Eine Forrester Total Economic Impact™
Studie im Auftrag von Varonis
Mai 2018

Der Total Economic Impact™ der Varonis-Datensicherheits-plattform

Kosteneinsparungen und Geschäftsvorteile durch die Varonis-Datensicherheitsplattform

FORRESTER®

Inhaltsverzeichnis

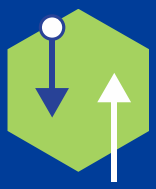
Projektleiter:
Joe Branca

FORRESTER®

ROI
346 %

PV-Vorteile
5,0 Mio. €

NPV
3,9 Mio. €



Amortisierung
< 6 Monate

Zusammenfassung

Sicherheitsverstöße können zu erheblichen finanziellen Verlusten führen, insbesondere wenn Unternehmen keine Maßnahmen zum Schutz wertvoller Daten ergriffen haben. In vielen Unternehmen werden Dateien und Ordner unnötig mit Hunderten oder sogar Tausenden von Mitarbeitern gemeinsam genutzt, und Benutzer haben Zugriff auf weitaus mehr Daten, als sie es zur Ausführung ihrer Aufgaben benötigen. Hierdurch bleiben sensible Daten vor externen Angreifern und böswilligen Insidern ungeschützt, da die Anmeldedaten für ein einzelnes Konto Zugriff auf eine Vielzahl von ungesicherten Informationen bieten, angefangen bei Geschäftsplänen bis hin zu Mitarbeiter- und Kundendaten.

Selbst wenn Unternehmen feststellen können, wo sensible Daten gespeichert werden, kann sich die Aufgabe, sie zu sichern, als sehr kompliziert erweisen. Die Korrektur des Zugriffs auf einen einzelnen Ordner kann Stunden dauern und die Teilnahme von Rechtsabteilung, Unternehmensleitung und Sicherheit erforderlich machen. Dieser Prozess kann kostspielig sein und ohne die Möglichkeit zu bestimmen, wer auf Daten zugreifen muss, besteht immer ein Risiko, geschäftliche Abläufe erheblich zu beeinträchtigen.

Varonis bietet eine Datensicherheitsplattform, die seinen Kunden dabei hilft zu verstehen, wo ihre sensiblen Daten vorliegen, wer darauf Zugriff hat, und vor allem, wer diesen Zugriff benötigt. Auf diese Weise können IT-Organisationen einen Status der geringstmöglichen Berechtigungen anstreben, wodurch das mit einem Datensicherheitsvorfall verbundene Risiko drastisch reduziert und der Status langfristig beibehalten wird. Durch die integrierte Maschinenlernfunktion und die Benutzerverhaltensanalyse werden sensible Daten geschützt, da Unternehmen schnell Verstöße, Fehlkonfigurationen und andere Probleme erkennen können.

Varonis hat Forrester Consulting beauftragt, eine TEI-Studie (Total Economic Impact™) durchzuführen und den potenziellen Return on Investment (ROI) zu untersuchen, den Unternehmen durch die Bereitstellung der Varonis-Datensicherheitsplattform realisieren können. Der Zweck dieser Studie ist es, Lesern einen Bezugsrahmen zur Evaluierung der potenziellen finanziellen Auswirkungen der Datensicherheitsplattform in ihrem Unternehmen zu liefern. Um die mit diesem Investment verbundenen Vorteile, Kosten und Risiken besser zu verstehen, hat Forrester ein Unternehmen aus der Gesundheitsbranche mit jahrelanger Erfahrung in der Nutzung von Varonis-Produkten befragt.

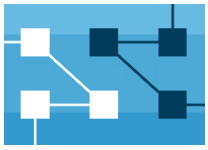
Vor dem Bereitstellen von Schlüsselkomponenten der Varonis-Datensicherheitsplattform hatte der Kunde keinen klaren Einblick in das, was auf seinen Dateiservern geschah. Das Unternehmen wusste, dass es für Ransomware und andere Sicherheitsrisiken anfällig war, aber nicht die Tools zur Verfügung standen, um die genaue Art der Bedrohung zu verstehen und erste Schritte zu ergreifen. Es nutzte Varonis-Software und wurde außerdem durch das Varonis Professional Services Team unterstützt, um den Zugriff auf mehr als 1,5 Millionen Hochrisiko-Ordner zu korrigieren. Auf diese Weise konnte das Risikoprofil der Organisation drastisch reduziert werden.

Die wichtigsten Ergebnisse

- **Quantifizierter Nutzen.** Das befragte Unternehmen konnte die folgenden risikobereinigten Barwerte (Present Value, PV) verzeichnen:
- **Zeitersparnisse bei Audit-Untersuchung in Höhe von umgerechnet 37.824 €.** Die Varonis-Plattform ermöglicht die Durchführung von Audits und Untersuchungen des Benutzerverhaltens mit 90 % weniger Aufwand, wodurch 420 Stunden an Zeit für Sicherheitsanalysten eingespart werden.

FORRESTER®

Nutzen und Kosten



Zeiteinsparungen beim Korrektur- und Berechtigungsmanagement sowie Kostenvermeidung:

3.360.401 €

Geringeres Risikopotenzial:

1.604.109 €

Kosten für Softwarekauf und -wartung:

761.053 €

- **Zeitersparnisse für die Bereitstellung von Dateizugriff in Höhe von umgerechnet 31.145 €.** Nach der Bereitstellung von Varonis hat die Bereitstellung von Dateizugriff – eine alltägliche Aufgabe für Sicherheitsexperten – 75 % weniger Zeit in Anspruch genommen, was zu jährlichen Zeiteinsparungen von mehr als 300 Stunden führte.
- **Zeiteinsparungen beim Korrektur- und Berechtigungsmanagement sowie Kostenvermeidung in Höhe von 3.360.401 €.** Das Kundenunternehmen hat die Berechtigungen für mehr als 1,5 Millionen Hochrisikoordner zurückgesetzt. Diese Analyse geht jedoch davon aus, dass das Unternehmen ohne spezielle Software lediglich versucht hätte, den Zugang zu nur 1 % dieser Ordner zu korrigieren, um hochsensible Daten zu schützen. Für jeden Ordner wurden durch die Verwendung von Varonis, anstatt zu versuchen, diesen Prozess manuell abzuschließen, 4,5 Stunden für Sicherheitsexperten eingespart (3 Stunden für einen Sicherheitsanalysten und 1,5 Stunden für einen Mitarbeiter auf Führungsebene).
- **Die Vorteile der Risikominimierung belaufen sich insgesamt auf umgerechnet 1.604.109 €.** Die Varonis-Lösung half dem Kundenunternehmen, sein Risikoprofil um 65 % zu reduzieren. Bei einem großen Sicherheitsvorfall entstehen Gesundheitsorganisationen im Schnitt Kosten von 9.177.9560 €. In jedem Jahr besteht eine Chance von 14 %, dass es zu einem solchen Vorfall kommt. Hierdurch entstand für das Unternehmen ein Gesamtrisiko von mehr als 1,3 Millionen €. Durch die Korrektur des globalen, gemeinsam genutzten Zugriffs auf Daten und die Bereitstellung verbesserter Erkennungs- und Reaktionsmöglichkeiten konnte dieses Risikopotenzial mit Varonis reduziert werden.

Kosten. Bei dem befragten Unternehmen wurden die folgenden risikobereinigten Barkosten verzeichnet:

- **Kosten für Softwarekauf und -wartung in Höhe von 761.053 €.** Der Kunde bezahlt Varonis eine einmalige Gebühr für die Lizenzierung seiner Softwareprodukte. Darüber hinaus zahlt der Kunde eine jährliche Wartungsgebühr in Höhe von 20 % des ursprünglichen Kaufpreises.
- **An Varonis gezahlte Gebühren für Implementierung, Operationalisierung und Korrektur in Höhe von insgesamt 362.559 €.** Dem Kunden entstanden Kosten für Professional Services von Varonis, um die Implementierung und die Operationalisierung der Varonis-Datensicherheitsplattform sowie die erste Korrektur des Zugriffs auf Daten, die auf den Dateisystemen des Kunden gespeichert sind, abzuschließen.
- **Kosten für den internen Aufwand für Planung und Bereitstellung von insgesamt 4.845 €.** Dem Kunden entstanden außerdem Kosten für die internen Ressourcen, die für die Planung und Implementierung der Varonis-Datensicherheitsplattform vorgesehen waren, die im Laufe eines Monats vonstatten ging.

Das befragte Unternehmen kaufte von Anfang an eine umfassendere Produktsuite von Varonis als viele andere. Dies hat die Vorteile während des dreijährigen Analysezeitraums erhöht, jedoch auch zu höheren Kosten geführt. Die meisten Kunden erwerben zunächst die Kernkomponenten der Plattform. Ein typisches Starterpaket für eine Organisation, die 1.000 Benutzer überwacht, beläuft sich auf ca. 131.000 €. Im Laufe der Zeit werden dann weitere Produkte und Komponenten hinzugefügt.

Die Befragung des Bestandskunden durch Forrester und die daran anschließende Finanzanalyse ergaben, dass das Unternehmen über drei Jahre Nutzen im Wert von 5.033.479 € gegenüber Kosten von 1.1128.457 € erreicht, was einen Nettobarwert (Net Present Value, NPV) von 3.905.022 € und einen ROI von 346 % ergibt.

Die TEI-Methodik unterstützt Unternehmen darin, den materiellen Wert von IT-Initiativen gegenüber der Geschäftsführung und anderen wichtigen Entscheidungsträgern aufzuzeigen, zu begründen und zu veranschaulichen.

TEI-Bezugsrahmen und -Methodik

Anhand der Daten aus der Befragung hat Forrester einen Total Economic Impact™ TEI-Bezugsrahmen (Total Economic Impact™) für Unternehmen erstellt, die eine Implementierung der Varonis-Datensicherheitsplattform erwägen.

Dieser Bezugsrahmen hat den Zweck, die Kosten, den wirtschaftlichen Nutzen, die Flexibilität und die Risikofaktoren zu ermitteln, die Einfluss auf die Investitionsentscheidung haben. Forrester ging zur Bewertung der Auswirkungen, die sich durch die Varonis-Datensicherheitsplattform für ein Unternehmen ergeben können, in mehreren Schritten vor:

DUE DILIGENCE
Es wurden Varonis-Stakeholder und Forrester-Analysten befragt, um Daten bezüglich der Varonis-Datensicherheitsplattform zu sammeln.

KUNDENBEFRAGUNG
Um Daten in Bezug auf Kosten, Nutzen und Risiken zu erhalten, wurde ein Unternehmen befragt, das die Varonis-Datensicherheitsplattform verwendet.

FINANZMODELL-BEZUGSRAHMEN
Mit der TEI-Methodik wurde ein für die Befragung repräsentatives Finanzmodell erstellt und auf Grundlage der Themen und Belange der befragten Unternehmen risikobereinigt.

FALLSTUDIE
Bei der TEI-Modellierung zur Auswirkung der Varonis-Datensicherheitsplattform wurden vier fundamentale Elemente berücksichtigt: Nutzen, Kosten, Flexibilität und Risiken. In Anbetracht der zunehmenden Erfahrung von Unternehmen mit ROI-Analysen für IT-Investitionen soll die TEI-Methodik von Forrester ein vollständiges Bild der gesamten wirtschaftlichen Auswirkungen von Kaufentscheidungen zeichnen. Weitere Informationen zur TEI-Methodik finden Sie in Anhang A.

Die „Customer Journey“ bei Datensicherheitsplattformen

VOR UND NACH DER INVESTITION IN DIE DATENSICHERHEITSPLATTFORM

Befragtes Unternehmen

Für diese Studie befragte Forrester den Leiter der Cybersicherheit und einen Sicherheitsanalysten im Dienste eines milliardenschweren Krankenversicherungsanbieters. Das Unternehmen bietet Krankenversicherungen für Einzelpersonen und Arbeitgebern in allen 50 US-Bundesstaaten an und beschäftigt rund 3.000 Mitarbeiter.

Die folgenden übergeordneten Metriken beschreiben die Dateiserver und die Active Directory-Struktur des Unternehmens:

- 76 TB Daten
- 8,2 Millionen Ordner
- 170 Millionen Dateien
- 8.500 Benutzerkonten
- 11.300 Gruppen

Wegen der Branche, in der das Unternehmen tätig ist, verwaltet es seine Daten gemäß HIPAA-Vorschriften (Health Insurance Portability and Accountability Act).

Das Unternehmen verwendet die folgenden Varonis-Produkte:

- **DatAdvantage*.** Bietet IT-Organisationen einen effizienten Ansatz für Berechtigungsverwaltung, Benutzer-Audits und Bereitstellung von Dateizugriff.
- **DatAlert.** Nutzt maschinelles Lernen und Verhaltensanalysen, um vor verdächtigen Aktivitäten auf den Dateiservern zu warnen.
- **DataPrivilege.** Bietet Geschäftsbenutzern die Möglichkeit, Zugriffskontrollen ohne Unterstützung durch IT zu prüfen und zu verwalten.
- **Data Classification Engine:** Überprüft Ihren Bestand auf sensible Daten und wendet zur Verbesserung von Sicherheit und Compliance Klassifizierungsregeln an.

Das Unternehmen entschied sich nach einer gründlichen Prüfung der auf dem Markt verfügbaren Optionen für Varonis. „Es war eine klare Entscheidung für uns“, so der Leiter der Cybersicherheit.

**Enthält die Komponenten für Windows, SharePoint, Exchange, Active Directory und UNIX.*

Risikoabschätzung und Gegenmaßnahmen – Zusammenfassung

Vor Beginn des Projekts führte Varonis eine Überprüfung der Datenspeicher und Repositorys des Kunden in Übereinstimmung mit den Branchenstandards und den Best Practices von Varonis aus, um Risiken in den Bereichen Zugriffskontrolle, Active Directory-Struktur, NTFS, Freigabeberechtigungsstruktur und Datenaufbewahrung aus.

„Wenn Sie mit Unternehmen vertraut sind, die über Jahrzehnte hinweg Dateiserver und -berechtigungen weitergeführt haben, dann wissen Sie, was für ein Chaos dabei am Ende entsteht. Wir benötigten einen klaren Einblick darein, was auf diesen Dateiservern los war und wer Zugriff hatte. Nun können wir zweifelsfrei sagen, dass dies die Person ist, die hier Zugriff hatte und etwas geändert hat. Wir haben das vor Varonis nicht gekonnt, und deshalb sind diese Tools von großer Bedeutung für uns.“

Leiter der Cybersicherheit

FORRESTER®

Bei dieser Prüfung wurden mehrere Hochrisikobereiche identifiziert, die nach Empfehlungen von Varonis umgehend behoben werden mussten:

- 1,5 Millionen Ordner in der gesamten Umgebung mit globalen Berechtigungen.
- 160.000 Dateien mit vertraulichen Daten; 27 % dieser Dateien waren in den vergangenen sechs Monaten nicht genutzt worden.
- 14.000 Dateien mit globalen Berechtigungen, die vertrauliche Daten enthalten.
- 3.700 Benutzer mit Empfehlungen zur Entfernung.
- 3.000 irrelevante Benutzer mit aktivierten Berechtigungen (z. B. Mitarbeiter und Auftragnehmer, die das Unternehmen verlassen haben).

Die Überprüfung ergab auch eine Reihe von Bereichen mit mittlerem und geringem Risiko:

- 4,1 Millionen Ordner mit fast 17 TB an veralteten Daten.
- 1.750 Benutzer mit nicht ablaufenden Passwörtern.
- 960.000 Ordner, auf die direkt oder indirekt spezielle Berechtigungen angewendet und weitergegeben wurden.
- 60.000 Ordner mit individuell (anstatt auf Gruppenebene) zugeordneten Benutzersteuerungseinträgen (ACEs).

Der Kunde beauftragte das Varonis Professional Services-Team, um das Unternehmen bei der Korrektur der Berechtigungen für sein Dateisystem zu unterstützen. Das anfängliche Projekt, das sechs Monate in Anspruch nahm, sah Korrekturmaßnahmen für die folgenden Datenbestände vor:

- 850.000 Ordner mit globalen Berechtigungen.
- 12.000 Ordner mit globalen Berechtigungen, die sensible Daten enthielten.
- 45.000 Dateien mit globalen Berechtigungen, die sensible Daten enthielten.
- Der Abschluss des Korrekturvorgangs und das Erreichen eines Zustands mit so wenig Berechtigungen wie möglich dauerte weitere 90 Tage.

> „Aus Sicht der Aufbewahrung bestehen immer Bedenken, dass jemand diese Dateien noch gebrauchen könnte. Ist es also angemessen, sie zu entfernen, oder sollen wir sie lieber für immer aufbewahren? Mit Varonis können wir dem Rest des Unternehmens Feedback geben, dass Dateien in sechs Monaten oder einem Jahr nicht genutzt wurden. Sie sind nicht mehr erforderlich, also können wir sie archivieren oder ganz löschen.“
>
> *Leiter der Cybersicherheit*

Zentrale Herausforderungen

Während der Interviews hoben die Führungskräfte des Kunden die folgenden wichtigen Herausforderungen hervor, die zur Investition in die Varonis-Datensicherheitsplattform geführt hatten:

- **Überblick über den Zugriff.** Das Unternehmen hatte keinen Überblick darüber, wer Zugriff auf Daten hatte, die auf seinen Dateiservern gespeichert waren, und wer sie für Arbeitszwecke benötigt. Die Zugriffsrechte waren über mehrere Jahrzehnte hinweg weitergeführt worden. Sie wurden häufig uneinheitlich angewendet, und viele waren veraltet, sodass Benutzer auf wesentlich mehr Daten zugreifen konnten, als sie zur Erledigung ihrer Arbeit benötigten. Ohne spezielle Software waren die Zugriffskontrollen in einem derartigen Umfang jedoch nur schwer zu analysieren.
- **Verständnis und Begrenzung des Risikos.** Das Unternehmen sah die Auswirkungen von Datenschutzverletzungen in den Nachrichten und suchte nach Möglichkeiten zur Begrenzung der Risiken. Ihm fehlten jedoch die technischen Möglichkeiten, sensible Daten in den Dateisystemen ausfindig zu machen. Selbst wenn es die sensiblen Daten hätte lokalisieren können, war es trotzdem nicht in der Lage, die Berechtigungen auf effiziente Weise zurückzusetzen und Beschwerden von Geschäftsbenutzern zu vermeiden.

- **Erkennung und Umgang mit Sicherheitsvorfällen.** Vor dem Einsatz der Varonis-Plattform verfügte das Kundenunternehmen zwar über Sicherheitstools, laut Aussagen der Befragten waren diese jedoch äußerst ungeeignet. Die Sicherheitsanalysten verließen sich weitgehend auf Endbenutzer, die sie auf Probleme aufmerksam machten. In manchen Fällen war dies nicht der Fall, sodass Malware für mehrere Stunden unentdeckt blieb. Da die Berechtigungen für Dateien und Ordner zu weitreichend waren, war ein deutlich größerer Anteil der Unternehmensdaten davon betroffen. Im Nachhinein war es für die Sicherheitsteams nur schwer nachvollziehbar, welche Daten betroffen waren, und sie hatten Schwierigkeiten, der Geschäftsführung angemessene Gegenmaßnahmen zu unterbreiten.

Die wichtigsten Ergebnisse

Während der Interviews hoben die Führungskräfte des Kunden die folgenden Resultate hervor, die sich aus der Investition in die Varonis-Datensicherheitsplattform ergeben haben:

- **Eine drastische Senkung des Risikos im Zusammenhang mit einem Datensicherheitsvorfall.** Durch die Begrenzung des Zugriffs auf die Mitarbeiter, die diesen für ihre Arbeit benötigten, ist es dem Unternehmen gelungen, sein Risikoprofil zu reduzieren. Mit Varonis-Produkten und der Unterstützung durch das Varonis Professional Services Team hat das Unternehmen den Zugriff auf mehr als 1,5 Millionen Ordner mit offenem Zugriff korrigiert, darunter viele vertrauliche Daten.
- **Verbesserte Workflows.** Varonis ermöglicht Sicherheitsanalysten, alltägliche Aufgaben mit höherer Effizienz durchzuführen, wodurch ihnen mehr Zeit für wichtigere Aktivitäten bleibt. Die Bereitstellung des Zugriffs auf Dateien und Ordner, die bei jedem neuen Mitarbeiter neu ausgeführt werden muss, ist mit Lösungen von Varonis weitaus einfacher. Gleiches gilt für den Fall, dass ein Mitarbeiter Daten auf eine Art und Weise nutzt, auf die er sie nicht nutzen sollte. Den Zugriff des Mitarbeiters auf Dateien und Ordner zu überprüfen, ist jetzt weitaus weniger aufwändig.
- **Effektivere Aufbewahrung und Archivierung.** Das Unternehmen kann jetzt veraltete Daten effektiver identifizieren und auf Grundlage der geschäftlichen Anforderungen aufbewahren oder archivieren. Bei der anfänglichen Risikobewertung wurden mehr als 16 TB veralteter Daten identifiziert. Dies entspricht 22 % aller Daten in der von Varonis überwachten Umgebung. Diese Daten sind mit einer erheblichen Verantwortung verbunden, da Benutzer, die diese nicht nutzen müssen, dennoch darauf zugreifen können. Sie unterliegen darüber hinaus branchenspezifischen Regeln und Vorschriften, und Varonis ermöglicht es Sicherheitsanalysten, die Teams der Rechtsabteilung bei der Einhaltung der Compliance zu unterstützen.

„Wenn wir eine Warnung erhalten, sich bestimmte Verhaltensweisen einer bestimmten Malware abzeichnen und wir wissen, dass diejenige Person die volle Kontrolle über ein bestimmtes Verzeichnis oder eine Gruppe von Verzeichnissen hat, können wir sofort Maßnahmen ergreifen, um die Gefahr einzudämmen. Früher hatten wir nichts von alledem. Jemand musste erst einmal etwas melden, und bis dahin war die Hälfte unserer Dateien bereits verschlüsselt.“

Leiter der Cybersicherheit

„Mit Varonis geben Sie einen Benutzernamen ein und das Dateiverzeichnis wird angezeigt. Sie wissen, dass er oder sie über eine bestimmte Zugriffsebene verfügt. Sie springen dorthin, wo Änderungen erforderlich sind, nehmen die Änderungen vor und übernehmen sie dann alle gleichzeitig.“

Sicherheitsanalyst

Analyse der Nutzen

QUANTIFIZIERTE NUTZDATEN

Gesamtnutzen

REF.	NUTZEN	ANFÄNGLICH	JAHR 1	JAHR 2	JAHR 3	GESAMT	BARWERT
Atr	Zeiteinsparungen bei Audits	0 €	15.210 €	15.210 €	15.210 €	45.629 €	37.824 €
Btr	Zeiteinsparungen bei der Bereitstellung von Dateizugriff	0 €	12.524 €	12.524 €	12.524 €	37.572 €	31.145 €
Ctr	Zeiteinsparungen beim Korrektur- und Berechtigungsmanagement sowie Kostenvermeidung	1.749.685 €	1.496.572 €	158.577 €	158.577 €	3.563.411 €	3.360.401 €
Dtr	Geringeres Risikopotenzial	0 €	532.436 €	709.915 €	709.915 €	1.952.266 €	1.604.109 €
	Gesamtnutzen (risikobereinigt)	1.749.685 €	2.056.741 €	896.226 €	896.226 €	5.598.877 €	5.033.479 €

Zeiteinsparungen bei Audits

Die Varonis-Lösung ermöglicht es den Sicherheitsanalysten des Kunden, schneller zu untersuchen und prüfen, wie Benutzer auf Dateien und Ordner zugreifen.

Vor der Bereitstellung von DatAdvantage konnte es bis zu zwei Tage dauern, bis ein Audit oder eine Untersuchung abgeschlossen wurde, falls dies überhaupt möglich war. Die Protokolldateien erlaubten es den Sicherheitsanalysten nur, den Ordnerzugriff innerhalb der vergangenen 36 Stunden zu verfolgen. Wenn das fragliche Verhalten also weiter zurücklag, konnten keine Datensätze dazu abgerufen werden.
Mit Varonis können Analysten laut Aussagen der Befragten Berichte über den Benutzerzugriff innerhalb von Minuten erstellen.

Das Finanzmodell stellt die folgenden Ergebnisse dar:

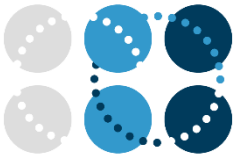
- Vor der Bereitstellung der Varonis-Plattform benötigten Sicherheitsanalysten 12 Stunden, um einen Audit der Dateizugriffshistorie eines Benutzers abzuschließen.
- Jedes Jahr werden Sicherheitsanalysten auf 35 Vorfälle hingewiesen, die weitere Untersuchungen erfordern.
- Mit Varonis können Sicherheitsanalysten eine Untersuchung zur Dateizugriffshistorie eines Benutzers mit 90 % weniger Aufwand durchführen.

Die folgenden Faktoren könnten diesen Vorteil beeinträchtigen:

- Der Prozess, mit dem Unternehmen diese Aufgabe erledigt haben, bevor sie auf Varonis umstellen.
- Die Häufigkeit, mit der Unternehmen diese Aufgabe ausführen müssen.

Um diese Risiken zu berücksichtigen, hat Forrester eine Risikobereinigung von 5 % angesetzt, sodass sich über drei

In der Tabelle oben werden die Gesamtsumme aus den berechneten Nutzwerten in allen unten beschriebenen Bereichen sowie der Barwert (Present Value, PV) mit einem Diskontierungssatz von 10 % aufgeführt. Über einen Zeitraum von drei Jahren ist für das befragte Unternehmen ein risikobereinigte Gesamtnutzen mit einem Barwert (Present Value, PV) in Höhe von mehr als 5,0 Mio. € zu erwarten.



Vor der Bereitstellung der Varonis-Lösung benötigten Sicherheitsanalysten 12 Stunden, um einen Audit der Dateizugriffshistorie eines Benutzers abzuschließen.

FORRESTER®

Jahre ein risikobereinigter Gesamt-PV von 37.824 Mio. € ergibt.

Zeitersparnisse bei Audit-Untersuchung: Berechnungstabelle						
REF.	**KENNZAHL**	**BER.**	**ANFÄNGLICH**	**JAHR 1**	**JAHR 2**	**JAHR 3**
A1	Aufwand für Einzel-Audit ohne Varonis	Stunden		12	12	12
A2	Vorfälle, die geprüft und untersucht werden müssen (jährlich)			35	35	35
A3	Prozentuale Reduzierung des Aufwands für die Erstellung von Audit-Berichten			90 %	90 %	90 %
A4	Durchschnittlicher Stundensatz für Sicherheitsanalyst, inklusive aller Kosten			42 €	42 €	42 €
At	Zeiteinsparungen bei Audits	A1*A2*A3*A4	0 €	16.010 €	16.010 €	16.010 €
	Risikobereinigung	↓5 %				
Atr	Zeiteinsparungen bei Audits (risikobereinigt)		0 €	15.210 €	15.210 €	15.210 €

Zeiteinsparungen bei der Bereitstellung von Dateizugriff

Dank der Varonis-Plattform können Sicherheitsanalysten den Zugriff auf Dateien und Ordner schneller bereitstellen.

Einem Sicherheitsanalysten zufolge, der mindestens 8 Stunden pro Woche mit dieser Aufgabe beschäftigt war, war die Bereitstellung von Zugriff auf Dateien und Ordner früher ein manueller und fehleranfälliger Prozess. Er erklärte, wie Varonis diesen Vorgang vereinfacht hat: „Mit Varonis geben Sie einen Benutzernamen ein und das Dateiverzeichnis wird angezeigt. Sie wissen, dass er oder sie über eine bestimmte Zugriffsebene verfügt. Sie springen dorthin, wo Änderungen erforderlich sind, nehmen die Änderungen vor und übernehmen sie dann alle gleichzeitig."

(Zum Zeitpunkt des Gesprächs hatte die Kundenorganisation noch nicht begonnen, die Anforderungs- und Genehmigungsfunktion von DataPrivilege zu nutzen, mit der Geschäftsanwender den Zugriff auf Dateien und Ordner anfordern und genehmigen können. Sie nutzte DatAdvantage, um schnell Einblick in die Zugriffsebene eines Benutzers zu erhalten und Änderungen effizient vorzunehmen.)

Das Finanzmodell stellt die folgenden Ergebnisse dar:

- Vor der Implementierung von Varonis haben Sicherheitsanalysten pro Jahr 415 Stunden mit der Bereitstellung von Zugriff auf Dateien und Ordner zugebracht.
- Mit der Varonis-Software können Sicherheitsanalysten den Zugriff auf Dateien und Ordner mit 75 % weniger Aufwand bereitstellen.

Die folgenden Faktoren könnten diesen Vorteil beeinträchtigen:

- Der Prozess, mit dem Unternehmen diese Aufgabe erledigt haben, bevor sie auf Varonis umstellen.
- Die Häufigkeit, mit der Unternehmen diese Aufgabe ausführen müssen.

Um diese Risiken zu berücksichtigen, hat Forrester eine Risikobereinigung von 5 % angesetzt, sodass sich über drei Jahre ein risikobereinigter Gesamt-PV von 31.145 € ergibt.

Vor der Implementierung von Varonis haben Sicherheitsanalysten pro Jahr 415 Stunden mit der Bereitstellung von Dateien und Ordnern zugebracht.

FORRESTER®

Zeiteinsparungen bei der Bereitstellung von Dateizugriff: Berechnungstabelle						
REF.	**KENNZAHL**	**BER.**	**ANFÄNGLICH**	**JAHR 1**	**JAHR 2**	**JAHR 3**
B1	Aufwand für die Bereitstellung von Dateizugriff vor Varonis (jährlich)	Stunden		415	415	415
B2	Prozentuale Reduzierung des Aufwands für die Bereitstellung von Dateizugriff			75 %	75 %	75 %
B3	Durchschnittlicher Stundensatz für Sicherheitsanalyst, inklusive aller Kosten			42 €	42 €	42 €
Bt	Zeiteinsparungen bei der Bereitstellung von Dateizugriff	B1*B2*B3	0 €	13.183 €	13.183 €	13.183 €
	Risikobereinigung	↓5 %				
Btr	Zeiteinsparungen bei der Bereitstellung von Dateizugriff (risikobereinigt)		0 €	12.524 €	12.524 €	12.524 €

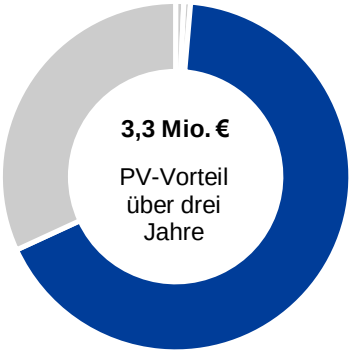
Zeiteinsparungen beim Korrektur- und Berechtigungsmanagement sowie Kostenvermeidung

Die Varonis-Plattform ermöglichte es dem Kunden, unnötig freigegebene Dateien und Ordner zu identifizieren und den Zugriff auf diese zu korrigieren, ohne die geschäftlichen Abläufe zu beeinträchtigen.

Nachdem seit Jahren die Zugriffsrechte einfach weitergeführt worden waren, gab es Unmengen von Dateien und Ordnern, auf die Benutzer unnötigerweise zugreifen konnten. Doch für die IT-Abteilung gab es keine einfache Möglichkeit herauszufinden, wer Zugriff auf Dateien und Ordner hatte und wer diesen tatsächlich benötigte, um seine Aufgaben zu erledigen. Sofern überhaupt möglich, würde es extrem aufwändig werden, den Zugriff auf diese Dateien ohne eine spezielle Softwarelösung zu korrigieren.

Das Finanzmodell stellt die folgenden Ergebnisse dar:

- Die Kundenorganisation nutzte die Varonis-Lösung, um zu verstehen, wer in der Organisation Zugriff auf Dateien und Ordner hatte und wer den Zugriff zur Erledigung seiner Aufgaben benötigte.
- Die Risikobeurteilung von Varonis identifizierte 1,5 Millionen Ordner mit umfassenden Zugriffsrechten, die als hohes Risiko eingestuft wurden.
- Der Kunde korrigierte zusammen mit dem Professional Services Team von Varonis zunächst den Zugriff auf 850.000 Ordner; im 1. Jahr wurde dann der Zugriff auf weitere 650.000 Ordner eingeschränkt.
- Ohne eine Lösung wie die von Varonis wäre die Kundenorganisation diese Aufgabe gar nicht erst angegangen. Deshalb wäre es unsinnig, den Nutzen auf Grundlage der Gesamtzahl von Ordnern zu berechnen, für die der Zugriff korrigiert wurde.
- Die Kundenorganisation hätte versucht, den Zugriff auf Ordner mit hochvertraulichen Daten zu identifizieren und zu korrigieren. Die Anzahl der Ordner, die mit einem manuellen Prozess identifiziert hätte werden können, entspricht 1 % der 1,5 Millionen Hochrisiko-Ordner, die von Varonis identifiziert wurden. Dieser Nutzen wird nur auf Grundlage dieser 1 % der Ordner berechnet.
- Ohne eine spezialisierte Lösung wie die von Varonis würde es im Durchschnitt mindestens 4,5 Stunden dauern, um den Zugriff auf einen einzelnen Ordner zu korrigieren. Hierzu gehören 3 Stunden für einen



Zeiteinsparungen beim Korrektur- und Berechtigungs-management sowie Kostenvermeidung: **67 %** des Gesamtnutzen

FORRESTER®

Sicherheitsanalysten sowie 1,5 Stunden für einen Mitarbeiter auf Führungsebene.

- Die durchschnittlichen Kosten pro Stunde für diese Mitarbeiter gehen von einem Stundenlohn von 42 € für den Sicherheitsanalysten und 74,12 € für einen Mitarbeiter auf Führungsebene (jeweils inklusive aller Kosten) aus. Diese Schätzungen entsprechen den von der Kundenorganisation bereitgestellten Stundensätzen und stimmen mit den Bedingungen am regionalen Arbeitsmarkt überein.
- Nach der ersten Korrektur ermöglichte die Varonis-Software es dem Kundenunternehmen, den Status der geringstmöglichen Rechte mit zwei Vollzeitäquivalenten (FTEs) weniger aufrecht zu erhalten, als dafür normalerweise erforderlich gewesen wären.

Die folgenden Faktoren könnten diesen Vorteil beeinträchtigen:

- Der Zustand der Dateisysteme des Unternehmens vor der Bereitstellung von Varonis.
- Die Kosten für die Einstellung und den Einsatz von Sicherheitsexperten auf dem regionalen Arbeitsmarkt des Unternehmens.

Um diese Risiken zu berücksichtigen, hat Forrester eine Risikobereinigung von 10 % angesetzt, sodass sich über drei Jahre ein risikobereinigter Gesamt-PV von 3.360.401 € ergibt.

Zeiteinsparungen beim Korrektur- und Berechtigungsmanagement sowie Kostenvermeidung: Berechnungstabelle

REF.	KENNZAHL	BER.	ANFÄNGLICH	JAHR 1	JAHR 2	JAHR 3
C1	Entfernte Ordner mit globalem Zugriff		850.000	650.000		
C2	Prozentsatz der Ordner mit vertraulichen Daten		1,0 %	1,0 %		
C3	Aufwand für die Identifizierung und Korrektur von globalem Ordnerzugriff vor Varonis	Stunden	4,5	4,5		
C4	Durchschnittliche Lohnkosten pro Stunde		51 €	51 €		
C5	Dank Varonis-Datensicherheitsplattform vermiedene Korrekturkosten insgesamt	C1*C2*C3*C4	1.944.095 €	1.486.661 €		
C6	FTEs, die bei der laufenden Verwaltung von Berechtigungen eingespart werden	Kundenbefragung		2	2	2
C7	Jahresgehalt Sicherheitsanalyst (inkl. aller Kosten)	Kundenbefragung		88.098 €	88.098 €	88.098 €
C8	Gesamteinsparung für FTE-Gehälter	C6*C7		176.197 €	176.197 €	176.197 €
Ct	Zeiteinsparungen beim Korrektur- und Berechtigungsmanagement sowie Kostenvermeidung	C5+C8	1.944.095 €	1.662.857 €	176.197 €	176.197 €
	Risikobereinigung	↓10 %				
Ctr	Zeiteinsparungen beim Korrektur- und Berechtigungsmanagement sowie Kostenvermeidung (risikobereinigt)		1.749.685 €	1.496.572 €	158.577 €	158.577 €

Geringeres Risikopotenzial

Die Varonis-Lösung trug zweifach dazu bei, das Risikopotenzial auf Seiten des Kundenunternehmens zu senken: 1) durch Korrektur des globalen gemeinsamen Zugriffs, wodurch die Auswirkungen eines Datenlecks gelindert werden, und 2) durch verbesserte Erkennung und Reaktion.

Laut Ponemon Institute entstanden Unternehmen aus dem Gesundheitssektor im Jahr 2017 durchschnittlich 322 € an Kosten für jeden Datensatz, der bei einem Datenleck verloren ging oder gestohlen wurde.[1] Im Allgemeinen gilt, dass je mehr Datensätze verloren gehen oder gestohlen werden, umso höher die Gesamtkosten, die einem Unternehmen entstehen.

Mit einem Modell für die Aufrechterhaltung von geringstmöglichen Berechtigungen haben die Mitarbeiter des Unternehmens (sowie Auftragnehmer und Berater) lediglich Zugriff auf die Daten, die sie für geschäftliche Zwecke benötigen. Durch die Einschränkung des Zugriffs auf Daten im gesamten Unternehmen reduzieren Unternehmen das Risiko gegenüber externen Bedrohungen, wenn ein einzelnes Benutzerkonto kompromittiert wird. Die Möglichkeit, einen Vorfall nach dem Auftreten rasch zu identifizieren, schränkt das Risiko in Zusammenhang mit Sicherheitsverletzungen weiter ein. Aus diesen Gründen sieht der Kunde in der Varonis-Lösung „eine Kernkomponente der Risikomanagementstrategie des Unternehmens insgesamt“.

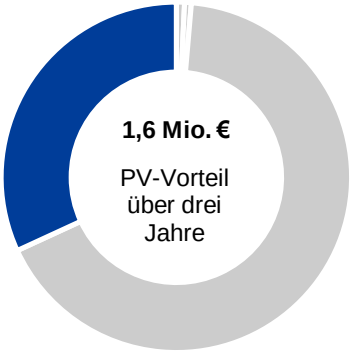
Das Finanzmodell stellt die folgenden Ergebnisse dar:

- In einem bestimmten Jahr besteht für den Kunde eine 14-prozentige Wahrscheinlichkeit, dass eine erhebliche Sicherheitsverletzung auftritt.
- Die durchschnittliche Anzahl der Kundendatensätzen, die bei einer Sicherheitsverletzung betroffen sind, beträgt für US-Unternehmen 28.512.
- Im Gesundheitswesen entstehen Unternehmen durchschnittlich 322 € an Kosten für jeden Datensatz, der von einem Datenleck betroffen ist.
- Durch die Möglichkeit, den Zugriff auf Dateien und Ordner einzuschränken, ermöglichte Varonis dem Kundenunternehmen, das Risikopotential bei einer Sicherheitsverletzung um 50 % zu senken.
- Durch einen schnelleren Erkennungs- und Reaktionsmechanismus reduziert Varonis die Gefährdung der Organisation bei einem Datenleck um weitere 15 Prozentpunkte.

Die folgenden Faktoren könnten diesen Vorteil beeinträchtigen:

- Der Reifegrad der Sicherheitspraktiken, die vor der Bereitstellung der Varonis-Lösung vorhanden waren.
- Die Art der verwalteten Daten, da dies sich auf die Gesamtkosten ihrer Offenlegung auswirkt.

Um diese Risiken zu berücksichtigen, hat Forrester eine Risikobereinigung von 15 % angesetzt, sodass sich über drei Jahre ein risikobereinigter Gesamt-PV von 1.604.109 € ergibt.



Geringeres Risikopotential: **32 %** des Gesamtnutzens

FORRESTER®

Reduziertes Risikopotential: Berechnungstabelle

9	KENNZAHL	BER.	ANFÄNGLICH	JAHR 1	JAHR 2	JAHR 3
D1	Durchschnittliche Anzahl der Kundendatensätze von US-Unternehmen, die bei einer Sicherheitsverletzung betroffen sind.	Ponemon		28.512	28.512	28.512
D2	Durchschnittliche Kosten pro Datensatz (Gesundheitswesen)	Ponemon		322 €	322 €	322 €
D3	Durchschnittliche Kosten für ein erhebliches Sicherheitsproblem	D1*D2		9.177.956 €	9.177.956 €	9.177.956 €
D4	Wahrscheinlichkeit der Datensicherheitsverletzung in einem bestimmten Jahr	Ponemon		14 %	14 %	14 %
D5	Geringeres Risikopotential bei Sicherheitsverstößen durch Korrektur des globalen gemeinsamen Zugriffs			50 %	50 %	50 %
D6	Geringeres Risikopotential bei Sicherheitsverstößen durch verbesserte Erkennung und Reaktion			15 %	15 %	15 %
D7	Verringerung des Risikopotentials bei Sicherheitsverletzungen insgesamt	D5+D6		65 %	65 %	65 %
D8	Erzielter Nutzen in Prozent			75 %	100 %	100 %
Dt	Geringeres Risikopotenzial	D3*D4*D7*D8	0 €	626.395,48 €	835.193,98 €	835.193,98 €
	Risikobereinigung	↓15 %				
Dtr	Geringeres Risikopotenzial (risikobereinigt)		0 €	532.436 €	709.915 €	709.915 €

Flexibilität

Flexibilität hat für jeden Kunden einen unterschiedlichen Wert – und auch die Art und Weise ihrer Quantifizierung variiert von Unternehmen zu Unternehmen. Es gibt zahlreiche Szenarien, in denen sich ein Kunde für die Implementierung einer oder mehrerer Komponenten der Varonis-Datensicherheitsplattform entscheiden könnte und später vielleicht weitere Anwendungs- und Geschäftsmöglichkeiten erkennt. Die folgenden Beispiele für erwartete zukünftige Vorteile wurden vom Kunden genannt, den Forrester für diese Fallstudie befragt hat:

- **Effektivere Aufbewahrung.** Bei vielen Unternehmen entsteht eine erhebliche Verantwortung, wenn sie Daten zu lange aufbewahren. Dennoch zögern sie oft, Daten zu verschieben oder zu löschen, aus Angst, dies könnte sich negativ auf das Geschäft auswirken. „Mit Varonis können wir dem Rest des Unternehmens Feedback geben, dass Dateien beispielsweise seit sechs Monaten oder einem Jahr nicht genutzt wurden und wir sie deshalb archivieren oder löschen können“, so der Leiter der Cybersicherheit. Durch das Löschen einer Datei wird das Risikoprofil der Organisation verringert, aber die Auswirkungen gehen über diese eine Datei hinaus. Da die Daten repliziert werden und es eine Vielzahl von Backups gibt, wird durch das Löschen einer Quelldatei Primär- und Sekundärspeicher frei.
- **Migration von Dateien auf kostengünstigeren Speicher.** Das Kundenunternehmen ist nach wie vor mit der Entwicklung seiner DLP- (Data Loss Prevention) und Klassifizierungsstrategien beschäftigt. Wenn es jedoch einmal feste Richtlinien gibt, zielt es darauf ab, die Datenklassifizierungs-Engine zu nutzen, um Daten auf kostengünstigere Speichermedien zu migrieren. Große Dateien wie MP3-Dateien und Videos, die auf gemeinsam genutzten Laufwerken gespeichert werden, gehören zu den besten Beispielen für Dateien, die für die Migration vorgesehen sind. Laut Aussage der Befragten gibt es jedoch bei allen Datentypen eine Vielzahl von Möglichkeiten.
- **Durchsetzung der Klassifizierungsrichtlinien.** Die sensiblen Dokumente des Kunden werden mit „vertraulich“ und „nur für den internen Gebrauch“ gekennzeichnet. Allerdings existieren diese Einschränkungen nur auf dem Papier. In Zukunft will das Unternehmen Varonis-Lösungen nutzen, um realistische, durchsetzbare Richtlinien für die Klassifizierung und Freigabe von Dokumenten zu schaffen.

Die Flexibilität wurde auch bei der Bewertung im Rahmen eines konkreten Projekts quantifiziert (ausführlichere Beschreibung in Anhang A).

Flexibilität stellt laut TEI-Methodik stellt eine Investition in eine zusätzliche Kapazität oder Funktionalität dar, die in einen zukünftigen geschäftlichen Nutzen umgewandelt werden können. Dies bietet einem Unternehmen das „Recht“ oder die Möglichkeit – nicht aber die Pflicht –, sich an zukünftigen Initiativen zu beteiligen.

Analyse der Kosten

QUANTIFIZIERTE KOSTENDATEN

Gesamtkosten

REF.	KOSTEN	ANFÄNGLICH	JAHR 1	JAHR 2	JAHR 3	GESAMT	BARWERT
Etr	Softwarekauf- und Wartungskosten	508.260 €	101.652 €	101.652 €	101.652 €	813.216 €	761.053 €
Ftr	An Varonis gezahlte Gebühren für Implementierung, Operationalisierung und Korrektur	214.316 €	163.067 €	0 €	0 €	377.383 €	362.559 €
Gtr	Kosten für den internen Planungs- und Bereitstellungsaufwand	4.845 €	0 €	0 €	0 €	4.845 €	4.845 €
	Gesamtkosten (risikobereinigt)	727.422 €	264.719 €	101.652 €	101.652 €	1.195.444 €	1.128.457 €

Softwarekauf- und Wartungskosten

Der Kunde bezahlt Varonis eine einmalige Gebühr für die Lizenzierung seiner Softwareprodukte. Darüber hinaus zahlt Kunde zahlt eine jährliche Wartungsgebühr in Höhe von 20 % des ursprünglichen Kaufpreises.

Zunächst gab der Kunde insgesamt 508.260 € dafür aus, das DatAdvantage-Basisprodukt, die Add-ons für UNIX, SharePoint, Exchange und Directory Services sowie Dataalert, DataPrivilege und das Classification Framework zu lizenzieren. In jedem nachfolgenden Jahr entrichtete der Kunde eine Wartungsgebühr von 101.652 € für den unterbrechungsfreien Zugriff auf Software-Updates, Patches, technischen Support und die Varonis Connect-Community.

Forrester hat keine Risikoanpassung für die Kosten der Softwareprodukte und Wartungskosten angesetzt, da Varonis Forrester die Kosten bereitgestellt hat und diese vom Kunden bestätigt wurden. Sie sind repräsentativ für die Kosten anderer Unternehmen, die für eine ähnliche Produktkonfiguration anfallen.

Die Gesamtkosten für Software und Wartung als Barwert belaufen sich auf 761.053 €.

In der Tabelle oben sind die Gesamtkosten für alle unten beschriebenen Bereiche sowie die Barwerte (PVs) mit einem Diskontierungssatz von 10 % aufgeführt. Über einen Zeitraum von drei Jahren sind für das befragte Unternehmen risikobereinigte Gesamtkosten mit einem Barwert (Present Value, PV) in Höhe von mehr als 1,1 Mio. € bzu erwarten.

Das „Implementierungsrisiko“ steht für das Risiko, dass eine mögliche Investition von den ursprünglichen oder erwarteten Anforderungen abweichen und zu höheren Kosten als erwartet führen könnte. Je größer die Unsicherheit, umso größer ist die potenzielle Bandbreite der Ergebnisse für die Nutzenschätzungen.

FORRESTER®

Kosten für Softwarekauf und -wartung: Berechnungstabelle						
REF.	KENNZAHL	BER.	ANFÄNGLICH	JAHR 1	JAHR 2	JAHR 3
E1	Softwarekosten		508.260 €	0 €	0 €	0 €
E2	Wartungsgebühren in Prozent des anfänglichen Einkaufspreises		0 €	101.652 €	101.652 €	101.652 €
Et	Softwarekauf- und Wartungskosten	E1+E2	508.260 €	101.652 €	101.652 €	101.652 €
	Risikobereinigung	0 %				
Etr	Softwarekauf- und -Wartungskosten (risikobereinigt)		508.260 €	101.652 €	101.652 €	101.652 €

Das befragte Unternehmen kaufte von Anfang an eine umfassendere Produktsuite von Varonis als viele andere. Dies hat die Vorteile während des dreijährigen Analysezeitraums erhöht, jedoch auch zu höheren Kosten geführt. Ein typischer Kunde wird zu Beginn eines Projekts in die folgenden Komponenten der Plattform investieren:

- DatAdvantage für einen einzelnen Datenspeicher (z. B. Windows oder Office 365).
- DatAlert Suite.
- Datenklassifizierungs-Engine.

Diese Investition bietet Zugriff auf Funktionen wie Berechtigungsverwaltung, Dateianalyse, Bedrohungserkennung, Analyse des Benutzerverhaltens, Erkennung von sensiblen Daten und Compliance-Reporting zu einem Preis von ca. 131.300 € (für ca. 1.000 Benutzer).

An Varonis gezahlte Gebühren für Implementierung, Operationalisierung und Korrektur

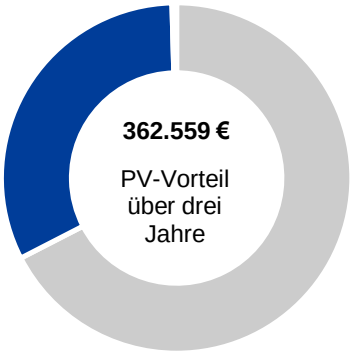
Dem Kunden entstanden Kosten für die Implementierung und die Operationalisierung der Varonis-Datensicherheitsplattform sowie für die erste Korrektur von Dateisystemen.

Aufgrund der einzigartigen Herausforderungen der Umgebung entschied sich der Kunde, das Team von Varonis Professional Services mit einem Großteil der Implementierungsarbeiten zu beauftragen. Es entschied sich wegen der vorhandenen Expertise für die direkte Zusammenarbeit mit Varonis, anstatt auf einen externen Systemintegrator zu vertrauen.

Als Teil der anfänglichen Implementierung und Operationalisierung der Lösung hat das Team von Varonis Professional Services eine Überprüfung der unstrukturierten Daten und Verzeichnisdienste des Kunden ausgeführt und die Mitarbeiter des Kunden geschult.

Diese Kategorie von Kosten beinhaltet auch die Korrektur des Zugriffs auf freigegebene Dateien und Ordner, die vom Professional Services Team von Varonis geleitet wurde.

- Zunächst wurde die Korrektur an 850.000 Risiko-Ordnern durchgeführt.
- Im ersten Jahr wurde die Korrektur an weiteren 650.000 Risiko-Ordnern durchgeführt.



An Varonis gezahlte Gebühren für Implementierung, Operationalisierung und Korrektur: **32 %** der Gesamtkosten.

FORRESTER®

Forrester nahm eine Risikobereinigung der an Varonis für die Implementierung, Operationalisierung und Korrektur bezahlten Gebühren vor und erhöhte diese um 10 %, um die Schwankungen zu berücksichtigen, zu denen es in Unternehmen aufgrund der folgenden Faktoren kommen kann:

- Die Komplexität der Bereitstellung.
- Die Größe und der Zustand der Dateisysteme vor der Bereitstellung von Varonis.

Diese Anpassung ergab über einen Zeitraum von drei Jahren Gesamtkosten mit einem Barwert von 362.559 €.

An Varonis gezahlte Gebühren für Implementierung, Operationalisierung und Korrektur: Berechnungstabelle

REF.	KENNZAHL	BER.	ANFÄNGLICH	JAHR 1	JAHR 2	JAHR 3
F1	An Varonis gezahlte Gebühren für Implementierung, Operationalisierung und Korrektur		194.833 €	148.243 €	0 €	0 €
Ft	An Varonis gezahlte Gebühren für Implementierung, Operationalisierung und Korrektur		194.833 €	148.243 €	0 €	0 €
	Risikobereinigung	↑10 %				
Ftr	An Varonis gezahlte Gebühren für Implementierung, Operationalisierung und Korrektur (risikobereinigt)		214.316 €	163.067 €	0 €	0 €

Kosten für den internen Planungs- und Bereitstellungsaufwand

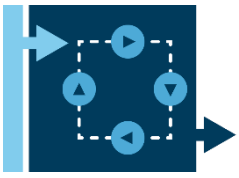
Dem Kunden entstanden Kosten für die internen Ressourcen, die für den Planungs- und Implementierungsprozess abgestellt wurden.

Die Planung und Implementierung erfolgte im Zeitraum von einem Monat, obwohl ein Großteil dieser Zeit darauf verwandt wurde, die Pläne für die Varonis-Bereitstellung bekannt zu machen. Keiner der Mitarbeiter wurde für dieses Projekt in Vollzeit abgestellt: Während der Vorbereitungsphase waren zwei Sicherheitsanalysten und ein Projektleiter mit Fachkenntnissen beteiligt, die jeweils 25 % (oder 10 Stunden pro Woche) bzw. 15 % (oder 6 Stunden pro Woche) ihrer Arbeitszeit darauf verwendeten. Umgerechnet auf das Jahresgehalt beträgt der ortsübliche Stundensatz für diese Mitarbeiter 42 € pro Stunde (inklusive aller Nebenkosten).

Forrester nahm eine Risikobereinigung des internen Aufwands für Planung und Implementierung vor und erhöhte diesen um 10 %, Unternehmen aufgrund der folgenden Faktoren kommen kann:

- Die Komplexität der Bereitstellung.
- Das Know-how, das für die erfolgreiche Implementierung der Lösung erforderlich ist.

Diese Anpassung ergab über einen Zeitraum von drei Jahren Gesamtkosten mit einem Barwert von 4.845 €.



Die Planung und Implementierung erfolgte im Zeitraum von einem Monat, obwohl ein Großteil dieser Zeit darauf verwandt wurde, die Pläne für die Bereitstellung bekannt zu machen.

FORRESTER®

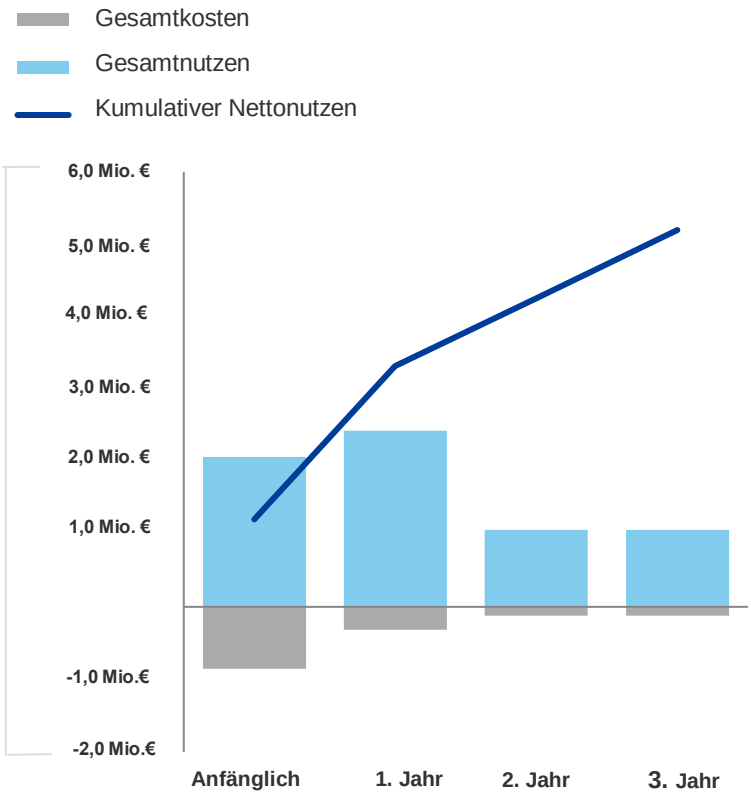
Kosten für den internen Planungs- und Bereitstellungsaufwand: Berechnungstabelle

REF.	KENNZAHL	BER.	ANFÄNGLICH	JAHR 1	JAHR 2	JAHR 3
G1	Stundensatz für Sicherheitsanalyst (inklusive aller Kosten)		42 €			
G2	Sicherheitsanalysten speziell für Planung und Implementierung		2			
G3	Wöchentlicher Einsatz pro Analyst	Stunden	10			
G4	Stundensatz für IT-Projektmanager (inklusive aller Kosten)		42 €			
G5	Wöchentlicher Einsatz durch Projekt-Manager		6			
G6	Anzahl der Wochen von Planung bis Bereitstellung		4			
Gt	Kosten für den internen Planungs- und Bereitstellungsaufwand	((G1*G2*G3)+ (G4*G5))*G6	4.405 €	0 €	0 €	0 €
	Risikobereinigung	↑10 %				
Gtr	Kosten für den internen Planungs- und Bereitstellungsaufwand (risikobereinigt)		4.845 €	0 €	0 €	0 €

Finanzübersicht

KONSOLIDIERTE, ÜBER DREI JAHRE RISIKOBEREINIGTE KENNZAHLEN

Cashflow-Diagramm (risikobereinigt)



Die in den Nutzen- und Kostenabschnitten berechneten finanziellen Ergebnisse können zur Bestimmung von ROI, NPV und Amortisierungszeitraum für die Investition des befragten Unternehmens genutzt werden. Forrester geht in dieser Analyse von einem jährlichen Diskontierungssatz von 10 % aus.

Die risikobereinigten Werte für ROI, Nettobarwert (Net Present Value, NPV) und Amortisierungszeitraum werden berechnet, indem die Risikobereinigungsfaktoren auf die unbereinigten Ergebnisse aus jedem Nutzen- und Kostenabschnitt angewendet werden.

Cashflow-Tabelle (risikobereinigt)

	ANFÄNGLICH	JAHR 1	JAHR 2	JAHR 3	GESAMT	BARWERT
Gesamtkosten	(727.422 €)	(264.719 €)	(101.652 €)	(101.652 €)	(1.195.444 €)	(1.128.457 €)
Gesamtnutzen	1.749.665 €	2.056.741 €	896.226 €	896.226 €	5.598.877 €	5.033.479 €
Nettonutzen	1.022.263 €	1.792.023 €	794.574 €	794.574 €	4.403.433 €	3.905.022 €
ROI						346 %
Amortisationszeitraum						< 6 Monate

FORRESTER®

Anhang A: Total Economic Impact

Total Economic Impact ist eine von Forrester Research, Inc. entwickelte Methodik, die die technologiebezogenen Entscheidungsprozesse von Unternehmen optimieren und Anbieter dabei unterstützen soll, Kunden das Nutzenversprechen ihrer Produkte und Dienstleistungen zu vermitteln. Die TEI-Methodik unterstützt Unternehmen darin, den materiellen Wert von IT-Initiativen gegenüber der Geschäftsführung und anderen wichtigen Entscheidungsträgern aufzuzeigen, zu begründen und zu veranschaulichen.

Ansatz des Total Economic Impact

Nutzen repräsentiert den Wert, den das Unternehmen durch das Produkt erhält. Die TEI-Methodik legt das gleiche Gewicht auf die Ermittlung der Vorteile und Kosten, was eine vollständige Untersuchung der Auswirkung zulässt, den die Technologie auf das Unternehmen insgesamt hat.

Kosten beinhalten alle Aufwendungen, die zur Realisierung des Werts oder Nutzens des Produkts erforderlich sind. Die Kostenkategorie in TEI erfasst alle über die gegenwärtige Umgebung hinaus anfallenden Mehrkosten für die laufenden Kosten in Verbindung mit der Lösung.

Flexibilität stellt den strategischen Wert dar, der durch zukünftige Zusatzinvestitionen realisiert werden kann, die auf der bereits getätigten Erstinvestition aufbauen. Die Möglichkeit, diesen Vorteil zu nutzen, stellt einen PV dar, der geschätzt werden kann.

Risiken messen die Unsicherheit der gegebenen Nutzen- und Kostenschätzungen: 1) die Wahrscheinlichkeit, dass die Schätzung den ursprünglichen Prognosen gerecht wird und 2) die Wahrscheinlichkeit, dass die Schätzungen im Laufe der Zeit nachverfolgt werden. Die TEI-Risikofaktoren basieren auf der „Dreiecksverteilung“.

Die Spalte mit den Erstinvestitionen enthält Kosten, die zum „Zeitpunkt 0“ oder zu Beginn des ersten Jahres anfallen und für die keine Abzinsung berechnet wurde. Für alle übrigen Cashflows werden zum Ende des Jahres unter Anwendung des Diskontierungssatzes Diskontierungen berechnet. Barwert-Berechnungen (Present Value, PV) werden für jede Schätzung von Gesamtkosten/-nutzen separat durchgeführt. Die Nettobarwert-Berechnungen (Net Present Value) in den zusammenfassenden Tabellen ergeben sich aus der Summe der Erstinvestition und der diskontierten Cashflows in den einzelnen Jahren. Die Summen und Barwertberechnungen des Gesamtnutzens, der Gesamtkosten und der Cashflow-Tabellen entsprechen aufgrund von Rundungen möglicherweise nicht exakt der Gesamtsumme.

Present Value (PV)

Dies ist der Barwert oder Gegenwartswert der (diskontierten) Kosten-/Nutzenschätzungen bei einem gegebenen Zinssatz (dem Diskontierungssatz). Der Present Value für Kosten und Nutzen fließt in den Gesamt-Nettobarwert (Net Present Value) der Cashflows ein

Net Present Value (NPV)

Das ist der Barwert oder Gegenwartswert von (diskontierten) zukünftigen Netto-Cashflows bei einem gegebenen Zinssatz (dem Diskontierungsfaktor). Ein positiver Projektkapitalwert gibt normalerweise an, dass eine Investition durchgeführt werden sollte, sofern nicht andere Projekte höhere Kapitalwerte aufweisen.

Return on Investment (ROI)

Dies ist die erwartete Rendite eines Projekts, angegeben als Prozentwert. Der ROI wird durch die Teilung der Nettonutzen (Nutzen abzüglich Kosten) durch die Kosten berechnet.

Diskontier-ungssatz

Der in der Cashflow-Analyse verwendete Zinssatz, der den Zeitwert von Geld mit einbezieht. Unternehmen verwenden üblicherweise Diskontierungssätze zwischen 8 % und 16 %.

Amortisations-zeitraum

Die Gewinnschwelle einer Investition. Dies ist der Zeitpunkt, an dem der Nettonutzen (Nutzen minus Kosten) gleich den Anfangsinvestitionen oder -kosten ist.

FORRESTER®

Endnoten

[1] Quelle: „2017 Cost of Data Breach: Global Overview“, Ponemon Institute, 13. Juni 2017 (https://www.ponemon.org/library/2017-cost-of-data-breach-study-united-states).