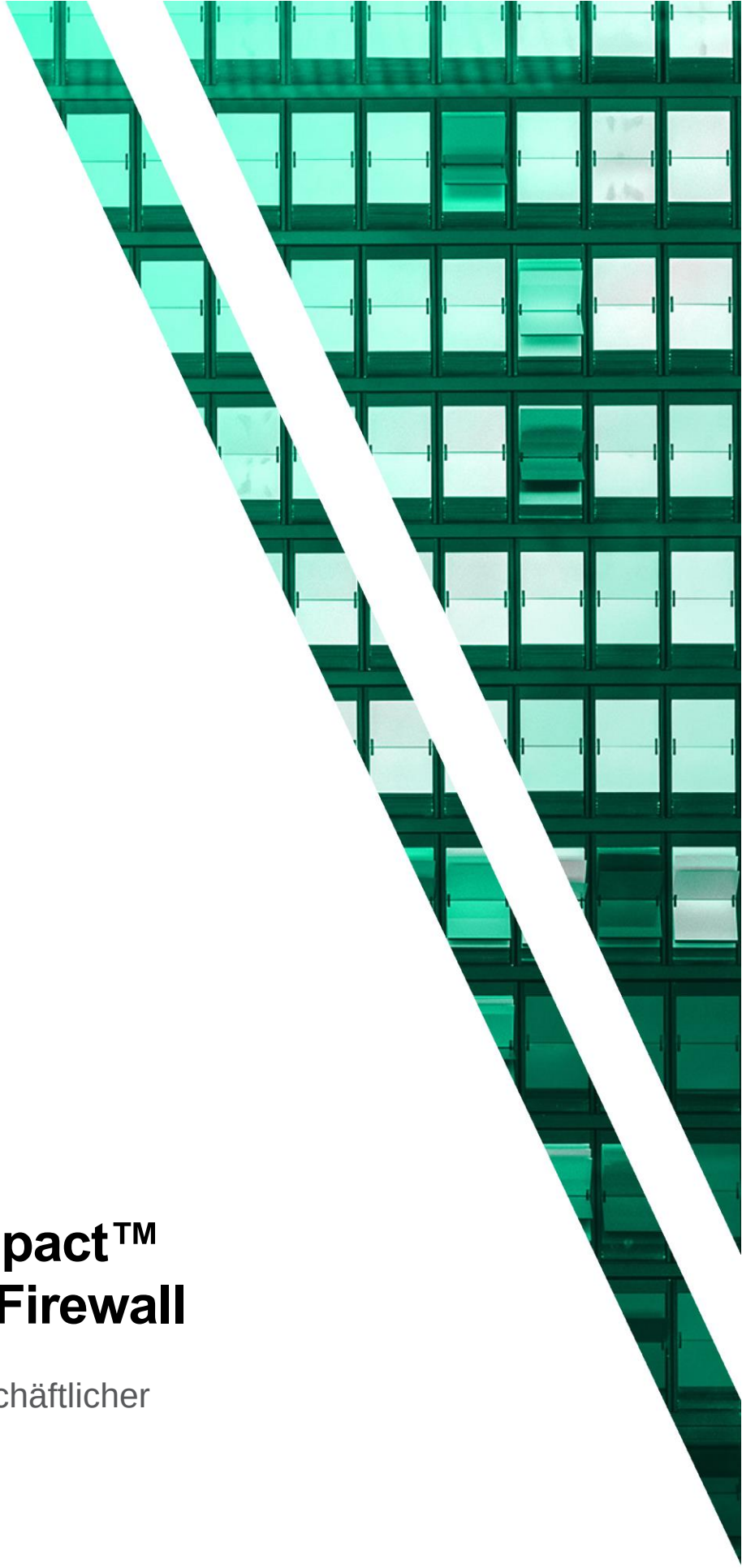
FORRESTER®



Total Economic Impact™ von Cisco Secure Firewall

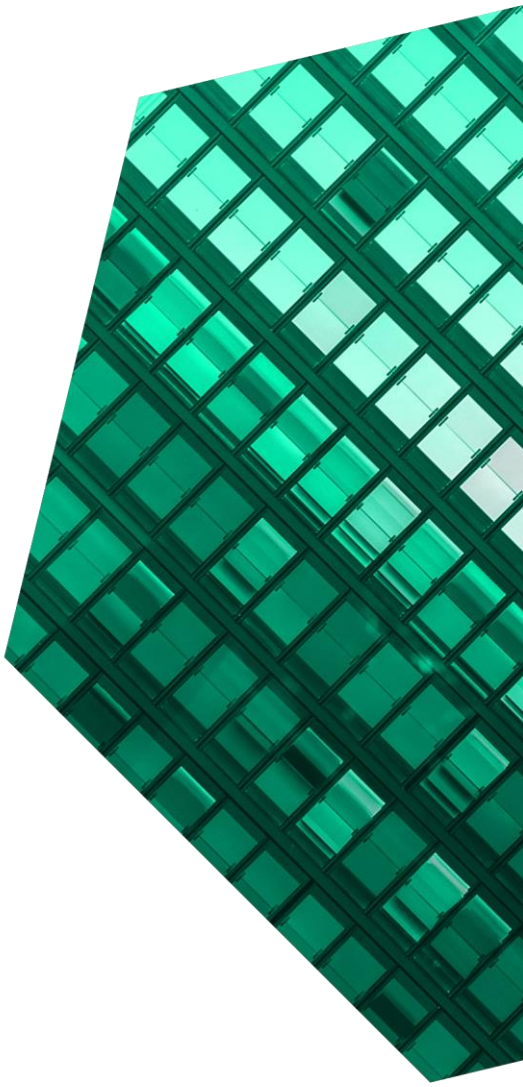
Kosteneinsparungen und geschäftlicher Nutzen durch Secure Firewall

MÄRZ 2022

EINE FORRESTER TOTAL ECONOMIC IMPACT™-STUDIE IM AUFTRAG VON CISCO

Inhalt

Beratungsteam: *Henry Huang*
Nick Mayberry



Kurze Zusammenfassung

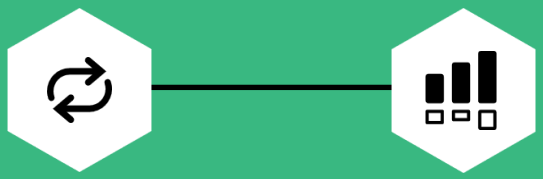
Cisco Secure Firewall und Firewall Management Center verbessern Transparenz und Kontrolle von Unternehmen hinsichtlich ihrer Netzwerksicherheit. Die Unternehmen der Befragungsteilnehmer sparten 95 % der fachlichen Arbeiten in Bezug auf Firewalls und bis zu 83 % des zugehörigen fachlichen Arbeitsaufwands für sicherheitsbezogene Aspekte. Außerdem reduzierten sie das Risiko schwerwiegender Sicherheitsverletzungen um bis zu 80 % und erzielten gleichzeitig eine Verbesserung der Endnutzerproduktivität, indem sie Störungen bei Netzwerken und VPNs minimierten. Der Sicherheitsstatus wurde sogar verbessert, während die Firewall-Bereitstellungen um 25 % reduziert wurden.

Cisco Secure Firewall ist eine Layer-7-Netzwerksicherheitslösung der nächsten Generation, die Organisationen vor externen und internen Bedrohungen schützt und Netzwerk- und Sicherheitsteams die Verwaltung von Firewalls und Bedrohungen erleichtert. Organisationen können Cisco Secure Firewall mit Firewall Management Center (FMC) verwalten. FMC fungiert als zentraler Hub für die Firewall-Verwaltung und Bedrohungsabwehr und ermöglicht Netzwerk- und Sicherheitsteams bessere, einheitlichere und – selbst auf der Anwendungsebene – umfassendere Einblicke in Netzwerkaktivitäten und Bedrohungen, die in verschlüsseltem Datenverkehr festgestellt werden. Zudem bietet die Lösung das IPS (Intrusion Prevention System) Snort 3 für eine bessere Kontrolle und umfasst Software-Erweiterungen für die URL-Filterung und die Verteidigung gegen Schadsoftware.

Lizenzen für Cisco Secure Firewall beinhalten die Nutzung von SecureX, der integrierten Plattform von Cisco. Damit können Organisationen Daten zu Bedrohungen aus dem Cisco Secure-Portfolio und Drittanbieter-Tools in einer einzigen globalen Sicht von mit Kontextinformationen angereicherten Daten konsolidieren, um rasche Analysen und Reaktionen zu erzielen.

Cisco beauftragte Forrester Consulting mit der Durchführung einer Total Economic Impact™ (TEI)-Studie zur Untersuchung der potenziellen Kapitalrendite (ROI), die Unternehmen durch den Einsatz von Secure Firewall erzielen können.[1] Ziel dieser Studie ist es, den Lesern eine Rahmenstruktur zur Beurteilung der potenziellen finanziellen Auswirkungen von Secure Firewall auf ihr Unternehmen bereitzustellen.

WICHTIGE KENNZAHLEN



Kapitalrendite (ROI)
195 %

Kapitalwert (KW)
12,29 Mio. USD

Um den Nutzen, die Kosten und die Risiken in Verbindung mit dieser Investition besser zu verstehen, befragte Forrester zehn Entscheidungsträger aus acht Organisationen mit Erfahrung im Einsatz von Secure Firewall. Die Erfahrungen der befragten Entscheidungsträger wurden für diese Studie von Forrester zusammengefasst und dienten als Grundlage zur Konstruktion eines Modellunternehmens.

Die Befragten erklärten, dass ihrer Organisationen vor der Verwendung von Secure Firewall die Transparenz und Funktionen fehlten, die sie für eine angemessene Verwaltung und effiziente Sicherung ihrer Netzwerke benötigten. Die Befragten gaben an, dass ihre netzwerkbezogenen Arbeitsabläufe wie die Firewall-Bereitstellung, das Erstellen von Richtlinien, Firewall-Upgrades und Richtlinienaktualisierungen ohne diese Einblicke und eine effiziente grafische Benutzeroberfläche (GUI) mit einem erheblichen Zeitaufwand verbunden waren. Zudem musste viel Zeit auf sicherheitsbezogene Arbeitsabläufe wie die Untersuchung und Beseitigung von Bedrohungen und die Fernzugriffsadministration aufgewendet werden. Die Befragten gaben außerdem an, dass sie in Zeiten hoher Nachfrage mit schlechter Netzwerkleistung und Komplikationen durch die Verwaltung von Lösungen mehrerer Anbieter zu kämpfen hatten.

Nach der Investition in Secure Firewall konnten die Befragten nicht nur den Zeitaufwand für die zuvor genannten netzwerk- und sicherheitsbezogenen Arbeitsabläufe verringern, sondern auch die Sicherheit ihrer Organisationen insgesamt verbessern. Zudem steigerten die Organisationen die Produktivität ihrer Mitarbeiter durch die schnellere Aktualisierung von Richtlinien, erweiterte Überprüfungen von Netzwerkverkehr und eine insgesamt verbesserte Netzwerkleistung. Gleichzeitig konnten sie Altlösungen außer Betrieb nehmen und die damit verbundenen Kosten für Verwaltungszeiten größtenteils einsparten.

Gesamtnutzen

18,6 Mio. USD

WESENTLICHE ERGEBNISSE

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

- **Verringerung von Arbeitsabläufen für den Netzwerkbetrieb um bis zu 95 %.** Dank der neuesten Funktionen von Cisco Secure Firewall und der einfachen Verwaltung über Firewall Management Center gelang es den Unternehmen der Befragten, den Zeitaufwand für Tätigkeiten zu reduzieren:
  - Firewall-Bereitstellungen um 36 %
  - Firewall-Aktualisierungen um 90 %
  - Aktualisierung von Firewall-Richtlinien verglichen mit herkömmlichen Firewalls der Serie ASA (Adaptive Security Appliance) 5500-X um 95 %
  - Aktualisierung von Firewall-Richtlinien verglichen mit frühen Versionen der Firewall Threat Defense (FTD)-basierten Richtlinien um 80 %
  - Aktualisierung von virtuellen Firewalls um 80 %
- **Reduzierung der Zeiten für Arbeitsabläufe wie Sicherheitsuntersuchungen und -reaktionen um bis zu 83 %.** Die Befragten gaben außerdem erhebliche Einsparungen bei Arbeiten von Sicherheitsfachkräften an. Dies war auf die Kombination aus Cisco Secure Firewall und Firewall Management Center zurückzuführen, da die Informationen dort besser für Nutzungs- und Analysezwecke organisiert sind. Die Befragten beobachteten zudem einen Rückgang des Zeitaufwands für die Untersuchung potenzieller Bedrohungen um 49 % und für entsprechende Reaktionen darauf um 83 %. Die Verwendung von SecureX in Verbindung mit Secure Firewall und FMC ermöglichte es Organisationen, bis zu 77 % der übrigen Zeit einzusparen, die für Untersuchungen und Maßnahmen aufgewendet wurde.

> **„Wir sind sehr sicherheitsbewusst und möchten Produkte nutzen, um unser Unternehmen zu schützen. Darum haben wir uns für Cisco entschieden. Bei Cisco dreht sich alles um die Sicherheit. Sicherheitsfunktionen sind nicht nur eine bloße Beigabe.“**
> *Leitender Netzwerktechniker, Fertigungsbranche*

- **Verringerung des Risikos von Sicherheitsverletzungen um bis zu 80 %.** Die Kombination aus Transparenz und Kontrolle, die Cisco Secure Firewall und Firewall Management Center ermöglichen, versetzte die Unternehmen der Befragten in die Lage, das Risiko potenzieller schwerwiegender Sicherheitsverletzungen und die damit verbundenen Kosten zu reduzieren. Im Vergleich zu herkömmlichen Firewalls der Serie ASA 5500-X verringerten diese Lösungen das Risiko von Sicherheitsverletzungen um 80 % und verglichen mit frühen FTD-basierten Firewalls um 15 %. SecureX ermöglichte es den Unternehmen der Befragten, die üb-

rigen Risiken und Kosten einer Sicherheitsverletzung um bis zu weitere 23 % zu reduzieren.

- **Die verbesserte Endnutzerproduktivität wurde mit nahezu 2 Mio. USD jährlich bewertet.** Der Einsatz von Cisco Secure Firewall und Firewall Management Center verbesserte die Produktivität der befragten Unternehmen auf zweierlei Art. Zunächst konnten Netzwerkexperten damit Fehler bei Richtlinienaktualisierungen, die Störungen verursachten, 80 % schneller beheben. Zweitens verringerte die Lösung den Schweregrad von Beeinträchtigungen der Netzwerkleistung, wodurch jeder betroffene Endanwender nahezu 9 Stunden Arbeitszeit jährlich hinzugewann.
- **Verringerung der Kosten durch die Außerbetriebnahme veralteter Tools.** Die Befragten gaben außerdem an, dass sie durch Cisco Secure Firewall ihre zuvor implementierten, teuren und veralteten Sicherheitslösungen außer Betrieb nehmen konnten. Außerdem bezifferten die Befragten ihre Einsparungen für eigenständige IPS auf Hunderttausende von Dollar jährlich. Durch die Vermeidung von Kosten zur Ersetzung ihrer vorhandenen Sicherheitslösungen wurden mehrere Millionen Dollar eingespart. Zusätzlich reduzierten sich die Kosten um 25 %, da Cisco Secure Firewall dasselbe Maß an Schutz mit einer geringeren Anzahl Firewalls ermöglichte.

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

- **Produktivitäts- und Sicherheitserweiterungen für das VPN.** Cisco Secure Firewall ermöglichte auch eine bessere VPN-Produktivität und -Sicherheit per Fernzugriff durch Clustering, lokale Authentifizierung und die Authentifizierung mit mehreren Zertifikaten. Endbenutzer bauten bessere Verbindungen per VPN auf und die Organisation hatte eine stärkere Kontrolle über den Zugriff.
- **Verbesserung der Abläufe für die Arbeit im Homeoffice.** Die Kontrollen von Cisco Secure Firewall trugen auch dazu bei, einen reibungslosen Betrieb aufrechtzuerhalten, als die VPN-Nutzung durch die Umstellung von Mitarbeitern auf das Arbeiten im Homeoffice geradezu explodierte. Netzwerkfachkräfte profitierten von der Bandbreitenbeschränkung sowie von Redundanzoptimierungen, die zu einer Verbesserung des Mitarbeitererlebnisses und zu Produktivitätssteigerungen selbst bei sehr hoher Nachfrage beitrugen.
- **Einfacher Umstieg auf die Cloud.** Schließlich berichteten die Befragten, dass sie ihre Cloud-Initiativen dank Cisco Secure Firewall leichter durchführen konnten, da die zentrale Plattform den Traffic innerhalb von Standorten, zwischen Standorten und zwischen der Organisation und mehreren Cloud-Plattformen schützt. Cisco stellt insbesondere standardisierte Richtlinien und validierte Bereitstellungswege für die Secure Firewall über Cloud-Plattform-Marktplätze bereit.

Kosten. Die risikobereinigten barwertigen Kosten umfassen Folgendes:

- **Lizenzkosten.** Obwohl die Lizenzkosten zu den höchsten Kosten zählten, die bei den Unternehmen der Befragten anfielen, sparten sie durch den Abschluss einer Cisco Enterprise-Lizenzvereinbarung Hunderttausende von Dollar für zusätzliche Funktionen und Lösungen ein, die ihnen vorher fehlten und die nun das Sicherheitsniveau der Organisationen erhöhen. Die SecureX-Lizenzberechtigung ist in Secure Firewall inbegriffen.
- **Kosten für Implementierung, Richtlinienerstellung und Schulung.** Die Befragten gaben an, dass für die Implementierung und die Bereitstellung von Firewalls und für die Erstellung entsprechender Richtlinien interne Kosten anfielen. Die Bereitstellung einer Firewall dauert nach Schätzungen 6 Stunden pro Standort und das Erstellen von Richtlinien schätzungsweise 30 Stunden. Die Implementierung von SecureX erfordert zusätzlich 20 Stunden Arbeit und die laufende Verwaltung 100 Stunden pro Jahr. Einige der Befragten gaben auch Schulungsbedarf für ihre Netzwerk- und Sicherheitsfachkräfte zur Nutzung von Cisco Secure Firewall und Firewall Management Center an. Die internen Schulungskosten beliefen sich auf 2 Stunden pro geschultem Mitarbeiter, wobei die Befragten angaben, dass sie öffentlich verfügbare Schulungsvideos von Cisco Sicherheitsexperten nutzten.

Die Befragung von Entscheidungsträgern und die Finanzanalyse ergaben, dass sich für ein Modellunternehmen über einen Zeitraum von drei Jahren ein Nutzen in Höhe von 18,59 Mio. USD gegenüber Kosten in Höhe von 6,30 Mio. USD ergibt, was einem Kapitalwert (KW) von 12,29 Mio. USD und einem ROI von 195 % entspricht.

ROI
195 %

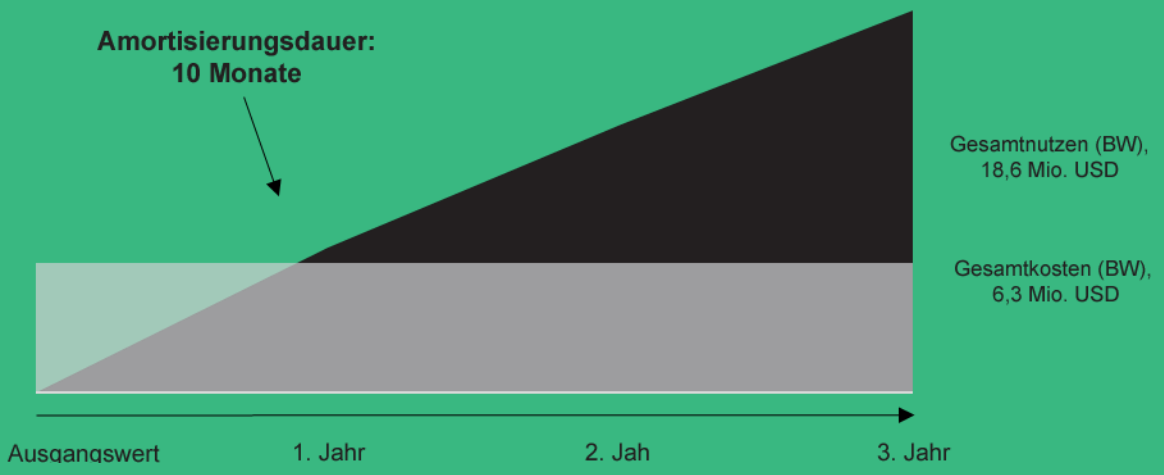
NUTZEN (BW)
18,59 Mio. USD

KAPITALWERT
12,29 Mio. USD

AMORTISIERUNG
10 Monate

Nutzen (über drei Jahre)

Zusammenfassung der finanziellen Ergebnisse



TEI-BEZUGSRAHMEN UND -METHODIK

Aus den in der Befragung erfassten Daten hat Forrester eine Rahmenstruktur zum Total Economic Impact™ für Unternehmen erstellt, die eine Investition in Cisco Secure Firewall in Erwägung ziehen.

Dieser Bezugsrahmen dient dazu, Kosten, Nutzen, Flexibilität und Risikofaktoren zu ermitteln, die für die Investitionsentscheidung von Bedeutung sind. Forrester hat ein mehrere Schritte umfassendes Verfahren verwendet, um die Auswirkungen zu bewerten, die Secure Firewall auf ein Unternehmen haben kann.

ANGABEN

Die Leser werden auf Folgendes hingewiesen:

Diese Studie wurde von Cisco 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 oder Organisationen erzielen werden. Forrester empfiehlt den Lesern dringend, mithilfe der in der Studie dargelegten Rahmenstruktur eigene Prognosen zu erstellen, um die Angemessenheit einer Investition in Secure Firewall zu ermitteln.

Zwar hat Cisco Überprüfungen vorgenommen und Forrester Rückmeldung gegeben, doch behält sich Forrester 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.

Cisco hat die Kundennamen für die Befragungen angegeben, an den Befragungen jedoch nicht teilgenommen.

SORGFALTSPFLICHT

Befragung von Cisco-Vertretern und Forrester-Analysten zur Erhebung von Daten zu Secure Firewall.

BEFRAGUNG VON ENTSCHEIDUNGSTRÄGERN

Um Daten zu Kosten, Nutzen und Risiken zu erheben, wurden zehn Entscheidungsträger in Unternehmen befragt, die Secure Firewall einsetzen.

MODELLUNTERNEHMEN

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

FINANZMODELLRAHMEN

Auf der Grundlage der von den Entscheidungsträgern angesprochenen Themen und Belange wurde mithilfe der Methodik des Total Economic Impact ein für die Befragungen repräsentatives Finanzmodell erstellt und risikobereinigt.

FALLSTUDIE

Vier fundamentale Elemente des Total Economic Impact 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 Methodik des Total Economic Impact von Forrester ein umfassendes Bild der finanziellen Gesamtauswirkung von Kaufentscheidungen. Weitere Informationen zur TEI-Methodik finden Sie in Anhang A.

Die Kundenerfahrung mit Cisco Secure Firewall

Entscheidende Faktoren für die Investition in Secure Firewall

Befragte Entscheidungsträger

Befragte Person	Branche	Region	Gesamtzahl der Mitarbeiter
IT-Services-Manager	IT-Dienstleistungen	Nordamerika	750
Leitender Infrastrukturtechniker	Finanzdienstleistungen	Nordamerika	2.800
Direktionsassistent im Bereich Telekommunikationsdienste	Finanzdienstleistungen	Nordamerika	2.800
Leitender Techniker für Cybersicherheit	Sicherheitsservices	Nordamerika	3.000
Leitender Netzwerktechniker	Fertigungsbranche	Weltweit	5.500
Leitender Netzwerktechniker	Technologie	Weltweit	40.000
Leitender Sicherheitstechniker	Technologie	Weltweit	40.000
Teamleiter Sicherheitsbetrieb	Aus- und Weiterbildung	Nordamerika	46.000
Infrastrukturarchitektur-Mitarbeiter	Industrie	Weltweit	205.000
Leitender Netzwerktechniker	Technologie	Weltweit	275.000

ZENTRALE HERAUSFORDERUNGEN

Vor der Bereitstellung von Cisco Secure Firewall und Firewall Management Center nutzten die Unternehmen der Befragten größtenteils herkömmliche Firewalls der Serie ASA 5500-X, um ihre Umgebungen zu schützen. Manche der Befragten vollzogen den Umstieg von herkömmlichen ASA-basierten Firewalls zu frühen FTD-basierten Firewalls vor einigen Jahren und stellten nach dem Upgrade auf die neueste FTD-Version von Cisco Secure Firewall und Firewall Management Center zusätzliche Vorteile fest.

Die Befragten sprachen über die typischen Herausforderungen, mit denen ihre Unternehmen zu kämpfen hatten:

- **Eingeschränkte Transparenz.** Die Befragten gaben an, dass ihre früheren Umgebungen, die sich alle auf Firewalls der Serie ASA 5500-X stützten, nur begrenzte Einblicke in den Gesamtsicherheitsstatus boten. Eine Ursache dafür war die fehlende Integration. In früheren Umgebungen war es für die Organisationen der Befragten schwierig, verschiedene Sicherheitslösungen zum Aufbau einer einheitlichen Verwaltung und konsistenter Richtlinien zu integrieren und gleichzeitig eine zentrale Sicht auf ihre Sicherheitsinfrastruktur zu erhalten. Ein anderer Grund für die begrenzte Transparenz war, dass die Erstellung einer zentralen Netzwerkansicht in den vorherigen Umgebungen auf Port-Überprüfungen basierte. Die Befragten gaben an, dass dies verhinderte, dass sie einen tiefer gehenden Einblick in die Daten erhielten. Die Anwendungstransparenz war daher gering und es stand nur begrenzter historischer Kontext zur Verfügung.

> **„Zuvor fehlten uns Funktionen wie eine moderne Anwendungskontrolle. Wir wussten nicht, wie unsere Anwender das Netzwerk nutzten, und konnten daher nicht angemessen auf diese Nutzung reagieren.“**
> *Teamleiter Sicherheitsbetrieb, Bildungswesen*

- **Hohe Zeitkosten für die Implementierung und Verwaltung von Firewalls.** Die Befragten gaben außerdem an, dass die Bereitstellung und die Verwaltung ihrer veralteten Firewalls mit einem hohen Zeitaufwand verbunden waren. Vieles davon war auf die fehlende Möglichkeit zurückzuführen, Updates an mehrere Geräte gleichzeitig weiterzuleiten. Einschätzungen des Teamleiters für den Sicherheitsbetrieb aus dem Bildungswesen zufolge dauerte die Bereitstellung einer einfachen Firewall-Regel 45 Minuten bis eine Stunde. Außerdem gaben die Befragten an, dass die fehlende Transparenz ihrer früheren Umgebungen dazu führte, dass sie unverhältnismäßig viel Zeit darauf verwendeten, Korrelationen zwischen Daten verschiedener Systeme herzustellen, um Sicherheitsstatus nachzuweisen.

„Die einfache Verwaltung und Integration ist einer der Vorteile von Cisco. Wir profitieren außerdem von einer Datenanreicherung, da der Datenfluss zwischen verschiedenen Systemen einfacher verläuft. Darüber hinaus haben wir autonome Reaktionen auf bestimmte Bedrohungen eingerichtet. All das war vorher nicht möglich.“
Leitender Techniker für Cybersicherheit, Sicherheitsservices

- **Schlechte Leistung.** Weiterhin sprachen die Befragten von der Leistungsschwäche ihrer früheren Systeme. Der Teamleiter für den Sicherheitsbetrieb aus dem Bildungswesen gab etwa an, dass die früheren Lösungen bei extrem hohen Anforderungen an die Netzwerk- und Sicherheitsinfrastruktur „regelmäßig abstürzten und neu gestartet wurden und Pakete deswegen verworfen wurden.“ Dies ging so weit, dass es sich auf die Produktivität auswirkte. „Wenn Lehrer der Klasse ein Video oder eine Präsentation über das Netzwerk vorführen wollten, funktionierte es nicht.“
- **Anbietermanagement.** Schließlich gaben die Befragten an, dass die Tatsache, dass sich ihre früheren Umgebungen aus Lösungen mehrerer Anbieter zusammensetzten, das Anbietermanagement erschwerte. Der leitende Infrastrukturtechniker des Finanzdienstleistungsunternehmens sagte: „Da wir mehrere Anbieter hatten, mussten wir alle Aufgaben mehrmals durchführen. Jede Änderung oder Aktualisierung musste auf einer anderen Plattform vorgenommen werden, um sie auf die unterschiedlichen Systeme anzuwenden.“

MODELLUNTERNEHMEN

Basierend auf den Befragungen hat Forrester eine TEI-Rahmenstruktur entwickelt, ein Modellunternehmen konstruiert und eine ROI-Analyse erstellt, die die Bereiche veranschaulicht, in denen mit finanziellen Auswirkungen zu rechnen ist. Das Modellunternehmen ist repräsentativ für die neun von Forrester befragten Entscheidungsträger und dient zur Darstellung der zusammengefassten Finanzanalyse im nächsten Abschnitt. Die Eigenschaften des Modellunternehmens sind nachfolgend aufgelistet.

Beschreibung des Modellunternehmens. Das Modellunternehmen ist ein B2B-Technologieunternehmen mit einem Jahresumsatz von 5 Mrd. US-Dollar und 16.000 Mitarbeitern. Es betreut Kunden in aller Welt. Die Organisation ist auf eine hohe Verfügbarkeit ihrer Rechenzentren angewiesen, um einen einheitlichen Kundenzugriff auf die dort gespeicherten Daten sicherzustellen. Diese Rechenzentren erfordern auch eine erhöhte Sicherheit, um sensible Kundendaten vor unerwünschten Zugriffen oder Angriffen zu schützen. Zusätzlich zu den Rechenzentren verfolgt die Organisation mit der Nutzung einer Multicloud-Umgebung einen zunehmend stärker verteilten Ansatz. Darüber hinaus setzt die Organisation auch Secure Firewalls ein, um ihre Standorte/Niederlassungen am Netzwerkrand zu schützen.

Merkmale der Implementierung. Das Modellunternehmen hat bereits in Cisco-Firewalls der nächsten Generation investiert. Seine Firewalls setzen sich zu zwei Dritteln aus Cisco Firepower-Geräten und zu einem Drittel aus Firewalls der Serie ASA 5500-X zusammen. Nun erfolgt noch die Umstellung der 102 Firewalls für Homeoffices, Rechenzentren und die Hauptniederlassung auf die neueste Version von Cisco Secure Firewall, die Aktualisierung seiner 68 Firepower-Geräte sowie die Ersetzung der 34 ASA-basierten Geräte. Manche der Befragten entschieden sich für die Aktualisierung vorhandener herkömmlicher Geräte auf FTD-Software ohne einen Hardware-Austausch. Das Modellunternehmen setzt in seinen Rechenzentren außerdem virtuelle Firewalls aus Cisco Secure Firewall ein, um den East-West-Traffic zwischen den Rechenzentren und den Niederlassungen sowie den Datenverkehr zwischen den Rechenzentren und mehreren Public-Cloud-Plattformen zu verarbeiten. Es nutzt die Einbeziehung von SecureX in seiner Secure Firewall-Lizenz, um die Arbeit seines Sicherheitsteams zu Untersuchung von Bedrohungen und deren Abwehr zu verbessern.

Grundlegende Annahmen

- **5 Mrd. USD Umsatz**
- **16.000 Mitarbeiter**
- **Austausch von 34 ASA-basierten Firewalls**
- **Aktualisierung von 68 Firepower-Firewalls auf die neueste Cisco Secure Firewall**

Nutzenanalyse

Daten zum quantifizierten Nutzen, angewendet auf das Modellunternehmen

Gesamtnutzen

Ref.	Nutzen	1. Jahr	2. Jahr	3. Jahr	Gesamtwert	Barwert
Atr	Verbesserungen der Firewall-Verwaltung	134.951 USD	25.556 USD	25.556 USD	186.064 USD	163.005 USD
Btr	Verbesserungen von Sicherheitsarbeitsabläufen	2.669.879 USD	3.685.484 USD	3.685.484 USD	10.040.848 USD	8.241.976 USD
Ctr	Verringertes Risiko von schwerwiegenden Sicherheitsverletzungen und Produktivitätsverlust	1.291.446 USD	1.393.402 USD	1.520.848 USD	4.205.696 USD	3.468.249 USD
Dtr	Leistungsvorteile für die Produktivität von Mitarbeitern	1.656.403 USD	1.656.403 USD	1.656.403 USD	4.969.210 USD	4.119.230 USD
Etr	Kosteneinsparungen durch außer Betrieb genommene Altlösungen	1.985.115 USD	503.513 USD	503.513 USD	2.992.142 USD	2.599.074 USD
	Gesamtnutzen (risikobereinigt)	7.737.795 USD	7.264.360 USD	7.391.805 USD	22.393.959 USD	18.591.534 USD

VERBESSERUNGEN DER FIREWALL-VERWALTUNG

Fakten und Daten. Die befragten Entscheidungsträger gaben an, dass sie nach der Bereitstellung von Cisco Secure Firewall Zeit und Kosten im Zusammenhang mit der Verwaltung von Firewalls einsparten, unabhängig davon, ob sie eine Umstellung von Legacy-Firewalls oder Aktualisierungen von frühen Versionen von Firepower Threat Defense durchführten. Ein beträchtlicher Teil dieser Verbesserungen ist auf die Tatsache zurückzuführen, dass Netzwerkexperten dank der einheitlichen Ansicht von Firewall Management Center die Firewalls zentral verwalten und Änderungen auf mehreren Geräten gleichzeitig bereitstellen können.

„Mit FMC können wir Firewalls zentral verwalten und aktualisieren, anstatt wie früher zwischen verschiedenen Firewalls hin- und herzuspringen.“
IT-Services-Manager, IT-Dienstleistungen

Alle Organisationen der Befragten stellten fest, im Zusammenhang mit der Bereitstellung von Firewalls Zeit und Kosten zu sparen. In Bezug auf herkömmliche ASA-basierte Firewalls gaben die Befragten an, dass die Firewall-Bereitstellung einen erheblichen Zeitaufwand erforderte, etwa für das Verfassen fallspezifischer Firewall-Regeln und deren manuelle Verteilung an die Vielzahl von vorhandenen Firewall-Richtlinien.

„Mit Cisco Secure Firewall konnten wir neue Firewalls schnell bereitstellen und hochfahren. Wir benötigten für den Ausbau unserer Firewalls keine zusätzlichen Mitarbeiter.“
Leitender Netzwerktechniker, Technologieunternehmen

Nach dem Umstieg auf Cisco Secure Firewall und Firewall Management Center berichteten die Befragten von Einsparungen zwischen 30 % und 40 % der Bereitstellungszeit von

Firewalls. Die Zeiteinsparung beruhte auf der Möglichkeit zum Automatisieren der Bereitstellung von Cisco Secure Firewall.

Der leitende Netzwerktechniker aus der Technologiebranche sagte beispielsweise: „Wir haben die Bereitstellung mit Cisco Secure Firewall automatisiert. Wir haben die Provisionierung der Box, die Zuweisung der IP-Adresse, das Einrichten des Chassis und das Anwenden der Richtlinie automatisiert."

„Die integrierte Automatisierung bringt uns die größte Zeitersparnis, sogar bei Upgrades. Ich muss jetzt nicht mehr wie ein Babysitter den Upgrade-Prozess überwachen, wie es bei den ASAs der Fall war. Ich kann etwas anderes tun, und Firepower informiert mich darüber, falls die Firewall nicht in angemessener Zeit wieder online geht."
Leitender Netzwerktechniker, Technologieunternehmen

Die Automatisierung half den Befragten außerdem bei der Verwaltung und Pflege ihrer Cisco Secure Firewalls nach der Bereitstellung. Cisco Secure Firewall umfasst integrierte automatisierte Upgrades. Die Befragten gaben an, dass Upgrades des ASA-basierter Firewalls mehrere Stunden dauern konnten. Die Firewalls kamen nacheinander an die Reihe und es wurden jeweils Dateien hochgeladen und die Systeme neu gestartet. Den Befragten zufolge sind bei Cisco Secure Firewall und Firewall Management Center die Upgrades der Firewalls mit einigen wenigen Klicks auf der Benutzeroberfläche erledigt. 30 Minuten später kann überprüft werden, ob die Upgrades erfolgreich abgeschlossen wurden.

„Bei der Richtlinienverwaltung verzeichnen wir eine Zeitersparnis von 60 bis 70 %, seit wir von ASA auf Cisco Secure Firewall umgestiegen sind."
IT-Services-Manager, IT-Dienstleistungen

Die Befragten gaben an, dass sie mit Cisco Secure Firewall und Firewall Management Center die Richtlinien mithilfe eines objektorientierten Systems ohne umfangreiche Zugriffskontrolllisten (Access Control Lists, ACLs) in Kategorien und Zonen organisieren konnten. Im Gegensatz zur früheren manuellen Aktualisierung jedes einzelnen Geräts konnten Richtlinien damit nun auch automatisch bereitgestellt und aktualisiert werden.

„Cisco Secure Firewall stellt automatisch 90 % der Richtlinien bereit. Wir arbeiten nicht mehr mit einmaligen Konfigurationen."
Leitender Netzwerktechniker, Technologieunternehmen

Die Befragten berichteten außerdem von zusätzlichen Zeiteinsparungen nach dem Upgrade von den früheren auf die aktuellen FTDs mit Cisco Secure Firepower. Der leitende Infrastrukturtechniker aus dem Finanzdienstleistungssektor gab an, dass die Richtlinienbereitstellung bei frühen FTDs zwischen 10 und 15 Minuten beanspruchte und die Bereit-

„Die Richtlinienverwaltung mit Cisco Secure Firewall ist kinderleicht. Die Benutzeroberfläche von Firewall Management Center ist unkompliziert, schlank und intuitiv."
Leitender Netzwerktechniker, Technologieunternehmen

stellungszeiten nach dem Upgrade der FTDs auf etwa 3 Minuten zurückgingen.

Einer der Befragten nutzte nicht Firewall Management Center, sondern verwaltete Firewalls über Cisco Defense Orchestrator (CDO) als Cloud-Software-as-a-Service (Cloud-SaaS). In Bezug auf CDO äußerte der Infrastrukturarchitekt Folgendes: „Die Einführung von CDO verlief reibungslos. Da unsere Techniker bereits mit Cisco Security Manager (CSM) vertraut waren, konnten sie die Befehlszeilenschnittstelle nutzen und Makros erstellen. Das war wesentlich leichter als der Wechsel zu einem anderen Anbieter, was das Erlernen neuer Konzepte in den oberen Schichten und somit mehr Komplexität bedeutet hätte."

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

- 34 herkömmliche ASA-5500-X-Firewalls werden durch Cisco Secure Firewalls ersetzt.
- Das Modellunternehmen spart sich die 55 Stunden Arbeit, die die Bereitstellung und die Erstellung von Richtlinien für das Ersetzen jeder herkömmlichen Firewall erfordern würde.
- Das Modellunternehmen spart sich 90 % der 30 Minuten, die es jedes Quartal für das Upgrade jeder Firewall aufwenden musste.
- Das Modellunternehmen aktualisiert jede Firewall-Richtlinie im Durchschnitt einmal am Tag. Durch den Umstieg auf Cisco Secure Firewall spart es sich 95 % der 1 Stunde Arbeit, die es auf die Durchführung dieser Updates aufgewendet hatte.
- Der Stundensatz inklusive Nebenkosten für einen NetSecOps-Experten (Experte im Bereich des Netzwerksicherheitsbetriebs) beträgt 65 USD.
- Für 68 FTD-Firewalls wird ein Upgrade auf die neueste Version von Cisco Secure Firewall durchgeführt. Für jede tägliche Richtlinienaktualisierung spart das Modellunternehmen 80 % der Zeit, die es für die Bereitstellung von frühen FTD-Firewalls benötigte.
- Zudem verzeichnet das Modellunternehmen Einsparungen von 80 % der Zeit, die für die Aktualisierung virtueller Firewall-Richtlinien nötig gewesen war.

Risiken. Verbesserungen beim Firewall-Management hängen von folgenden Faktoren ab:

- Art und Anzahl der vorhandenen Firewalls
- Anzahl der durch Cisco Secure Firewalls ersetzten Firewalls und die Bereitstellungsquote
- Die Entscheidung zur Bereitstellung virtueller Firewalls in Rechenzentren, um East-West- und Public-Cloud-Traffic zu verarbeiten

Ergebnisse. Zur Berücksichtigung dieser Risiken hat Forrester diesen Nutzen um 10 % nach unten korrigiert, was über drei Jahre einen risikobereinigten Gesamtbarwert (mit 10 % diskontiert) von rund 163.000 USD ergibt.

Verbesserungen der Firewall-Verwaltung					
Ref.	**Messgröße**	**Quelle**	**1. Jahr**	**2. Jahr**	**3. Jahr**
A1	Anzahl von Firewalls der nächsten Generation, die Legacy-Firewalls ersetzen	Modellunternehmen; 1/3 von insg. 102	34	0	0
A2	Einsparung bei der Bereitstellung der einzelnen Firewalls in Stunden	Befragungen	55,00	55,00	55,00
A3	Einsparung bei der Aktualisierung der einzelnen ASA-Firewalls in Stunden	90 % * 17 Stunden pro Quartal	61,2	61,2	61,2
A4	Einsparung bei der manuellen Aktualisierung der Richtlinien für ASA-Firewalls in Stunden	95 % * 1 Stunde, einmal täglich * 33 % der Umgebung	114	114	114
A5	Stundensatz von NetSecOps-Experten	Modellunternehmen	65 USD	65 USD	65 USD
A6	Zwischensumme: Reduzierung des Zeitaufwands für Bereitstellung und Upgrade herkömmlicher Layer-4-Firewalls auf Firewalls der nächsten Generation	((A1*A2)+(A3+A4))*A5	132.938 USD	11.388 USD	11.388 USD
A7	Anzahl der aktualisierten FTD-Firewalls	Modellunternehmen; 2/3 von insg. 102	68	68	68
A8	Vorheriger Zeitaufwand in Stunden für die Bereitstellung von Richtlinien mit frühen FTDs	Befragungen	0,25	0,25	0,25
A9	Zeiteinsparung für die Richtlinienbereitstellung nach dem Upgrade auf spätere FTDs	Befragungen; von 15 auf 3 Minuten	80 %	80 %	80 %
A10	Zwischensumme: Zeiteinsparung für die Bereitstellung von Richtlinien für Firepower von älteren Layer-7-Firewalls	365*A8*A9*A5*A7/102	3.163 USD	3.163 USD	3.163 USD
A11	Gesamtzahl der virtuellen Firewalls	Modellunternehmen	100	100	100
A12	Eingesparte Stunden für die Aktualisierung von Richtlinien für virtuelle Firewalls pro Jahr	80 % * 266 Stunden pro Jahr	213	213	213
A13	Zwischensumme: Zeiteinsparung für das Management virtueller Firewalls	A12*A5	13.845 USD	13.845 USD	13.845 USD
At	Verbesserungen der Firewall-Verwaltung	A6+A10+A13	149.946 USD	28.396 USD	28.396 USD
	Risikobereinigung	↓10 %			
Atr	Verbesserungen des Firewall-Managements (risikobereinigt)		134.951 USD	25.556 USD	25.556 USD
	Dreijahresgesamtwert: 186.064 USD			**Dreijahresbarwert: 163.005 USD**	

VERBESSERUNGEN VON SICHERHEITSARBEITSABLÄUFEN

Fakten und Daten. Die Bereitstellung von Cisco Secure Firewall und die Nutzung von FMC halfen den Befragten auch dabei, ihre Sicherheitsarbeitsabläufe zu optimieren. Die Entscheidungsträger gaben an, dass die ASA-basierten Geräte mehrere separate Tools zum Nachverfolgen und Protokollieren von Events über Firewalls hinweg erforderten. Mit FMC wurden die Daten von Cisco Secure Firewall an einem zentralen Ort konsolidiert, wodurch Kompromittierungsindikatoren (Indicators of Compromise, IOCs) und abgewehrte Angriffe nachverfolgt oder konsistent auf eine höhere Ebene in eine Lösung für Security Information & Event Management (SIEM) gebracht werden konnten. Mit FMC erhielten die Befragten die Möglichkeit, Verbindungen, Events und Telemetrie als Ganzes in einer stärker korrelierten Weise im gesamten Netzwerk zu prüfen.

„Sicherheitsuntersuchungen gaben einem früher das Gefühl, als müsste man ein Puzzle mit nur einem Stück zusammensetzen."
Teamleiter Sicherheitsbetrieb, Bildungswesen

Die Befragten gaben an, dass sie durch die Konsolidierung über Firewall Management Center die Zeitkosten für Sicherheitsuntersuchungen reduzieren konnten. Der leitende Techniker für Cybersicherheit aus der Sicherheitsservicebranche etwa verzeichnete aufgrund von Secure Firewall und Firewall Management Center einen Rückgang des zeitlichen Aufwands von mehreren Stunden auf 3 bis 5 Minuten. Vorher habe er mehrere Systeme durchgehen müssen, einschließlich eines SIEM und einer E-Mail-Konsole, wo er sich jeweils anmelden und Daten koordinieren musste. Nun kann er sich am FMC anmelden und nach bestimmten IOCs in dieser Umgebung suchen.

„Firewall Management Center dient uns als einzige Konsole, mit der wir alle Cisco Secure Firewalls managen. Das erleichtert die Verwaltung und spart Zeit beim Untersuchen und Kategorisieren von Events, um Entscheidungen bezüglich bösartiger Aktivitäten zu treffen.“
IT-Services-Manager, IT-Dienstleistungen

Die Befragten gaben außerdem an, dass sie heute schneller auf Bedrohungen reagieren können. Der Teamleiter für den Sicherheitsbetrieb aus der Bildungsbranche merkte an, dass er vor der Investition in die Cisco Secure Firewall mehrmals pro Woche Kundensupport-Tickets erstellen musste. Der Support musste den Benutzer dann finden und Malware-Tests durchführen. Die entsprechenden Scans konnten mehrere Stunden dauern. Dann habe das Team des Befragten das System bereinigen oder ein Reimaging durchführen müssen. Dieser Vorgang konnte bis zu einem Tag dauern. Mit Cisco Secure Firewall erstellt dieser Befragte einmal pro Monat ein solches Ticket und behebt das Problem direkt über FMC, was nur etwa eine Stunde dauert.

„Unsere Legacy-Firewalls verursachten viel Mehraufwand bei der Behebung von Sicherheitsvorfällen; es dauerte sehr lange und war sehr kostenintensiv. Mit Firepower verzeichnen wir erhebliche Zeiteinsparungen und müssen deutlich seltener auf Vorfälle reagieren, da mehr blockiert wird.“
Teamleiter Sicherheitsbetrieb, Bildungswesen

Befragte, die von einer frühen auf eine aktuelle FTD-Version umstellten, profitierten auch von Vorteilen im Zusammenhang mit Arbeitsabläufen für Sicherheitsuntersuchungen und -reaktionen. Wie der leitende Infrastrukturtechniker aus dem Finanzdienstleistungssektor mitteilte, war mit einer früheren FTD-Version zwar eine aggregierte Sicht auf die Sicherheitswarnungen über Firewall Management Center möglich, nach dem Upgrade verbesserten sich jedoch die Funktionen für Definitionen und Auslöser. Dieser Befragte gab außerdem an, dass die weiteren Integrationen mit Cisco-Produkten, einschließlich AMP und Umbrella, noch mehr Vorteile durch zusätzliche Korrelationen bieten.

„FMC bietet uns umfassende Transparenz. Aufgrund dieser Einblicke verbringen wir mehr Zeit damit, die Lage zu überprüfen und sicherzustellen, dass alles in Ordnung ist. Das kostet uns aber immer noch weniger Zeit, als wir früher für die Behebung von Vorfällen aufgewendet haben.“
Teamleiter Sicherheitsbetrieb, Bildungswesen

Die Organisationen, die die Vorteile der Einbeziehung von SecureX in ihre Secure Firewall-Lizenz nutzten, verbesserten die betriebliche Effizienz ihrer Sicherheitsteams durch Transparenz und Personalisierung noch weiter. Der Teamleiter für den Sicherheitsbetrieb aus dem Bildungswesen gab beispielsweise auch an, dass SecureX personalisierte, anpassbare Dashboards ermöglichte, sodass sein Team nicht nur von zusätzlichen Einblicken in die Umgebung profitierte, sondern auch unterschiedlichen Benutzern die wichtigsten Informationen für ihre Verantwortungsbereiche bereitstellen konnte.

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

- Gesamtzahl der Sicherheitswarnungen pro Jahr: 100.000
- 26 % davon erfordern die Aufmerksamkeit von Sicherheitsanalysten.
- 70 % der Warnmeldungen, die Aufmerksamkeit erfordern, ziehen auch Untersuchungen nach sich.
- Mit Cisco Secure Firewall und Firewall Management Center lassen sich 49 % der 2,8 Stunden einsparen, die für die Untersuchung der Warnungen benötigt wurden.
- 10 % der zu untersuchenden Warnmeldungen erfordern eine Reaktion.
- Mit Cisco Secure Firewall und Firewall Management Center lassen sich 83 % der 6 Stunden einsparen, die für die Reaktion benötigt wurden.
- SecureX ermöglicht zusätzliche Zeiteinsparungen bei Arbeitsabläufen zur Untersuchung und Reaktion von 42 % im ersten Jahr und 77 % im zweiten und dritten Jahr.

Risiken. Die Verbesserung der Sicherheitsarbeitsabläufe hängt von folgenden Faktoren ab:

- Anzahl der Warnmeldungen (pro Jahr/die Aufmerksamkeit erfordern/die Untersuchungen nach sich ziehen/die eine Reaktion erfordern).
- Stundensatz (inkl. Nebenkosten) für NetSecOps-Fachkräfte

Ergebnisse. Zur Berücksichtigung dieser Risiken hat Forrester diesen Nutzen um 15 % nach unten korrigiert, was über drei Jahre einen risikobereinigten Gesamtbarwert (BW) von 8,2 Mio. USD ergibt.

Verbesserungen von Sicherheitsarbeitsabläufen					
Ref.	**Messgröße**	**Quelle**	**1. Jahr**	**2. Jahr**	**3. Jahr**
B1	Gesamtzahl der jährlichen Warnungen	Modellunternehmen	100.000	100.000	100.000
B2	Warnungen, die die Aufmerksamkeit von Analysten erfordern	Untersuchungen durch Forrester; 26 %	26.000	26.000	26.000
B3	Prozentsatz der Warnungen, die Untersuchungen erfordern	Befragungen	70 %	70 %	70 %
B4	Früherer Stundendurchschnitt für Untersuchungen	Befragungen	2,8	2,8	2,8
B5	Zeiteinsparung für Untersuchungen mit FMC	Befragungen	49 %	49 %	49 %
B6	Warnmeldungen, die Reaktionen erfordern	Befragungen	260	260	260
B7	Früherer Stundendurchschnitt für Reaktionen	Befragungen	6	6	6
B8	Zeiteinsparung für Reaktionen mit FMC	Befragungen	83 %	83 %	83 %
B9	Zusätzliche Einsparung bei Untersuchungen und Reaktionen mit SecureX	Befragungen	42 %	77 %	77 %
B10	Stundensatz (inkl. Nebenkosten) für eine Sicherheitsfachkraft	A5	65 USD	65 USD	65 USD
Bt	Verbesserungen von Sicherheitsarbeitsabläufen	((B2*B3*B4*B5)+(B6*B7*B8)+(B2*B3*B4*B5)+(B6*B7*B9))*B10	3.141.034 USD	4.335.864 USD	4.335.864 USD
	Risikobereinigung	↓15 %			
Btr	Verbesserungen von Sicherheitsarbeitsabläufen (risikobereinigt)		2.669.879 USD	3.685.484 USD	3.685.484 USD
	Dreijahresgesamtwert: 10.040.848 USD		**Dreijahresbarwert: 8.241.976 USD**		

VERRINGERTES RISIKO VON SCHWERWIEGENDEN SICHERHEITSVERLETZUNGEN UND PRODUKTIVITÄTSVERLUST

Fakten und Daten. Die Befragten gaben auch an, dass sie nach der Bereitstellung von Cisco Secure Firewall aufgrund der Reduzierung des Risikos von schwerwiegenden Sicherheitsverletzungen und den damit verbundenen Produktivitätskosten von finanziellen Vorteilen profitierten.

Die Sicherheitslage der befragten Organisationen verbesserte sich zum Beispiel durch die zusätzliche Transparenz, die Cisco Secure Firewall und Firewall Management Center schaffen. Der Teamleiter für den Sicherheitsbetrieb aus dem Bildungswesen merkte Folgendes an: „Verglichen mit herkömmlichen ASAs bietet uns die Cisco Secure Firewall mehr Transparenz. Das ist vor allem deshalb wichtig, da Benutzer immer mehr Mobilgeräte in unser Netzwerk bringen und auf Services wie Drucken über das Netzwerk

„Wir erlebten eine enorme Verbesserung bei der Anzahl der Bedrohungen und der blockierten IOCs. Die Größenordnungen haben sich verschoben. Vorher war unser Geschäft täglich in Gefahr, wenn wir Secure Firewall nicht ausführten. Nun verfügen wir über bessere Einblicke und die Risiken haben sich enorm verringert. Jetzt fühlen wir uns wohl.“
IT-Services-Manager, IT-Dienstleistungen

zugreifen. Durch das Upgrade auf Firepower erhalten wir bessere Einblicke und die Möglichkeit, internen Netzwerkverkehr sowie North-South-Traffic zu filtern."

Die verbesserte automatisierte Blockierung trug auch dazu bei, das potenzielle Risiko einer erfolgreichen Ausnutzung von Sicherheitsschwachstellen zu reduzieren. Der leitende Netzwerktechniker aus dem Technologiesektor gab an: „Firepower ist ein branchenführendes IPS. Wir haben unser Sicherheitsniveau erhöht und können Probleme jetzt unmittelbar beheben. Bei jedem potenziellen Vorfall, den wir frühzeitig beheben, sparen wir Geld." Derselbe Kunde berichtete von einer Verbesserung bei Blockierungen um 80 %, nachdem das Unternehmen von einem ASA-basierten System auf Cisco Secure Firewall umgestellt hatte.

„Mit Secure Firewall konnten wir umgehend 80 % unserer Bedrohungen beseitigen, ohne dafür zusätzliches Personal einzustellen."
Leitender Netzwerktechniker, Technologieunternehmen

Die Befragten loben vor allem das bessere Blockieren nach der Aktualisierung der FTD-Firewalls auf die neueste Version. Der leitende Netzwerktechniker des Technologieunternehmens gab an, dass das Upgrade auf die neueste FTD-Version zwischen 10 und 15 % mehr automatisierte Blockierungen ermöglichte als frühere Versionen.

Dieser Befragte teilte auch eine Anekdote über die Auswirkungen einer automatisierten Blockierung: „Wir erlebten einmal eine potenzielle Kompromittierung auf Basis von Social Engineering. Dem Hacker gelang es, sich ein 24 Stunden gültiges Zugriffstoken von einem authentifizierten Benutzer anzueignen. Als der Hacker versuchte, das Token zu nutzen, griffen die Cisco Secure Firewalls und boten uns Schutz. Wir konnten die Lage unter Kontrolle halten und prüfen, ob der Angreifer einen Unternehmensrechner verwendete. Secure Firewall verweigerte dem Hacker automatisch den Zugriff auf das VPN. Ohne diese Funktion hätte der Hacker Zugang zu unserem Unternehmensnetzwerk erlangt, was schwerwiegende Folgen für uns hätte haben können."

„Cisco Secure Firewall bietet alles aus einer Hand. Die Lösung verfügt über Funktionen zur Integration anderer Tools, die relevante Daten zur Sicherheit bereitstellen. Außerdem ist sie sehr vielseitig. Wir können die unterschiedlichen Anforderungen an den Durchsatz erfüllen und sowohl vertikal als auch horizontal skalieren. Mit Cisco Secure Firewall erhalten wir alle nötigen Funktionen, um heutigen Sicherheitsrisiken zu begegnen – und die Lösung wird ständig verbessert."
Leitender Netzwerktechniker, Internetbranche

Der leitende Netzwerktechniker des Technologieunternehmens nannte außerdem einen Sicherheitsvorteil von Secure Firewall, der durch die Möglichkeit entsteht, den Zugriff auf Anwendungsebene zu verwalten: „Wir stellten eine enorme Nutzung von BitTorrent in unserem Gästenetzwerk fest. Indem wir FTD zum Blockieren von BitTorrent nutzen, verhindern wir nicht nur potenzielle Bedrohungen für andere Gäste. Wir senkten außerdem unsere Netzwerknutzung um rund 400 Mbit/s."

Die Befragten merkten an, dass Cisco Secure Firewall neben den Funktionen zur Erkennung und Abwehr auf der Anwendungsebene auch auf automatisierte Threat-Feeds von Snort zurückgreift. Dadurch verringert sich das Risiko einer erfolgreichen schwerwiegenden Sicherheitsverletzung für die Organisation zusätzlich. Der leitende Infrastrukturtechniker aus dem Finanzdienstleistungssektor sagte: „Wir entschieden uns für Cisco Secure Firewall aufgrund der zusätzlichen Transparenz und der automatisierten Snort-basierten Reaktionen, die es uns zum Bei-

spiel ermöglichen, nicht gepatchte Server zu finden, die über das Internet zugänglich sind, und den schädlichen Datenverkehr umfassend zu blockieren."

Diejenigen Organisationen, die die Einbeziehung von SecureX in ihrer Secure Firewall-Lizenz nutzten, verringerten das Risiko und die Kosten von schwerwiegenden Sicherheitsverletzungen noch weiter. Der leitende Infrastrukturtechniker aus dem Finanzdienstleistungssektor merkte etwa an, dass SecureX seiner Organisation mehr Transparenz für die Identifizierung von Sicherheitsproblemen und die Ermittlung der eigentlichen Ursache potenzieller Bedrohungen bietet.

„SecureX kann uns eine einheitliche Sicht auf unsere gesamte Sicherheitsumgebung bieten. FMC verschafft uns einen Überblick über alle unsere Firewalls, und mit SecureX erhalten wir Einblick in FMC sowie in alle unsere integrierten Cisco-Sicherheitslösungen."
Teamleiter Sicherheitsbetrieb, Bildungswesen

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

- Eine vorherige Anzahl von jährlichen Sicherheitsverletzungen in Höhe von drei.
- Die durchschnittlichen kombinierten internen und externen Kosten einer schwerwiegenden Sicherheitsverletzung betragen 968.480 USD.
- Der Prozentsatz von externen Angriffen, internen Incidents und Angriffen/Vorfällen, bei denen Partner und Dritte involviert sind, beträgt 79 %.
- Cisco Secure Firewall und Firewall Management Center verringern das Risiko einer Sicherheitsverletzung für den Anteil der Organisation, die zuvor durch herkömmliche ASA-Firewalls abgesichert war, um 80 %.
- Cisco Secure Firewall und Firewall Management Center verringern das Risiko einer Sicherheitsverletzung für den Anteil der Organisation, der zuvor durch herkömmliche FTD-basierte Firewalls abgesichert war, um 15 %.
- Von jeder Sicherheitsverletzung sind 66 % der Mitarbeiter des Modellunternehmens betroffen. Da Cisco Secure Firewall und Firewall Management Center das Risiko von Sicherheitsverletzungen reduzieren, gewinnen diese Mitarbeiter 70 % ihrer Produktivität zurück.
- Der Stundensatz (inkl. Nebenkosten) für allgemeine Mitarbeiter beträgt 40 USD.

Risiken. Das verringerte Risiko einer schwerwiegenden Sicherheitsverletzung hängt von folgenden Faktoren ab:

- Anzahl der aktuell aufgetretenen schwerwiegenden Sicherheitsverletzungen
- Gesamtsumme der internen und externen Kosten einer schwerwiegenden Sicherheitsverletzung
- Prozentsatz von externen Angriffen, internen Incidents und Angriffen/Vorfällen, bei denen Partner und Dritte involviert sind
- Art und Anzahl der vorhandenen Firewalls
- Anzahl der Mitarbeiter, die von einer schwerwiegenden Sicherheitsverletzung betroffen sind, deren Stundensatz einschließlich Nebenkosten und deren Fähigkeit, die Produktivität zurückzugewinnen, wenn diese schweren Sicherheitsverletzungen reduziert werden

Ergebnisse. Zur Berücksichtigung dieser Risiken hat Forrester diesen Nutzen um 15 % nach unten bereinigt, was über drei Jahre einen risikobereinigten Gesamtbarwert (BW) von knapp 3,5 Mio. US-Dollar ergibt.

Verringertes Risiko von schwerwiegenden Sicherheitsverletzungen und Produktivitätsverlust					
Ref.	**Messgröße**	**Quelle**	**1. Jahr**	**2. Jahr**	**3. Jahr**
C1	Durchschnittliche Anzahl schwerwiegender Sicherheitsverletzungen	Untersuchungen durch Forrester	3	3	3
C2	Durchschnittliche Kosten pro schwerwiegender Sicherheitsverletzung	Untersuchungen durch Forrester	968.480 USD	968.480 USD	968.480 USD
C3	Prozentsatz von externen Angriffen, internen Incidents und Angriffen/Vorfällen, bei denen Partner und Dritte involviert sind	Befragungen	79 %	79 %	79 %
C4	Prozentsatz der Organisation, der von ASA auf Firepower umgestellt hat	Modellunternehmen	33 %	33 %	33 %
C5	Prozentuale Risikoverringerung dank Firepower	Befragungen	80 %	80 %	80 %
C6	Prozentsatz der Organisation, der von früheren auf aktuelle Firepower-Versionen umgestellt hat	Modellunternehmen	67 %	67 %	67 %
C7	Prozentuale Risikoverringerung dank Firepower	Befragungen	15 %	15 %	15 %
C8	Zusätzliche Verringerung durch SecureX	Befragungen	14 %	18 %	23 %
C9	Zwischensumme: Reduziertes Risiko von Sicherheitsverletzungen	(C1*C2*C3*(C4*C5+C6*C7))+(C1*C2*C3*C8)	1.162.951 USD	1.254.763 USD	1.369.528 USD
C10	Zahl der von den einzelnen Sicherheitsverletzungen betroffenen Anwender	Untersuchungen durch Forrester	10.600	10.600	10.600
C11	Durchschnittlicher Stundensatz (inkl. Nebenkosten) je allgemeiner Mitarbeiter	Modellunternehmen	40 USD	40 USD	40 USD
C12	Produktivitätsrückgewinnung	Modellunternehmen	70 %	70 %	70 %
C13	Zwischensumme: Produktivitätssteigerung aufgrund geringeren Risikos von Sicherheitsverletzungen	(C1*C10*C11*C12*C3*(C4*C5+C6*C7))+(C1*C10*C11*C12*C3*C8	356.397 USD	384.534 USD	419.705 USD
Ct	Verringertes Risiko von schwerwiegenden Sicherheitsverletzungen und Produktivitätsverlust	C9+C13	1.519.348 USD	1.639.297 USD	1.789.232 USD
	Risikobereinigung	↓15 %			
Ctr	Verringertes Risiko von schwerwiegenden Sicherheitsverletzungen und Produktivitätsverlust (risikobereinigt)		1.291.446 USD	1.393.402 USD	1.520.848 USD
	Dreijahresgesamtwert: 4.205.696 USD		**Dreijahresbarwert: 3.468.249 USD**		

LEISTUNGSVORTEILE FÜR DIE PRODUKTIVITÄT VON MITARBEITERN

Fakten und Daten. Cisco Secure Firewall ermöglichte es den Organisationen der Befragten, die Mitarbeiterproduktivität auf zweierlei Weise beträchtlich zu verbessern: 1) durch mehr Transparenz und Kontrolle auf Anwendungsebene, wodurch sich die Netzwerkleistung verbesserte, und 2) durch weniger Ausfallzeiten bei Richtlinienaktualisierungen.

Die Befragten gaben an, dass sich ihre Netzwerkleistung nach der Implementierung von Cisco Secure Firewall weniger häufig verschlechterte, was auf die Funktionen zur Kontrolle des Netzwerkzugriffs in der Anwendungsschicht zurückzuführen ist. Die Befragten berichteten, dass die Netzwerkgeschwindigkeit davor häufig eingebrochen war. Dadurch hatte sich die Netzwerkleistung so stark verringert, dass die Mitarbeiter in ihrer Produktivität beeinträchtigt waren, wenn bestimmte Anwendungen, vor allem im Zusammenhang mit Videomedien, viel Leistung beanspruchten. Der Teamleiter für den Sicherheitsbetrieb aus dem Bildungswesen äußerte Folgendes: „Zwar verlangsamte sich das Netzwerk eigentlich Tag für Tag, aber alle paar Wochen war der Leistungsabfall so stark, dass die Produktivität beeinträchtigt wurde. Dies war meist der Fall, wenn es eine starke Aktivitätszunahme gab, etwa wenn Tausende von Benutzern sich ein Video ansahen."

Da Cisco Secure Firewall die befragten Organisationen in die Lage versetzte, die Netzwerksicherheitsrichtlinie auf mehreren Ebenen, einschließlich der Anwendungsebene, festzulegen, erhielten sie eine präzisere Kontrolle über die Netzwerkberechtigungen. Folglich konnten die Unternehmen besser steuern, welche Anwendungen wann auf das Netzwerk zugreifen konnten. So verhinderten sie eine Überlastung des Netzwerks aufgrund von Anwendungen, die eine hohe Bandbreite beanspruchen. Dadurch verbesserte sich die Netzwerkleistung und die Produktivität der Mitarbeiter stieg.

„Cisco Secure Firewall bietet uns deutlich bessere Einblicke in die Netzwerknutzung und die Möglichkeit, diese Nutzung zu steuern. Derzeit überwachen wir 4.000 unterschiedliche Systeme. Wenn ich wollte, könnte ich nachsehen, in welchem Maß [ein beliebtes Videoportal] letzte Woche genutzt wurde. Wir können Regeln korrigieren, um bestimmte Arten von Datenverkehr bei Bedarf zu unterbinden.“
Teamleiter Sicherheitsbetrieb, Bildungswesen

Andere Befragte gaben an, dass in ihren Unternehmen die Mitarbeiterproduktivität gestiegen sei, seitdem menschliche Fehler bei der Richtlinienaktualisierung verhindert werden. Der IT-Services-Manager des IT-Dienstleisters gab beispielsweise an, dass Richtlinien mit Firewall Management Center wesentlich schneller erstellt und aktualisiert werden können. Das Unternehmen kann daher heute auch schneller überprüfen, ob eine Aktualisierung erfolgreich durchgeführt wurde.

Bevor dieses Unternehmen Secure Firewall implementierte, dauerte es 15 Minuten, um eine Richtlinie zu aktualisieren und weitere 15 Minuten, um zu erfahren, ob sie korrekt festgelegt wurde. Falls nicht, dauerte es noch einmal 15 Minuten, um die Richtlinie ein zweites Mal zu aktualisieren. Früher hatte eine fehlerhaft aktualisierte Richtlinie häufiger negative Auswirkungen auf die Mitarbeiterproduktivität, besonders in Produktionsumgebungen.

Nach dem Upgrade auf die neueste FTD-Version mit Cisco Secure Firewall stellte der Engineering Services Manager einen Rückgang des Zeitaufwands für das Aktualisieren von Richtlinien und das Warten auf Rückmeldungen auf je 3 Minuten fest. Die Gesamtzeit für Aktualisierung, Feedback und Fehlerbehebung verringerte sich somit von 60 auf 12 Minuten, d. h. um 80 %.

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

- Es dauert eine volle Stunde, um eine fehlerhaft aktualisierte Richtlinie zu korrigieren (15 Minuten zum Senden der fehlerhaften Aktualisierung, 15 Minuten bis zur Rückmeldung und 30 Minuten, um nach der Behebung die Aktualisierung durchzuführen und Feedback zu erhalten).
- Cisco Secure Firewall und Firewall Management Center verringern den Zeitaufwand für die Korrektur fehlerhafter Richtlinien um 80 %.
- Es ist davon auszugehen, dass im Durchschnitt 2 % der Organisation von fehlerhaften Richtlinienaktualisierungen betroffen sind.
- Früher kam es regelmäßig zu einer gravierenden Verschlechterung der Netzwerkleistung, sodass die Produktivität von Mitarbeitern etwa einmal alle zwei Wochen für 20 Minuten beeinträchtigt wurde.
- 33 % der Mitarbeiter, die früher durch herkömmliche ASA-Firewalls abgedeckt wurden, waren von der schlechteren Netzwerkleistung beeinträchtigt.

Risiken. Die Leistungsvorteile für die Mitarbeiterproduktivität hängen von folgenden Faktoren ab:

- Prozentsatz der Mitarbeiter, die von fehlerhaften Richtlinienaktualisierungen betroffen sind
- Häufigkeit und Dauer der schlechteren Netzwerkleistung, die sich auf die Mitarbeiterproduktivität auswirkt
- Anzahl der Mitarbeiter, die von der schlechteren Netzwerkleistung betroffen sind

Ergebnisse. Zur Berücksichtigung dieser Risiken hat Forrester diesen Nutzen um 10 % nach unten korrigiert, was über drei Jahre einen risikobereinigten Gesamtbarwert (BW) von 4,1 Mio. US-Dollar ergibt.

Leistungsvorteile für die Produktivität von Mitarbeitern

Ref.	Messgröße	Quelle	1. Jahr	2. Jahr	3. Jahr
D1	Vorheriger Zeitaufwand in Stunden für das Anpassen von Richtlinien mit alten FTD-Versionen	Befragungen	1	1	1
D2	Heutiger Aufwand in Stunden zur Anpassung von Richtlinien mit aktueller FTD-Version	Befragungen	0,2	0,2	0,2
D3	Durchschnittlich betroffene Mitarbeiter	Modellunternehmen	320	320	320
D4	Durchschnittlicher Stundensatz (inkl. Nebenkosten) je allgemeiner Mitarbeiter	C10	40 USD	40 USD	40 USD
D5	Produktivitätsrückgewinnungsrate	Modellunternehmen	25 %	25 %	25 %
D6	Zwischensumme: Produktivitätssteigerungen durch frühzeitigeres Feedback zu Richtlinien	365*(D1–D2)*D3*D4*D5	934.400 USD	934.400 USD	934.400 USD
D7	Häufigkeit der Leistungsbeeinträchtigungen aufgrund missbräuchlicher Netzwerknutzung	Befragungen	26	26	26
D8	Durchschnittliche Dauer der Leistungsbeeinträchtigungen in Stunden	Befragungen	0,33	0,33	0,33
D9	Anzahl der betroffenen Mitarbeiter (nur ASA-Migrationen)	Modellunternehmen	5.280	5.280	5.280
D10	Durchschnittlicher Stundensatz (inkl. Nebenkosten) je allgemeiner Mitarbeiter	C11	40 USD	40 USD	40 USD
D11	Produktivitätsrückgewinnungsrate	Modellunternehmen	50 %	50 %	50 %
D12	Zwischensumme: höhere Produktivität von Endbenutzern im Unternehmen	D7*D8*D9*D10*D11	906.048 USD	906.048 USD	906.048 USD
Dt	Leistungsvorteile für die Produktivität von Mitarbeitern	D6+D12	1.840.448 USD	1.840.448 USD	1.840.448 USD
	Risikobereinigung	↓10 %			
Dtr	Leistungsvorteile für die Produktivität von Mitarbeitern (risikobereinigt)		1.656.403 USD	1.656.403 USD	1.656.403 USD
	Dreijahresgesamtbarwert: 4.969.210 USD		**Dreijahresbarwert: 4.119.230 USD**		

GERINGERE UND VERMIEDENE KOSTEN FÜR VORHERIGE LÖSUNGEN

Fakten und Daten. Durch die Migration ihrer Netzwerksicherheitsinfrastruktur auf die neueste Version von Cisco Secure Firewall konnten die Organisationen der Befragten die mit ihrer veralteten Netzwerkinfrastruktur verbundenen Kosten reduzieren beziehungsweise einsparen. Dementsprechend überrascht es nicht, dass die Befragten Kosteneinsparungen bei der Neulizenzierung ihrer herkömmlichen ASA-basierten Firewalls sowie bei früheren FTD-basierten Firewalls angaben, nachdem diese durch Cisco Secure Firewalls ersetzt wurden.

Zusätzlich zu den physischen und virtuellen Firewall-Ersetzungen nahmen die Organisationen der Befragten, die einen Umstieg von ASA-basierten Umgebungen vollzogen, ihre eigenständigen IPS-Lösungen außer Betrieb, da Cisco Secure Firewall bereits ein IPS beinhaltet.

„Bei herkömmlichen ASA-Firewalls mussten wir zusätzlich in IPS-Lösungen investieren, die zwischen den Verbindungen und der Firewall positioniert wurden. Bei Cisco Secure Firewall ist das IPS bereits integriert. Wir müssen nun keine zwei unterschiedlichen Lösungen mit verschiedenen Ökosystemen mehr verwalten und sind nicht mehr auf IPS-Techniker angewiesen.“
Leitender Netzwerktechniker, Technologieunternehmen

Ein weiterer wichtiger Punkt ist, dass die Befragten zusätzliche Einsparungen feststellten, nachdem sie die Firewalls der Organisation von früheren FTD-Versionen auf Cisco Secure Firewall aktualisierten. Aufgrund der Effizienz dieser hochmodernen Firewalls gaben die Befragten an, dass sie zwischen 20 und 25 % weniger Firewalls benötigten, um dieselben Ergebnisse zu erzielen.

„Durch die Aktualisierung auf die neuesten FTDs von Cisco Secure Firewall konnten wir eine höhere Verarbeitungseffizienz verzeichnen. Cisco Secure Firewall ist zwischen 20 und 25 % effizienter als frühere Iterationen, das heißt, wir benötigen weniger Firewalls.“
Leitender Netzwerktechniker, Internetbranche

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

- Reduzierung der Lizenzkosten für eigenständige IPS-Lösungen durch die Ersetzung herkömmlicher ASA-Firewalls durch Cisco Secure Firewalls in Höhe von 171.600 US-Dollar pro Jahr
- Einsparung von Wartungskosten für eigenständige IPS-Lösungen, was einem Wert von etwa 20 % der Lizenzgebühren entspricht
- Reduzierung der laufenden Verwaltungskosten im Zusammenhang mit IPS-Lösungen (30 Minuten für 2 VZÄ pro Woche) um 80 %
- Kosteneinsparungen für die Ersetzung vorhandener Firewalls durch Firewalls eines ähnlichen Typs in Höhe von mehr als 1,3 Mio. US-Dollar im ersten Jahr
- Kosteneinsparungen für die Ersetzung virtueller Firewalls in Höhe von 300.000 US-Dollar pro Jahr
- Kosteneinsparungen von zusätzlich 25 % bei physischen Firewalls aufgrund der Effizienz der Cisco Secure Firewalls

„Nach der Bereitstellung von Cisco Secure Firewall konnten wir endlich unsere kostspieligeren und weniger leistungsfähigen IPS-Appliances außer Betrieb nehmen.“
Leitender Infrastrukturtechniker, Finanzdienstleistungssektor

Risiken. Die Reduzierung der Kosten für Altlösungen variiert abhängig von den folgenden Faktoren:

- Anzahl und Typ der vorhandenen Firewalls
- Möglichkeit zur Außerbetriebnahme von eigenständigen IPS-Lösungen

Ergebnisse. Zur Berücksichtigung dieser Risiken hat Forrester diesen Nutzen um 10 % nach unten korrigiert, was über drei Jahre einen risikobereinigten Gesamtbarwert (BW) von knapp 2,6 Mio. US-Dollar ergibt.

Kosteneinsparungen durch außer Betrieb genommene Altlösungen

Ref.	Messgröße	Quelle	1. Jahr	2. Jahr	3. Jahr
E1	Kosteneinsparungen bei Legacy-IPS	Befragungen	171.600 USD	171.600 USD	171.600 USD
E2	Einsparungen bei Wartungskosten	E1*20 %	34.320 USD	34.320 USD	34.320 USD
E3	Kosteneinsparungen für das laufende Management von Legacy-IPS	Befragungen	53.539 USD	53.539 USD	53.539 USD
E4	Kosteneinsparungen bei Firewalls im Ersetzungszyklus	Modellunternehmen	1.616.980 USD	300.000 USD	300.000 USD
E5	Kosteneinsparungen durch höhere Firewall-Effizienz	Modellunternehmen	329.245 USD	0 USD	0 USD
Et	Kosteneinsparungen durch außer Betrieb genommene Altlösungen	E1+E2+E3+E4+E5	2.205.684 USD	559.459 USD	559.459 USD
	Risikobereinigung	↓10 %			
Etr	Kosteneinsparungen durch außer Betrieb genommene Altlösungen (risikobereinigt)		1.985.115 USD	503.513 USD	503.513 USD
	Dreijahresgesamtwert: 2.992.142 USD			**Dreijahresbarwert: 2.599.074 USD**	

NICHT QUANTIFIZIERTER NUTZEN

Weitere Vorteile für die Unternehmen, die jedoch nicht quantifiziert werden konnten, sind:

- **Verbesserungen der VPN-Produktivität und -Sicherheit.** Die Befragten gaben auch an, dass Cisco Secure Firewall eine bessere VPN-Produktivität und -Sicherheit beim Remotezugriff ermöglichte. Secure Firewall bietet Clustering zur Verteilung von Sitzungen auf verschiedene Gerätegruppen. Dies ermöglicht eine höhere Leistung, Resilienz und Endnutzerproduktivität. Außerdem können die Benutzer dank der lokalen Authentifizierung von Secure Firewall weiter produktiv arbeiten, wenn ein AAA-Remoteserver nicht mehr zugänglich ist. Aus Sicherheitsgründen ermöglicht Cisco Secure Firewall neben der persönlichen Validierung der Endbenutzer eine Authentifizierung mit mehreren Zertifikaten, damit Organisationen sicherstellen können, dass ein Remotegerät vom Unternehmen ausgegeben wurde.
- **Verbesserte Compliance.** Die Befragten merkten auch an, dass Cisco Secure Firewall und Firewall Management Center einen nicht quantifizierbaren Nutzen für Compliance-Arbeitsabläufe bieten. Der leitende Infrastrukturtechniker des Finanzdienstleistungsunternehmens gab an, dass das Compliance-Berichtswesen vor der Bereitstellung von Secure Firewall und FMC schwieriger war. Früheren Lösungen fehlte eine benutzerfreundliche Berichtsfunktion. Secure Firewall und FMC ermöglichen es Organisationen jedoch, Berichte zu erstellen, die mehr Komponenten abdecken und detaillierte Angaben zu Aktivitäten enthalten. Die Befragten merkten außerdem an, dass Cisco Secure Firewall den Verschlüsselungsstandard Transport Layer Security (TLS) 1.3 unterstützt. Der leitende Netzwerktechniker des Internetunternehmens bemerkte etwa, dass sein Team solche Flows aufgrund des Verwaltungsaufwands derzeit nicht entschlüsselte. Nach der Investition in Cisco Secure Firewall wurde die Entschlüsselung mit TLS 1.3 einfacher und effizienter.

„Vorher konnten wir für viele der unterschiedlichen Konfigurationskomponenten keine Berichte erstellen. Heute können wir umfassende und detaillierte Berichte einfacher abrufen. Ich habe gerade einen Bericht über jede von mir vorgenommene Zugriffssteuerungsänderung für das letzte Jahr erhalten. Er enthält Informationen über alle Seitenaufrufe und vorgenommenen Änderungen.“
Leitender Infrastrukturtechniker, Finanzdienstleistungssektor

- **Verbesserung der Mitarbeiter-Experience.** Die Befragten gaben zudem an, dass sich die Mitarbeitererfahrung in ihren Organisationen verbessert hatte. Der leitende Netzwerktechniker des Internetunternehmens sagte etwa: „Dadurch, dass wir den Anwendungszugang zu unseren Netzwerken besser steuern konnten, verbesserte sich die Zufriedenheit unserer Mitarbeiter. Für unsere lokalen IT-Teams war es früher schwierig, Benutzer nachzuverfolgen, um sie zu bitten, bestimmte Apps nicht mehr zu verwenden, oder ihren Zugriff zu blockieren. Mit Secure Firewall und FMC können wir das nun per Fernzugriff erledigen.“

FLEXIBILITÄT

Kunden schätzen Flexibilität individuell unterschiedlich hoch ein. Es sind mehrere Szenarien denkbar, in denen ein Kunde sich für die Implementierung von Secure Firewall entscheidet und zusätzliche Verwendungen und Geschäftsmöglichkeiten erst später erkennt, z. B.:

- **Zusätzliche Integrationen mit Cisco Security.** Neben den Vorteilen von SecureX gaben die Befragten an, dass das Ökosystem der Sicherheitsprodukte von Cisco ihren Unternehmen ausreichend viel Flexibilität bietet, um das Sicherheitsniveau weiter zu erhöhen. Der IT-Services-Manager des IT-Dienstleistungsunternehmens erläuterte dies so: „Cisco Security bietet ein umfassendes Paket aus integrierten Sicherheitslösungen. Damit tun sich andere Anbieter schwer. Es ist nicht nur Secure Firewall, es sind all die anderen Bestandteile, die sich gut integrieren lassen und die es uns ermöglichen, eine bessere Abwehr zu errichten.“
- **Verbesserung der Abläufe für die Arbeit im Homeoffice.** Die Kontrollen von Cisco Secure Firewall trugen auch dazu bei, einen reibungslosen Betrieb aufrechtzuerhalten, als die VPN-Nutzung durch die Umstellung von Mitarbeitern auf das Arbeiten im Homeoffice geradezu explodierte. Der leitende Netzwerktechniker des Internetunternehmens merkte dazu Folgendes an: „Während der Corona-Pandemie stiegen unsere simultanen VPN-Verbindungen von durchschnittlich 100.000 auf nahezu 350.000 weltweit an. Um die Funktionsfähigkeit unseres Netzwerks aufrechtzuerhalten, nutzen wir Cisco Secure Firewall, um Ratenbegrenzungen festzulegen und so einen reibungslosen Betrieb zu ermöglichen.“
- **Einfacher Umstieg auf die Cloud.** Schließlich äußerten die Befragten, dass sie durch Cisco Secure Firewall ihre Cloud-Initiativen leichter umsetzen konnten. Der Engineering Services Manager des IT-Dienstleistungsunternehmens sagte: „Wir benötigten eine zentrale Plattform, um unsere Ziele vor Ort, an externen Standorten und auch für die Cloud zu erreichen. Allerdings musste die Bereitstellung einfach sein. Bei Cloud-Plattformen können wir einfach eine FTD-Box platzieren, sie sofort installieren und an Firewall Management Center anbinden. Der Zeitaufwand für Konfiguration und Bereitstellung ist praktisch gleich null. Zudem konnten wir per Pushverfahren eine standardisierte Richtlinie an diese Boxen weiterleiten.“

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
Ftr	Lizenzkosten	6.000.690 USD	0 USD	0 USD	0 USD	6.000.690 USD	6.000.690 USD
Gtr	Kosten für Implementierung, Richtlinienerstellung und Schulung	278.220 USD	7.924 USD	7.924 USD	7.924 USD	301.990 USD	297.924 USD
	Gesamtkosten (risikobereinigt)	6.278.910 USD	7.924 USD	7.924 USD	7.924 USD	6.302.680 USD	6.298.614 USD

LIZENZKOSTEN

Fakten und Daten. Allen Kunden entstanden verschiedene Kosten in Verbindung mit ihrer Investition in Secure Firewall, darunter:

- Kosten für die physische Firewall, je nach benötigtem Durchsatz
- Für Rechenzentren bereitgestellte virtuelle Firewalls, die den East-West-Traffic verarbeiten
- Lizenzkosten für Threat Protection, Malware Defense und URL-Filterung
- Lizenzen für Firewall Management Center

„Wir haben keine andere Option gefunden, die eine derartig umfassende Architektur, ein solches Toolset und vergleichbare Funktionen wie Cisco Secure Firewall in einer Komplettlösung bietet. Hinzu kam, dass das Preis-Leistungs-Verhältnis ebenfalls überzeugend war.“
Leitender Infrastrukturtechniker, Finanzdienstleistungssektor

Die befragten Entscheidungsträger gaben an, dass sie Cisco SecureX ohne Zusatzkosten bereitstellen konnten, da es bereits in ihren Lizenzen für Secure Firewall enthalten war.

Modellerstellung und Annahmen. Forrester legt für das Modellunternehmen mit 100 Niederlassungen und vier physischen Rechenzentren, die Redundanz erfordern, Folgendes zugrunde:

- Alle Lizenzen zum Listenpreis für eine Laufzeit von drei Jahren
- Die Kosten einer Firewall für die Hauptniederlassung betragen 328.443 US-Dollar. Die Hauptniederlassung benötigt eine große Firewall der Enterprise-Klasse mit einem Durchsatz von bis zu 75 GBit/s.
- Die Kosten der Rechenzentrums-Firewalls belaufen sich auf 978.067 US-Dollar. Das Modellunternehmen stellt in jedem Rechenzentrum ein Paket mit Perimeter-Clustering oder Hochverfügbarkeit mit zwei physischen Firewalls bereit, um den North-South-Traffic in und aus dem Rechenzentrum zu verarbeiten.
- Die Kosten für 100 virtuelle Firewalls betragen 2.628.561 US-Dollar. Diese virtuellen Firewalls verarbeiten den East-West-Traffic innerhalb des Rechenzentrums sowie zwischen den Rechenzentren und den Public-Cloud-Plattformen.

- Die physischen und virtuellen Firewalls in den Rechenzentren umfassen alle eine zusätzliche Lizenz für Threat Protection zum Dreijahresabonnement-Preis. Dies bietet zusätzliche Sicherheit, da es Snort 3 zur besseren Erkennung und Abwehr von Kompromittierungsindikatoren und schädlichem Traffic beinhaltet.
- Die Gesamtkosten für 60 Firewalls für Niederlassungen betragen 1.848.160 US-Dollar. 60 Niederlassungen benötigen Secure Firewalls mit einem Durchsatz von bis zu 1,9 GBit/s.
- Die Gesamtkosten für 39 Firewalls für kleinere Niederlassungen betragen 137.779 US-Dollar. Für die 39 verbleibenden Niederlassungen wird lediglich ein Durchsatz von bis zu 650 MBit/s benötigt.
- Sämtliche Firewalls an Niederlassungen verfügen über zusätzliche Lizenzen für Threat Protection, Malware Defense und URL-Filterung zum Preis eines Dreijahresabonnements.
- Der Lizenzumfang für Firewall Management Center ist ebenfalls so gestaltet, dass er alle diese Firewalls angemessen abdeckt. Die Kosten für Firewall Management Center betragen 79.680 US-Dollar.

Risiken. Die Lizenzkosten für Cisco Secure Firewall und Firewall Management Center hängen von folgenden Faktoren ab:

- Anzahl der gewünschten virtuellen Firewalls
- Anzahl der benötigten Firewalls der Enterprise-Klasse
- Größe und Anzahl der Rechenzentren und Bedarf an Hochverfügbarkeit
- Größe und Anzahl der Niederlassungen

Ergebnisse. Da Forrester den Preis für das Modellunternehmen direkt mit Cisco vereinbart hat, sind diese Kosten nicht risikobereinigt und belaufen sich auf einen Gesamtbarwert über drei Jahre (diskontiert mit 10 %) von 6 Mio. US-Dollar.

„Mit unserer Cisco Enterprise-Sicherheitsvereinbarung sind unsere Gesamtkosten niedriger, als wenn wir alles einzeln kaufen würden. Obgleich Firepower das Gros dieser Kosten ausmacht, sparen wir Hunderttausende von Dollar, da wir zusätzlichen Schutz durch Produkte erhalten, die wir vorher nicht hatten.“
Teamleiter Sicherheitsbetrieb, Bildungswesen

Lizenzkosten

Ref.	Messgröße	Quelle	Ausgangswert	1. Jahr	2. Jahr	3. Jahr
F1	Kosten für virtuelle Firewalls	Cisco	2.628.561 USD			
F2	Kosten für die Firewall der Hauptniederlassung	Cisco	328.443 USD			
F3	Kosten für die physischen Firewalls des Rechenzentrums	Cisco	978.067 USD			
F4	Kosten für Firewalls kleiner Niederlassungen	Cisco	137.779 USD			
F5	Kosten für Firewalls großer Niederlassungen	Cisco	1.848.160 USD			
F6	Kosten für Firewall Management Center	Cisco	79.680 USD			
Ft	Lizenzkosten	F1+F2+F3+F4+F5+F6	6.000.690 USD	0 USD	0 USD	0 USD
	Risikobereinigung	0 %				
Ftr	Lizenzkosten (risikobereinigt)		6.000.690 USD	0 USD	0 USD	0 USD
	Dreijahresgesamtwert: 6.000.690 USD			**Dreijahresbarwert: 6.000.690 USD**		

KOSTEN FÜR IMPLEMENTIERUNG, RICHTLINIENERSTELLUNG UND SCHULUNG

Fakten und Daten. Die Befragten äußerten, dass bei ihnen intern Zeitaufwand und Lohnkosten in Verbindung mit der Bereitstellung und der Implementierung von Firewalls in den Rechenzentren und Büros anfielen. Der erste Kostenblock beinhaltete die physische Bereitstellung der Firewalls an den einzelnen Standorten. Der zweite umfasste die Implementierung dieser Firewalls. Dies erfolgte, indem die entsprechenden Richtlinien für die jeweiligen Firewalls erstellt und bereitgestellt wurden.

„Die Implementierung und Bereitstellung erfolgten wirklich schnell und waren relativ einfach. Die eigentliche Umstellung dauerte drei Wochen, da wir bereits ein Konzept hatten und wussten, wie alles zu aktivieren war.“
Teamleiter Sicherheitsbetrieb, Bildungswesen

Schließlich berichteten die befragten Entscheider noch, dass ihnen Zeitkosten im Zusammenhang mit Schulungen entstanden. Die Mitarbeiterschulung, um die Bereitstellung und Verwaltung von Cisco Secure Firewalls zu erlernen, dauerte rund zwei Stunden. Einige der Befragten gaben an, dass sie öffentlich verfügbare Schulungsvideos von Cisco-Sicherheitsexperten nutzten.

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

- Im Durchschnitt sind 6 Stunden Implementierungszeit bei jedem der zwei Rechenzentren und den 100 Niederlassungen erforderlich.
- Die Erstellung von Richtlinien dauert durchschnittlich 30 Stunden pro Firewall.
- Für SecureX sind 20 Stunden Arbeit vorab für die Implementierung und zusätzlich 100 Stunden jährlich für die laufende Verwaltung nötig.
- Anfänglich werden Schulungen für 15 Mitarbeiter benötigt und dann aufgrund der Personalfluktuation für drei weitere Mitarbeiter jährlich.

Risiken. Die Kosten für die Implementierung und die Erstellung von Richtlinien hängen von den folgenden Faktoren ab:

- Anzahl der bereitzustellenden Cisco Secure Firewalls
- Anzahl der Mitarbeiter, die anfänglich geschult werden müssen
- Mitarbeiter-Fluktuationsrate
- Stundensatz (inkl. Nebenkosten) für NetSecOps-Fachkräfte

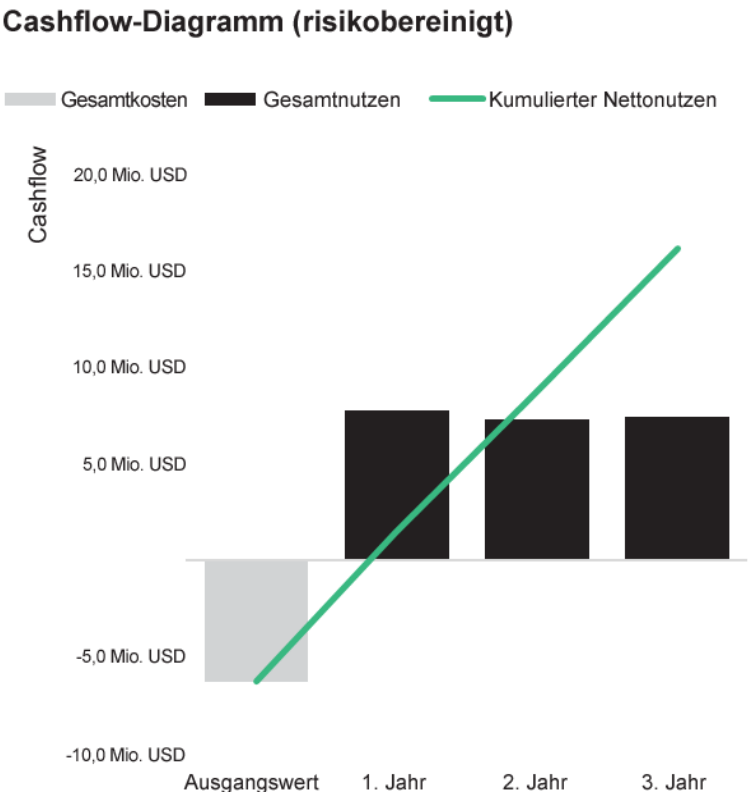
Ergebnisse. Zur Berücksichtigung dieser Risiken hat Forrester diese Kosten um 15 % nach oben korrigiert, was über drei Jahre einen risikobereinigten Gesamtbarwert (BW) von weniger als 298.000 USD ergibt.

Kosten für Implementierung, Richtlinienerstellung und Schulung

Ref.	Messgröße	Quelle	Ausgangswert	1. Jahr	2. Jahr	3. Jahr
G1	Bereitstellungsstandorte	Modellunternehmen	102			
G2	Durchschnittlicher Aufwand in Stunden für die physische Implementierung an einzelnen Standorten	Modellunternehmen	6			
G3	Aufwand in Stunden für die Erstellung von Richtlinien	Befragungen	30			
G4	Aufwand in Stunden für die Implementierung und Verwaltung von SecureX	Befragungen	20	100	100	100
G5	Mitarbeiter mit Schulungsbedarf	Befragungen	15	3	3	3
G6	Aufwand in Stunden für Schulungsmaßnahmen	Befragungen	2	2	2	2
G7	Durchschnittlicher Stundensatz (inkl. Nebenkosten) für NetSecOps-Fachkräfte	A5	65 USD	65 USD	65 USD	65 USD
Gt	Kosten für Implementierung, Richtlinienerstellung und Schulung	((G1*(G2+G3))+,G4+(G5*G6))*G7	241.930 USD	6.890 USD	6.890 USD	6.890 USD
	Risikobereinigung	↑15 %				
Gtr	Kosten für Implementierung, Richtlinienerstellung und Schulung (risikobereinigt)		278.220 USD	7.924 USD	7.924 USD	7.924 USD
	Dreijahresgesamtwert: 301.990 USD			**Dreijahresbarwert: 297.924 USD**		

Zusammengefasste betriebswirtschaftliche Ergebnisse

KONSOLIDIERTE RISIKOBEREINIGTE MESSGRÖSSEN FÜR EINEN ZEITRAUM VON DREI JAHREN



Die in den Abschnitten zu Nutzen und Kosten berechneten finanziellen Ergebnisse können zur Bestimmung des ROI, des Kapitalwerts und eines Amortisierungszeitraums für die Investition des Modellunternehmens verwendet werden. Forrester hat dieser Analyse einen jährlichen Diskontierungssatz 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	(6.278.910 USD)	(7.924 USD)	(7.924 USD)	(7.924 USD)	(6.302.680 USD)	(6.298.614 USD)
Gesamtnutzen	0 USD	7.737.795 USD	7.264.360 USD	7.391.805 USD	22.393.959 USD	18.591.534 USD
Nettonutzen	(6.278.910 USD)	7.729.871 USD	7.256.436 USD	7.383.881 USD	16.091.279 USD	12.292.920 USD
ROI						195 %
Amortisierungsdauer (in Monaten)						10

Anhang A: Total Economic Impact

Total Economic Impact (TEI) ist eine von Forrester Research entwickelte Methodik, die die Entscheidungsprozesse von Unternehmen zu technischen Fragen optimiert und Anbietern dabei hilft, Kunden das Wertversprechen ihrer Produkte und Dienstleistungen zu vermitteln. Die Methodik des Total Economic Impact hilft Unternehmen dabei, 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

Nutzen ist der Wert, der der Organisation durch das Produkt entsteht. Die Methodik des Total Economic Impact 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.

Kosten berücksichtigen alle Ausgaben, die zur Schaffung des angestrebten Mehrwerts oder Nutzens durch das Produkt erforderlich sind. Die Kostenkategorie innerhalb des Total Economic Impact erfasst die Mehrkosten in Bezug auf die gegenwärtige Umgebung 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 nachgehalten werden. Risikofaktoren der Methodik des Total Economic Impact 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 Diskontierungssatzes 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 Diskontierungssatz). 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 Diskontierungssatz). 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.

DISKONTIERUNGSSATZ

Der in der Cashflow-Analyse verwendete Zinssatz, mit dem der Zeitwert des Geldes ermittelt wird. Organisationen verwenden in der Regel Diskontierungssätze 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: Schlussbemerkungen

[1] Total Economic Impact (TEI) ist eine von Forrester Research entwickelte Methodik, die die Entscheidungsprozesse von Unternehmen zu technischen Fragen optimiert und Anbietern dabei hilft, Kunden das Wertversprechen ihrer Produkte und Dienstleistungen zu vermitteln. Die Methodik des Total Economic Impact hilft Unternehmen dabei, den messbaren Wert von IT-Initiativen gegenüber der oberen Führungsebene und anderen wichtigen geschäftlichen Stakeholdern zu demonstrieren, zu rechtfertigen und zu veranschaulichen.


FORRESTER®