

Total Economic Impact™ von Cisco

TrustSec

Vereinfachte Sicherheitstechnik
und reduzierte Betriebskosten
durch Cisco

WISSENSWERTES ZU FORRESTER CONSULTING

Forrester Consulting bietet unabhängige und objektive, auf Forschungsergebnissen basierende Beratungsdienstleistungen und unterstützt Führungskräfte dabei, ihr Unternehmen zum Erfolg zu führen. Die Beratungsdienste von Forrester reichen von kurzen Strategiesitzungen bis hin zu speziell auf den Kunden abgestimmten Projekten. Bei Forrester stehen Sie in direktem Kontakt mit Analysten aus der Marktforschung, die mit ihrem Fachwissen auf die speziellen Anforderungen Ihres Unternehmens eingehen können. Weitere Informationen finden Sie unter www.forrester.com/consulting.

Zusammenfassung

Forrester Consulting hat im Auftrag von Cisco den Total Economic Impact™ (TEI) und den potenziellen Return on Investment untersucht, den Unternehmen durch die softwaredefinierte Segmentierung mit Cisco TrustSec erzielen können. Der Zweck dieser Studie besteht darin, Lesern einen Rahmen zur Bewertung der möglichen finanziellen Auswirkungen von Cisco auf ihr jeweiliges Unternehmen bereitzustellen.

Um den Nutzen sowie die Kosten und Risiken von TrustSec besser einschätzen zu können, befragte Forrester vier Kunden, die TrustSec implementiert hatten. Die softwaredefinierte Segmentierungslösung TrustSec vereinfacht die Bereitstellung und Verwaltung des sicheren Zugriffs auf Netzwerkservices und -anwendungen. Anders als Zugangskontrollmechanismen für eine Netzwerktopologie arbeiten die TrustSec-Richtlinien mit logischer Gruppierung. Hochsicherer Zugriff wird konsistent beibehalten, auch wenn Ressourcen in mobile und virtuelle Netzwerke verschoben werden. Eine ausführliche Beschreibung von TrustSec finden Sie auf der in diesem Dokument enthaltenen Übersichtsseite zu Cisco TrustSec.

Die befragten Kunden hatten umfassende Ziele für die Implementierung von TrustSec. Dazu zählten Risikominimierung, Compliance sowie die gesteigerte Effizienz des IT-Betriebs. Diese Kunden wollten ihre Anwendungen an allen Standorten schützen und den kontrollierten Zugriff auf geprüfte Ressourcen beschränken. In Anwendungsfällen für TrustSec mussten die befragten Kunden den mobilen Zugriff für Tablets und Mobilgeräte und die Netzwerksegmentierung im gesamten Unternehmen verwalten, den Zugriff auf kritische Anwendungen im Rechenzentrum beschränken sowie auf ein identitätsbasiertes Zugriffsmodell für sämtliche Ressourcen umsteigen.

TRUSTSEC REDUZIERT BETRIEBSKOSTEN, VEREINFACHT SICHERHEITSTECHNIK UND ERHÖHT DIE FLEXIBILITÄT

Die Befragung unserer vier bestehenden Kunden und darauffolgende Finanzanalysen ergaben für eine Modellorganisation nach dem Muster dieser Unternehmen den risikobereinigten ROI sowie Nutzen und Kosten wie in Abbildung 1 gezeigt.ⁱ

Die Analyse der Modellorganisation zeigt einen Nutzen von 1.663.914 US-Dollar gegenüber 3.989.498 US-Dollar Implementierungskosten für klassische Lösungen. Damit ergibt sich ein Kapitalwert (KW) von 2.325.584 US-Dollar. TrustSec führte bei den befragten Unternehmen dank der Vermeidung von Kosten für eine alternative, klassische perimeterbasierte Sicherheitslösung zu reduzierten Betriebskosten, zu einem geringeren Bedarf an zusätzlichen IT-Mitarbeitern sowie zu verbesserter Netzwerkstabilität mit geringerem Risiko von Ausfallzeiten.

Weitere Vorteile, die von befragten Unternehmen genannt wurden, umfassen die schnellere Markteinführungszeit bei Projektbereitstellung, konsistente und effektive Netzwerksegmentierung, vereinfachte Sicherheitstechnik und Sicherheitsrichtlinien sowie die verbesserte, automatisierte Verwaltung von Firewallregeln. Weitere Vorteile sind optimierte Flexibilität, die Möglichkeit, Sicherheitsrichtlinien zu skalieren, ein verbesserter Sicherheitsstatus für Netzwerke und die optimierte Erfüllung gesetzlicher Auflagen.

ABBILDUNG 1

Übersicht der risikobereinigten finanziellen Ergebnisse über drei Jahre

ROI:
140 %

Kapitalwert:
2,33 Millionen
US-Dollar

IT-Betriebs-
kosten:
▼ bis zu 80 %

Zeit, Netzwerk-
änderungen zu
implementieren:
▼ 98 %

„TrustSec vereinfacht das Sicherheitszugriffsmodell und reduziert den Aufwand für die Richtlinienwartung.“

— Enterprise Architect,
Bildungseinrichtung

› **Nutzen:** Die Modellorganisation profitierte von den folgenden risikobereinigten Barwertvorteilen, die denen der befragten Unternehmen entsprechen:

- **Einsparungen durch Kostenvermeidung von alternativen herkömmlichen Lösungen**
Durch die Nutzung von TrustSec anstelle einer anderen herkömmlichen Segmentierungslösung wie VLANs und Firewalls konnte die Modellorganisation über den Analysezeitraum von drei Jahren mehr als 2,7 Mio. US-Dollar einsparen.
- **Reduzierung der IT-Betriebskosten** TrustSec reduziert die Kosten für die Zugriffsverwaltung, besonders im Hinblick auf den notwendigen Verwaltungsaufwand für herkömmliche Lösungen wie VLANs und Firewalls. Die befragten Unternehmen berichteten von einer Betriebskostensenkung von 25 bis zu 80 Prozent. Ohne TrustSec würde die Modellorganisation vier zusätzliche Netzwerktechniker einstellen müssen. So konnte das Unternehmen 945.402 US-Dollar einsparen.
- **Verbesserte Netzwerkstabilität mit geringerem Risiko von Ausfallzeiten** TrustSec verbessert auch die Netzwerkstabilität eines Unternehmens und führt somit zu einem geringeren Risiko von Ausfallzeiten. Um eine Stunde jährlich verringerte Ausfallzeiten bewirken bei 4.000 Benutzern eine Einsparung von 319.716 US-Dollar für die Modellorganisation.
- Weitere von den befragten Unternehmen angegebene Vorteile sind:
 - **Schnellere Markteinführungszeit bei Projektbereitstellung**
 - **Vereinfachte und automatisierte Verwaltung von Firewallregeln sowie damit verknüpfte Betriebseinsparungen**
 - **Verbesserte Erfüllung gesetzlicher Auflagen**
 - **Konsistente und effiziente Netzwerksegmentierung**
 - **Vereinfachte Sicherheitstechnik durch Vereinfachung der Sicherheitsrichtlinien**
 - **Mehr Flexibilität sowie die Möglichkeit der Skalierung von Sicherheitsrichtlinien**
 - **Verbesserter Sicherheitsstatus für das Netzwerk**

› **Kosten** Sowohl die klassische Implementierung als auch die softwaredefinierte Segmentierung von TrustSec ist mit Kosten verbunden: Klassische Segmentierungskosten sind in Tabelle 1 dargestellt. Der Modellorganisation sind die folgenden risikobereinigten Barwertkosten für die softwaredefinierte Segmentierung von TrustSec entstanden:

- **TrustSec – Infrastrukturkosten** Die Modellorganisation hat 346.500 US-Dollar in die TrustSec-Infrastruktur investiert. Darin sind die Kosten für die Appliance Cisco Identity Services Engine (ISE) und zugehörige Lizenzen enthalten. Nicht enthalten sind Netzwerkupgrades, da die Modellorganisation die Implementierung von TrustSec mit dem geplanten Austausch der Netzwerkinfrastruktur zum Ende von deren Lebenszyklus abgestimmt hat.
- **Cisco Advanced Services – Kosten** Die Modellorganisation verwendete Cisco Advanced Services für Low-Level- und High-Level-Design im Wert von 231.000 US-Dollar. Nicht alle befragten Kunden verwendeten Cisco Advanced Services bei der Planung der TrustSec-Implementierung.
- **Kosten für Professional Services** Für die Modellorganisation fielen für die Implementierung von TrustSec zudem Kosten in Höhe von 404.250 US-Dollar für Professional Services an. Nicht alle befragten Kunden nutzen Professional Services bei der Implementierung von TrustSec.

-
- **Innerbetrieblicher Arbeitsaufwand für Implementierung und Testen** Die Modellorganisation gab 130.680 US-Dollar für die sechsmonatige Implementierung von TrustSec aus.
 - **Laufende Verwaltungs- und Supportkosten** Die Modellorganisation beschäftigte zwei Techniker für die laufende Verwaltung und das Testen der regelmäßigen Software-Updates für das Netzwerk. Über den Analysezeitraum von drei Jahren sind dafür Kosten in Höhe von 551.484 US-Dollar entstanden.

Haftungsausschluss

Hinweise für den Leser:

- › Die Studie wurde im Auftrag von Cisco durch Forrester Consulting erstellt. Sie stellt keine Wettbewerbsanalyse dar.
- › Forrester macht keine Annahmen bezüglich des potenziellen ROI, den andere Unternehmen erzielen. Forrester empfiehlt dem Leser nachdrücklich, eigene Schätzungen innerhalb des Rahmens dieses Berichts zu verwenden, um die Angemessenheit einer Investition in Cisco TrustSec zu bewerten.
- › Cisco hat das Dokument geprüft und mit Forrester besprochen. Forrester behält sich jedoch die redaktionelle Kontrolle über die Studie und ihre Ergebnisse vor und genehmigt keine Änderungen an der Studie, die den Erkenntnissen von Forrester widersprechen oder das Ergebnis der Studie verfälschen würden.
- › Cisco stellte die Namen der Kunden für die Befragungen zur Verfügung, nahm jedoch nicht selbst an den Befragungen teil.

Klicken Sie [hier](#), um den vollständigen Bericht aufzurufen.