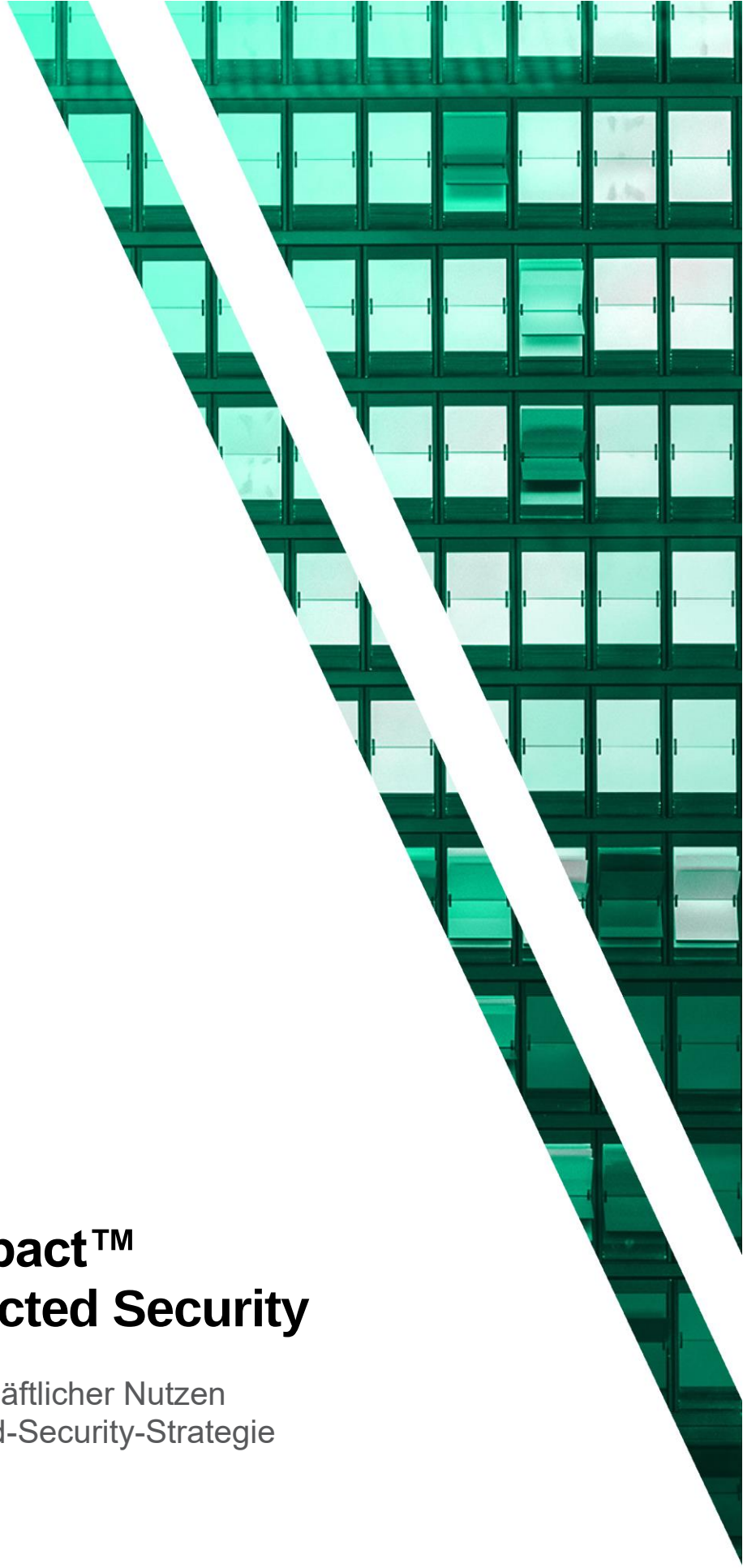
FORRESTER®



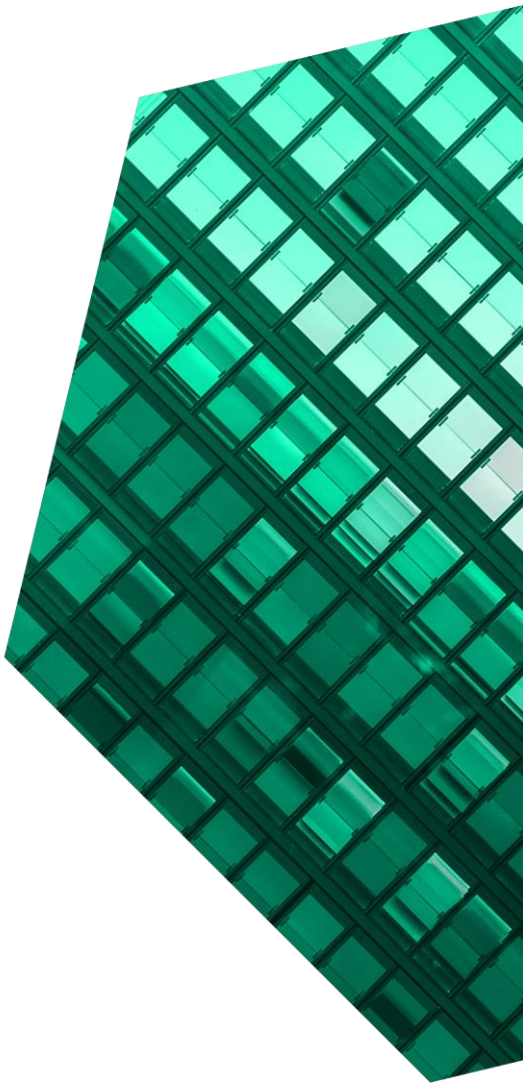
Total Economic Impact™ von Juniper Connected Security

Kosteneinsparungen und geschäftlicher Nutzen Ermöglicht durch die Connected-Security-Strategie von Juniper Networks

JUNI 2021

Contents

Beraterteam: *Casey Sirotnak*
Sanitra Desai



Zusammenfassung

Analysen von Forrester zufolge möchten viele Unternehmen Netzwerkkonzepte, -produkte oder -technologien implementieren, um damit bestimmte strategische Ziele bezüglich ihrer Netzwerkinfrastruktur zu erreichen. Jedoch haben sie diese Ziele oft gar nicht klar definiert. Im besten Fall läuft ein Unternehmen ohne durchdachte Strategie Gefahr, dass das Netzwerk viele Lücken aufweist, die den Teams zu viel Freiraum und alternative Routen bieten. Im schlimmsten Fall jedoch könnte sich das Netzwerk als echter Klotz am Bein erweisen und Digitalisierungs-projekte behindern – ein ernsthaftes Risiko für die Wettbewerbsfähigkeit des Unternehmens.[1]

Juniper ist auf Full-Stack-Sicherheitslösungen spezialisiert und bietet verschiedene Dashboards und Tools, mit denen SecOps-Abläufe effizienter gestaltet und gleichzeitig wertvolle Erkenntnisse zur Netzwerkstabilität und -aktivität gewonnen werden.

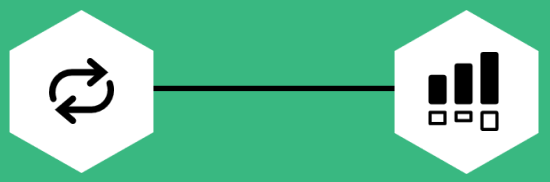
Juniper Networks beauftragte Forrester Consulting mit der Durchführung einer Studie zum Total Economic Impact™ (TEI) sowie mit der Untersuchung der potenziellen Kapitalrendite (ROI), die Unternehmen durch den Einsatz von Juniper Connected Security erzielen können. Diese Studie soll den Lesern einen Bezugsrahmen bereitstellen, mit dem sie die potenziellen finanziellen Auswirkungen von Juniper Connected Security auf ihr Unternehmen beurteilen können.

Zum besseren Verständnis der Vorteile, Kosten und Risiken, die mit dieser Investition verbunden sind, befragte Forrester ein Unternehmen, das bereits Erfahrungen mit Juniper Connected Security gesammelt hat. Anhand der so erhaltenen Informationen erstellte Forrester daraufhin eine Finanzprognose über einen Zeitraum von drei Jahren.

Vor der Nutzung von Juniper Connected Security besaß das betreffende Unternehmen eine veraltete Sicherheitsausstattung, deren einzelne Komponenten von unterschiedlichen Anbietern stammten. Folglich war die Verwaltung der veralteten Hardware für Netzwerksicherheit recht kompliziert, da mehrere Anbieter und verschiedene Arten von Programmcode unter einen Hut gebracht werden mussten und es an der nötigen Transparenz zur Gewähr-leistung einer stabilen Umgebung mangelte. Diese Einschränkungen verursachten einen messbaren Mehraufwand bei der Verwaltung und erhöhten in der früheren Netzwerkumgebung obendrein das Risiko von Zwischenfällen.

Nach der Investition in Juniper Connected Security konnte das Unternehmen seine Netzwerkausstattung modernisieren und optimieren. Zudem stammten nun alle

WICHTIGE KENNZAHLEN



Kapitalrendite
283 %

Kapitalwert
657.700 $

Komponenten vom selben Anbieter, nämlich von Juniper. Insbesondere verringerte sich durch diese Investition der Verwaltungsaufwand, während die höhere Stabilität und Zuverlässigkeit der Sicherheitsumgebung gleichzeitig für mehr Vertrauen in die Infrastruktur bei den technischen SecOps-Teams und den Endanwendern im Unternehmen sorgten.

WESENTLICHE ERGEBNISSE

Quantifizierter Nutzen. Der quantifizierte Nutzen, angegeben als risikobereinigter Barwert, umfasst die folgenden Elemente:

- **Verringerung des Verwaltungsaufwands für SecOps-Teams um 60 Prozent.** SecOps-Teams profitierten von verständlichen Tools, Dashboards und Berichtsfunktionen sowie von einer Gesamt-orchestrierung, die zu besseren Netzwerkdiagnosen und Problemlösungen führte. Zusätzlich konnte das Netzwerk durch transparentere Daten besser überwacht werden, was zu einer stabileren Umgebung mit weniger Zwischenfällen und klareren Reaktionspfaden führte.

Jährlich vermiedene Ausfallzeiten pro Mitarbeiter

20 Stunden

Insgesamt sparte das Unternehmen durch diese Effizienzsteigerungen über einen Zeitraum von drei Jahren 354.500 US-Dollar ein.

- **Verbesserung der Systemverfügbarkeit um 10 Prozent und Verringerung der jährlichen Ausfallzeiten je Mitarbeiter um rund 20 Stunden.** Durch die höhere Sicherheit und Zuverlässigkeit des Netzwerks dank Juniper verbesserte sich auch die Systemleistung und es gab weniger Ausfallzeiten für die Endanwender im Unternehmen. So konnten sich die Mitarbeiter ungestört auf ihre produktiven Aufgaben und die Erfüllung von Aufträgen konzentrieren, was sowohl den Umsatz steigerte als auch ausfallbedingte Kosten im Verlauf der drei Jahre in Höhe von 439.700 US-Dollar einsparte.
- **Vermeidung anfänglicher Investitionskosten von 45.000 US-Dollar und jährlicher Wartungskosten von 35.000 US-Dollar.** Nach der Ausmusterung der veralteten Ausstattung sanken die diesbezüglichen jährlichen Wartungskosten des Unternehmens um 35.000 US-Dollar. Da Juniper Full-Stack-Lösungen bietet, verringerten sich außerdem die konsolidierten Investitionskosten für Hardware im ersten Jahr um 45.000 US-Dollar. Insgesamt ergaben sich für das Unternehmen über drei Jahre Einsparungen von 121.600 US-Dollar.

Nicht quantifizierter Nutzen. Dem Unternehmen zufolge gab es einen weiteren Vorteil, der sich im Rahmen dieser Studie nicht quantifizieren ließ: das Vertrauen in die Netzwerkinfrastruktur war gestiegen. Juniper sorgte für stabilere Sicherheitskomponenten, was wiederum die IT-Teams und Mitarbeiter zu innovativeren Ansätzen motivierte. Durch die gestiegene Effizienz verlor die IT-Abteilung weniger Zeit und konnte sich vermehrt darauf konzentrieren, modernere Architekturen zur Beschleunigung der geschäftlichen Transformation zu implementieren. Ähnliches galt für die Endanwender im Unternehmen: Aufgrund der verbesserten Systemleistung hatten sie seltener mit technischen Schwierigkeiten zu tun und hatten somit mehr Zeit für die Erstellung kreativer Inhalte, die ebenfalls der geschäftlichen Transformation zugutekamen.

Kosten. Die risikobereinigten barwertigen Kosten umfassen die folgenden Positionen:

- **Investitionskosten und laufende Zahlungen an Anbieter (einschließlich Juniper) sowie Kosten für den Zeitaufwand zur Schulung des internen Personals.** Die Vorlaufkosten im Zusammenhang mit der Investition in Juniper umfassten anfallende Hardwarekosten, die an Juniper gezahlt wurden, sowie Gebühren für Implementierungsservices, die von einem Drittanbieter ausgeführt wurden. Außerdem mussten interne Mitarbeiter, die künftig für die Wartung und Verwaltung der Lösung von Juniper zuständig sein würden, vorab rund 40 Stunden Zeit aufwenden, um sich mit den Netzwerkkomponenten und verfügbaren Tools vertraut zu machen. Danach war nur noch ein minimaler Schulungsaufwand nötig, der pro Jahr etwa 10 Stunden in Anspruch nahm. Diese laufenden Schulungen widmeten sich vor allem neuen Optionen und Funktionen, um die Juniper seine Lösung erweitert hatte.

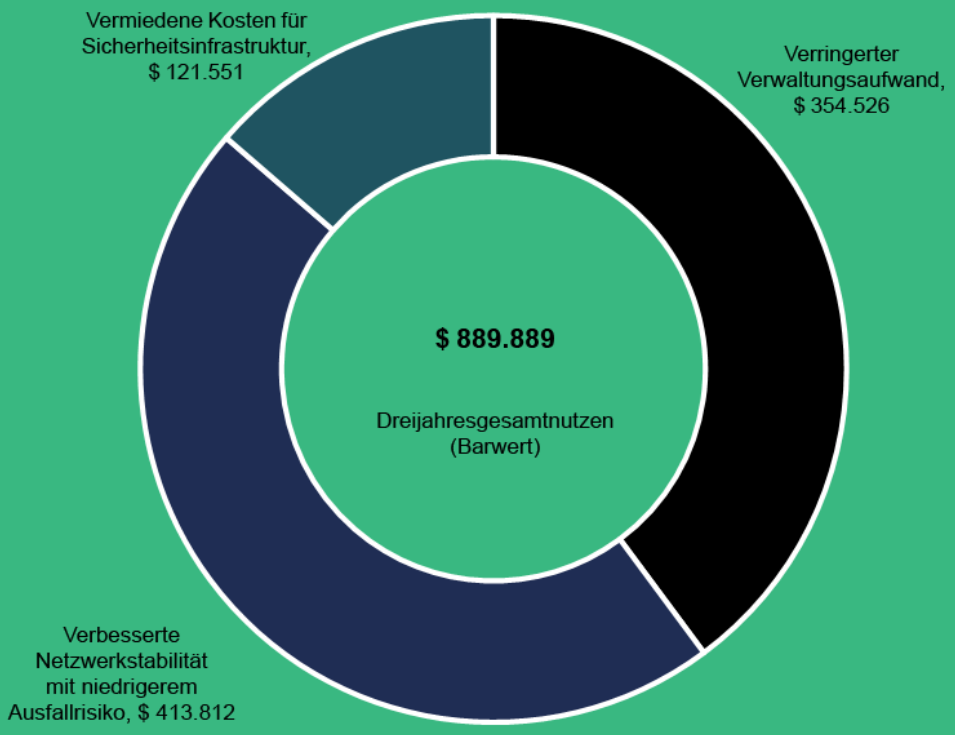
Die Befragung und die Finanzanalyse ergaben, dass diesem Unternehmen innerhalb von drei Jahren ein Nutzen im Wert von 889.900 US-Dollar gegenüber Kosten in Höhe von 232.200 US-Dollar entstand. Dies ergibt einen Kapitalwert von 657.700 US-Dollar und eine Kapitalrendite von 283 Prozent.

ROI
283 %

NUTZEN (BW)
889.900 $

KW
657.700 $

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 Juniper Connected Security in Erwägung ziehen.

Dieser Bezugsrahmen dient dazu, Kosten, Nutzen, Flexibilitätsvorteile und Risikofaktoren zu ermitteln, die für eine Investitionsentscheidung von Bedeutung sind. Zur Bewertung der Auswirkungen, die Juniper Connected Security auf ein Unternehmen haben kann, hat Forrester ein mehrere Schritte umfassendes Verfahren verwendet.

DUE DILIGENCE
Es wurden Juniper Stakeholder und Forrester Analysten befragt, um relevante Daten zu Juniper Connected Security zu sammeln.

KUNDENBEFRAGUNG
Um Daten zu Kosten, Nutzen und Risiken zu erfassen, wurden Entscheidungsträger in einem Unternehmen befragt, das bereits Juniper Connected Security einsetzt.

FINANZMODELLRAHMEN
Erstellung eines für die Befragung repräsentativen Finanzmodells anhand der TEI-Methodik sowie eine Risikogewichtung des Finanzmodells basierend auf Problemen und Bedenken des befragten Unternehmens.

FALLSTUDIE
Vier grundlegende TEI-Elemente bilden die Grundlage für die Modellierung der Investitionseffekte: Nutzen, Kosten, Flexibilität und Risiken. Mit den zunehmend ausgereiften 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.

HINWEISE

Die Leser werden auf Folgendes hingewiesen:

Diese Studie wurde von Juniper in Auftrag gegeben und von Forrester Consulting durchgeführt. Sie ist nicht als Wettbewerbsanalyse zu verstehen.

Forrester äußert hierin keine Vermutungen über die potenzielle Kapitalrendite, die 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 Juniper Connected Security zu ermitteln.

Juniper 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.

Juniper hat den Kundennamen für die Befragung bereitgestellt, an der Befragung jedoch nicht teilgenommen.

Juniper Connected Security – Customer Journey

Entscheidende Faktoren für die Investition in Juniper Connected Security

BEFRAGTES UNTERNEHMEN

Das von Forrester befragte Unternehmen setzt Juniper Connected Security bereits ein und zeichnet sich durch folgende Merkmale aus:

- Es handelt sich um einen Multimediadienstleister mit siebenstelligem Umsatz.
- Ein Team mit 2 Mitarbeitern ist derzeit für den internen Netzwerkbetrieb zuständig.
- Ein wesentlicher Grund für diese Investition war der geschäftliche Vorteil, den man sich durch die Beseitigung technischer Hürden und die Realisierung einer kreativen und kollaborativen Umgebung für die 200 Mitarbeiter im Bereich Contenterstellung erhoffte.

„Wir suchten [für unsere Sicherheitsarchitektur] eine modernere Lösung – und zwar idealerweise ein Full-Stack-Angebot, sodass der nötige Aufwand zur Einarbeitung in das neue System minimiert wird und auch die Administration des täglichen Netzwerkbetriebs sowie die Implementierung von Änderungen vereinfacht würden. Unsere ältere Ausstattung stammte aus unterschiedlichen Zeiten, das heißt, auf jeder Komponente lief eine andere Codebasis.“
IT-Leiter, Multimediabranche

„Im Hinblick auf die Sicherheit herrschte bei unseren vorhandenen Tools absolute Funkstille. Wir mussten regelrecht im Black-Box-Modus arbeiten. Die Tools lieferten uns einfach keine verwertbaren Daten zu internen Netzwerk-aktivitäten.“
IT-Leiter, Multimediabranche

ZENTRALE HERAUSFORDERUNGEN

Vor der Investition in Juniper nutzte das befragte Unternehmen in seiner Sicherheitsarchitektur eine Kombination aus älteren Lösungen verschiedener Anbieter.

Daraus ergaben sich für das Unternehmen diverse typische Herausforderungen:

- **Höherer Aufwand für die SecOps-Teams bei der Verwaltung.** Durch die veraltete Ausstattung von mehreren Anbietern mussten die SecOps-Teams mit unterschiedlichen Arten von Code arbeiten und mit einer Vielzahl an Personen interagieren, um Netzwerkdiagnosen zu erstellen oder Probleme zu beheben. Außerdem fehlten der bisherigen Ausstattung geeignete Tools, Dashboards und Berichtsfunktionen, die in modernen Lösungen für Transparenz sorgen und verwertbare Daten zu Netzwerkaktivitäten liefern. Folglich vergeudete das Unternehmen wertvolle Zeit mit Prozessen zur Gewährleistung der Sicherheit.

- **Eingeschränkte Verfügbarkeit, Leistung und Kapazität von Personalressourcen.** Bei den für die Sicherheitsverwaltung eingeteilten Ressourcen handelte es sich um vielseitig tätige Mitarbeiter mit zahlreichen Verantwortlichkeiten, zu denen auch die Netzwerk-administration zählte. Das Unternehmen arbeitete mit einem schlanken Team und die Entscheidungsträger hatten weder die Möglichkeit noch den Wunsch, Mitarbeiter extra für diese administrativen Aufgaben abzustellen oder wertvolle Zeit des Personals fest dafür einzuplanen.
- **Undurchsichtigkeit des bestehenden Netzwerks mit höherem Risiko von unbemerkten Sicherheitsverstößen.** Die veraltete Ausstattung lieferte nur begrenzte Einblicke in die Netzwerk-stabilität und -aktivität. Dadurch kamen im Unter-nehmen Zweifel an der Sicherheit des Netzwerks auf, weil die für den Betrieb zuständigen Teams zu keiner Zeit genügend Informationen zum Ausmaß einer Bedrohung oder zur Anzahl potenzieller Zwischenfälle hatten. Das Unternehmen war also anfälliger für Sicherheitsverstöße und ihre möglicherweise schwerwiegenden Folgen.

„Ich bin Generalist und habe ein sehr schlankes Team. Unsere bisherige Ausstattung war in die Jahre gekommen und hatte quasi das Ende ihrer Lebensdauer schon erreicht. Zudem stammten die Geräte noch aus einer ganz anderen Zeit der Netzwerktechnik. Somit verursachte die Nutzung der alten Ausstattung für uns einen erheblichen administrativen Mehraufwand. Wenn Änderungen am Netzwerk nötig waren, ließen sie sich nur auf äußerst mühsame Weise realisieren.“
IT-Leiter, Multimediabranche

LÖSUNGSANFORDERUNGEN UND INVESTITIONSZIELE

Da das befragte Unternehmen vor einem Umzug in neue Büroräume stand, bot sich den Entscheidungsträgern eine praktische Gelegenheit, die Herangehensweise an die Netzwerksicherheit zu überdenken und gegebenenfalls einen Anbieterwechsel zu vollziehen.

Der IT-Leiter sagte: „Wir haben diesen Umzug als Chance genutzt, um unsere Kernkomponenten für den Netzwerkbetrieb komplett zu überholen und die alte Ausstattung hinter uns zu lassen. Manche unserer alten Geräte hatten zu dem Zeitpunkt schon sieben, acht oder gar zehn Jahre auf dem Buckel. Der Umzug verlieh uns also den nötigen Impuls für ein Upgrade. Außerdem musste das Netzwerk in den neuen Büroräumen unabhängig von unseren alten Räumlichkeiten eingerichtet werden.“

Somit beschlossen die Entscheidungsträger die Ausmusterung der veralteten Ausstattung des Unternehmens und den Neustart mit einer modernen Lösung, die folgende Ziele erfüllen sollte:

- Modernisierung der Netzwerkinfrastruktur und Verringerung der Zahl genutzter Anbieter mittels Full-Stack-Funktionalität.
- Umzug in die neuen Büroräume und Migration aller Systeme ohne Ausfallzeiten und mit möglichst minimalen Beeinträchtigungen für das Personal.
- Verringerung des Verwaltungsaufwands durch intuitive Tools sowie eine Gesamtorchestrierung, die zu einem besseren Einblick in das Netzwerk und einer allgemein stabileren Umgebung führt.

Nach der Evaluierung mehrerer Anbieter entschied sich das Unternehmen für Juniper Connected Security und begann mit der Implementierung. Die Befragten betonten folgende Ergebnisse:

- Das Unternehmen konnte seine Sicherheitsarchitektur mit Juniper in den künftigen Büroräumen von Grund auf neu einrichten.
- Da Juniper ein Full-Stack-Anbieter ist, wurden die zugrunde liegenden Stacks des Netzwerks für den gesamten Geschäftsstandort zentralisiert und die Zahl an Zugriffspunkten deutlich reduziert.

- Außerdem sorgte Juniper im gesamten Netzwerk für mehr Redundanz als in der früheren Umgebung, insbesondere durch duale Firewalls, duale Glasfaser-Switches und duale Verwaltungskonsolen für den Unternehmenscampus und das Datencenter.

Wir haben uns für Juniper entschieden, weil uns das Angebot wirklich überzeugt hat, vor allem durch den niedrigeren Verwaltungsaufwand und dass wir mit [dem Junos Betriebssystem] ein einheitliches Betriebssystem für alle Geräte hatten. Außerdem bietet uns Junos wertvolle Einblicke in unser Netzwerk, die wir früher in dieser Form nicht hatten. Und dank der Webschnittstelle fällt die Einarbeitung sehr leicht.

– IT-Leiter, Multimediabranche

Nutzenanalyse

Daten zum quantifizierten Nutzen

Gesamtnutzen						
Ref.	**Nutzen**	**Jahr 1**	**Jahr 2**	**Jahr 3**	**Gesamtwert**	**Barwert**
Atr	Verringerter Verwaltungsaufwand	142.560 $	142.560 $	142.560 $	427.680 $	354.526 $
Btr	Verbesserte Netzwerkstabilität mit niedrigerem Ausfallrisiko	166.400 $	166.400 $	166.400 $	499.200 $	413.812 $
Ctr	Vermiedene Kosten für Sicherheitsinfrastruktur	76.000 $	33.250 $	33.250 $	142.500 $	121.551 $
	Gesamtnutzen (risikobereinigt)	384.960 $	342.210 $	342.210 $	1.069.380 $	889.889 $

VERRINGERTER VERWALTUNGSAUFWAND

Fakten und Daten. Das befragte Unternehmen arbeitete mit einem schlanken Team aus vielfältig tätigen Ressourcen, die sich um zahlreiche Aufgaben kümmerten, einschließlich Netzwerkadministration. Die bisherige Systemumgebung bestand aus veralteter Ausstattung verschiedener Anbieter und war nicht nur fehleranfälliger und schwieriger zu überblicken, sondern erforderte auch die Arbeit mit seltenen Codebasen sowie anbieter-spezifische Kenntnisse zur Implementierung nötiger Änderungen oder zur Behebung von Problemen. Juniper Connected Security wird durch Juniper Security Director verwaltet und bietet eine moderne Sicherheitsinfrastruktur für Netzwerke. Der Funktionsumfang umfasst verständliche Tools und übersichtliche Dashboards. Zudem sorgt die Orchestrierung für mehr Transparenz und Effizienz bei der Verwaltung sowie für eine insgesamt stabilere Umgebung. Dadurch konnte das Unternehmen den Aufwand für die Netzwerkadministration enorm senken.

- Der IT-Leiter erklärte, wie die dank Juniper hinzugewonnene Effizienz den nötigen Zeitaufwand für die Netzwerkadministration verringerte: „Bisher benötigten wir in unseren alten Büros geschätzt 50 Prozent der Zeit von einem Mitarbeiter zur Behebung von Netzwerkproblemen. Und ich selbst habe bestimmt auch noch 10 oder 15 Prozent meiner Zeit dafür aufgewendet. Insgesamt mussten sich also etwa zwei erfahrene Fachkräfte um das Netzwerk kümmern. Das verursacht natürlich gewisse Kosten. [Mit Juniper] sparen wir 30 bis 35 Prozent dieses Zeitaufwands ein und müssen uns keine Sorgen mehr über die Netzwerkkonnektivität machen.“

  Das Unternehmen konnte außerdem die Zahl der für die Netzwerk- und Sicherheitsadministration zuständigen Ressourcen verringern. Der Befragte sagte: „Der Verwaltungsaufwand ist jetzt viel geringer. Wir haben nun eine Person weniger zugeteilt [im Vergleich zur bisherigen Umgebung] und können trotzdem alle im Zusammenhang mit dem Netzwerk anfallenden administrativen Aufgaben erledigen, weil die Betriebsabläufe deutlich vereinfacht wurden.“

- Das Unternehmen schreibt die dank Juniper erreichte Effizienzsteigerung zu großen Teilen den verständlichen Verwaltungs- und Orchestrierungstools und Visualisierungen von Juniper Security Director zu. Mithilfe des Dashboards von Junos kann der Befragte mit seinem Team auch ohne spezielles Fachwissen oder zusätzliche Fachkräfte zuversichtlich die Sicherheit im Netzwerk gewährleisten. In den Worten des Befragten: „Der Verwaltungsaufwand war in unserer früheren Umgebung einfach viel zu hoch. Nach unserem Umzug wollten wir unbedingt weniger Zeit mit diesen mühsamen Aufgaben verschwenden. Dazu mussten wir aber schnellstmöglich lernen, worauf bei unserem Netzwerk und seiner Konfiguration zu achten war. Anfangs haben wir uns dabei sehr stark auf die Webschnittstelle

von Junos verlassen – quasi wie mit Stützrädern am Fahrrad. Da ich noch nie als Netzwerkadministator gearbeitet habe, war es für mich natürlich sehr hilfreich, dass ich per Browser auf die Informationen zugreifen und Visualisierungen abrufen konnte, ohne eine Befehlszeilenschnittstelle nutzen zu müssen."

- Mit Juniper konnte das Unternehmen seine bisher genutzte Ausstattung konsolidieren. Da das neue Ökosystem von Juniper mehr Transparenz bietet und die gesamte Ausstattung vom selben Anbieter stammt und auf einheitlichem Code basiert, sind Diagnosen schneller möglich und Probleme leichter zu beheben. Die höhere Transparenz sorgt zudem dafür, dass Zwischenfälle oder Warnungen, die schnelles Handeln erfordern, besser erkannt werden. Der Befragte sagte: „Wenn wir in der Vergangenheit Probleme mit der Netzwerkkonnektivität hatten, ließ sich die Ursache nur sehr schwer herausfinden, da wir sozusagen fragmentierte Verwaltungsprozesse und unterschied-liche Geräte aus verschiedenen Zeiten genutzt haben. Und selbst wenn wir irgendwann die Ursache gefunden haben, war das Problem ja dadurch noch gar nicht gelöst. Mit Juniper Connected Security fällt es mir nun viel leichter, Fehlalarme zu erkennen oder verdächtige Verhaltensweisen abzuklären, die nicht unbedingt Gegenmaßnahmen erfordern."
- Das Netzwerk von Juniper und die zugehörigen Tools sorgten für eine insgesamt stabilere Sicherheits-architektur mit deutlich niedrigerem Verwaltungs-aufwand. Dazu äußerte sich der Befragte: „Einer der Gründe, warum die Verwaltung so wenig Aufwand verursacht, ist die Tatsache, dass die Lösung nun viel stärker unseren Anforderungen entspricht. Wir haben im Prinzip alles optimiert, was man hinsichtlich unserer internen Netzwerksituation optimieren kann. Wir haben unsere VLANs (Virtual Local Area Networks) ebenso umgestaltet wie die Verbindungen zwischen unseren Standorten. Seitdem ist das Netzwerk bestens gesichert."

Modellierung und Annahmen. Um zu berechnen, inwiefern sich der Verwaltungsaufwand verringert, geht Forrester von folgenden Annahmen aus:

- Die frühere Umgebung erforderte 3 Mitarbeiter für die Verwaltung, die sich den anfallenden Aufgaben in variablem Umfang widmeten. Nach dem Wechsel zu Juniper konnte das Unternehmen 1 Mitarbeiter anderen Aufgaben zuteilen und den Zeitaufwand für die verbleibenden 2 Mitarbeiter verringern.
- Im ersten Jahr erzielte das Unternehmen sofort eine Effizienzsteigerung von 60 Prozent bei den SecOps-Mitarbeitern. Aufgrund der Stabilität der Sicherheits-architektur blieb auch dieses Effizienzniveau im Verlauf der drei Jahre stabil.
- Das durchschnittliche Jahresgehalt von SecOps-Ressourcen beträgt 110.000 US-Dollar.
- Rund 80 Prozent der hinzugewonnenen Zeit durch bessere Tools, Netzwerktransparenz und Stabilität konnten für andere wertschöpfende Aufgaben genutzt werden.

Risiken. Die Verringerung des Verwaltungsaufwands kann abhängig von folgenden Faktoren variieren:

„Den größten Vorteil unserer neuen Lösung sehe ich in den Tools selbst sowie in den besseren Einblicken in das Netzwerk. Dadurch können wir bei der Verwaltung besser sehen und verstehen, wer im Netzwerk aktiv ist und was genau vorgeht, und auch unsere Richtlinien lassen sich über mehrere Umgebungen hinweg besser durchsetzen."
IT-Leiter, Multimediabranche

- Zustand der bisherigen Netzwerkumgebung (z. B. Alter, Anbieter usw.) und Anzahl der zur Verwaltung eingeteilten SecOps-Ressourcen
- Grad der Beteiligung einer zugeteilten Ressource an der Netzwerkadministration und ihr entsprechendes Jahresgehalt
- Gehaltsunterschiede je nach Region
- Anteil der zurückgewonnenen Produktivität des SecOps-Teams, der anderen wertschöpfenden Aufgaben zukommen kann (ggf. abhängig von parallel laufenden technischen oder geschäftlichen Projekten)

Zur Berücksichtigung dieser Risiken hat Forrester diesen Nutzen um 10 Prozent nach unten korrigiert, was über drei Jahre einen risikobereinigten Gesamtbarwert von 354.526 US-Dollar ergibt.

Verringerter Verwaltungsaufwand

Ref.	Kennzahl	Quelle	Jahr 1	Jahr 2	Jahr 3
A1	Eingesetzte SecOps-Mitarbeiter für die Netzwerkadministration vor Juniper Connected Security	Befragung	3	3	3
A2	Verringerter Verwaltungsaufwand mit Juniper Connected Security	Befragung	60 %	60 %	60 %
A3	Durchschnittliches Jahresgehalt von SecOps-Mitarbeiter	Annahme	110.000 $	110.000 $	110.000 $
A4	Zurückgewonnene Produktivität	Annahme	80 %	80 %	80 %
At	Verringerter Verwaltungsaufwand	A1*A2*A3*A4	158.400 $	158.400 $	158.400 $
	Risikobereinigung	↓ 10 %			
Atr	Verringerter Verwaltungsaufwand (risikobereinigt)		142.560 $	142.560 $	142.560 $
	Dreijahresgesamtwert: 427.680 $			**Dreijahresbarwert: 354.526 $**	

VERBESSERTE NETZWERKSTABILITÄT MIT NIEDRIGEREM AUSFALLRISIKO

Fakten und Daten. In der Vergangenheit gab es immer wieder Zwischenfälle, die zu Ausfallzeiten für die Mitarbeiter des Unternehmens führten. Durch diese wiederholten Beeinträchtigungen entwickelten die Mitarbeiter ein regelrechtes Misstrauen gegenüber dem Netzwerk, da es sie von ihren eigentlichen kreativen und kollaborativen Aufgaben abhielt. Nach dem Wechsel zu Juniper verringerten sich die Ausfallzeiten für die Mitarbeiter deutlich, sodass sie sich ohne technische Unterbrechungen ganz der Bereitstellung von Medieninhalten für ihre Kunden widmen konnten.

- Die frühere Ausstattung zur Gewährleistung der Netzwerksicherheit bestand aus Black-Box-Komponenten, die nur schwierig zu überblicken und zu verwalten waren. Dadurch war das Unternehmen einem größeren Risiko von schwerwiegenden Zwischenfällen ausgesetzt. Dank Juniper erhöhte sich die Transparenz und Stabilität des Netzwerks, wodurch die Gefahr eines verheerenden Zwischenfalls sank. Der Befragte sagte: „Angesichts der fehlenden Transparenz in unserer alten Umgebung hätte ein Sicherheitsverstoß wirklich schwerwiegende Folgen haben müssen, damit er überhaupt bemerkt würde. Es ist also durchaus möglich, dass einige Netzwerkausfälle durch Sicherheitsverstöße verursacht wurden, die uns schlicht nicht aufgefallen sind. Das Risiko

eines katastrophalen Ausfalls war in unserer alten Umgebung somit sehr hoch. Mit Juniper bin ich jetzt zuversichtlicher, dass derartige Zwischen-fälle verhindert werden können, weil wir nun viel bessere Einblicke in das System haben."

- Die Probleme der früheren Umgebung äußerten sich vor allem in Form von Ausfällen, die sich auf die Mitarbeiterproduktivität auswirkten und die Umgebung anfällig für Angriffe machten. Der Befragte erklärte dazu: „In unserem alten System ließ die Switch-Konnektivität sehr zu wünschen übrig. Mit Portschnittstellen gab es ebenfalls Probleme und folglich auch mit der VLAN-Konnektivität, Updates, Upgrades und damit zusammenhängenden Ausfall-zeiten. Es ist uns, glaube ich, bei keiner einzigen Komponente gelungen, die aktuellste Version zu implementieren. Stattdessen hatten wir einen fortlaufenden Update-Zeitplan, durch den es aber regelmäßig Unterbrechungen gab, die zu Ausfallzeiten für Mitarbeiter führten und das Risiko für unsere Systemumgebung erhöhten – trotz unserer Bemühungen, die Updates außerhalb der regulären Arbeitszeiten durchzuführen."
- Die Lösung von Juniper sorgte für eine deutliche Verbesserung der Netzwerkleistung und somit auch für eine geringere Beeinträchtigung der Mitarbeiter. Der Befragte sagte: „Seit wir die Ausstattung von Juniper nutzen, hatten wir keine Netzwerkausfälle oder Sicherheitsvorfälle. Tatsächlich zählen die Verfügbarkeitswerte aus den letzten drei Jahren zu den besten meiner gesamten Karriere. Sie sind bei allen Komponenten locker im Bereich von 99 Prozent, einschließlich Netzwerk. Früher lagen die Werte eher im Bereich von 90 Prozent. Wir sprechen also von einer Verbesserung um etwa 10 Prozent."
- Durch die verbesserte Stabilität des Netzwerks stieg auch das Vertrauen der Mitarbeiter in die Infrastruktur. Ohne technische Unterbrechungen konnten sich die Kreativteams viel besser auf die Erstellung von Inhalten für ihre Kunden konzentrieren. Dem Befragten zufolge war die Verbesserung unverkennbar: „Die Anwender hatten nun das Gefühl, dass ihre Arbeit durch ein solides Fundament unterstützt wird und nicht mehr in einer chaotischen, unzuverlässigen Umgebung verrichtet werden muss, die man nur mit lautstarken Beschwerden quittieren konnte."

Modellierung und Annahmen. Um zu berechnen, inwiefern sich die Netzwerkstabilität verbessert und das Risiko von Ausfallzeiten sinkt, geht Forrester von folgenden Annahmen aus:

- Das Unternehmen beschäftigt 200 Mitarbeiter, die sich auf die Contenterstellung konzentrieren und durch potenzielle Ausfälle in ihrer Produktivität beeinträchtigt würden.
- Die Systemverfügbarkeit erreichte in der früheren Umgebung einen Wert von 89 Prozent. Das heißt, in 11 Prozent der Zeit (229 Stunden pro Jahr) war das Unternehmen anfällig für Ausfälle mit verheerenden Folgen und potenziellen Beeinträchtigungen für Mitarbeiter.
- Nach dem Wechsel zu Juniper verbesserte das Unternehmen seine Systemverfügbarkeit um 10 Prozent und verringerte somit das jährliche Risiko von schwerwiegenden Ausfällen.
- Es wirken sich jedoch nicht alle Ausfälle auf die Mitarbeiter aus. Forrester geht davon aus, dass nur 10 Prozent dieser Zwischenfälle auch zu Ausfallzeiten für Mitarbeiter führen.
- Die Kosten eines Ausfalls belaufen sich pro Anwender (bzw. Mitarbeiter) auf 50 US-Dollar und ergeben sich einerseits aus den Stundensätzen der Mitarbeiter (da sie ja bei einem Ausfall nur bedingt arbeitsfähig sind) und andererseits aus den Auswirkungen für das Geschäft. Systemausfälle hindern Mitarbeiter außerdem daran, ihren Kunden den gewünschten Content bereitzustellen, wodurch weitere Einbußen durch entgangene Geschäftschancen entstehen.

Risiken. Der erzielte Nutzen aufgrund der verbesserten Netzwerkstabilität mit dadurch niedrigerem Ausfallrisiko kann abhängig von folgenden Faktoren variieren:

- Anzahl der Mitarbeiter des Unternehmens
- Grad der Systemverfügbarkeit in der früheren Umgebung sowie die durch Juniper bewirkte Verbesserung
- Anteil der potenziellen Ausfälle, der sich auf Mitarbeiter auswirken würde

- Durchschnittlicher Stundensatz der Mitarbeiter, der je nach Branche, Region und Position im Unternehmen variiert, sowie Tätigkeitsschwerpunkt dieser Mitarbeiter, der sich auf die Höhe der ausfallbedingten Einbußen durch entgangene Geschäftschancen auswirkt. (Bei Tätigkeiten mit direktem Kundenkontakt sind diese Opportunitätskosten entsprechend höher.)

Zur Berücksichtigung dieser Risiken hat Forrester diesen Nutzen um 20 Prozent nach unten korrigiert, was über drei Jahre einen risikobereinigten Gesamtbarwert von 413.812 US-Dollar ergibt.

Verbesserte Netzwerkstabilität mit niedrigerem Ausfallrisiko

Ref.	Kennzahl	Quelle	Jahr 1	Jahr 2	Jahr 3
B1	Anzahl der Anwender/Mitarbeiter	Befragung	200	200	200
B2	Ausfallzeiten durch Netzwerkstörungen pro Jahr vor Juniper (in Stunden)	Annahme	229	229	229
B3	Ausfallzeiten durch Netzwerkstörungen pro Jahr mit Juniper (in Stunden)	Annahme	21	21	21
B4	Anteil der Ausfälle mit direkter Beeinträchtigung für Mitarbeiter	Annahme	10 %	10 %	10 %
B5	Ausfallkosten je Anwender	Annahme	50 $	50 $	50 $
Bt	Verbesserte Netzwerkstabilität mit niedrigerem Ausfallrisiko	B1*((B2-B3)*B4)*B5	208.000 $	208.000 $	208.000 $
	Risikobereinigung	↓ 20 %			
Btr	Verbesserte Netzwerkstabilität mit niedrigerem Ausfallrisiko (risikobereinigt)		166.400 $	166.400 $	166.400 $
	Dreijahresgesamtwert: 499.200 $		**Dreijahresbarwert: 413.812 $**		

VERMIEDENE KOSTEN FÜR SICHERHEITSINFRASTRUKTUR

Fakten und Daten. Das befragte Unternehmen konnte bestimmte Kosten vermeiden, weil die Entscheidungsträger sich zur Ausmusterung der veralteten Ausstattung entschlossen und die neue Sicherheitsarchitektur mit Lösungen eines einzelnen Anbieters implementierten. Die bisherige Ausstattung war veraltet und verursachte somit enorme jährliche Wartungskosten. Durch den Wechsel zu Juniper konnte das Unternehmen diese Kosten vermeiden. Da Juniper zudem als Full-Stack-Anbieter agiert, ließen sich die Investitionskosten für nötige Hardware besser planen und verringern.

- Der IT-Leiter des Unternehmens erläuterte diese Vermeidung unnötiger Kosten wie folgt: „Mit Kosteneinsparungen meine ich vor allem die Anschaffungskosten sowie einen Teil der Gesamtbetriebskosten, die sich aufgrund unserer ausgehandelten Supportverträge verringerten. Bei der Anschaffung ergaben sich Einsparungen durch niedrigere Investitionen in Hardware und weitere Ausstattung. Das Angebot von Juniper – ein Full-Stack-Anbieter – umfasste alle nötigen Komponenten und Services zu einem guten Preis und hat uns daher am meisten überzeugt.“
- Der Befragte bezifferte die Einsparungen bei den Investitionskosten für die Neuanschaffung, Einrichtung und Konfiguration der Lösung von Juniper auf etwa 40.000 bis 45.000 US-Dollar. Zusätzlich verringerten sich dem Befragten zufolge durch die Ausmusterung der Altgeräte auch die jährlichen Wartungskosten um etwa 35.000 US-Dollar.

Eingesparte Investitionskosten

45.000 $

Eingesparte laufende Wartungskosten

35.000 $ pro Jahr

Modellierung und Annahmen. Um die Höhe der eingesparten Kosten für die Sicherheitsinfrastruktur zu berechnen, geht Forrester von folgenden Annahmen aus:

- Die Investitionskosten für die Hardware von Juniper liegen 45.000 US-Dollar unter den Kosten der alternativen Lösung.
- Der Wartungsaufwand der bisherigen Lösung verursachte Kosten von jährlich 35.000 US-Dollar, die mit der Lösung von Juniper vermieden werden.

Risiken. Die Höhe der vermiedenen Kosten für die Sicherheitsinfrastruktur kann abhängig von folgenden Faktoren variieren:

- Wartungsanforderungen der bisherigen Lösung gemäß jährlichem Vertrag
- Auswahl potenzieller alternativer Lösungen (beeinflusst die Höhe der Einsparungen bei Investitionskosten)

Zur Berücksichtigung dieser Risiken hat Forrester diesen Nutzen um 5 Prozent nach unten korrigiert, was über drei Jahre einen risikobereinigten Gesamtbarwert von 121.600 US-Dollar ergibt.

Vermiedene Kosten für Sicherheitsinfrastruktur

Ref.	Kennzahl	Quelle	Jahr 1	Jahr 2	Jahr 3
C1	Investitionskosten, die bei Juniper Connected Security entfallen	Befragung	45.000 $	0 $	0 $
C2	Entfallene Wartungskosten der bisherigen Lösung	Befragung	35.000 $	35.000 $	35.000 $
Ct	Vermiedene Kosten für Sicherheitsinfrastruktur	C1+C2	80.000 $	35.000 $	35.000 $
	Risikobereinigung	↓ 5 %			
Ctr	Vermiedene Kosten für Sicherheitsinfrastruktur (risikobereinigt)		76.000 $	33.250 $	33.250 $
	Dreijahresgesamtwert: 142.500 $		**Dreijahresbarwert: 121.551 $**		

NICHT QUANTIFIZIERBARER NUTZEN

Für das befragte Unternehmen ergaben sich weitere Vorteile, die jedoch nicht quantifiziert werden konnten:

- **IT-Teams konnten ausgefeiltere und modernere Architekturen entwickeln.** Durch Juniper Connected Security verringerte sich der Aufwand bei der Netzwerk- und Sicherheitsadministration deutlich, während sich gleichzeitig die Stabilität der System-umgebung erhöhte. Dadurch hatten IT-Teams mehr Zeit für Innovationsprojekte und trauten sich zudem häufiger, auch kompliziertere Architekturelemente wie eine Hybrid Cloud in die Systemumgebung einzubinden.

- **Mitarbeiter können sich auf die Contenterstellung und Zusammenarbeit konzentrieren.** Dank der verbesserten Netzwerkstabilität legte die Technik den Benutzern nicht mehr ständig Steine in den Weg. So konnten sie sich darauf konzentrieren, eine kreative und kollaborative Arbeitsumgebung aufrechtzuerhalten – ein entscheidender Faktor für den geschäftlichen Erfolg.

„Unsere vorherige Sicherheitsarchitektur bestand aus unterschiedlichen Ebenen mit verschiedener Ausstattung, die aufeinander abgestimmt werden musste. Mit Juniper verfügen wir jetzt über ein solides Fundament, das alle nötigen Sicherheitstools in einem einzigen Stack vereint. Die Netzwerkkonfiguration von Juniper hat uns dabei geholfen, die Funktionen unserer Sicherheitssysteme und -tools besser zu verstehen. Nun trauen wir uns auch an neue und andere technische Herausforderungen heran.“
IT-Leiter, Multimediabranche

„Einige Benutzer hatten das Vertrauen in unsere vorherigen Systeme verloren. Diese Systeme wieder einsatzfähig zu machen und auch die Benutzer zurückzugewinnen, ist eher eine Marketing-/PR-Aufgabe, keine technische Herausforderung. Es geht hier wirklich um Vertrauen und in diesem Punkt schneidet die neue Lösung eindeutig besser ab. Wir haben jetzt den Idealzustand erreicht.“
IT-Leiter, Multimediabranche

FLEXIBILITÄT

Unternehmen schätzen Flexibilität individuell unterschiedlich hoch ein. Es sind mehrere Szenarien denkbar, in denen ein Unternehmen sich für die Implementierung von Juniper Connected Security entscheidet und zusätzliche Nutzungs- und Geschäftsmöglichkeiten erst später erkennt.

Ein Beispiel ist die bessere Unterstützung der geschäftlichen Transformation. Nach der Investition in Juniper Connected Security experimentierten IT-Teams häufiger mit komplexeren, flexibleren und moderneren Architekturen wie Hybrid Clouds, ohne dass die Mitarbeiter durch technische Schwierigkeiten bei der Arbeit gestört wurden. Das Unternehmen konnte also seine Energie stärker auf den geschäftlichen Wandel konzentrieren und wurde durch die technische Lösung von Juniper dabei nicht behindert, sondern unterstützt. Folglich rechnen Entscheidungsträger damit, dass diese neu gewonnene technische Freiheit und Flexibilität zu weiteren Innovationen im Unternehmen führen wird.

Flexibilität lässt sich auch quantifizieren, wenn sie im Rahmen eines spezifischen Projekts bewertet wird. Eine ausführlichere Beschreibung enthält Anhang A.

Kostenanalyse

Daten zu quantifizierten Kosten

Gesamtkosten							
Ref.	**Kosten**	**Jahr 0**	**Jahr 1**	**Jahr 2**	**Jahr 3**	**Gesamtwert**	**Barwert**
Dtr	Investitionskosten und laufende Zahlungen an Anbieter	0 $	218.500 $	17.250 $	17.250 $	253.000 $	225.853 $
Etr	Zeitaufwand interner Ressourcen für Onboarding und Schulung	0 $	4.865 $	1.216 $	1.216 $	7.298 $	6.342 $
	Gesamtkosten (risikobereinigt)	0 $	223.365 $	18.466 $	18.466 $	260.298 $	232.195 $

INVESTITIONSKOSTEN UND LAUFENDE ZAHLUNGEN AN ANBIETER

Fakten und Daten. Das befragte Unternehmen bezahlte an Juniper die Investitionskosten für die Connected Security Hardware und zugehörige Software sowie für die Implementierungsservices. Zusätzlich handelte das Unternehmen einen Wartungsvertrag mit Juniper für fortlaufende Instandhaltungs- und Supportleistungen aus.

Modellierung und Annahmen. Um die Höhe der anfänglichen und laufenden Zahlungen an Anbieter zu berechnen, geht Forrester von folgenden Annahmen aus:

- Die Vorlaufkosten entstehen durch die direkt an Juniper entrichteten Ausgaben für die Hardware und Software sowie durch die Gebühren für Implementierungsservices und erforderliche Integrationen, die über Juniper an einen Drittanbieter gezahlt werden. Die Hardware-, Software- und Implementierungskosten fallen nur im ersten Jahr an.
- Die Implementierung wurde an einem einzigen Wochenende erledigt und kostete das Unternehmen insgesamt 175.000 US-Dollar.
- Die laufenden Kosten entstehen durch die Wartungs- und Supportleistungen, die das befragte Unternehmen mit Juniper vertraglich vereinbart hat. Insgesamt betragen diese Kosten 15.000 US-Dollar pro Jahr.

Risiken. Die Höhe der anfänglichen und laufenden Zahlungen an Anbieter kann abhängig von folgenden Faktoren variieren:

- Höhe und Umfang der Investition in Juniper hinsichtlich der nötigen Hardware und Software zum Betrieb der zugehörigen Sicherheitsarchitektur
- Erwartungen hinsichtlich der Implementierungsfristen
- Konditionen des mit Juniper ausgehandelten Wartungsvertrags (Anzahl der Jahre, in denen entstehende Kosten bereits durch die Anschaffungs-kosten abgedeckt sind, sowie Wert der fortlaufenden Wartungsservices, die nicht durch die Anschaffungs-kosten abgedeckt sind.)

Zur Berücksichtigung dieser Risiken hat Forrester diese Kosten um 15 Prozent nach oben korrigiert, was über drei Jahre einen risikobereinigten Gesamtbarwert von 225.853 US-Dollar ergibt.

Investitionskosten und laufende Zahlungen an Anbieter						
Ref.	**Kennzahl**	**Quelle**	**Jahr 0**	**Jahr 1**	**Jahr 2**	**Jahr 3**
D1	Anfängliche Hardware- und Projektkosten, die an Juniper und externe Implementierungs-partner gezahlt wurden	Befragung	0 $	175.000 $	0 $	0 $
D2	Laufende Zahlungen an Juniper	Befragung	0 $	15.000 $	15.000 $	15.000 $
Dt	Investitionskosten und laufende Zahlungen an Anbieter	D1+D2	0 $	190.000 $	15.000 $	15.000 $
	Risikobereinigung	↑ 15 %				
Dtr	Investitionskosten und laufende Zahlungen an Anbieter (risikobereinigt)		0 $	218.500 $	17.250 $	17.250 $
	Dreijahresgesamtwert: 253.000 $			**Dreijahresbarwert: 225.853 $**		

ZEITAUFWAND INTERNER RESSOURCEN FÜR ONBOARDING UND SCHULUNG

Fakten und Daten. Dem befragten Unternehmen zufolge entstanden neben den Zahlungen an Juniper und andere Drittanbieter auch Kosten durch den Zeitaufwand, den interne Ressourcen im Zusammenhang mit Juniper Connected Security in Onboarding und Schulungen investierten.

Modellierung und Annahmen. Um die Höhe des Zeitaufwands interner Ressourcen für Onboarding und Training zu berechnen, geht Forrester von folgenden Annahmen aus:

- Das Unternehmen nutzt ein schlankes Team im Umfang von 2 SecOps-Mitarbeitern, die sich der laufenden Wartung und Verwaltung von Juniper Connected Security widmen.
- Zu Beginn investieren die SecOps-Mitarbeiter Zeit im Umfang von 40 Stunden, um sich vollständig mit dem System von Juniper vertraut zu machen und den effektiven Einsatz der Tools zu erlernen.
- In den Folgejahren sind nur noch wenige Schulungsmaßnahmen nötig, um sich in neue Funktionen einzuarbeiten. Der jährliche Gesamtaufwand beträgt dann 10 Stunden.

Risiken. Der Zeitaufwand interner Ressourcen für Onboarding und Schulung kann abhängig von folgenden Faktoren variieren:

- Anzahl der SecOps-Mitarbeiter und Umfang ihrer Beteiligung an der Verwaltung von Juniper Connected Security
- Vertrautheit mit Hardware und Software für Sicherheitsarchitekturen
- Höhe und Umfang der Investition in Juniper

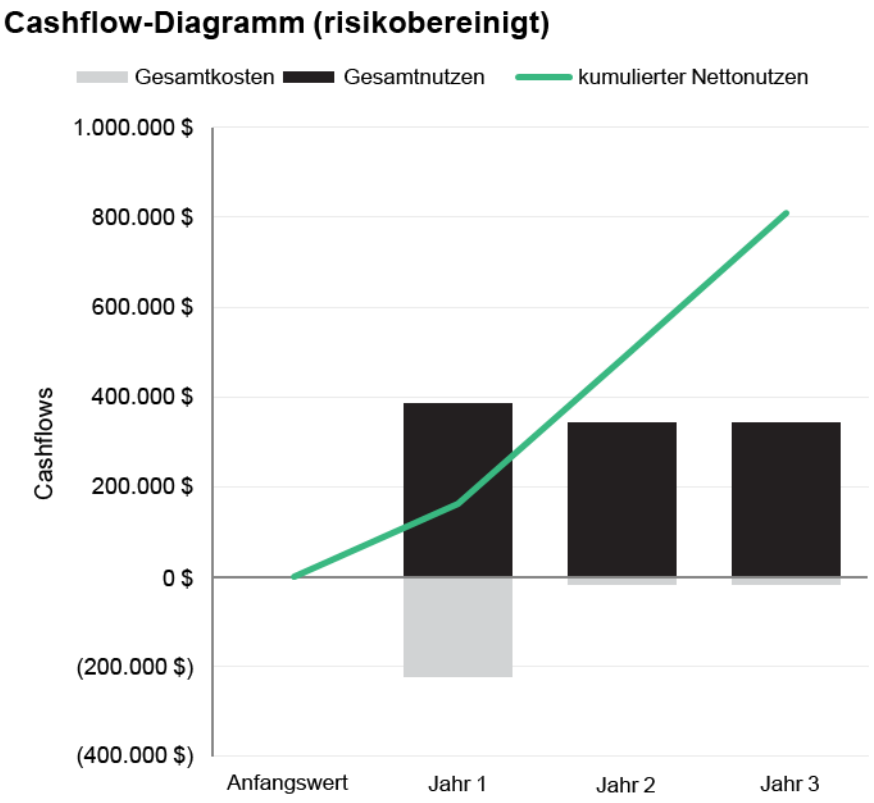
Zur Berücksichtigung dieser Risiken hat Forrester diese Kosten um 15 Prozent nach oben korrigiert, was über drei Jahre einen risikobereinigten Gesamtbarwert von 6.342 US-Dollar ergibt.

Zeitaufwand interner Ressourcen für Onboarding und Schulung

Ref.	Kennzahl	Quelle	Jahr 0	Jahr 1	Jahr 2	Jahr 3
E1	Anzahl der zugeteilten Mitarbeiter für laufende Wartung und Verwaltung von Juniper	Befragung	0	2	2	2
E2	Nötige Zeit für Onboarding und Schulung (in Stunden)	Befragung	0	40	10	10
E3	Durchschnittlicher Stundensatz der SecOps-Mitarbeiter	Annahme	0 $	53 $	53 $	53 $
Et	Zeitaufwand interner Ressourcen für Onboarding und Schulung	E1*E2*E3	0 $	4.231 $	1.058 $	1.058 $
	Risikobereinigung	↑ 15 %				
Etr	Zeitaufwand interner Ressourcen für Onboarding und Schulung (risikobereinigt)		0 $	4.865 $	1.216 $	1.216 $
	Dreijahresgesamtwert: 7.298 $			**Dreijahresbarwert: 6.342 $**		

Zusammenfassung der Finanzergebnisse

KONSOLIDIERTE RISIKOBEREINIGTE KENNZAHLEN FÜR EINEN ZEITRAUM VON DREI JAHREN



Die in den Abschnitten „Nutzen“ und „Kosten“ berechneten Finanzergebnisse können zur Bestimmung des ROI und des Kapitalwerts für die Investition des Modellunternehmens herangezogen werden. Forrester hat dieser Analyse einen jährlichen Diskontierungszinssatz von 10 % zugrunde gelegt.

Diese risikobereinigte Kapitalrendite und die Kapital-werte werden durch die Anwendung von Risikoanpassungsfaktoren auf die nicht angepassten Ergebnisse eines jeden Nutzen- und Kostenabschnitts ermittelt.

Cashflow-Analyse (risikobereinigte Schätzungen)

	Jahr 0	Jahr 1	Jahr 2	Jahr 3	Gesamtwert	Barwert
Gesamtkosten	0 $	(223.365 $)	(18.466 $)	(18.466 $)	(260.298 $)	(232.195 $)
Gesamtnutzen	0 $	384.960 $	342.210 $	342.210 $	1.069.380 $	889.889 $
Nettonutzen	0 $	161.595 $	323.744 $	323.744 $	809.082 $	657.694 $
ROI						283 %

Anhang A: Total Economic Impact

Total Economic Impact (TEI) ist eine von Forrester Research entwickelte Methode, die die Entscheidungs-prozesse von Unternehmen zu technischen Fragen optimiert und Anbietern dabei hilft, ihren Kunden die Wertversprechen ihrer Produkte und Dienstleistungen zu vermitteln. Mit der TEI-Methode können Unternehmen ihrer Geschäftsleitung und anderen wichtigen Stakeholdern den Wert einer IT-Initiative aufzeigen, rechtfertigen und veranschaulichen.

KONZEPT DES TOTAL ECONOMIC IMPACT

Nutzen stellt den Wert dar, der dem Unternehmen durch das Produkt entsteht. Die TEI-Methodik gewichtet Nutzen und Kosten gleich. Dadurch wird eine umfassende Untersuchung der Auswirkungen der Technologie auf das Gesamtunternehmen ermöglicht.

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

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

Risiken messen die Unsicherheit von Nutzen- und Kostenschätzungen angesichts 1) der Wahrscheinlichkeit, dass die Schätzungen den ursprünglichen Prognosen entsprechen, und 2) der Wahrscheinlichkeit, dass die Schätzungen im Laufe der Zeit mit den tatsächlichen Werten abgeglichen werden. Die Risikofaktoren der TEI-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 abgezinst. Alle anderen Cashflows werden unter Verwendung des Diskontierungszinssatzes am Ende des Jahres abgezinst. Berechnungen des Barwerts werden für jede Gesamtkosten- und Gesamtnutzenschätzung vorgenommen. Die Berechnungen des Kapitalwerts in den Übersichtstabellen entsprechen der Summe der anfänglichen Investition und des abgezinsten Cashflows für die einzelnen Jahre. Die Summen und Barwertberechnungen in den Tabellen für Gesamtnutzen, Gesamtkosten und Cashflow ergeben möglicherweise nicht den exakten Gesamtwert, da einige Beträge eventuell gerundet sind.

BARWERT (BW)

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

KAPITALWERT (KW)

Der Barwert oder aktuelle Wert des (diskontierten) zukünftigen Netto-Cashflows zu einem gegebenen Zinssatz (dem Diskontierungszinssatz). Ein positiver Projektkapitalwert bedeutet in der Regel, dass die Investition empfehlenswert ist, sofern nicht andere Projekte höhere Kapitalwerte aufweisen.

RETURN ON INVESTMENT (ROI)

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

DISKONTIERUNGSZINSSATZ

Der in der Cashflow-Analyse verwendete Zinssatz, mit dem der Zeitwert von Geld berücksichtigt wird. Unternehmen verwenden in der Regel Diskontsätze zwischen 8 % und 16 %.

AMORTISATIONSZEITRAUM

Der Break-Even-Point einer Investition. Dies ist der Zeitpunkt, an dem der Nettonutzen (Nutzen abzgl. Kosten) gleich der Anfangsinvestition bzw. den Anfangskosten ist.

Anhang B: Schlussbemerkungen

[1] Quelle: „Now Tech: Virtual Network Infrastructure Switching Fabric, Q2 2020“, Forrester Research, Inc., 22. April 2020.


FORRESTER®