

Gesamtnutzen						
Ref.	**Nutzen**	**1. Jahr**	**2. Jahr**	**3. Jahr**	**Gesamtwert**	**Barwert**
Atr	Firewall-Implementierung und -Wartung	531.498 $	517.624 $	518.780 $	1.567.902 $	1.300.736 $
Btr	Erreichen eines bestimmten Sicherheitsstatus	381.758 $	56.858 $	56.858 $	495.473 $	436.760 $
Ctr	Effizienz im Sicherheits- und IT-Betrieb	96.562 $	96.562 $	96.562 $	289.686 $	240.136 $
Dtr	Kürzere Ausfallzeiten für Endbenutzer	198.398 $	198.398 $	198.398 $	595.195 $	493.387 $
Etr	Kostensenkung und Einsparungen bei der Sicherheitsinfrastruktur	240.996 $	224.121 $	225.527 $	690.645 $	573.754 $
Ftr	Geringeres Risiko von Datenschutzverletzungen	105.083 $	157.624 $	210.166 $	472.873 $	383.699 $
	Gesamtnutzen (risikobereinigt)	1.554.294 $	1.251.188 $	1.306.291 $	4.111.774 $	3.428.472 $

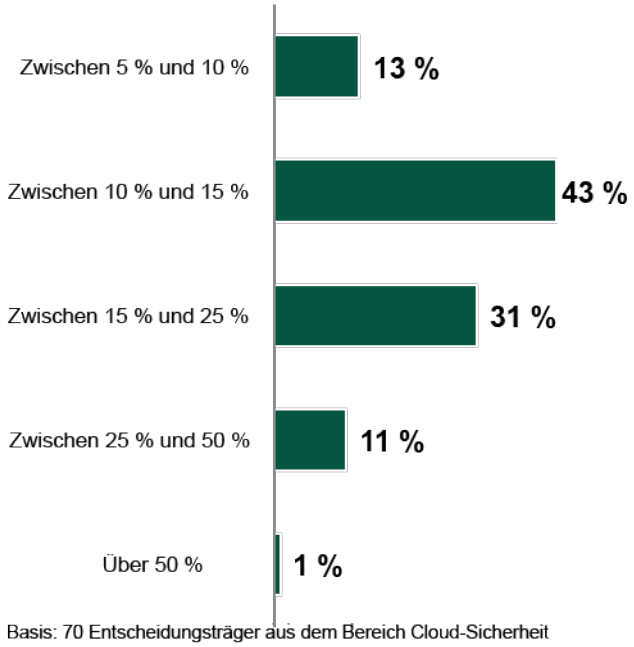
FIREWALL-IMPLEMENTIERUNG UND -WARTUNG

Daten und Fakten. Die Befragten gaben an, dass Bereitstellung und Wartung von Firewalls der VM-Serie dank ihres virtuellen Formfaktors weit weniger Zeit erfordern als bei traditionellen Lösungen. Zuvor verwendeten ihre Unternehmen vorwiegend herkömmliche physische Geräte, deren Installation und Konfiguration manuelle Arbeit erforderlich machten und die zudem lange Lieferzeiten aufwiesen. Befragte aus Unternehmen, die native Lösungen von Cloud-Service-Anbietern verwendet hatten, betonten die Möglichkeit, Implementierungen der VM-Serie über Panorama zu verwalten. Dies ermöglichte eine erhebliche Zeitersparnis und die Schaffung eines einheitlichen Richtlinienmodells für lokale und cloudbasierte Implementierungen.

- Ein Network Engineer bei einem Unternehmen für Kommunikationsinfrastruktur sagte: „Nachdem wir alle Geräte ausgemustert hatten, waren die Supportkosten auf einmal viel niedriger. Außerdem entfielen Arbeitszeiten für Aufstellung, Inbetriebnahme und Konfiguration dieser Hardware. Die erzielten Einsparungen waren daher beträchtlich. Wenn eine unserer alten Firewalls beispielsweise auf einer nicht ausreichend dimensionierten Appliance implementiert war, dann mussten wir eine andere – größere – Appliance kaufen. Bei den virtuellen Firewalls der VM-Serie hingegen holt man sich einfach nur eine andere Lizenz und schon passt die Dimensionierung.“
- Ein EVP of Engineering bei einem IT-Dienstleistungsunternehmen meinte: „Wenn Sie Sicherheitsservices implementieren und eine Firewall betreiben, dann hat Sicherheit höchste Priorität, nicht wahr? Daher ist die Anzahl der für die Aktualisierung einzelner Firewalls erforderlichen Arbeitsstunden beim Einsatz mehrerer Lösungen schlicht untragbar. In der Vergangenheit haben wir, wenn etwas implementiert werden musste, allein für Inbetriebnahme, Netzwerkkonfiguration und Einrichtung zwei bis drei Stunden pro Firewall gebraucht. Und da waren noch keine Regelwerke, Optimierungen usw. dabei. Jetzt ist das alles in kaum zehn Minuten erledigt und unser Implementierungsteam kann zudem mehrere Firewalls gleichzeitig konfigurieren. Wir brauchen also nicht mehr zwei oder drei Stunden pro Firewall, sondern nur noch maximal zehn Minuten – bei mehreren Firewalls parallel. So konnten wir die Implementierungsfähigkeit massiv erweitern.“

- Ein Global Head of Engineering bei einem Getränkeunternehmen erklärte: „Die virtuellen Firewalls der VM-Serie nutzen Vorlagen und Schablonen. Wenn die erst einmal vorhanden sind, kann man eine Menge automatisieren. Meiner Einschätzung nach konnten wir Kosten und Aufwand für Bereitstellung und Konfiguration um mindestens 90 % senken.“
- Derselbe Befragte beschrieb auch die mühsame Inbetriebnahme einer herkömmlichen Lösung: „Wenn man die Kosten für den Versand der physischen Komponenten, die Verzögerungen bei der Geräteauslieferung und die Rackmontage mit einbezieht, dann ist der Zeitverlust, bis die Firewall überhaupt in Betrieb genommen werden kann, schon immens.“
- 92 % der Befragten gaben an, dass virtuelle Firewalls der VM-Serie (und Sicherheitsservices) den Verwaltungs-, Administrations- und Betriebsaufwand in ihrem Unternehmen im Bereich Cybersicherheit reduziert haben (Abbildung 1). Nach Angaben von 58 % dieser Befragten profitierten die jeweiligen Unternehmen von einer schnelleren Bereitstellung der Sicherheitslösungen von Palo Alto Networks, die keine physischen Firewalls sind, und 57 % gaben an, dass Implementierung und Konfiguration von Sicherheitsrichtlinien in ihrem Unternehmen beschleunigt wurden (Abbildung 4).

Abbildung 4: „Sie haben angegeben, dass die virtuellen Firewalls der VM-Serie von Palo Alto Networks (auch im gemeinsamen Einsatz mit einem beliebigen Sicherheitsservice) eine schnellere Sicherheitsimplementierung gestatten. Wie hoch (in %) schätzen Sie die Verbesserung im Vergleich zu Ihrer vorherigen Umgebung ein?“



Basis: 70 Entscheidungsträger aus dem Bereich Cloud-Sicherheit
Quelle: Studie im Auftrag von Palo Alto Networks, vorgelegt im Juni 2021 von Forrester Consulting

Modellerstellung und Annahmen. Forrester nimmt für das Modellunternehmen Folgendes an:

- Das Unternehmen implementiert im ersten Jahr 100 Firewalls der VM-Serie.
- Aufgrund steigender Anforderungen nimmt dieser Bestand pro Jahr um 25 % zu.
- Bei herkömmlichen Lösungen nahm die vollständige Implementierung und Konfiguration 5 Stunden in Anspruch.
- Ein Team von zehn Angestellten war für die Verwaltung der Altlösung zuständig, d. h. für die Lösungsinstallation, die Verwaltung der Sicherheitsrichtlinien und das Aufspielen von Updates und Infrastruktur-Patches. Diese Ressourcen widmeten 75 % ihrer Zeit ausschließlich den Firewalls.
- Das durchschnittliche Jahresgehalt der für die Verwaltung der Altlösung zuständigen Angestellten liegt bei 112.500 US-Dollar.
- Firewalls der VM-Serie erfordern 90 % weniger Aufwand für die virtuelle Bereitstellung. Zudem steigerte das Firewall-Team seine Effizienz dank zentraler Richtliniensteuerung, automatischer Updates, Patching und entfallener Montagearbeiten um 80 %.
- 80 % der eingesparten Zeit werden wieder in produktive Arbeit umgesetzt.

Risiken. Folgende Risiken können sich auf die Realisierung dieser Vorteile auswirken:

- Größe und Qualifikation des Sicherheitsmanagementteams im Unternehmen.

- Bereits vor Implementierung der virtuellen Firewalls der VM-Serie vorhandene Kompetenzen und Systeme.
- Durchschnittsgehälter von Teammitgliedern in den Bereichen Netzwerk, Sicherheit und IT-Betrieb.

Ergebnisse. Zur Berücksichtigung dieser Risiken hat Forrester diesen Nutzen um 5 % nach unten korrigiert, was über drei Jahre einen risikobereinigten (mit 10 % diskontierten) Gesamtbarwert von 1,3 Mio. US-Dollar ergibt.

Firewall-Implementierung und -Wartung

Ref.	Messgröße	Quelle	1. Jahr	2. Jahr	3. Jahr
A1	Neu in Betrieb genommene Firewalls (netto)	Modellunternehmen	100	25	31
A2	Für die Inbetriebnahme von herkömmlichen Firewalls erforderliche Zeit (Stunden)	Befragungen	5	5	5
A3	Zeitersparnis bei der Inbetriebnahme einer Firewall der VM-Serie	Befragungen	90 %	90 %	90 %
A4	Gesamtzeitersparnis bei der Inbetriebnahme pro Jahr (Stunden)	A1*A2*A3	450	113	141
A5	Erforderliche VZÄ im Firewall-Team	Modellunternehmen	10	10	10
A6	Anteil der für Firewalls aufgewendeten Arbeitszeit	Annahme	75 %	75 %	75 %
A7	Verbesserungen bei Firewall-Sicherheit und Netzwerkmanagement (z. B. zentrale Steuerung, einheitliche Richtlinien, Montage, Routing und Patching)	Befragungen	80 %	80 %	80 %
A8	Zeitersparnis bei der Verwaltung (Stunden)	A5*2.080 Stunden*A6*A7	12.480	12.480	12.480
A9	Produktivitätsrückgewinnung	Annahme	80 %	80 %	80 %
A10	Durchschnittlicher Stundensatz eines IT-Teammitglieds (NetOps, SecOps, IT-Betrieb)	Annahme	54 $	54 $	54 $
At	Firewall-Implementierung und -Wartung	(A4+A8)*A9*A10	559.471 $	544.868 $	546.085 $
	Risikobereinigung	↓5 %			
Atr	Firewall-Implementierung und -Wartung (risikobereinigt)		538.498 $	517.624 $	518.780 $
	Dreijahresgesamtwert: 1.567.902 $		**Dreijahresbarwert: 1.300.736 $**		

ERREICHEN EINES BESTIMMTEN SICHERHEITSSTATUS

Daten und Fakten. Nach Angaben der Befragten erreichten ihre Unternehmen dank der konsistenten Technologie, einheitlichen Plattform und erweiterten Verwaltungsmöglichkeiten von Palo Alto Networks schneller einen stabilen Zustand. Sie konnten ihre Sicherheits-Stacks schneller bereitstellen, den Implementierungsaufwand senken und mit ihren Sicherheitsteams eher zur Feinabstimmung übergehen als beim Einsatz von Punktlösungen.

Mit Palo Alto Networks konnten die Unternehmen alle Komponenten auf einer gemeinsamen Plattform integrieren und ein weitgehend einheitliches Erscheinungsbild schaffen. Dies beschleunigte die Implementierung und schuf zeitliche Kapazitäten für die Feinabstimmung der Lösung, die Implementierung automatisierter Arbeitsabläufe und die Suche nach Möglichkeiten zur Effizienzsteigerung für Sicherheits-, IT- und Geschäftsanwender.

Modellerstellung und Annahmen. Forrester nimmt für das Modellunternehmen Folgendes an:

- Das Unternehmen setzt in beiden Szenarien dasselbe Implementierungsteam ein. Dieses umfasst im ersten

Jahr der Implementierung zwölf SecOps-Mitarbeiter und acht NetOps-Mitarbeiter.

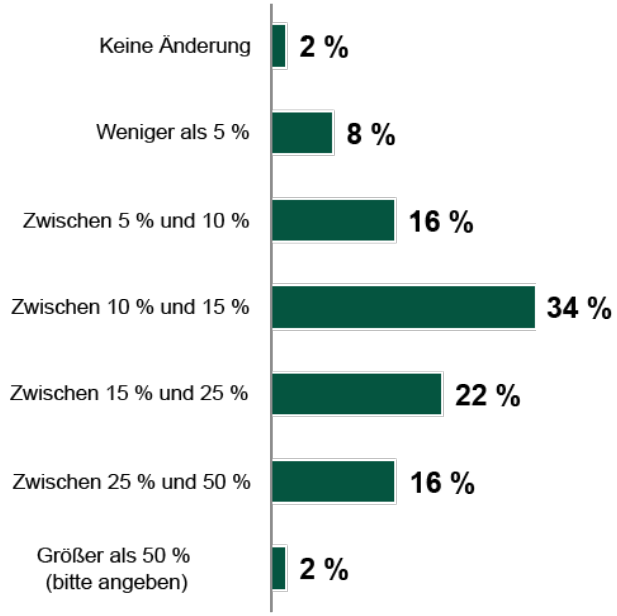
- Das durchschnittliche Jahresgehalt eines SecOps-Mitarbeiters (inkl. Nebenkosten) beträgt 121.500 US-Dollar.
- Das durchschnittliche Jahresgehalt eines NetOps-Mitarbeiters (inkl. Nebenkosten) beträgt 135.000 US-Dollar.
- Mit Palo Alto Networks erzielt das Unternehmen einen stabilen Sicherheitsstatus um 30 % schneller als mit Punktlösungen, d. h., der zeitliche Bedarf reduziert sich von 6,3 auf 4,4 Monate.

Risiken. Folgende Risiken können sich auf die Realisierung dieser Vorteile auswirken:

- Größe des Implementierungsteams und jeweilige Gehälter
- Konkret implementierte Komponenten und die zum Erreichen eines stabilen Status erforderliche Zeit

Ergebnisse. Zur Berücksichtigung dieser Risiken hat Forrester diesen Nutzen um 5 % nach unten bereinigt, was über drei Jahre einen risikobereinigten Gesamtbarwert von 436.800 US-Dollar ergibt.

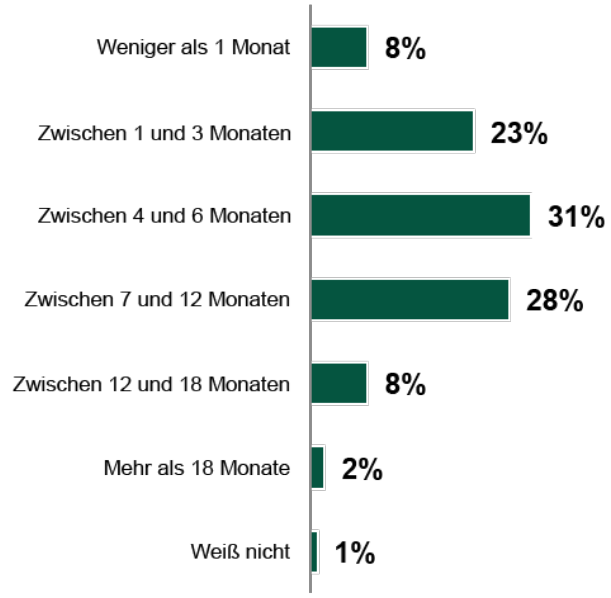
Abbildung 5: „Sie haben angegeben, dass Sie dank der virtuellen Firewalls der VM-Serie von Palo Alto Networks (auch im gemeinsamen Einsatz mit einem beliebigen Sicherheitsservice) bei Audits schneller Informationen erhalten. Wie hoch (in %) schätzen Sie die Verbesserung im Vergleich zu Ihrer vorherigen Umgebung ein?“



Basis: 50 Entscheidungsträger aus dem Bereich Cloud-Sicherheit

Quelle: „PAN Virtual Firewalls TEI“, Studie im Auftrag von Palo Alto Networks, vorgelegt im Juni 2021 von Forrester Consulting

Abbildung 6: „Sie haben angegeben, dass die virtuellen Firewalls der VM-Serie von Palo Alto Networks (auch im gemeinsamen Einsatz mit einem beliebigen Sicherheitsservice) das Cybersecurity-Risiko Ihres Unternehmens gesenkt haben. Können Sie abschätzen, wie lange Ihr Unternehmen zuvor beim Einsatz von Punktlösungen gebraucht hat, um einen ‚stabilen Sicherheitsstatus‘ zu erreichen?“



Basis: 119 Entscheidungsträger aus dem Bereich Cloud-Sicherheit

Quelle: „PAN Virtual Firewalls TEI“, Studie im Auftrag von Palo Alto Networks, vorgelegt im Juni 2021 von Forrester Consulting

Erreichen eines bestimmten Sicherheitsstatus					
Ref.	**Messgröße**	**Quelle**	**1. Jahr**	**2. Jahr**	**3. Jahr**
B1	SecOps-VZÄ, Jahresgehalt inkl. Sozialleistungen	Annahme	121.500 $	121.500 $	121.500 $
B2	NetOps-VZÄ, Jahresgehalt inkl. Sozialleistungen	Annahme	135.000 $	135.000 $	135.000 $
B3	Erforderliche SecOps-VZÄ	Modellunternehmen	12	2	2
B4	Erforderliche NetOps-VZÄ	Modellunternehmen	8	1	1
B5	Erforderliche Zeit bis zum Erreichen eines angemessenen Sicherheitsstatus mit Punktlösungen (Monate)	Umfrageergebnisse	6,3	6,3	6,3
B6	Erforderliche Zeit bis zum Erreichen eines angemessenen Sicherheitsstatus mit Palo Alto Networks (Monate)	Umfrageergebnisse	4,4	4,4	4,4
B7	Anfänglicher und laufender Zeitunterschied zwischen Punktlösungen und virtuellen Firewalls der VM-Serie (gerundet)	1-(B6/B5)	30 %	30 %	30 %
B8	Kosten eines stabilen Zustands bei Punktlösungen	(B1*B3/12*B5)+(B2*B4/12*B5)	1.332.450 $	198.450 $	198.450 $
B9	Kosten eines stabilen Zustands bei virtuellen Firewalls der VM-Serie	(B1*B3/12*B6)+(B2*B4/12*B6)	930.600 $	138.600 $	138.600 $
Bt	Erreichen eines bestimmten Sicherheitsstatus	B8-B9	401.850 $	59.850 $	59.850 $
	Risikobereinigung	↓5 %			
Btr	Erreichen eines bestimmten Sicherheitsstatus (risikobereinigt)		381.758 $	56.858 $	56.858 $
	Dreijahresgesamtwert: 495.473 $		**Dreijahresbarwert: 436.760 $**		

EFFIZIENZ IM SICHERHEITS- UND IT-BETRIEB

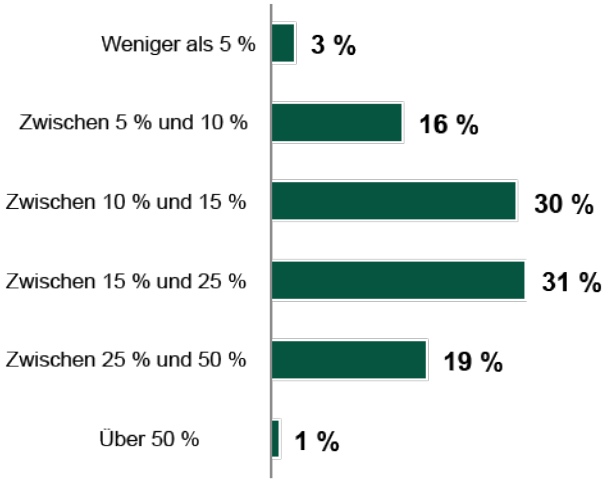
Daten und Fakten. Die Befragten gaben an, dass die SecOps- und IT-Teams von der Implementierung der VM-Serie im Unternehmen profitierten, nämlich in Form einer geringeren Anzahl von Untersuchungen, einer kürzeren MTTR und einer niedrigeren Zahl von Sicherheitsproblemen mit Auswirkungen auf die Geräte. Die SecOps- und IT-Betriebsteams automatisierten zuvor manuell ausgeführte Prozesse und verbesserten die Transparenz des Netzwerkverkehrs, was wiederum eine schnellere Reaktion auf Probleme ermöglichte. Darüber hinaus nutzten die befragten Unternehmen die Vorteile der Protokollverfolgung und -analyse in Prisma Cloud zu einer weiteren Reduzierung der MTTR.

- Der Global Head of Engineering bei einem Getränkeunternehmen äußerte dazu: „Die Erkennungsquote von Palo Alto Networks ist beeindruckend hoch und die Möglichkeit der täglichen Aktualisierung von Inhalten und Richtlinien ausgesprochen praktisch. Mit der VM-Serie haben wir von Anfang an anwendungsgesteuerte Benutzerrichtlinien umgesetzt. Wir konnten allein durch die Möglichkeit des Threat Modeling die Zahl der Fehlalarme, die ein menschliches Eingreifen erfordern, um 40 % bis 50 % und die Zahl anfallender Tickets um mindestens 40 % reduzieren. Unser Supportteam erhält jetzt weniger Anfragen. Daher ist im Falle einer neuen Anfrage sofort klar, dass es sich gewiss nicht um eine Bagatelle handelt, sondern um eine Angelegenheit, die wirklich der Aufmerksamkeit des Supportteams bedarf.“

MTTR reduziert um

25 %

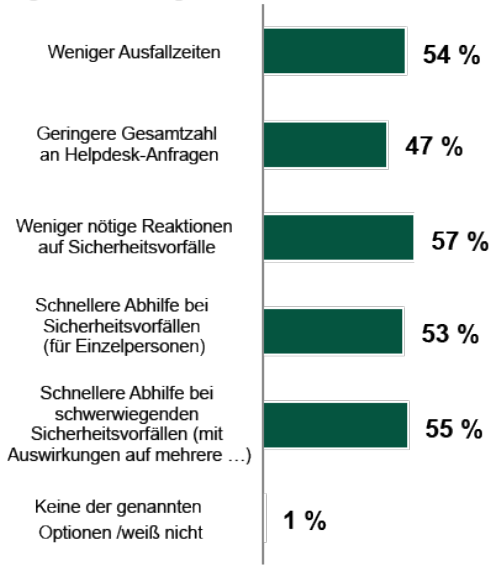
Abbildung 7: „Sie haben angegeben, dass die mittlere Erkennungsdauer bei Sicherheitsvorfällen dank der virtuellen Firewalls der VM-Serie von Palo Alto Networks (auch im gemeinsamen Einsatz mit einem beliebigen Sicherheitsservice) reduziert werden konnte. Wie hoch (in %) schätzen Sie die Verbesserung im Vergleich zu Ihrer vorherigen Umgebung ein?“



Basis: 70 Entscheidungsträger aus dem Bereich Cloud-Sicherheit
Quelle: Studie im Auftrag von Palo Alto Networks, vorgelegt im Juni 2021 von Forrester Consulting

- Der Network Engineer eines Unternehmens für Kommunikationsinfrastruktur meinte: „Die Verwaltung ist so viel einfacher. Die Logdaten aus der Cloud, die über das Netzwerk auf die Logserver von Palo Alto Networks gelangen, vermitteln einen umfassenden Einblick in die Vorgänge in der Cloud. Wir starten Panorama, geben die erforderliche Konfiguration ein und spielen sie im System auf. Die Zeitersparnis gegenüber der Eingabe dieser Informationen auf jeder einzelnen Firewall ist daher enorm. Außerdem ist alles innerhalb weniger Minuten erledigt. So können unsere Sicherheitsexperten auf Probleme, die aus den Logdaten hervorgehen, sofort reagieren und eine Menge Zeit einsparen.“

Abbildung 8: „Sie haben angegeben, dass die virtuellen Firewalls der VM-Serie von Palo Alto Networks (auch im gemeinsamen Einsatz mit einem beliebigen Sicherheitsservice) zu einer Produktivitätssteigerung bei den Endbenutzern beigetragen haben. Welche der folgenden Erfahrungen haben Sie gemacht?“

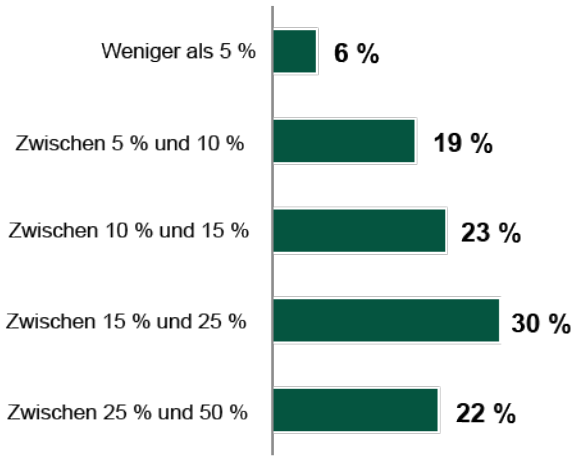


Basis: 113 Entscheidungsträger aus dem Bereich Cloud-Sicherheit
Quelle: Studie im Auftrag von Palo Alto Networks, vorgelegt im Juni 2021 von Forrester Consulting

Modellerstellung und Annahmen. Forrester nimmt für das Modellunternehmen Folgendes an:

- Mit der zuvor eingesetzten Lösung erforderten 154 Sicherheitsvorfälle pro Woche eine mehrstufige und komplexe Untersuchung durch das SecOps-Team. Mit Richtlinien, die im Handumdrehen angepasst sind und sowohl in lokalen Infrastrukturen als auch cloudübergreifend konsistent eingesetzt werden, steigert das Modellunternehmen die Transparenz, erhöht den Schutz vor Bedrohungen und reduziert gleichzeitig die Anzahl der Vorfälle um 18 %.
- Vor der Implementierung von Firewalls der VM-Serie betrug die durchschnittliche MTTR im Modellunternehmen 45 Minuten. Dank besserer kontextbezogener Daten und einer geringeren Anzahl von Fehlalarmen wird die MTTR nun um 25 % verkürzt.
- Das durchschnittliche Jahresgehalt eines SecOps-Teammitglieds (inkl. Nebenkosten) beträgt 121.500 US-Dollar. Der Stundensatz beläuft sich auf 58 US-Dollar.

Abbildung 9: „Sie haben angegeben, dass die virtuellen Firewalls der VM-Serie von Palo Alto Networks (auch im gemeinsamen Einsatz mit einem beliebigen Sicherheitsservice) zu einer Senkung der Fehlalarmquote beigetragen haben. Wie hoch (in %) schätzen Sie die Verbesserung im Vergleich zu Ihrer vorherigen Umgebung ein?“



Quelle: „PAN Virtual Firewalls TEI“, Studie im Auftrag von Palo Alto Networks, vorgelegt im Juni 2021 von Forrester Consulting

- 80 % der eingesparten Zeit werden für die Erledigung anderer produktiver Aktivitäten aufgewendet.

Risiken. Folgende Risiken können sich auf die Realisierung dieser Vorteile auswirken:

- Anzahl der Sicherheitsvorfälle, die ein manuelles Eingreifen erfordern, vor der Implementierung virtueller Firewalls der VM-Serie
- Gesamtauswirkungen auf die MTTR

Ergebnisse. Zur Berücksichtigung dieser Risiken reduzierte Forrester diesen Nutzen um 10 %, was über drei Jahre einen risikobereinigten Gesamtbarwert von 240.100 US-Dollar ergab.

Effizienz im Sicherheits- und IT-Betrieb

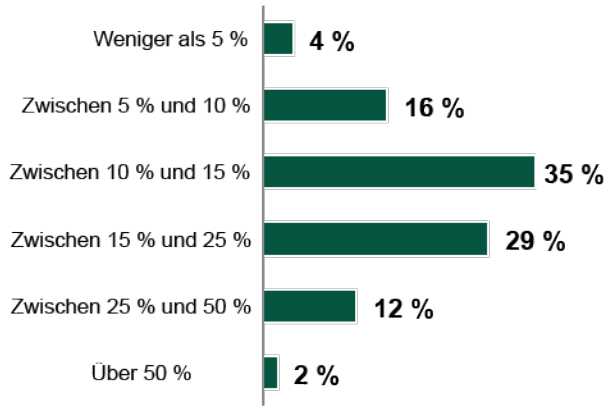
Ref.	Messgröße	Quelle	1. Jahr	2. Jahr	3. Jahr
C1	Anzahl der Sicherheitsvorfälle, die bei der Legacy-Sicherheitslösung manuelle Untersuchungen/Eingriffe erforderten	Modellunternehmen	8.008	8.008	8.008
C2	Reduktion der Sicherheitsvorfälle, die manuelle Untersuchungen/Eingriffe erfordern, mit virtuellen Firewalls der VM-Serie	Umfrageergebnisse	18 %	18 %	18 %
C3	Vermiedene Sicherheitsvorfälle, die manuelle, mehrstufige Untersuchungen erfordern (gerundet)	C1*C2	1.441	1.441	1.441
C4	MTTR bei vorheriger Lösung (Minuten)	Umfrageergebnisse	45	45	45
C5	Zwischensumme: Dank Firewalls der VM-Serie vermiedene Untersuchungen und Abhilfemaßnahmen	C3*C4/60*C8	62.703 $	62.703 $	62.703 $
C6	Verbesserung der MTTR dank Firewalls der VM-Serie	Umfrageergebnisse	25 %	25 %	25 %
C7	Zeitersparnis pro Sicherheitsvorfall (Minuten)	C4*C6	11	11	11
C8	Durchschnittlicher Stundenlohn (inkl. Nebenkosten) eines SecOps-Teammitglieds (gerundet)	Annahme	58 $	58 $	58 $
C9	Zwischensumme: Effizienz im Sicherheitsbetrieb bezogen auf kritische Warnmeldungen (gerundet)	((C1-C3)*C7/60)*C8	71.411 $	71.411 $	71.411 $
C10	Produktivitätsrückgewinnung bei Sicherheits-VZÄ	Annahme	80 %	80 %	80 %
Ct	Effizienz im Sicherheits- und IT-Betrieb	(C5+C9)*C10	107.291 $	107.291 $	107.291 $
	Risikobereinigung	↓10 %			
Ctr	Effizienz im Sicherheits- und IT-Betrieb (risikobereinigt)		96.562 $	96.562 $	96.562 $
	Dreijahresgesamtwert: 289.686 $		**Dreijahresbarwert: 240.136 $**		

KÜRZERE AUSFALLZEITEN FÜR ENDBENUTZER

Daten und Fakten. Die interviewten Personen gaben an, dass das Implementieren konsistenter Richtlinien in einer Vielzahl von Umgebungen (z. B. in lokaler Infrastruktur, in der Public Cloud usw.) mit der VM-Serie sehr einfach wurde. Die konsequente Durchsetzung sorgte dafür, dass bedrohungsbedingte Ausfallzeiten seltener auftraten, und die zentrale Verwaltung von Firewalls der VM-Serie ermöglichte kürzere Reaktionszeiten.

- Den Umfrageteilnehmern zufolge waren vor der Implementierung von Firewalls der VM-Serie durchschnittlich 18,1 % der Endanwender von Ausfallzeiten betroffen. Nach der Einführung sank dieser Anteil auf 5,6 %.
- Ein IT-Dienstleistungsunternehmen, das B2B-Cloud-Services anbietet, verwendet Firewalls der VM-Serie zur Segmentierung von Kundenumgebungen. In der Vergangenheit verursachten Hardwareausfälle Serviceunterbrechungen bei ganzen Gruppen von Kunden. Dagegen beschränkt sich beim Ausfall einer Firewall der VM-Serie eine solche Unterbrechung auf genau einen Kunden. Der Lead Architect des Unternehmens sagte: „Wann immer wir ein Update aufspielen mussten, hatte dies einen einstündigen Ausfall zur Folge. Und das bekamen alle Kunden zu spüren, die die betreffende Appliance nutzten. Bei der VM-Serie hat dagegen jeder Kunde seine eigene Firewall. Wir haben bislang noch keine Ausfälle erlebt, aber selbst wenn es dazu käme, wären die Auswirkungen doch sehr begrenzt.“
- Den Befragten zufolge tragen NGFW-Funktionen wie die Möglichkeit zur Traffic-Verlagerung dazu bei, dass die Anwender nicht von den Firewalls beeinträchtigt werden. Der Global Head of IT Engineering bei einem Getränkeunternehmen meinte: „Mit der richtlinien-basierten Verwaltung konnten wir Datenverkehr, der nicht überwacht werden musste, ganz einfach auslagern. Dazu gehörten beispielsweise die Websites auf unserer Positivliste und alle Audio- und Videodateien. Die Nutzung nimmt stetig zu, aber jetzt kann ich den Traffic an einem lokalen Punkt mit nur einem Mausklick auslagern. Andere Tools sind dazu nicht in der Lage. Wir konnten also jetzt Traffic auslagern, dadurch den Durchsatz im Netzwerk steigern und so ein positives Nutzererlebnis bieten.“

Abbildung 10: „Sie haben angegeben, dass die virtuellen Firewalls der VM-Serie von Palo Alto Networks (auch im gemeinsamen Einsatz mit einem beliebigen Sicherheitsservice) zu einer Senkung der durchschnittlichen Triagedauer beigetragen haben. Wie hoch (in %) schätzen Sie die Verbesserung im Vergleich zu Ihrer vorherigen Umgebung ein?“



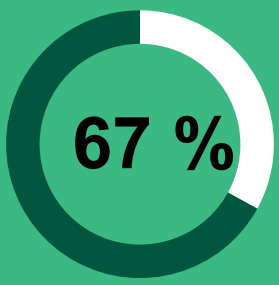
Basis: 49 Entscheidungsträger aus dem Bereich Cloud-Sicherheit

Quelle: Studie im Auftrag von Palo Alto Networks, vorgelegt im Juni 2021 von Forrester Consulting

Modellerstellung und Annahmen. Forrester nimmt für das Modellunternehmen Folgendes an:

- Vor der Einführung der VM-Serie waren 18 % der 7.500 Angestellten mindestens einmal pro Jahr von einem Ausfall betroffen. Mit den Firewalls der VM-Serie sinkt dieser Wert um 67 %, d. h. nur noch 6 % der Angestellten fallen einem Ausfallereignis zum Opfer.
- In der Vergangenheit dauerten die Ausfälle im Schnitt 4,5 Stunden. Nach der Implementierung von Firewalls

Reduzierung der Ausfallzeiten für Benutzer



der VM-Serie sinkt dieser Wert bei denjenigen Anwendern, die immer noch von Ausfallzeiten betroffen sind, um 45 % (d. h. um 2 Stunden).

- Das durchschnittliche Jahresgehalt (inkl. Nebenkosten) für einen Endbenutzer beträgt 87.750 US-Dollar. Der Stundensatz beläuft sich auf 42 US-Dollar.

Risiken. Folgende Risiken können sich auf die Realisierung dieser Vorteile auswirken.

- Anteil der Sicherheitsvorfälle, die Endbenutzer betreffen
- Umfang der Ausfallzeiten aufgrund von Untersuchungen
- Durchschnittsgehälter (inkl. Nebenkosten) der Endbenutzer

Ergebnisse. Zur Berücksichtigung dieser Risiken hat Forrester diesen Nutzen um 5 % nach unten bereinigt, was über drei Jahre einen risikobereinigten Gesamtbarwert von 493.400 US-Dollar ergibt.

Kürzere Ausfallzeiten für Endbenutzer

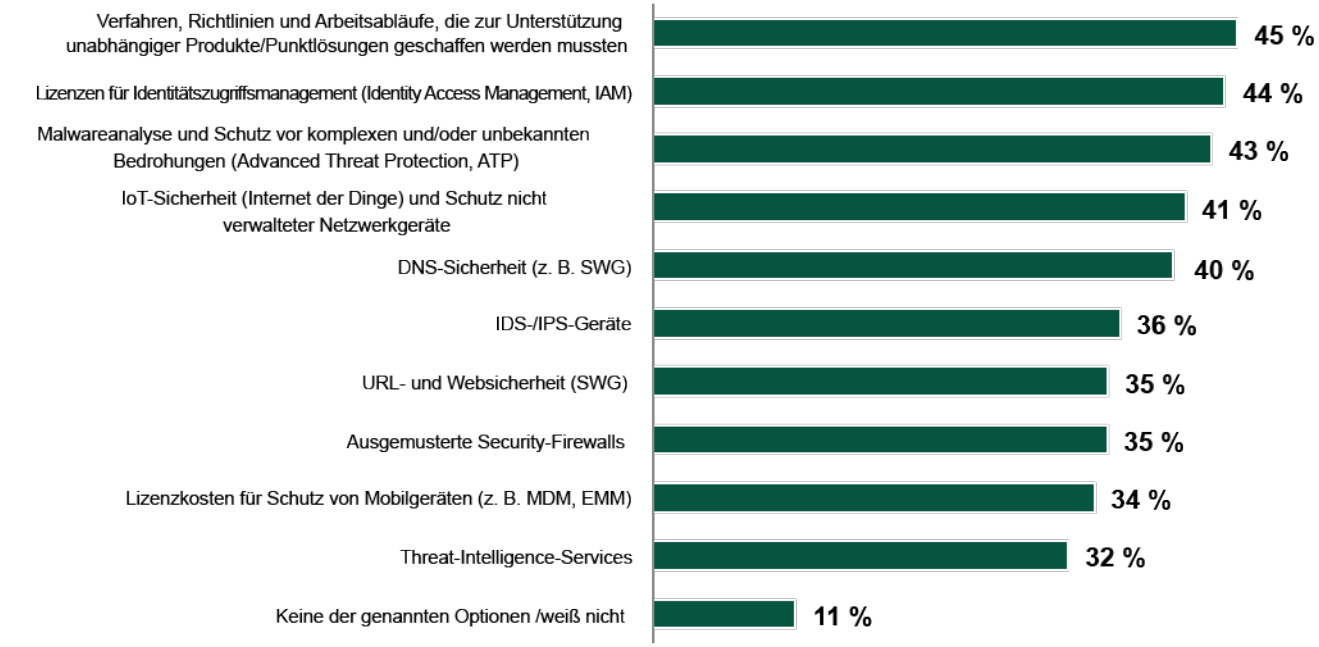
Ref.	Messgröße	Quelle	1. Jahr	2. Jahr	3. Jahr
D1	Zahl der Anwender	Modellunternehmen	7.500	7.500	7.500
D2	Anteil der Benutzer, die vor der Einführung von Firewalls der VM-Serie von Ausfallzeiten betroffen waren	Befragungen	18 %	18 %	18 %
D3	Reduzierung der Ausfallzeiten mit Firewalls der VM-Serie	Befragungen	67 %	67 %	67 %
D4	Benutzer, die Ausfallzeiten mit Firewalls der VM-Serie vermeiden	D1*D2*D3	904,5	904,5	904,5
D5	Durchschnittsdauer der Ausfallzeiten im vorherigen Zustand (Stunden)	Modellunternehmen	4,5	4,5	4,5
D6	Zeitersparnis für Endbenutzer durch vermiedene Ereignisse	D4*D5	4.070	4.070	4.070
D7	Endbenutzer, die auch nach Einführung der Firewalls der VM-Serie Ausfallzeiten verzeichnen	(D1*D2)-D6	445,5	445,5	445,5
D8	Reduzierung der Ausfallzeiten mit Firewalls der VM-Serie	Befragungen	45 %	45 %	45 %
D9	Durchschnittlich vermiedene Ausfallzeit pro betroffenem Benutzer mit Firewalls der VM-Serie (Stunden)	D5*D8	2,0	2,0	2,0
D10	Zeitersparnis für Endbenutzer bei aufgetretenen Ereignissen	D7*D9	902,1	902,1	902,1
D11	Durchschnittlicher Stundensatz pro geschäftlichem Benutzer (gerundet)	Annahme	42 $	42 $	42 $
Dt	Kürzere Ausfallzeiten für Endbenutzer	(D6+D10)*D11	208.840 $	208.840 $	208.840 $
	Risikobereinigung	↓5 %			
Dtr	Kürzere Ausfallzeiten für Endbenutzer (risikobereinigt)		198.398 $	198.398 $	198.398 $
	Dreijahresgesamtwert: 595.195 $		**Dreijahresbarwert: 493.387 $**		

KOSTENSENKUNG UND EINSPARUNGEN BEI DER SICHERHEITSINFRASTRUKTUR

Daten und Fakten. Die Firewalls der VM-Serie können mit Palo Alto Networks CDSS kombiniert werden, um Unternehmen zusätzlichen Schutz vor Bedrohungen zu bieten. Durch den Einsatz dieser Lösungen konnten die befragten Unternehmen die Ausgaben für vorhandene Punktlösungen innerhalb ihrer Sicherheits-Stacks senken.

- Die Unternehmen profitierten von der Implementierung von Palo Alto Networks Threat Prevention, DNS Security, GlobalProtect, WildFire und URL Filtering gemeinsam mit den Firewalls der VM-Serie. Ein Senior Security Engineer bei einem Dienstleistungsunternehmen sagte: „Im Grunde genommen entschieden wir, von der alten Infrastruktur auf eine Next-Gen-Firewall umzusteigen, damit wir diese ganzen Lösungen integrieren und über eine zentrale Plattform verwalten können.“
- Unternehmen erkannten einen zusätzlichen Nutzen durch die Skalierbarkeit der Firewalls der VM-Serie. Sie konnten so neue Firewalls nach Bedarf schnell implementieren, statt vorab Appliances beschaffen zu müssen, was oft zu unnötigen Ausgaben führte. Der CISO eines Unternehmens für medizinische Geräte erklärte: „Man kann wirklich ganz klein anfangen und dann bei Bedarf aufstocken. Und umgekehrt kann man abschalten, was man nicht mehr braucht. Wenn man ein internes On-Premises-System hat, muss man immer Hardware kaufen, immer die passende Kapazität zur Verfügung haben usw. Hier dagegen ist das total unproblematisch. Man kann die Firewall einschalten und wenn man sie in vier Monaten nicht mehr braucht, schaltet man sie einfach wieder aus und dann ist sie weg.“

Abbildung 11: „Sie haben angemerkt, dass durch die virtuellen Firewalls der VM-Serie von Palo Alto Networks (auch im gemeinsamen Einsatz mit einem beliebigen Sicherheitsservice) die Kosten für Softwarelizenzen, Hardware und/oder Wartungs- und Supportmanagement gesunken sind. Bei welchen der folgenden Optionen hat Ihr Unternehmen Kosteneinsparungen im Vergleich zur vorherigen Umgebung erzielt?“



Basis: 103 Entscheidungsträger aus dem Bereich Cloud-Sicherheit
Quelle: Studie im Auftrag von Palo Alto Networks, vorgelegt im Juni 2021 von Forrester Consulting

Modellerstellung und Annahmen. Forrester nimmt für das Modellunternehmen Folgendes an:

- Das Modellunternehmen nutzt alle Vorteile der CDSS-Produktsuite von Palo Alto Networks.
- Im alten Umfeld waren die Firewall-Ressourcen des Unternehmens um 25 % überdimensioniert (was durch das kürzlich angekündigte flexible Verbrauchsmodell behoben werden kann).

Risiken. Folgende Risiken können sich auf die Realisierung dieser Vorteile auswirken:

- Vor der Implementierung der VM-Serie eingesetzte Sicherheitslösungen und Möglichkeiten zur Kündigung von Verträgen
- Aktueller Sicherheitsbedarf und Nutzung der CDSS-Produkte von Palo Alto Networks
- Typische Wachstums- und Überdimensionierungspraktiken

Ergebnisse. Zur Berücksichtigung dieser Risiken reduzierte Forrester diesen Nutzen um 10 %, was über drei Jahre einen risikobereinigten Gesamtbarwert von 573.800 US-Dollar ergab.

Kostensenkung und Einsparungen bei der Sicherheitsinfrastruktur

Ref.	Messgröße	Quelle	1. Jahr	2. Jahr	3. Jahr
E1	Kosten für Threat-Intelligence-Services	Umfrageergebnisse	71.037 $	71.037 $	71.037 $
E2	Kosten für ausgemusterte Security-Firewalls	Umfrageergebnisse	63.665 $	63.665 $	63.665 $
E3	Kosten für IDS-/IPS-Geräte	Umfrageergebnisse	55.590 $	55.590 $	55.590 $
E4	Kosten für DNS-Sicherheit (z. B. sicheres Web-Gateway)	Umfrageergebnisse	21.704 $	21.704 $	21.704 $
E5	Kosten für Malware-Analyse und Schutz vor komplexen und/oder unbekannten Bedrohungen (z. B. Advanced Threat Protection)	Umfrageergebnisse	18.390 $	18.390 $	18.390 $
E6	Kosten für IoT-Sicherheit und Schutz nicht verwalteter Netzwerkgeräte	Umfrageergebnisse	12.389 $	12.389 $	12.389 $
E7	Vermiedene Überdimensionierung physischer Firewalls	A1*25 %*1000	25.000 $	6.250 $	7.813 $
Et	Kostensenkung und Einsparungen bei der Sicherheitsinfrastruktur	E1+E2+E3+E4+E5+E6+E7	267.774 $	249.024 $	250.586 $
	Risikobereinigung	↓10 %			
Etr	Kostensenkung und Einsparung bei der Sicherheitsinfrastruktur (risikobereinigt)		240.996 $	224.121 $	225.527 $
	Dreijahresgesamtwert: 690.645 $		**Dreijahresbarwert: 573.754 $**		

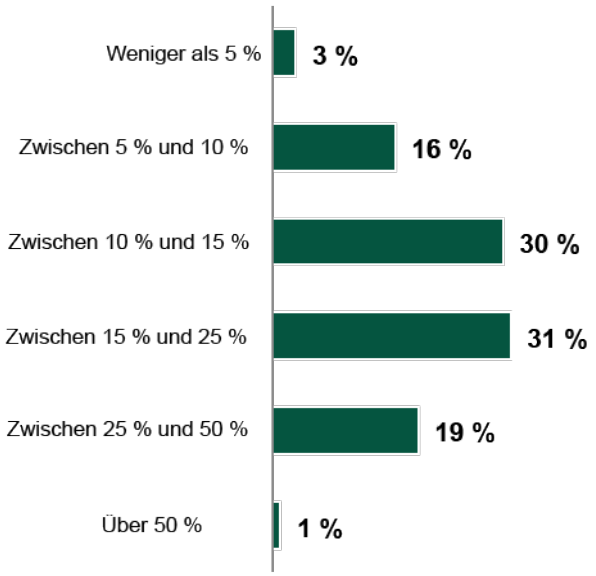
GERINGERES RISIKO VON DATENSCHUTZVERLETZUNGEN

Daten und Fakten. Die Befragten gaben an, dass ihre Unternehmen ihren allgemeinen Sicherheitsstatus verbessern, Angriffsflächen reduzieren und im Bereich der Netzwerksicherheit auf Zero-Trust-Modelle umsteigen konnten. Mit einer zentralisierten und vereinheitlichten Lösung konnten die Unternehmen das Zero-Trust-Modell umsetzen, das durch Technologie von Palo Alto Networks unterstützt wird.

„Wir haben eine native CSP-Firewall evaluiert und dabei festgestellt, dass sie keine Deep Packet Inspection durchführt. Es gab keinen Bedrohungsschutz, der eine Einbindung gestattet hätte. Die Protokolle waren recht unpraktisch. Und anders als bei Panorama gab es auch keine zentralisierte Verwaltung. Es fehlten also genau die Eigenschaften, die Sicherheit und Transparenz steigern und es uns so erlauben, unsere Arbeit effizienter zu erledigen.“
Information Security Engineer, Unternehmensdienstleistungen

- Die Befragten aus Unternehmen, die zuvor Punktlösungen eingesetzt hatten, gaben an, dass diese Lösungen sich nicht unbedingt ergänzten oder nicht optimal miteinander kommunizierten. Das Vorhandensein mehrerer Firewalls und komplexer Netzwerksicherheitslösungen führte zudem zu uneinheitlichen Richtlinien und Schutzlücken insbesondere zwischen On-Premises- und Cloud-Lösungen.
- Durch den Einsatz von Firewalls der VM-Serie erhielten die befragten Unternehmen einheitliche Lösungen, die eine zentrale Verwaltung ermöglichten, sodass die Sicherheitsteams etwaige Lücken leicht erkennen und schließen konnten. Die Zuverlässigkeit der Informationen, die zwischen den Sicherheitssystemen ausgetauscht werden, ist der Schlüssel zu einer wirksamen automatischen Abwehr von Verstößen. Palo Alto Networks CDSS stärkte die Netzwerksicherheit zusätzlich, denn das Unternehmen bietet Schutz und Support rund um die Uhr, einschließlich automatischer Updates aller Next-Generation-Firewalls zur Abwehr der neuesten Bedrohungen.
- Der Global Head of IT Engineering beim Getränkeunternehmen sagte: „Wir führen jedes Jahr interne Audits durch. Die Zahl der Auffälligkeiten im Bereich Netzwerktechnik und Firewalls ist dabei im Vergleich zum Vorjahr um 40 % zurückgegangen. Dies liegt zum Teil an der Governance und an den implementierten Richtlinien sowie an der Art der Regelerstellung. Wir können nicht mehr notwendige Richtlinien auf Grundlage von IP-Adressen, aber auch solche, die nicht anwendungsspezifisch erstellt wurden, leicht finden und korrigieren.“

Abbildung 12: „Sie haben angegeben, dass die mittlere Erkennungsdauer bei Sicherheitsvorfällen dank der virtuellen Firewalls der VM-Serie von Palo Alto Networks (auch im gemeinsamen Einsatz mit einem beliebigen Sicherheitsservice) reduziert werden konnte. Wie hoch (in %) schätzen Sie die Verbesserung im Vergleich zu Ihrer vorherigen Umgebung ein?“



Basis: 70 Entscheidungsträger aus dem Bereich Cloud-Sicherheit

Quelle: Studie im Auftrag von Palo Alto Networks, vorgelegt im Juni 2021 von Forrester Consulting

Modellerstellung und Annahmen. Forrester nimmt für das Modellunternehmen Folgendes an:

- Den Daten von Forrester zufolge würde das Modellunternehmen durchschnittlich 3,2 Sicherheitsverstöße pro Jahr verzeichnen müssen, wenn es auf Punktlösungen setzt.[2]
- Die Kosten eines solchen Verstoßes belaufen sich auf 53 US-Dollar pro Mitarbeiter, wobei der Produktivitätsverlust der Mitarbeiter noch gar nicht berücksichtigt ist. Die Kosten umfassen:
    - Bußgelder
    - Erstattungen an Kunden, Klagen
    - Reaktion auf Vorfälle und Abhilfemaßnahmen
    - Entgangene Umsätze
    - Wiederherstellung des Markenwerts
    - Kosten für die Wiedergewinnung von Kunden
- Mit den Firewalls der VM-Serie reduziert das Unternehmen die Wahrscheinlichkeit eines Datenverstoßes nach drei Jahren um bis zu 20 %.
- Jeder Verstoß betrifft 18 % aller Mitarbeiter und führt zu einem durchschnittlichen Zeitverlust von 3,6 Stunden je Mitarbeiter. Diese Kosten kommen zu den oben erwähnten Einzelkosten hinzu.

Risiken. Folgende Risiken können sich auf die Realisierung dieser Vorteile auswirken:

- Auswirkungen von Firewalls der VM-Serie auf den Sicherheitsstatus des Unternehmens insgesamt im Vergleich zur vorherigen Lösung
- Anteil der Mitarbeiter, die von einem Sicherheitsverstoß betroffen sind, und die damit verbundene Dauer der Ausfallzeit
- Durchschnittsgehälter der geschäftlichen Benutzer

Ergebnisse. Zur Berücksichtigung dieser Risiken reduzierte Forrester diesen Nutzen um 30 %, was über drei Jahre einen risikobereinigten Gesamtbarwert von 383.700 US-Dollar ergab.

Geringeres Risiko von Datenschutzverletzungen					
Ref.	**Messgröße**	**Quelle**	**1. Jahr**	**2. Jahr**	**3. Jahr**
F1	Durchschnittliche Anzahl der Datenschutzverletzungen	Untersuchungen durch Forrester	3,2	3,2	3,2
F2	Durchschnittliche potenzielle Kosten einer Datenschutzverletzung ohne Berücksichtigung der Ausfallzeiten interner Benutzer	Untersuchungen durch Forrester	265.000 $	265.000 $	265.000 $
F3	Geringere Wahrscheinlichkeit von Verstößen	Modellunternehmen	10 %	15 %	20 %
F4	**Vermiedene Kosten für Behebung, Lösung beim Kunden, Bußgelder, Wiederaufbau der Marke und alle weiteren extern entstehenden Kosten**	**F1*F2*F3**	**84.800 $**	**127.200 $**	**169.600 $**
F5	Anzahl interner Mitarbeiter	Modellunternehmen	7.500	7.500	7.500
F6	Durchschnittlicher Stundensatz pro geschäftlichem Benutzer	D8	42 $	42 $	42 $
F7	Beeinträchtigte/eingebüßte Produktivität interner Benutzer je Verstoß (Stunden)	Untersuchungen durch Forrester	3,6	3,6	3,6
F8	Durchschnittlicher Anteil betroffener Mitarbeiter pro Datenschutzverletzung	Modellunternehmen	18 %	18 %	18 %
F9	**Durch Verlust interner Produktivität entstehende Kosten**	**F1*F3*F5*F6*F7*F8**	**65.318 $**	**97.978 $**	**130.637 $**
Ft	Geringeres Risiko von Datenschutzverletzungen	F4+F9	150.118 $	225.178 $	300.237 $
	Risikobereinigung	↓30 %			
Ftr	Geringeres Risiko von Datenschutzverletzungen (risikobereinigt)		105.083 $	157.624 $	210.166 $
	Dreijahresgesamtwert: 472.873 $		**Dreijahresbarwert: 383.699 $**		

NICHT QUANTIFIZIERTER NUTZEN

Die Unternehmen profitierten zusätzlich von weiteren Vorteilen, die jedoch nicht quantifiziert werden konnten, darunter:

- **Ausnutzung bestehender Kompetenzen und dadurch Vermeidung von Schulungen und Neueinstellungen.** Die meisten befragten Unternehmen verfügten über interne Ressourcen, die sie zeitnah mit der Implementierung von Firewalls der VM-Serie beauftragen konnten. Befragte, bei denen dies nicht der Fall war, gaben dagegen an, dass es relativ einfach war, sich das erforderliche Know-how extern zu beschaffen, da Palo Alto Networks flächendeckend eingesetzt wird. Der CISO eines Unternehmens für medizinische Geräte meinte, „Die Produkte von Palo Alto Networks sind gängig, sodass sich die erforderlichen Fähigkeiten und Fachkräfte mit entsprechenden Kompetenzen leicht finden lassen.“
- **Steigerung von Skalierbarkeit und Flexibilität.** Die Befragten gaben an, dass die Firewalls der VM-Serie aufgrund ihres virtuellen Formfaktors nach Bedarf schnell eingesetzt oder aus dem Betrieb entfernt werden können. Dies gewährleistet, dass die Unternehmen sich innerhalb kürzester Zeit an veränderte Anforderungen anpassen können und gleichzeitig die Kosten im Griff behalten. Der CISO aus der Medizintechnikbranche erklärte: „Letztes Jahr mussten wir unsere Produktion infolge der COVID-19-Pandemie um das Zwanzigfache steigern. Dies erforderte eine erhebliche Hochskalierung von Systemen, die eigentlich gar nicht skalierbar waren. Mit Hardware hätten wir das nicht so schnell hinbekommen.“

- **Verbesserung der Wettbewerbsfähigkeit.** Einige der Befragten gaben an, dass ihr Unternehmen den Einsatz der Produkte von Palo Alto Networks als Wettbewerbsvorteil bei der Erbringung technischer Dienstleistungen betrachtet. Eine leitende Fachkraft aus der Netzwerktechnik in der IT-Servicebranche sagte: „Ich glaube, mein Unternehmen hat sich dies zunutze gemacht, um unseren Kunden neben der öffentlichen Cloud auch private Clouds schmackhaft zu machen. Wenn Vorschriften wie etwa die DSGVO Anwendung finden, können wir dem Kunden eine sichere Lösung in der privaten Cloud anbieten. Daher könnten wir davon durchaus profitieren."
- **Erforschung neuer Anwendungsfälle, Kostensenkung und Reduzierung neuer Bedrohungsvektoren.** Einige der Unternehmen setzten Firewalls der VM-Serie ein, um Assets am Netzwerk-Edge zu schützen, z. B. an Verkaufsstellen. Der Global Head of Engineering bei einem Getränkeunternehmen meinte: „Wir haben unsere Kioske in den Geschäften über ein privates 5G-Netzwerk betrieben und die Mitarbeiter hatten 5G-Karten. Allerdings wuchs das Programm zusehends und irgendwann erkannten wir, dass wir mit diesem Ansatz nicht weiterkommen würden. Die Leute haben unsere 5G-Karten geklaut! Also haben wir uns Palo Alto Networks als Partner genommen. Dort entwickelte man ein Paket speziell für uns, mit dem unsere Rechner mit unseren VM-Firewalls oder unserem VPN kommunizieren können. Jetzt können wir diese Geräte in der Kundenumgebung einsetzen und müssen keine Karten von 5G-Anbietern mehr kaufen. So funktioniert die Partnerschaft mit Palo Alto Networks. Sie haben für uns einen eigenen Endpunkt-Client entwickelt, den diese Geräte nutzen. Und das hat uns in diesem Bereich drastische Kosteneinsparungen beschert."
- **Gewährleistung, dass Sicherheit kein Hindernis für die digitale Transformation darstellt.** Sicherheitsteams haben den Auftrag, den Betrieb so sicher wie möglich zu machen, sollten aber der digitalen Transformation nicht im Wege stehen. Die Firewalls der VM-Serie lassen sich im Handumdrehen implementieren, sodass der nötige Sicherheitsstatus schnell erreicht wird und das Unternehmen die Vorteile von Public-Cloud- und Hybrid-Cloud-Migrationen ausnutzen kann.

FLEXIBILITÄT

Kunden schätzen Flexibilität individuell unterschiedlich hoch ein. Es sind mehrere Szenarien denkbar, in denen ein Kunde sich für den Einsatz von virtuellen Firewalls der VM-Serie von Palo Alto Networks entscheidet und zusätzliche Anwendungen und Geschäftsmöglichkeiten erst später erkennt.

Palo Alto Networks hat vor Kurzem ein flexibles Verbrauchsmodell anstelle der branchenüblichen unbefristeten Lizenzierung mit ELA-Modell (Enterprise License Agreement, Unternehmenslizenzvereinbarungen) eingeführt, wie sie nach Angaben der Befragten in den jeweiligen Unternehmen vorher eingesetzt wurde. Beim flexiblen Verbrauchsmodell zahlen Unternehmen nur für die Firewalls und Sicherheitsservices, die sie zum jeweiligen Zeitpunkt brauchen, und sie können diese je nach Bedarf hinzubuchen oder kündigen. Dieses Mehr an Flexibilität ermöglichte es den befragten Unternehmen, zusätzliche Einsparungen bei den Firewall-Kosten zu erzielen.

Flexibilität wird auch quantifiziert, wenn sie als Teil eines konkreten Projekts beurteilt wird. (Eine ausführliche Beschreibung entnehmen Sie bitte Anhang A.)

Kostenanalyse

Quantifizierte Kostendaten, angewendet auf das Modellunternehmen

Gesamtkosten

Ref.	Kosten	Ausgangswert	1. Jahr	2. Jahr	3. Jahr	Gesamtwert	Barwert
Gtr	Firewall-Lizenzierung	0 $	321.300 $	401.625 $	502.031 $	1.224.956 $	1.001.196 $
Htr	Interner Bereitstellungsaufwand	3.407 $	0 $	852 $	1.065 $	5.324 $	4.911 $
Itr	Laufende Verwaltung	0 $	177.188 $	177.188 $	177.188 $	531.563 $	440.639 $
Jtr	Whitebox-Appliances	105.000 $	0 $	26.250 $	32.813 $	164.063 $	151.347 $
	Gesamtkosten (risikobereinigt)	108.407 $	498.488 $	605.914 $	713.096 $	1.925.905 $	1.598.093 $

FIREWALL-LIZENZIERUNG

Daten und Fakten. Die Befragten gaben an, dass Palo Alto Networks wettbewerbsfähige Preise für Firewalls der VM-Serie in verschiedenen Größen und mit unterschiedlichen Abonnementstufen anbietet, um Kundenanforderungen gerecht zu werden.

Modellerstellung und Annahmen. Forrester nimmt für das Modellunternehmen Folgendes an:

- Das Modellunternehmen implementiert 100 Firewalls der VM-Serie in Jahr 1 und die Implementierungs- und Abonnementbasis wächst jährlich um 25 %.
- Zur Modellierung dieser Kosten für das Modellunternehmen nutzte Forrester die ELA-Modelle, die die Unternehmen der Befragten vor der Verwendung von Firewalls der VM-Serie einsetzten; mittlerweile aber ist Palo Alto Networks zu einem verbrauchsabhängigen Preismodell übergegangen.

Risiken. Risiken, die sich auf diese Kosten auswirken könnten, sind etwa:

- Größe der Firewall-Implementierung
- Anzahl der in der Cloud bereitgestellten Sicherheitsservices und dafür erforderlicher Support

Ergebnisse. Zur Berücksichtigung dieser Risiken hat Forrester diese Kosten um 5 % nach oben korrigiert, was über drei Jahre einen risikobereinigten Gesamtbarwert (diskontiert mit 10 %) von 1 Mio. US-Dollar ergibt.

Firewall-Lizenzierung

Ref.	Messgröße	Quelle	Ausgangswert	1. Jahr	2. Jahr	3. Jahr
G1	Lizenzkosten je Firewall der VM-Serie	Befragungen		3.060 $	3.060 $	3.060 $
G2	Gesamtzahl der implementierten Firewalls der VM-Serie	Modellunternehmen		100	125	156
Gt	Firewall-Lizenzierung	F1*F2		306.000 $	382.500 $	478.125 $
	Risikobereinigung	↑5 %				
Gtr	Firewall-Lizenzierung (risikobereinigt)		0 $	321.300 $	401.625 $	502.031 $
	Dreijahresgesamtwert: 1.224.956 $			**Dreijahresbarwert: 1.001.196 $**		

INTERNER BEREITSTELLUNGSAUFWAND

Daten und Fakten. Die Befragten gaben an, dass mit der Bereitstellung der Produkte von Palo Alto Networks in ihren Unternehmen zwar etwas Zeit und Aufwand verbunden war, sie aber reibungslos ablief und dank der einheitlichen Technologie und der Möglichkeit, Richtlinien automatisch im gesamten Netzwerk zu aktualisieren, keinerlei signifikante Verzögerungen oder Hürden auftraten.

Modellerstellung und Annahmen. Forrester nimmt für das Modellunternehmen Folgendes an:

- Das Unternehmen ist ein Bestandskunde von Palo Alto Networks.
- Die Implementierungskosten berücksichtigen nicht die für die Implementierung von Zusatzprodukten (z. B. Palo Alto Networks SD-WAN, Prisma Cloud, Panorama usw.) benötigte Zeit.
- Die Implementierung einer neuen Firewall der VM-Serie dauert 30 Minuten.
- Das durchschnittliche Jahresgehalt eines NetOps-Teammitglieds (inkl. Nebenkosten) beträgt 135.000 US-Dollar.

Risiken. Risiken, die sich auf diese Kosten auswirken könnten, sind etwa:

- Bereits im Unternehmen eingesetzte Produkte von Palo Alto Networks und Grad der Vertrautheit mit diesen Produkten
- Durchschnittsgehälter der Mitglieder des Implementierungsteams

Ergebnisse. Zur Berücksichtigung dieser Risiken hat Forrester diese Kosten um 5 % nach oben bereinigt, was über drei Jahre einen risikobereinigten Gesamtbarwert von 4.900 US-Dollar ergibt.

Interner Bereitstellungsaufwand

Ref.	Messgröße	Quelle	Ausgangswert	1. Jahr	2. Jahr	3. Jahr
H1	Implementierungsdauer (Stunden, gerundet)	A1*0,5	50		13	16
H2	Durchschnittlicher Stundensatz eines Mitglieds des Implementierungsteams	Annahme	65 $		65 $	65 $
Ht	Kosten für internen Bereitstellungsaufwand	H1*H2	3.245 $	0 $	811 $	1.014 $
	Risikobereinigung	↑5 %	·			
Htr	Interner Bereitstellungsaufwand (risikobereinigt)		3.407 $	0 $	852 $	1.065 $
	Dreijahresgesamtwert: 5.324 $			**Dreijahresbarwert: 4.911 $**		

LAUFENDE VERWALTUNG

Belege und Daten. Die Befragten merkten an, dass Firewalls der VM-Serie im Vergleich zu herkömmlichen Lösungen deutlich weniger laufende Verwaltung benötigten. Wenngleich ihre Unternehmen viele zuvor manuell ausgeführte Aufgaben automatisierten oder konsolidierten, erforderten die Verwaltung von Firewalls und Richtlinien, die Fehlerbehebung, das Aufspielen von Updates und weitere administrative Aufgaben dennoch einen gewissen Aufwand vonseiten interner Teams.

Modellerstellung und Annahmen. Forrester nimmt für das Modellunternehmen Folgendes an:

- Das Modellunternehmen beschäftigt zehn VZÄ mit der laufenden Verwaltung der implementierten Firewalls der VM-Serie.
- Interne Ressourcen widmen 15 % ihrer Zeit allein der Firewall-Verwaltung.
- Das durchschnittliche Jahresgehalt der betroffenen VZÄ beträgt 112.500 US-Dollar.

Risiken. Risiken, die sich auf diese Kosten auswirken könnten, sind etwa:

- Größe und Umfang der Implementierung.
- Interne Kompetenzen des Unternehmens und die Fähigkeit, Aufgaben zu automatisieren.
- Durchschnittliche Jahresgehälter.

Ergebnisse. Zur Berücksichtigung dieser Risiken hat Forrester diese Kosten um 5 % nach oben bereinigt, was über drei Jahre einen risikobereinigten Gesamtbarwert von 440.600 US-Dollar ergibt.

Laufende Verwaltung

Ref.	Messgröße	Quelle	Ausgangswert	1. Jahr	2. Jahr	3. Jahr
I1	Mit der laufenden Verwaltung befasste VZÄ	Modellunternehmen		10	10	10
I2	Anteil der für die Firewall-Verwaltung aufgewendeten Zeit	Befragungen		15 %	15 %	15 %
I3	Durchschnittlicher Jahresvergütungssatz der VZÄ	Annahme		112.500 $	112.500 $	112.500 $
It	Kosten für laufende Verwaltung	I1*I2*I3		168.750 $	168.750 $	168.750 $
	Risikobereinigung	↑5 %				
Itr	Laufende Verwaltung (risikobereinigt)		0 $	177.188 $	177.188 $	177.188 $
	Dreijahresgesamtwert: 531.563 $		**Dreijahresbarwert: 440.639 $**			

WHITEBOX-APPLIANCES

Belege und Daten. Viele der befragten Unternehmen, die mehrere Rechenzentren oder Niederlassungen betreiben, beschlossen, ihre Firewalls auf kostengünstiger Standardhardware zu installieren. Befragte aus Unternehmen, die sich für diesen Weg entschieden, gaben an, dass die Installation unkompliziert war und die Hardware auch von Mitarbeitern ohne IT-Erfahrung installiert werden konnte.

Modellerstellung und Annahmen. Forrester nimmt für das Modellunternehmen Folgendes an:

- Das Modellunternehmen implementiert seine Firewalls der VM-Serie auf neuen Whitebox-Appliances.
- Da der Umfang der Implementierung jährlich um 25 % zunimmt, kauft das Unternehmen weitere Appliances hinzu.
- Die durchschnittlichen Kosten für Standardhardware, die für die Bereitstellung einer Firewall der VM-Serie erforderlich ist, belaufen sich auf 1.000 US-Dollar.

Risiken. Risiken, die sich auf diese Kosten auswirken könnten, sind etwa:

- Größe der Implementierung
- Preise für gängige Hardware

Ergebnisse. Zur Berücksichtigung dieser Risiken hat Forrester diese Kosten um 5 % nach oben bereinigt, was

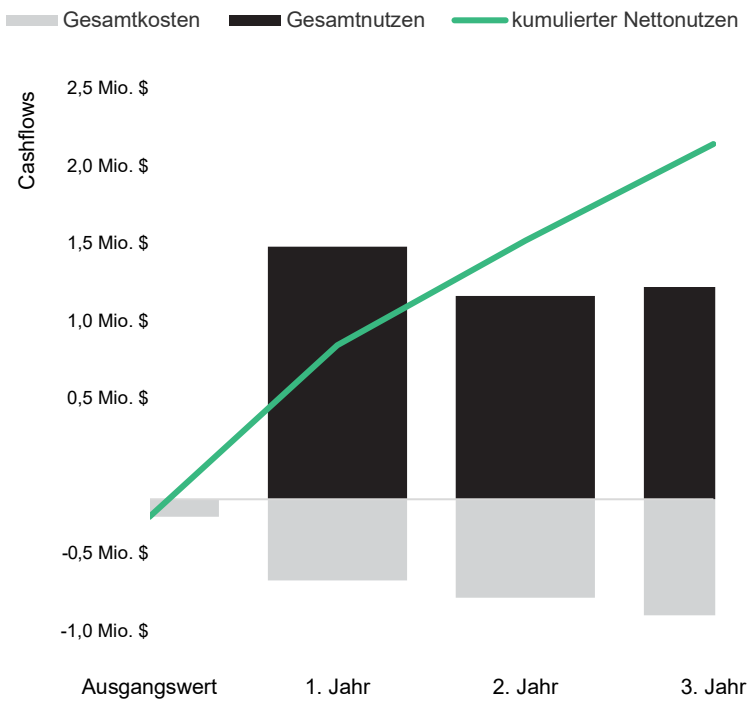
Whitebox-Appliances						
Ref.	**Messgröße**	**Quelle**	**Ausgangswert**	**1. Jahr**	**2. Jahr**	**3. Jahr**
J1	Whitebox-Appliances	Modellunternehmen	100	0	25	31
J2	Preis pro Appliance	Befragungen	1.000 $	1.000 $	1.000 $	1.000 $
Jt	Kosten für Whitebox-Appliances	J1*J2	100.000 $	0 $	25.000 $	31.250 $
	Risikobereinigung	↑5 %	·			
Jtr	Whitebox-Appliances (risikobereinigt)		105.000 $	0 $	26.250 $	32.813 $
	Dreijahresgesamtwert: 164.063 $			**Dreijahresbarwert: 151.347 $**		

über drei Jahre einen risikobereinigten Gesamtbarwert von 151.300 US-Dollar ergibt.

Zusammengefasste Finanzergebnisse

KONSOLIDIERTE RISIKOBEREINIGTE MESSGRÖßEN FÜR EINEN ZEITRAUM VON DREI JAHREN

Cashflow-Diagramm (risikobereinigt)



Die in den Abschnitten zu Nutzen und Kosten berechneten finanziellen Ergebnisse können zur Bestimmung des ROI, des KW und eines Amortisierungszeitraums für die Investition des Modellunternehmens verwendet werden. Forrester hat dieser Analyse einen jährlichen Diskontsatz von 10 % zugrunde gelegt.

Für die Ermittlung der risikobereinigten Werte für ROI, KW und Amortisierungszeitraum werden Risikoanpassungsfaktoren auf die unbereinigten Ergebnisse der einzelnen Nutzen- und Kostenabschnitte angewendet.

Cashflow-Analyse (risikobereinigte Schätzungen)

	Ausgangswert	1. Jahr	2. Jahr	3. Jahr	Gesamtwert	Barwert
Gesamtkosten	(108.407 $)	(498.488 $)	(605.914 $)	(713.096 $)	(1.925.905 $)	(1.598.093 $)
Gesamtnutzen	0 $	1.554.294 $	1.251.188 $	1.306.291 $	4.111.774 $	3.428.472 $
Nettonutzen	(108.407 $)	1.055.807 $	645.273 $	593.195 $	2.185.868 $	1.830.379 $
ROI						115 %
Amortisierungs-dauer (in Monaten)						<6

Anhang A: Total Economic Impact

Total Economic Impact ist eine von Forrester Research entwickelte Methodik, die die Entscheidungsfindungsprozesse eines Unternehmens zu technischen Fragen optimiert und Anbieter bei der Kommunikation des Leistungsversprechens ihrer Produkte und Dienstleistungen gegenüber Kunden unterstützt. Die TEI-Methodik erleichtert es Unternehmen, den messbaren Wert von IT-Initiativen gegenüber der oberen Führungsebene und anderen wichtigen geschäftlichen Stakeholdern zu demonstrieren, zu rechtfertigen und zu veranschaulichen.

TOTAL ECONOMIC IMPACT – ANSATZ

Der Nutzen ist der Wert, der dem Unternehmen durch das Produkt entsteht. Die TEI-Methodik gewichtet die Ermittlung des Nutzens und die Messung der Kosten gleichermaßen. Somit wird eine umfassende Untersuchung der Auswirkungen der Technologie auf die gesamte Organisation ermöglicht.

Die Kosten berücksichtigen alle Ausgaben, die zur Schaffung des angestrebten Mehrwerts oder Nutzens durch das Produkt erforderlich sind. Die Kostenkategorie in TEI erfasst die über die gegenwärtige Umgebung 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.

Die Risiken messen die Unsicherheit der Nutzen- und Kostenschätzungen in Bezug auf: 1) die Wahrscheinlichkeit, dass diese Schätzungen den ursprünglichen Prognosen entsprechen, und 2) die Wahrscheinlichkeit, dass diese Schätzungen im Laufe der Zeit zutreffen. Risikofaktoren der TEI-Methodik basieren auf einer „Dreiecksverteilung“.

Die Spalte für die anfängliche Investition enthält Kosten, die zum „Zeitpunkt 0“ oder zu Beginn von Jahr 1 entstanden sind. Diese Kosten werden nicht diskontiert. Alle anderen Cashflows werden unter Verwendung eines Diskontsatzes am Ende des Jahres diskontiert. Barwertberechnungen werden für jede Gesamtkosten- und Gesamtnutzenschätzung vorgenommen. Kapitalwertberechnungen in den Übersichtstabellen entsprechen der Summe der anfänglichen Investition und der diskontierten Cashflows für die einzelnen Jahre. Die Summen und Barwertberechnungen in den Tabellen für Gesamtnutzen, Gesamtkosten und Cashflow ergeben eventuell nicht den exakten Gesamtwert, da einige Beträge eventuell gerundet sind.

BARWERT (BW)

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

KAPITALWERT (KW)

Der Barwert oder aktuelle Wert von (diskontierten) zukünftigen Netto-Cashflows zu einem gegebenen Zinssatz (dem Diskontsatz). Ein positiver Projektkapitalwert bedeutet normalerweise, dass die Investition vorgenommen werden sollte, sofern nicht andere Projekte höhere Kapitalwerte aufweisen.

KAPITALRENDITE (ROI)

Die erwartete Rendite eines Projekts, angegeben als Prozentwert. Zur Berechnung des ROI wird der Nettonutzen (Nutzen abzgl. Kosten) durch die Kosten geteilt.

DISKONTSATZ

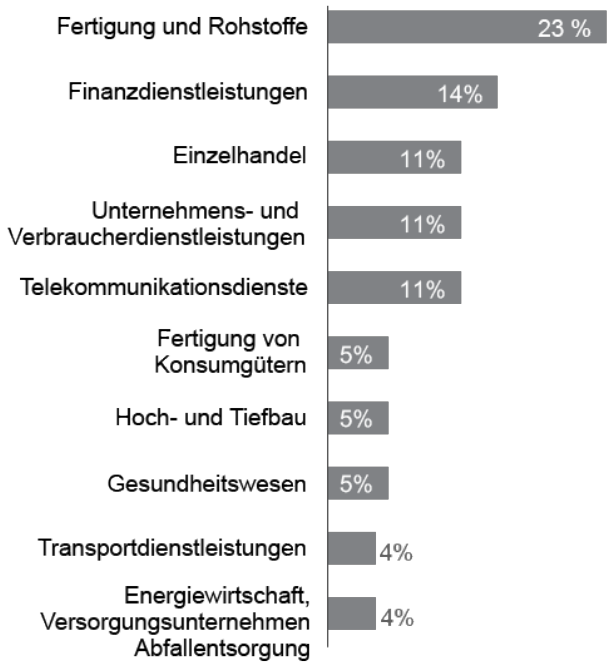
Der in der Cashflow-Analyse verwendete Zinssatz, mit dem der Zeitwert des Geldes ermittelt wird. Unternehmen verwenden in der Regel Diskontsätze zwischen 8 % und 16 %.

AMORTISIERUNGSZEITRAUM

Die Gewinnschwelle einer Investition. Dies ist der Zeitpunkt, an dem der Nettonutzen (Nutzen abzgl. Kosten) gleich der Anfangsinvestition bzw. den Eingangskosten ist.

Anhang B: Demografie

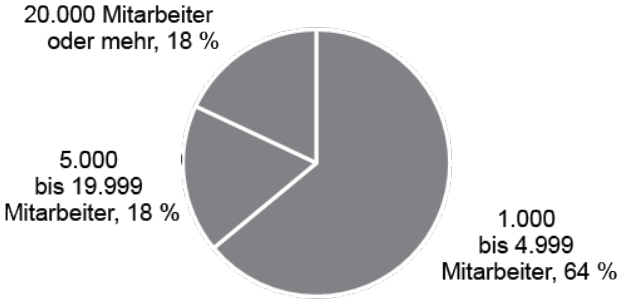
„Welcher der folgenden Branchen würden Sie Ihr Unternehmen am ehesten zuordnen?“



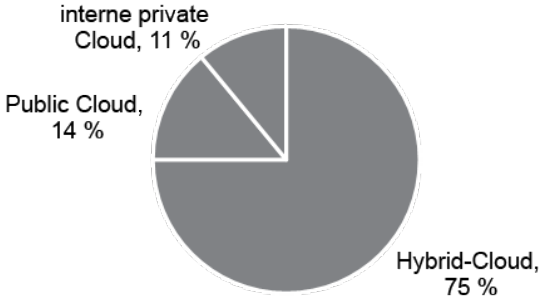
„In welchem Land sind Sie ansässig?“

53 %	USA
19 %	Deutschland
17 %	Vereinigtes Königreich
6 %	Frankreich
5 %	Australien

„Wie viele Mitarbeiter sind nach Ihrer Einschätzung weltweit für Ihr Unternehmen tätig?“



„Wo hostet Ihr Unternehmen derzeit seine Daten, Anwendungen und Workloads?“



Basis: 132 Entscheidungsträger im Bereich Cloud-Sicherheit (aufgrund von Rundungsfehlern ergeben die Prozentwerte nicht unbedingt 100 %)
Quelle: „PAN Virtual Firewalls TEI“, Studie im Auftrag von Palo Alto Networks, vorgelegt im Oktober 2021 von Forrester Consulting

Anhang C: Anmerkungen

[1] Total Economic Impact (TEI) ist eine von Forrester Research entwickelte Methodik, die die Entscheidungsfindungsprozesse eines Unternehmens zu technischen Fragen optimiert und Anbieter bei der Kommunikation des Leistungsversprechens ihrer Produkte und Dienstleistungen gegenüber Kunden unterstützt. Die TEI-Methodik erleichtert es Unternehmen, den messbaren Wert von IT-Initiativen gegenüber der oberen Führungsebene und anderen wichtigen geschäftlichen Stakeholdern zu demonstrieren, zu rechtfertigen und zu veranschaulichen.

[2] Quelle: „Forrester Consulting Cost Of A Cybersecurity Breach Survey, Q4 2020“.


FORRESTER®