A Forrester Total Economic Impact™
Study Commissioned By Varonis
May 2018

The Total Economic Impact™ Of The Varonis Data Security Platform

Cost Savings And Business Benefits Enabled By The Varonis Data Security Platform

FORRESTER®

Table Of Contents

Project Director:
Joe Branca

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

FORRESTER®

ROI
346%

Benefits PV
$5.9 million

NPV
$4.6 million

Payback
<6 months

Executive Summary

Security breaches can result in significant monetary loss, especially when companies haven't taken measures to protect valuable data. In many organizations, files and folders are shared unnecessarily with hundreds or even thousands of employees, and users have access to far more data than they need to perform their jobs. This leaves sensitive data overly exposed to outside attackers and malicious insiders, since credentials for a single account can provide access to a trove of unsecured information, ranging from business plans to employee and customer data.

Even if organizations can identify where sensitive data resides, the task of securing it can be daunting. Remediating access to a single folder can take hours and require the participation of legal, business, and security teams. This process can be costly and, without the ability to determine who needs access to data, there is always a risk of disrupting the business.

Varonis provides a data security platform that helps its customers understand where sensitive data lives, who has access to it, and, importantly, who needs that access. This enables IT organizations to pursue a state of least-privileged access, which can drastically reduce the risk associated with a data security incident and maintain that status over time. Built-in machine learning and user behavior analytics protect sensitive data by allowing organizations to quickly identify breaches, misconfigurations, and other issues.

Varonis commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying the Varonis Data Security Platform. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of the Data Security Platform on their organizations. To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed a healthcare company with several years of experience using Varonis' products.

Prior to deploying key components of the Varonis Data Security Platform, the customer lacked clear visibility into what was happening on its file servers. The company knew it was overly exposed to ransomware and other security risks but didn't have the tools to understand the exact nature of the threat and take initial steps to address it. It used Varonis' software, along with the assistance of Varonis' professional services team, to remediate access to more than 1.5 million high-risk folders, which helped to dramatically reduce the organization's risk profile.

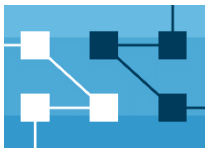
Key Findings

Quantified benefits. The interviewed organization experienced the following risk-adjusted present value (PV) quantified benefits:

- **Audit investigation time savings totaling $44,651**. The Varonis platform made it possible to complete audits and investigations of user behavior with 90% less effort, saving 420 hours of security analysts' time annually.
- **Time savings for provisioning file access totaling $36,767.** After deploying Varonis, provisioning file access — a common task for security analysts — took 75% less time, leading to annual time savings of more than 300 hours.

FORRESTER®

Benefits And Costs



Remediation and permissions management time savings and cost avoidance:
$3,966,948

Reduced risk exposure:
$1,893,648

Software purchase and maintenance costs:
$898,422

› **Remediation and permissions management time savings and cost avoidance totaling $3,966,948.** The customer organization rolled back permissions for more than 1.5 million high-risk folders. However, this analysis assumes that, without specialized software, the organization would have attempted to remediate access only to 1% of these folders to protect highly sensitive data. For each folder, it saved 4.5 hours of security professionals' time (3 hours of a security analyst's time and 1.5 hours of a senior-level employee's time) by using Varonis, rather than attempting to complete this process manually.

› **Risk reduction benefits totaling $1,893,648.** The Varonis solution helped the customer organization reduce its risk profile by 65%. In the event of a large-scale security incident, the average healthcare organization will incur costs of $10,834,560. In a given year, there is a 14% chance one will occur. This left the organization exposed to more than $1.5 million in total risk. By remediating global shared access to data and providing improved detection and response capabilities, Varonis limited that exposure.

Costs. The interviewed organization experienced the following risk-adjusted PV costs:

› **Software purchase and maintenance costs totaling $898,422.** The customer paid Varonis a one-time fee to license its software products; the customer also pays an annual maintenance fee equal to 20% of the initial purchase price.

› **Fees paid to Varonis for implementation, operationalization, and remediation totaling $488,000.** The customer incurred costs for professional services provided by Varonis to complete the implementation and operationalization of the Varonis Data Security Platform as well as the initial remediation of access to data stored on the customer's file systems.

› **Costs for internal effort for planning and deployment totaling $5,720.** The customer also incurred costs for the internal resources it dedicated to planning and implementation of the Varonis Data Security Platform, which took place over the course of one month.

The interviewed organization purchased a more comprehensive suite of products from Varonis than most do at the outset. This enhanced the benefits realized during the three-year period of analysis, but it also resulted in higher costs. Most customers will initially purchase core components of the platform — a typical starter package for an organization monitoring 1,000 users will total approximately $155,000 — and then add products and components over time.

Forrester's interview with this existing customer and subsequent financial analysis found that the interviewed organization experienced benefits of $5,942,014 over three years versus costs of $1,332,142, adding up to a net present value (NPV) of $4,609,872 and an ROI of 346%.

The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

TEI Framework And Methodology

From the information provided in the interview, Forrester has constructed a Total Economic Impact™ (TEI) framework for those organizations considering implementing the Varonis Data Security Platform.

The objective of the framework is to identify the cost, benefit, flexibility, and risk factors that affect the investment decision. Forrester took a multistep approach to evaluate the impact that the Varonis Data Security Platform can have on an organization:

DUE DILIGENCE
Interviewed Varonis stakeholders and Forrester analysts to gather data relative to the Varonis Data Security Platform.

CUSTOMER INTERVIEW
Interviewed one organization using the Varonis Data Security Platform to obtain data with respect to costs, benefits, and risks.

FINANCIAL MODEL FRAMEWORK
Constructed a financial model representative of the interview using the TEI methodology and risk-adjusted the financial model based on issues and concerns of the interviewed organization.

CASE STUDY
Employed four fundamental elements of TEI in modeling the Varonis Data Security Platform's impact: benefits, costs, flexibility, and risks. Given the increasing sophistication that enterprises have regarding ROI analyses related to IT investments, Forrester's TEI methodology serves to provide a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

The Data Security Platform Customer Journey

BEFORE AND AFTER THE DATA SECURITY PLATFORM INVESTMENT

Interviewed Organization

For this study, Forrester interviewed the director of cybersecurity and a security analyst for a multibillion-dollar health insurance provider. The company provides health insurance to individuals and employers in all 50 states in the US and employs approximately 3,000 people.

The following high-level metrics describe the organization's file servers and Active Directory structure:

- 76 TB of data.
- 8.2 million folders.
- 170 million files.
- 8,500 user accounts.
- 11,300 groups.

Owing to the nature of its business, the customer organization manages data subject to the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule.

The organization uses the following Varonis products:

- **DatAdvantage*.** Provides IT organizations with an efficient approach to permissions management, user audits, and file access provisioning.
- **DatAlert.** Leverages machine learning and behavioral analytics to surface alerts to suspicious activity on the file servers.
- **DataPrivilege.** Gives business users the ability to review and manage access controls without assistance from IT.
- **Data Classification Engine:** Scans for sensitive data and applies classification rules to improve security and compliance.

The organization chose Varonis after a thorough review of options available in the marketplace. "It seemed like a very clear-cut answer to us," said the director of cybersecurity.

**Includes the Windows, SharePoint, Exchange, Active Directory, and UNIX components.*

> "If you are familiar with any sort of organization that's rolled forward file servers and permissions over decades, it's a messy, ugly process. We needed clear visibility into what was happening on those file servers, who had access. So, now, we can say without a doubt that this is the person who touched something. We didn't have that prior to Varonis, and that's where having this tool set is invaluable for us."
>
> *Director of cybersecurity*

Risk Assessment And Remediation Summary

Prior to the start of the engagement, Varonis completed a review of the customer's data stores and repositories in accordance with industry standards and Varonis best practices to assess risks in the areas of access control, Active Directory structure, New Technology File System (NTFS) and sharing permissions structure, and data retention.

This review identified several high-risk concerns, which Varonis recommended targeting for remediation immediately:

- 1.5 million folders throughout the environment with global permissions.

- 160,000 files containing sensitive data; 27% of these files had not been touched in six months.
- 14,000 files with global permissions that contained sensitive files.
- 3,700 users with removal recommendations.
- 3,000 stale users with enabled permissions (e.g., employees and contractors who had left the company).

The review also identified several medium- and low-risk concerns:

- 4.1 million folders, representing nearly 17 TB, containing stale data.
- 1,750 users with non-expiring passwords.
- 960,000 folders to which unique permissions were applied, directly or directly, and inherited.
- 60,000 folders with direct — rather than group-level — user access control entries (ACEs).

The customer engaged Varonis' professional services team to assist with the remediation of permissions on its file systems. The initial engagement, which took place over the course of six months, included remediation of the following:

- 850,000 folders with global permissions.
- 12,000 folders with global permissions containing sensitive data.
- 45,000 files with global permissions containing sensitive data.

Completing the remediation process and reaching a state of least-privileged access took an additional 90 days.

> "From a retention standpoint, there's always a skittishness that somebody might need these files. So, is it appropriate to get rid of them, or do we keep them around forever? With Varonis, we can provide feedback to the rest of the organization that files haven't been touched in six months or a year, for example. They're no longer required, and we can archive or delete them."
>
> *Director of cybersecurity*

Key Challenges

During the interviews, the customer's managers highlighted the following key challenges, which prompted the investment in the Varonis Data Security Platform:

- **Understanding access.** The organization lacked a comprehensive understanding of who had access to data stored on its file servers and who needed it for work purposes. Permissions had been rolled forward over the course of several decades. They were often applied inconsistently, and many were out of date, giving users access to far more data than they needed to do their jobs. Yet, without specialized software, access controls were difficult to analyze on such a large scale.
- **Understanding and limiting risk.** The organization saw the impact of data breaches in the news and sought ways to limit risks. It lacked the means to locate sensitive data on its file systems. Even if it could locate sensitive data, it lacked the ability to roll back permissions in an efficient manner without generating complaints from business users.

- **Identifying and dealing with security incidents.** Prior to deploying the Varonis platform, the customer organization had security tools in place, but they were highly inadequate, according to interviewees. Security analysts relied heavily on end users to alert them to problems. In some cases, they failed to do so, leaving malware to run undetected for several hours. Because files and folders were over-permissioned, a much greater share of the organization's data was exposed. After the fact, security teams struggled to understand what data was exposed and articulate necessary next steps to senior leadership.

Key Results

During the interviews, the customer's managers highlighted the following key results from the investment in the Varonis Data Security Platform:

- **A drastic reduction in risk associated with a data breach.** By limiting access only to data employees needed to do their jobs, the organization reduced its risk profile. With Varonis' products, as well as the help of Varonis' professional services team, the organization remediated access to more than 1.5 million folders with open access, including many that contained sensitive data.
- **Improved workflows.** Varonis allows security analysts to carry out everyday tasks with greater efficiency, freeing up time to focus on higher-value activities. Provisioning access to files and folders — which is required every time a new employee joins the organization — is much easier with the solutions Varonis provides. Likewise, in the unfortunate event that an employee is suspected of accessing data in ways they shouldn't, completing an audit of that user's access to files and folders on the system now requires much less effort.
- **Better retention and archiving.** The organization can now better identify stale data and choose to retain or archive it based on business needs. The initial risk assessment identified more than 16TB of stale data, an amount equal to 22% of all data in the environment monitored by Varonis. This data represents a significant liability, as users who don't need to access it can still do so. It is also subject to industry-specific rules and regulations, and Varonis allows security analysts to assist legal teams in achieving compliance.

> "If we receive an alert and we start seeing certain behaviors of a particular malware, and we know that this person has full control over a particular directory or set of directories, we can take action immediately to contain the threat. In the past we had nothing. It would have to be reported by someone, and by that time half of our files were encrypted."
>
> *Director of cybersecurity*

> "With Varonis, you type in a user name, you hit enter, it shows you the file tree, you know they have a certain level of access, you go to where modifications are needed, you make all the changes, and then you commit all those changes at once."
>
> *Security analyst*

Analysis Of Benefits

QUANTIFIED BENEFIT DATA

Total Benefits

REF.	BENEFIT	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Atr	Audit investigation time savings	$0	$17,955	$17,955	$17,955	$53,865	$44,651
Btr	Time savings when provisioning file access	$0	$14,784	$14,784	$14,784	$44,353	$36,767
Ctr	Remediation and permissions management time savings and cost avoidance	$2,065,500	$1,766,700	$187,200	$187,200	$4,206,600	$3,966,948
Dtr	Reduced risk exposure	$0	$628,540	$838,053	$838,053	$2,304,646	$1,893,648
	Total benefits (risk-adjusted)	$2,065,500	$2,427,979	$1,057,993	$1,057,993	$6,609,464	$5,942,014

Audit Investigation Time Savings

The Varonis solution allows the customer's security analysts to more quickly complete audits and investigations of how users access files and folders.

Prior to deploying DatAdvantage, it could take one to two days to complete an audit or investigation, if it was at all possible. Log files only allowed security analysts to see folder access over the prior 36 hours, and if the behavior in question occurred earlier than that, records of it couldn't be retrieved. With Varonis, analysts can produce reports on user access within minutes, according to the interviewees.

The financial model represents the following findings:

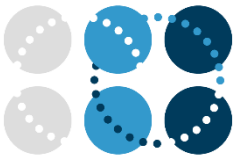
- Prior to deploying the Varonis platform, security analysts needed 12 hours to complete an investigation into a user's file access history.
- Each year, security analysts are alerted to 35 incidents that require further investigation.
- Varonis allows security analysts to complete an investigation into a user's file access history with 90% less effort.

The following risks may affect this benefit category:

- The process companies have in place for completing this task prior to a Varonis deployment.
- The frequency with which companies will need to carry out this task.

To account for these risks, Forrester applied a 5% risk adjustment, yielding a three-year, risk-adjusted total PV of $44,651.

The table above shows the total of all benefits across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the interviewed organization expects risk-adjusted total benefits to be a PV of more than $5.9 million.



Prior to deploying the Varonis solution, security analysts needed 12 hours to complete an audit of a user's file access history.

FORRESTER®

Audit Investigation Time Savings: Calculation Table						
REF.	METRIC	CALC.	INITIAL	YEAR 1	YEAR 2	YEAR 3
A1	Effort required for individual audit without Varonis in place	Hours		12	12	12
A2	Incidents requiring audit and investigation (annual)			35	35	35
A3	Percentage reduction in effort required to generate audit report			90%	90%	90%
A4	Security analyst average hourly rate, fully burdened			$50	$50	$50
At	Audit investigation time savings	A1*A2*A3*A4	$0	$18,900	$18,900	$18,900
	Risk adjustment	↓5%				
Atr	Audit investigation time savings (risk-adjusted)		$0	$17,955	$17,955	$17,955

Time Savings When Provisioning File Access

The Varonis platform allows security analysts at the customer organization to spend fewer hours provisioning access to files and folders.

Prior to deploying the Varonis platform, provisioning access to files and folders was a manual and error-prone process, according to a security analyst who previously dedicated at least 8 hours per week to this task. He explained how Varonis simplified the process: "With Varonis, you type in a user name, you hit enter, it shows you the file tree, you know they have a certain level of access, you go to where modifications are needed, you make all the changes, and then you commit all those changes at once."

(At the time of the interview, the customer organization had not yet begun to utilize the request and approval feature built into DataPrivilege, which allows business users to request and approve access to files and folders. It used DatAdvantage to quickly gain visibility into a user's level of access and to efficiently make changes.)

The financial model represents the following findings:

- Prior to the Varonis deployment, security analysts dedicated 415 hours each year to the task of provisioning access to files and folders.
- With the Varonis software, security analysts can provision access to files and folders with 75% less effort.

The following risks may affect this benefit category:

- The process companies have in place for completing this task prior to a Varonis deployment.
- The frequency with which companies will need to carry out this task.

To account for these risks, Forrester applied a 5% risk adjustment, yielding a three-year, risk-adjusted total PV of $36,767.

Prior to the Varonis deployment, security analysts dedicated 415 hours each year to the task of provisioning files and folders.

Time Savings When Provisioning File Access: Calculation Table						
REF.	METRIC	CALC.	INITIAL	YEAR 1	YEAR 2	YEAR 3
B1	Effort required for provisioning file access prior to Varonis (annual)	Hours		415	415	415
B2	Percentage reduction in effort required to provision file access			75%	75%	75%
B3	Security analyst average hourly rate, fully burdened			$50	$50	$50
Bt	Time savings when provisioning file access	B1*B2*B3	$0	$15,563	$15,563	$15,563
	Risk adjustment	↓5%				
Btr	Time savings when provisioning file access (risk-adjusted)		$0	$14,784	$14,784	$14,784

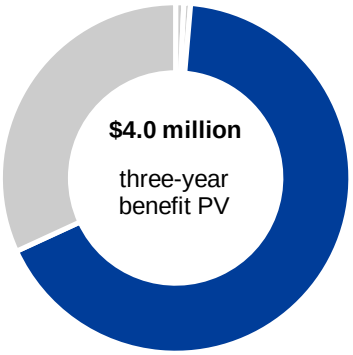
Remediation And Permissions Management Time Savings And Cost Avoidance

The Varonis platform enabled the customer organization to identify overshared files and folders and to remediate access to them without impacting the business.

After years of permissions being rolled forward, the customer's file systems were replete with overshared files and folders. Yet, the IT organization had no easy way to determine who had access to files and folders and who needed that access to do their jobs. To the extent that it was possible, the process of remediating access to overshared items without a specialized software solution in place would consume significant time and resources.

The financial model represents the following findings:

- The customer organization used the Varonis solution to understand who in the organization had access to files and folders as well as who needed that access to perform their jobs.
- Varonis' risk assessment identified 1.5 million folders with global access, which it deemed high-risk.
- The customer, along with Varonis' professional services team, initially remediated access to 850,000 folders; it remediated access to an additional 650,000 folders in Year 1.
- Without a solution like Varonis, the customer organization would not have attempted this task, making it impractical to calculate this benefit using the total number of folders for which access was remediated.
- The customer organization would have attempted to identify and remediate access to folders containing highly sensitive data; the number of folders it could identify and address using a manual process is equal to 1% of the 1.5 million high-risk folders identified by Varonis. This benefit is calculated with respect to only that 1% of folders.



Remediation and permissions management time savings and cost avoidance: **67%** of total benefits

FORRESTER®

- Without a specialized solution like Varonis, it would take at least 4.5 hours, on average, to remediate access to a single folder. This estimate includes 3 hours of a security analyst's time as well as 1.5 hours of a senior-level employee's time.
- The average hourly cost for these resources assumes a fully burdened hourly rate of $50.00 for the security analyst and a fully burdened hourly rate of $87.50 for the senior-level employee. These estimates are consistent with rates provided by the customer organization and are reflective of the regional marketplace in which they compete for talent.
- Following the initial remediation, Varonis software enabled the customer organization to maintain a state of least-privileged access with two fewer full-time equivalents (FTEs) than it otherwise would have required.

The following risks may affect this benefit category:

- The state of a company's file systems prior to deploying Varonis.
- The cost of hiring and employing security professionals in a company's regional marketplace.

To account for these risks, Forrester applied a 10% risk adjustment, yielding a three-year, risk-adjusted total PV of $3,966,948.

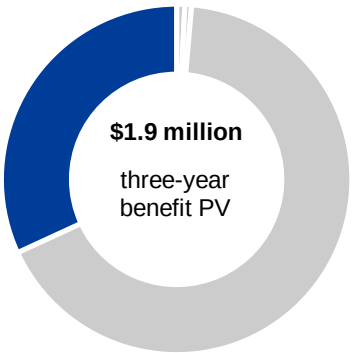
Remediation And Permissions Management Time Savings and Cost Avoidance: Calculation Table						
REF.	**METRIC**	**CALC.**	**INITIAL**	**YEAR 1**	**YEAR 2**	**YEAR 3**
C1	Total folders with global access removed		850,000	650,000		
C2	Percentage of folders with sensitive data		1.0%	1.0%		
C3	Effort required to identify and remediate folder global access prior to Varonis deployment	Hours	4.5	4.5		
C4	Average hourly cost of resources		$60	$60		
C5	Total remediation costs avoided due to Varonis Data Security Platform	C1*C2*C3*C4	$2,295,000	$1,755,000		
C6	FTEs avoided to manage permissions on ongoing basis	Customer interview		2	2	2
C7	Security analyst fully burdened annual salary	Customer interview		$104,000	$104,000	$104,000
C8	Total FTE salary cost savings	C6*C7		$208,000	$208,000	$208,000
Ct	Remediation and permissions management time savings and cost avoidance	C5+C8	$2,295,000	$1,963,000	$208,000	$208,000
	Risk adjustment	↓10%				
Ctr	Remediation and permissions management time savings and cost avoidance (risk-adjusted)		$2,065,500	$1,766,700	$187,200	$187,200

Reduced Risk Exposure

The Varonis solution helped the customer organization reduce its risk exposure in two ways: 1) by remediating global shared access, which can limit the impact of a breach, and 2) through improved detection and response.

In 2017, healthcare organizations incurred an average cost of $380 for each record lost or stolen in a data breach, according to the Ponemon Institute.[1] In general, the more records lost or stolen in a breach, the higher the total cost will be to the organization.

With a least-privileged model, the organization's employees (as well as contractors and consultants) have access only to the data they need for business purposes. By limiting access to data across the organization, organizations reduce their exposure to outside threats should an individual user account be compromised. Being able to quickly identify an incident when it occurs further limits the risk associated with a data breach. For these reasons, the customer views the Varonis solution as "a



Reduced risk exposure:
32% of total benefits

FORRESTER®

core component of the [organization's] overall risk management strategy."

The financial model represents the following findings:

- In a given year, the customer faces a 14% probability of experiencing a large-scale security incident.
- The average number of customer records exposed in a breach for US companies is 28,512.
- Healthcare companies incur an average cost of $380 for each customer record exposed in breach.
- By enabling it to remediate access to files and folders, Varonis reduced the customer organization's exposure to a data breach by 50% percentage points.
- By providing a faster detection and response mechanism, Varonis further reduced the organization's exposure to a data breach by 15% percentage points.

The following risks may affect this benefit category:

- The sophistication of security practices in place prior to the deployment of the Varonis solution.
- The type of data under management, which will affect the total cost of its exposure to the public.

To account for these risks, Forrester applied a 15% risk adjustment, yielding a three-year, risk-adjusted total PV of $1,893,648.

Reduced Risk Exposure: Calculation Table						
REF.	**METRIC**	**CALC.**	**INITIAL**	**YEAR 1**	**YEAR 2**	**YEAR 3**
D1	Average number of records exposed in a breach for US companies	Ponemon		28,512	28,512	28,512
D2	Average per record cost incurred for stolen healthcare data	Ponemon		$380	$380	$380
D3	Average cost of a major data security issue	D1*D2		$10,834,560	$10,834,560	$10,834,560
D4	Probability of a data breach in a given year	Ponemon		14%	14%	14%
D5	Reduced exposure to a data breach by remediating global shared access			50%	50%	50%
D6	Reduced exposure to a data breach through improved detection and response			15%	15%	15%
D7	Total reduction in exposure to a data breach	D5+D6		65%	65%	65%
D8	Percentage of benefits realized			75%	100%	100%
Dt	Reduced risk exposure	D3*D4*D7*D8	$0	$739,458.72	$985,944.96	$985,944.96
	Risk adjustment	↓15%				
Dtr	Reduced risk exposure (risk-adjusted)		$0	$628,540	$838,053	$838,053

Flexibility

The value of flexibility is clearly unique to each customer, and the measure of its value varies from organization to organization. There are multiple scenarios in which a customer might choose to implement one or more components of the Varonis Data Security Platform and later realize additional uses and business opportunities. The following examples of expected future value were provided by the customer Forrester interviewed for this case study:

Flexibility, as defined by TEI, represents an investment in additional capacity or capability that could be turned into business benefit for a future additional investment. This provides an organization with the "right" or the ability to engage in future initiatives but not the obligation to do so.

- **Better retention.** For many organizations, holding data too long creates a liability. Yet, they are often hesitant to move or delete data for fear that it will impact the business. “With Varonis, we can provide feedback to the rest of the organization that files haven’t been touched in six months or a year, for example, and they’re no longer required, so we can archive or delete them,” said the director of cybersecurity. Deleting a file reduces the organization’s risk profile, but its impact extends beyond that one item. Because data is replicated, and there are multiple backups, eliminating a source file frees up primary and secondary storage.
- **Migrating files to lower-cost storage.** Today, the customer organization is still developing its data loss prevention (DLP) and classification strategies. However, once it has firm policies in place, it aims to leverage the Data Classification Engine to identify opportunities to migrate data to lower-cost storage. Large files such as MP3s and videos stored on shared drives are among the best examples of files targeted for migration, though numerous opportunities exist across all types of data, according to interviewees.
- **Enforceable classification policy.** The customer organization’s sensitive documents are labeled “confidential” and “for internal use only,” though to date these restrictions are “just words on a paper,” according to the director of cybersecurity. Moving forward, the organization aims to leverage Varonis solutions to create realistic, enforceable policies for classification and sharing.

Flexibility would also be quantified when evaluated as part of a specific project (described in more detail in Appendix A).

Analysis Of Costs

QUANTIFIED COST DATA

Total Costs

REF.	COST	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Etr	Software purchase and maintenance costs	$600,000	$120,000	$120,000	$120,000	$960,000	$898,422
Ftr	Fees paid to Varonis for implementation, operationalization, and remediation	$253,000	$192,500	$0	$0	$445,500	$428,000
Gtr	Cost of internal effort required for planning and deployment	$5,720	$0	$0	$0	$5,720	$5,720
	Total costs (risk-adjusted)	$858,720	$312,500	$120,000	$120,000	$1,411,220	$1,332,142

Software Purchase And Maintenance Costs

The customer paid Varonis a one-time fee to license its software products; the customer also pays an annual maintenance fee equal to 20% of the initial purchase price.

Initially, the customer spent a total of $600,000 to license the DatAdvantage base product and the UNIX, SharePoint, Exchange, and Directory Services add-ons as well as DatAlert, DataPrivilege, and the Classification Framework. In each subsequent year, the customer paid a maintenance fee of $120,000 for uninterrupted access to software updates, patches, technical support, and the Varonis Connect community.

Forrester did not apply a risk adjustment to the cost of software products and maintenance costs as Varonis provided the costs to Forrester and they were confirmed by the customer. They are representative of costs other organizations can expect to incur for a similar configuration of products.

The total three-year cost for software and maintenance in PV is $898,422.

The table above shows the total of all costs across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the interviewed organization expects risk-adjusted total costs to be a PV of more than $1.3 million.

Implementation risk is the risk that a proposed investment may deviate from the original or expected requirements, resulting in higher costs than anticipated. The greater the uncertainty, the wider the potential range of outcomes for cost estimates.

Software Purchase And Maintenance Costs: Calculation Table						
REF.	METRIC	CALC.	INITIAL	YEAR 1	YEAR 2	YEAR 3
E1	Software costs		$600,000	$0	$0	$0
E2	Maintenance fees as percentage of initial purchase price		$0	$120,000	$120,000	$120,000
Et	Software purchase and maintenance costs	E1+E2	$600,000	$120,000	$120,000	$120,000
	Risk adjustment	0%				
Etr	Software purchase and maintenance costs (risk-adjusted)		$600,000	$120,000	$120,000	$120,000

The interviewed organization purchased a more comprehensive suite of products from Varonis than most do at the outset. This enhanced the benefits realized during the three-year period of analysis, but it also resulted in higher costs. A more typical customer will invest in the following components of the platform at the start of an engagement with Varonis:

- DatAdvantage for a single data store (e.g., Windows or Office 365).
- DatAlert Suite.
- Data Classification Engine.

This investment will provide access to functionality including permissions management, file analytics, threat detection, user behavior analysis, sensitive data discovery, and compliance reporting at a cost of approximately $155,000, assuming roughly 1,000 monitored users.

Fees Paid To Varonis For Implementation, Operationalization, And Remediation

The customer incurred costs for implementation and operationalization of the Varonis Data Security Platform as well as the initial remediation of file systems.

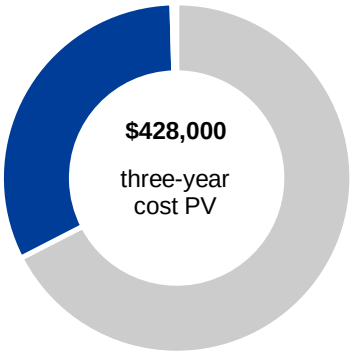
Owing to the unique challenges presented by its environment, the customer decided to entrust Varonis' professional services team with a majority of the implementation work. It chose to work directly with Varonis, as opposed to a third-party systems integrator, for its expertise.

As part of the initial implementation and operationalization of the solution, Varonis' professional services team performed a review of the customer's unstructured data and directory services environments and provided training for the customer's staff.

This category of costs also includes remediation of access to shared files and folders, an effort that was led by Varonis' professional services team.

- Initially, remediation was performed on 850,000 high-risk folders.
- In Year 1, remediation was performed on an additional 650,000 high-risk folders.

Forrester risk-adjusted fees paid to Varonis for implementation,



Fees paid to Varonis for implementation, operationalization, and remediation: **32%** of total costs

FORRESTER®

operationalization, and remediation upward by 10% to account for variability organizations may experience owing to the following factors:

- The complexity of the deployment.
- The size and state of file systems prior to the deployment of Varonis.

This adjustment yielded a three-year PV total cost of $428,000.

Fees Paid To Varonis For Implementation, Operationalization, And Remediation: Calculation Table

REF.	METRIC	CALC.	INITIAL	YEAR 1	YEAR 2	YEAR 3
F1	Fees paid to Varonis for implementation, operationalization, and remediation		$230,000	$175,000	$0	$0
Ft	Fees paid to Varonis for implementation, operationalization, and remediation		$230,000	$175,000	$0	$0
	Risk adjustment	↑10%				
Ftr	Fees paid to Varonis for implementation, operationalization, and remediation (risk-adjusted)		$253,000	$192,500	$0	$0

Cost Of Internal Effort Required For Planning And Deployment

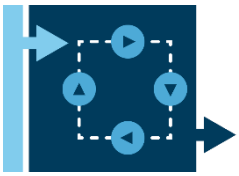
The customer also incurred costs for the internal resources it dedicated to the planning and implementation process.

Planning and implementation took place over one month, though much of this time was spent socializing plans for the Varonis deployment and making sure they were well understood. No individual was dedicated to this initiative full-time: Predeployment activities required a 25% commitment (or 10 hours per week) from two security analysts as well as a 15% commitment (or 6 hours per week) from a project manager with subject matter expertise. In the customer's regional market, these employees are compensated at a fully burdened annual rate of $50 per hour.

Forrester risk-adjusted the cost of internal effort for planning and implementation upward by 10% to account for variability organizations may experience owing to the following factors:

- The complexity of the deployment.
- The level of expertise required to successfully deploy the solution.

This adjustment yielded a three-year PV total cost of $5,720.



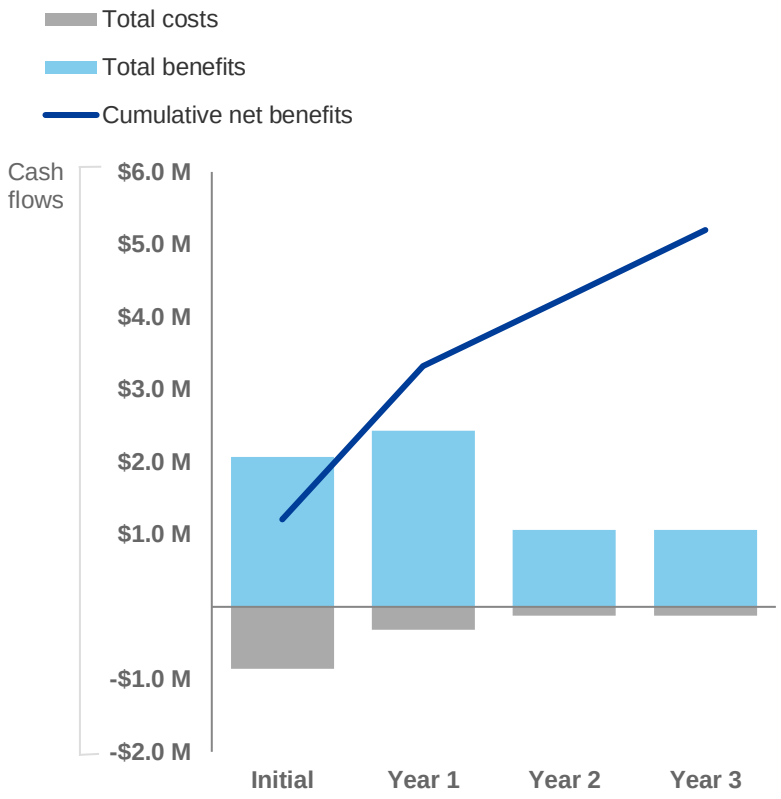
Planning and implementation took place over one month, though much of this time was spent socializing plans for the deployment.

Cost Of Internal Effort Required For Planning And Deployment: Calculation Table						
REF.	**METRIC**	**CALC.**	**INITIAL**	**YEAR 1**	**YEAR 2**	**YEAR 3**
G1	Security analyst hourly rate fully burdened		$50			
G2	Security analysts dedicated to planning and implementation		2			
G3	Weekly commitment per analyst	Hours	10			
G4	IT project manager hourly rate fully burdened		$50			
G5	Weekly commitment from project manager		6			
G6	Number of weeks from planning to deployment		4			
Gt	Cost of internal effort required for planning and deployment	((G1*G2*G3)+ (G4*G5))*G6	$5,200	$0	$0	$0
	Risk adjustment	↑10%				
Gtr	Cost of internal effort required for planning and deployment (risk-adjusted)		$5,720	$0	$0	$0

Financial Summary

CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS

Cash Flow Chart (Risk-Adjusted)



The financial results calculated in the Benefits and Costs sections can be used to determine the ROI, NPV, and payback period for the interviewed organization's investment. Forrester assumes a yearly discount rate of 10% for this analysis.

These risk-adjusted ROI, NPV, and payback period values are determined by applying risk-adjustment factors to the unadjusted results in each Benefit and Cost section.

Cash Flow Table (Risk-Adjusted)

	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Total costs	($858,720)	($312,500)	($120,000)	($120,000)	($1,411,220)	($1,332,142)
Total benefits	$2,065,500	$2,427,979	$1,057,993	$1,057,993	$6,609,464	$5,942,014
Net benefits	$1,206,780	$2,115,479	$937,993	$937,993	$5,198,244	$4,609,872
ROI						346%
Payback period						<6 months

FORRESTER®

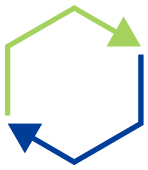
Appendix A: Total Economic Impact

Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

Total Economic Impact Approach

Benefits represent the value delivered to the business by the product. The TEI methodology places equal weight on the measure of benefits and the measure of costs, allowing for a full examination of the effect of the technology on the entire organization.

Costs consider all expenses necessary to deliver the proposed value, or benefits, of the product. The cost category within TEI captures incremental costs over the existing environment for ongoing costs associated with the solution.



Flexibility represents the strategic value that can be obtained for some future additional investment building on top of the initial investment already made. Having the ability to capture that benefit has a PV that can be estimated.

Risks measure the uncertainty of benefit and cost estimates given: 1) the likelihood that estimates will meet original projections and 2) the likelihood that estimates will be tracked over time. TEI risk factors are based on "triangular distribution."

The initial investment column contains costs incurred at "time 0" or at the beginning of Year 1 that are not discounted. All other cash flows are discounted using the discount rate at the end of the year. PV calculations are calculated for each total cost and benefit estimate. NPV calculations in the summary tables are the sum of the initial investment and the discounted cash flows in each year. Sums and present value calculations of the Total Benefits, Total Costs, and Cash Flow tables may not exactly add up, as some rounding may occur.

Present value (PV)

The present or current value of (discounted) cost and benefit estimates given at an interest rate (the discount rate). The PV of costs and benefits feed into the total NPV of cash flows.

Net present value (NPV)

The present or current value of (discounted) future net cash flows given an interest rate (the discount rate). A positive project NPV normally indicates that the investment should be made, unless other projects have higher NPVs.

Return on investment (ROI)

A project's expected return in percentage terms. ROI is calculated by dividing net benefits (benefits less costs) by costs.

Discount rate

The interest rate used in cash flow analysis to take into account the time value of money. Organizations typically use discount rates between 8% and 16%.

Payback period

The breakeven point for an investment. This is the point in time at which net benefits (benefits minus costs) equal initial investment or cost.

Endnotes

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