A Forrester Total Economic Impact™
Study Commissioned By Varonis
March 2020

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

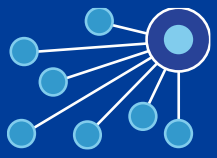
Project Director:
Connor Maguire
Sarah Musto

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®

Three-Year Benefits And Costs



Reduced risk of a security breach:
$2,070,852

Time savings from remediating global access to folders:
$4,795,188

Total cost of Varonis Data Security Platform including licensing, deployment, and upkeep:
$1,189,036

Executive Summary

Data security and privacy are key issues that all organizations that handle and store data must consider. A Forrester survey of global network security decision makers at enterprise organizations found that 51% of respondents reported at least one potential data breach in the last 12 months.[1] Data breaches can result in significant monetary losses and have lasting, sometimes irreparable, effects on brand image. Organizations must take every precaution when it comes to data security. However, many organizations have little to no visibility into what data they have and who has been accessing it. The result is a multitude of files containing sensitive information stored in folders with no insight into who can access them. This exposes organizations to malicious threats both externally and internally.

Visualizing and controlling who can access files can be just as difficult as understanding what information those files contain. Manual access provisioning processes are often cumbersome and can result in access being removed from users with a legitimate need. Organizations can dedicate significant resources to attempting to organize and understand their file systems with these legacy processes and still only make a small dent in the overall effort needed to secure them.

Varonis provides a data security solution that helps organizations gain visibility and control over their file and email systems both on-premises and in the cloud. Its platform uses machine learning and automation to detect threats and rapidly remediate data exposure, ultimately reducing risk and enabling compliance. 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 Varonis Data Security Platform on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four Varonis customers with years of experience using the Data Security Platform. These customers ranged in industry from healthcare to manufacturing.

Key Findings

Quantified benefits. The following risk-adjusted present value (PV) quantified benefits are representative of those experienced by the companies interviewed:

- **Reduced risk of a breach generates $2.1 million in cost avoidance over three years.** Increased visibility into what data is vulnerable and who is accessing sensitive files enables organizations to reduce their attack surfaces by enabling least privilege. The average data breach exposes 32,000 records with a reported cost to recover of $257 per record across the industries Forrester interviewed. Limiting exposure subsequently lowers the probability of a successful attack, allowing organizations to avoid significant financial risk.
- **More efficient data classification processes and improved ability to remove global access from folders creates $4.8 million in savings.** Customers use Varonis to identify high-risk folders, folders with sensitive data, and folders with global access. Automating this process allows customers to avoid the manual effort of sifting through the vast amounts

ROI
555%

Benefits PV
$7.8 million

NPV
$6.6 million

of data within their various data stores to identify folders containing sensitive data. Organizations can avoid 4.5 hours per folder that would otherwise be spent searching for sensitive data and modifying access permissions to the folder containing it.

- **Reducing the number of unnecessary data restores done annually generates $160,769 in savings.** Prior to investing in Varonis, employees would often mistakenly report a folder as deleted, causing security teams to initiate time-consuming investigations that ultimately resulted in restoring the missing data from a previous backup. The results of this process often left employees recreating significant amounts of work, lowering both their satisfaction and productivity. Varonis gives organizations the ability to track data movement so administrators can locate or restore data faster than they could without Varonis.
- **Reducing the time needed to investigate and respond to security alerts results in $399,513 in time savings.** The threat detection and response capabilities of the Varonis Data Security Platform help organizations quickly identify and respond to potential security threats. Customers use the capabilities provided by Varonis to reduce the amount of time it takes to investigate potential threats and take appropriate action.
- **Efficiencies in data accessing workflows leads to $362,521 in savings over three years.** Organizations using Varonis to provision access to data found that the workflows created with Varonis are efficient and cost-effective. Security analysts are no longer required to navigate complicated folder structures to provision access and can allot these tasks to data owners themselves. Without involvement from security or IT, users can complete these tasks over 2 hours faster.

Unquantified benefits. The interviewed organizations experienced the following benefits, which are not quantified for this study:

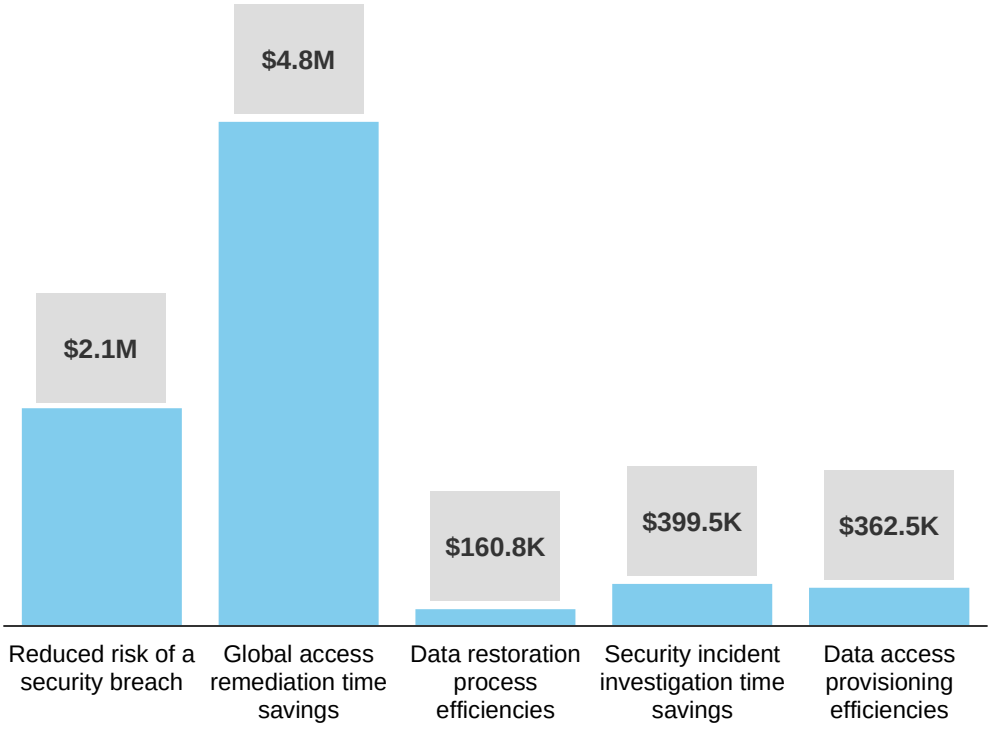
- **Increased employee satisfaction.** Organizations use Varonis to locate misplaced files as opposed to using an older backup eliminates rework, relieving anxieties about the data restoration process and leading to more satisfied employees. Additionally, Varonis enables more junior employees to assist with restoration, allowing security analysts to focus on more pressing and strategic business objectives.
- **Cost and performance efficiencies.** Using Varonis to identify stale data enables organizations to right-size their storage environments. In addition, customers report that they can move data nearing the end of its retention lifespan to less expensive storage options. Decreasing the amount of data in storage environments has the added benefits of increasing the overall performance of the storage environment and reducing the likelihood of a security breach.
- **Increased peace of mind for security teams.** Several customers noted that using Varonis to manage their file systems gives them added peace of mind. The alerts and notifications provided by Varonis as well as the automations they build into their threat detection and response processes make customers more confident in their ability to avoid costly breaches.

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

- **Software license and management costs.** Customers pay Varonis an annual fee for the continuing use of the components of the Data Security Platform.
- **Implementation and management of Varonis.** Organizations had several employees dedicate a portion of their time to implementing and maintaining Varonis. These employees participate in annual training and are responsible for training other users on the Varonis platform. The three-year cost to manage Varonis is $9,950.

Forrester's interviews with four existing customers and subsequent financial analysis found that an organization based on these interviewed organizations experiences benefits of $7.8 million over three years versus costs of $1.2 million, adding up to a net present value (NPV) of $6.6 million and an ROI of 555%.

Benefits (Three-Year)



FORRESTER®

TEI Framework And Methodology

From the information provided in the interviews, 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:

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

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

CUSTOMER INTERVIEWS
Interviewed four organizations using the Varonis Data Security Platform to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION
Designed a composite organization based on characteristics of the interviewed organizations.

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

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.

DISCLOSURES

Readers should be aware of the following:

This study is commissioned by Varonis and delivered by Forrester Consulting. It is not meant to be used as a competitive analysis.

Forrester makes no assumptions as to the potential ROI that other organizations will receive. Forrester strongly advises that readers use their own estimates within the framework provided in the report to determine the appropriateness of an investment in the Varonis Data Security Platform.

Varonis reviewed and provided feedback to Forrester, but Forrester maintains editorial control over the study and its findings and does not accept changes to the study that contradict Forrester's findings or obscure the meaning of the study.

Varonis provided the customer names for the interviews but did not participate in the interviews.

The Varonis Data Security Platform Customer Journey

BEFORE AND AFTER THE VARONIS DATA SECURITY PLATFORM INVESTMENT

Interviewed Organizations

For this study, Forrester conducted four interviews with Varonis Data Security Platform customers. Interviewed customers include the following:

INDUSTRY	ANNUAL REVENUE	INTERVIEWEE	VARONIS PRODUCTS CURRENTLY IN USE
Manufacturing	$1.4 billion	Information security manager	DatAdvantage Data Classification Engine DatAlert Suite Automation Engine Data Transport Engine Policy Pack
Healthcare	$2 billion	Security analyst	DatAdvantage Data Classification Engine DatAlert Suite DataPrivilege
Energy	$5 billion	IT security engineer	DatAdvantage Data Classification Engine DatAlert
Transportation	$3.2 billion	Senior manager of security and compliance	DatAdvantage Data Classification Engine DatAlert

Varonis Data Security Platform Products

Forrester designed a composite organization based on interviewees' experiences to model the benefits and costs of an investment in the Varonis Data Security Platform. The composite organization is reflective of a customer attempting to maximize its investment from the start. Many Varonis customers stated they started their investments with a portion of the platform and expanded over time. The products of the Varonis Data Security Platform used by the composite organization include:

- **DatAdvantage (for Windows).** Provides IT organizations with hybrid cloud visibility and an efficient approach to permissions management, user audits, and file access provisioning.
- **DatAlert.** Uses machine learning and behavioral analytics to surface alerts about suspicious activity and threats to their data.
- **Data Classification Engine (for Windows).** Scans for sensitive data and applies classification rules to improve security and compliance.
- **Automation Engine.** Automatically remediates folders with global access without interrupting access for users with a legitimate need for access.
- **DataPrivilege.** Gives data owners the power to review and manage access controls without IT assistance.

Key Challenges

During the interviews, the customers highlighted several key challenges, which prompted an investment in the Varonis Data Security Platform.

- **Desire to provide better visibility into data on-premises and in the cloud.** Prior to investing in Varonis, the interviewed organizations had minimal understanding of what data they had collected and no ability to monitor who was accessing this data. They wanted to gain better insight into what data their organizations had, who was accessing it, and how much of the data they kept on their data stores was stale. The senior manager of security and compliance for a transportation company explained: "Previously, the security department was very weak here. We did not have many security tools or much visibility into our data. Typically, we would have files getting deleted or folders getting moved and absolutely no insight into who deleted them or where they were moved to."
- **Improve data security to lower the chance of incurring a data breach.** Manual processes limited the ability to restrict access to files with sensitive information. The interviewees were looking for a solution that could help them reduce their attack surfaces and provide faster response to any security threats they encountered. One interviewee noted: "Prior to investing in Varonis, the security team for our organization was new, and we had consultants come in and do a deep dive into our environment, our architecture, what we had, and what we needed. They pointed out some of the data needed classification and securing of files, and that was one of the drivers that led us to Varonis."
- **Streamline the data access provisioning process to reduce inefficiencies in this workflow.** Legacy workflows made the process of provisioning access to the correct user extremely difficult. One interviewee noted: "Prior to Varonis, we had no good way of provisioning access. I was literally just manually going through clicking on folders and provisioning access through traditional provisioning workflows." This highly manual process often led to employees having access mistakenly removed from data required for their day-to-day activities, causing business disruptions and redundant work for administrators.
- **Put ownership of data into the hands of the data users to alleviate the workload of security analysts.** Organizations sought to shift data ownership from their security teams to data owners, allowing the security team to focus on more essential security tasks.

> "Previously, the security department was very weak here. We did not have many security tools or much visibility into our data. Typically, we would have files getting deleted or folders getting moved and absolutely no insight into who deleted them or where they were moved to."
>
> *Senior manager of security and compliance, transportation*

> "Prior to Varonis, we had no good way of provisioning access. I was literally just manually going through clicking on folders and provisioning access through traditional provisioning workflows."
>
> *Security analyst, healthcare*

> "With Varonis, everything is in one interface, and it's super easy to look through users and adjust their access. The confidence level that once you start it will finish, it's very, very high, very few errors. So, the minute you set that all up, you hit 'commit,' you can go ahead and close that ticket."
>
> *Security analyst, healthcare*

Key Results

The interviews revealed that key results from the Varonis Data Security Platform investment include:

- **Limiting data exposure by reducing the attack surface.** By using Varonis to identify files with sensitive data, remediate global access, and respond to potential security threats, organizations limit their exposure, reducing the probability of incurring a data breach. "There were times we found the permissions were lost, and users had visibility into folders they should not be able to see. Varonis really helped us track down who made those changes and when they were applied. Now we've got an extreme level of visibility, and we are able to clean up a lot of files with stale data, where we had credit card information just lying on these file shares and in these folders," noted the senior manager for compliance and security of a transportation company.
- **Creating more efficient data access provisioning processes.** The Varonis Data Security Platform provides organizations a broader view of how data is accessed. Administrators can quickly navigate through folder permissions allowing them to easily fine-tune who can access groups of folders. One interviewee shared: "With Varonis, everything is in one interface, and it's super easy to look through users and adjust their access. The confidence level that once you start it will finish, it's very, very high, there are very few errors. So, the minute you set that all up, you hit 'commit,' you can go ahead and close that ticket."
- **Reducing end user downtime with more effective data restoration methods.** Prior to investing in Varonis, employees would mistakenly submit a request to have their data restored from a backup when they could no longer find a folder. Often these folders had not been deleted but had been moved by another user. The visibility into the data environment provided by Varonis allows organizations to avoid many of these restoration events and reduces the amount of rework that employees have to do when working from a backup. One interviewee highlighted how Varonis has affected this process, saying: "In the past, the service desk would get a call where someone would say, 'Hey, I was accessing some files yesterday in a certain location and when I go out there today, they're not there.' Prior to Varonis, our service desk would immediately initiate the request for restore, which would then potentially put two copies of those files into our environment, because often they're not deleted; they're moved. Now issues are escalated to one of our admins for a lookup, and they do the research in Varonis to understand what happened so that we don't restore the data if we don't need to."
- **Decreasing time needed to investigate potential threats.** Organizations use Varonis threat detection capabilities and increased visibility into user behavior to identify and investigate both internal and external threats more quickly than they could with their existing security tools. The information security manager of a manufacturing organization stated that Varonis had the following impact on the organization's threat investigation processes: "If somebody starts mass deleting files in one of our locations, we are able to run a report and see exactly what folders were deleted. So, rather than manually going through and having to compare to what was there this morning, we are able to automate this process and quickly respond to the alert. That became a 30-minute process instead of something that could have taken half a day."
- **Reducing time spent searching for and identifying sensitive data.** Varonis enables customers to quickly identify sensitive data and restrict access to the folders that contain it. Some interviewees stated that due to the sheer volume of data their organizations collect, trying

"If somebody starts mass deleting files in one of our locations, we are able to run a report and see exactly what folders were deleted. So, rather than manually going through and having to compare to what was there this morning, we are able to automate this process and quickly respond to the alert. That became a 30-minute process instead of something that could have taken half a day."

Information security manager, manufacturing

"Without Varonis, identifying sensitive data would take hours or even multiple days. It's a very tedious process to manually go and look at all the files and folders that are being created. We're talking about thousands and thousands of files and folders. Now, it's basically right in front of me on the dashboard."

Senior manager of security and compliance, transportation

FORRESTER®

to manually classify data would have been impossible without Varonis. One customer highlighted this result: “Without Varonis, identifying sensitive data would take hours or even multiple days. It’s a very tedious process to manually go and look at all the files and folders that are being created. We’re talking about thousands and thousands of files and folders. Now, it’s basically right in front of me on the dashboard.”

Composite Organization

Based on the interviews, Forrester constructed a TEI framework, a composite company, and an associated ROI analysis that illustrates the areas financially affected. The composite organization is representative of the four companies that Forrester interviewed and is used to present the aggregate financial analysis in the next section. The composite organization that Forrester synthesized from the customer interviews has the following characteristics:

Description of composite. The composite organization is a global multibillion-dollar organization headquartered in the United States. The organization has approximately 5,000 employees and collects data from its employees and its customers. This includes sensitive data such as: social security numbers, credit card information, addresses, and GDPR- and CCPA-related information. The composite stores 80 TB data on Windows. The data environment is comprised of 8 million folders and approximately 100 million files. Of these files, approximately 1% contain sensitive information.

Deployment characteristics. The composite organization experienced the same businesses challenges as the interviewed organizations. It participates in a Risk Assessment administered by Varonis on 50% of its production data environment. During the risk assessment, Varonis identifies 500,000 folders with global access and sensitive data in 1% of these folders. In addition, the Risk Assessment identifies a significant amount of stale data being retained by the composite organization. After this initial assessment, the composite deploys the Data Security Platform across its entire data environment. The composite invests in the following Varonis products: DatAdvantage (for Windows), Data Classification Engine (for Windows), DatAlert Suite, Automation Engine, and DataPrivilege. The composite has two dedicated employees who spend a portion of their time managing the solution and has 25 additional IT and security employees who have access to the platform.

Key assumptions

5,000 employees
80 TB of data
100 million total files
1% of files contain sensitive information

Analysis Of Benefits

QUANTIFIED BENEFIT DATA AS APPLIED TO THE COMPOSITE

Total Benefits

REF.	BENEFIT	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Atr	Reduced risk of a security breach	$0	$832,720	$832,720	$832,720	$2,498,161	$2,070,852
Btr	Global access remediation time savings	$1,215,000	$2,673,000	$729,000	$729,000	$5,346,000	$4,795,188
Ctr	Data restoration process efficiencies	$0	$64,648	$64,648	$64,648	$193,943	$160,769
Dtr	Security incident investigation time savings	$0	$160,650	$160,650	$160,650	$481,950	$399,513
Etr	Data access provisioning efficiencies	$0	$145,775	$145,775	$145,775	$437,325	$362,521
	Total benefits (risk-adjusted)	$1,215,000	$3,876,793	$1,932,793	$1,932,793	$8,957,378	$7,788,843

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 composite organization expects risk-adjusted total benefits to be a PV of approximately $7.8 million.

Reduced Risk Of A Security Breach

Interviewees highlighted several ways in which using the Varonis Data Security platform reduces the risk of a security breach:

- Using various Varonis products, organizations limit the number of files in their data ecosystem that have global access. Through use of the Varonis Automation Engine and Classification Engine, organizations easily locate sensitive data and roll back access on these files, restricting users only to data that is relevant to their jobs. Taking these steps lowers the risk of a security breach since, in the event of a malicious attack, the likelihood that a specific user profile has access to data that could compromise the organization has been significantly reduced.
- In addition to locking down access to folders, interviewees identify a significant amount of stale data in their environment. Often this data is past established retention policies but had never been properly removed from the data environment. Eliminating this data further reduces the attack surface in customer environments. One interviewee noted: “With Varonis, we have an extreme level of visibility, and we are able to clean up a lot of files with stale data, where we had credit card information just lying on these file shares and these folders. Because of the nature of our business, we used to store emails, and they would contain our forms, which had the credit card information. So, Varonis was even able to track that kind of information very nicely.”
- The DatAlert Suite increases an organization’s ability to identify potential threats in its data environment. Setting up and fine-tuning security alerts allows customers to identify more potential security threats than they could with their legacy systems. Customers quickly investigate these threats to determine what actions need to be taken. One interviewee highlighted these efficiencies: “With Varonis, we see a lot of activity that might look like potential ransomware because of the

> “Over time, we have dramatically reduced the permissions to data for people who did not need it. In our legacy state, we would have people say, ‘I need a folder out on our share,’ and our security team might not give a thought to who needs access. Now we scrutinize each request to make sure access is only given to people who actually need it.”
>
> *IT security engineer, energy*

name of a file or because of the sheer quantity of files that a user is touching. We're able to get that alert in a matter of minutes, go ahead and look, and, usually, be able to tell a story as to why it is or is not malicious behavior."

For the composite analysis, Forrester assumes that:

- Each year the probability of facing a large-scale security breach is 14.8%.
- The average number of records exposed in an event for US-based companies is 32,434.
- The average cost of a breach is $257 for each customer record exposed, based on interviewed organizations' experiences. This cost is inclusive of direct and indirect costs that organizations incur when they suffer a security breach. These include the cost to investigate the breach and notify customers, as well as legal expenditures and regulatory fines.
- By remediating global access to folders and files and eliminating stale data from its environment, the composite reduces its exposure to a security breach by 60%.
- With faster security detection and response capabilities provided by the Varonis DatAlert Suite, the composite reduces its exposure to a security breach by 15%.

The following risks may affect this benefit category:

- The cost per record lost in a security breach will vary by industry and geography.
- The impact of Varonis on security threat detection and response will vary based on the sophistication of existing security solutions other than Varonis.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year risk-adjusted total PV of $2,070,852.

Using the Varonis Data Security Platform reduces exposure to potential threats by 75%.

Impact risk is the risk that the business or technology needs of the organization may not be met by the investment, resulting in lower overall total benefits. The greater the uncertainty, the wider the potential range of outcomes for benefit estimates.

Reduced Risk Of A Security Breach: Calculation Table

REF.	METRIC	CALCULATION	INITIAL	YEAR 1	YEAR 2	YEAR 3
A1	Average number of records exposed in a breach for US companies	Ponemon		32,434	32,434	32,434
A2	Average per record cost to organizations for stolen data	Ponemon		$257	$257	$257
A3	Average cost of breach	A1*A2		$8,335,538	$8,335,538	$8,335,538
A4	Probability of a breach in a given year	Ponemon		14.8%	14.8%	14.8%
A5	Reduced exposure by remediating global access	Interviews		60%	60%	60%
A6	Reduced exposure by improving detection and response practices	Interviews		15%	15%	15%
A7	Total reduction in exposure to a data breach	A5+A6		75%	75%	75%
At	Reduced risk of a security breach	A3*A4*A7	$0	$925,245	$925,245	$925,245
	Risk adjustment	↓10%				
Atr	Reduced risk of a security breach (risk-adjusted)		$0	$832,720	$832,720	$832,720

Global Access Remediation Time Savings

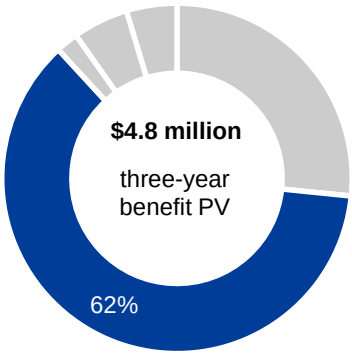
Interviewees highlighted several ways in which the Varonis Data Security platform improves the ability to remediate global access:

- One of the largest areas of benefit that Varonis provides is the ability to quickly identify sensitive data and limit who can access it. Most organizations store credit card and social security numbers, addresses, and other personal information for both their employees and their customers. After years of permissions being rolled forward, they had minimal insight into where this information was being stored or who was accessing it. Often, they stored this information in a folder that had no restrictions on who could access it. Searching for these folders was a time-consuming process and often proved to be an impossible task. The senior manager of security and compliance for a transportation company said: "If I were to look at all our data and try and find the sensitive information, it would take multiple days. It's a very tedious process to manually go and look at all the files and folders that are being created. We're talking about thousands and thousands of files and folders."
- Varonis can identify which files contain sensitive information in a matter of seconds after it is deployed across a data set. Using the same capabilities that allow customers to quickly provision access to data, Varonis can also restrict access to files with sensitive information. One interviewee noted: "If we're talking about folders with sensitive information, I can tell you that I personally had access to folders with sensitive information I should not have had access to, and this was common across our organization. We were at risk of exposure from either information disclosure or ransomware. I went from having access to 200 folders with this information to three." Restricting access to folders with sensitive information lowers the attack surface of customers' data environments, allows customers to maintain compliance with industry and government regulations, and removes the burden of searching for sensitive data from their security teams.

For the composite analysis, Forrester assumes that:

- The organization uses the Varonis solution to understand who in the organization has access to files and folders as well as which folders contain sensitive information.
- Varonis' Risk Assessment identifies 500,000 folders with global access, 1% of which it deems high-risk. Upon deploying the solution across the entire data environment, Varonis identifies additional folders with global access. The composite works to remediate access to these remaining folders while also monitoring and correcting access on new folders that are created during the modeled time frame.
- The composite works with Varonis' professional services team to remediate access to the initial 500,000 folders. The organization remediates access to an additional 1.1 million folders in Year 1. The composite remediates access to 300,000 folders in both Years 2 and 3. These represent folders that remain from legacy provisioning workflows and also folders that were created annually.
- The composite organization had made previous attempts to identify and remediate access to folders containing highly sensitive data; however, this process proved to be too time-consuming. Without a specialized solution like Varonis, it would take at least 4.5 hours, on average, to locate and remediate access to a single folder.

> "If I were to look at all our data and try and find the sensitive information, it would take multiple days. It's a very tedious process to manually go and look at all the files and folders that are being created. We're talking about thousands and thousands of files and folders."
>
> *Senior manager of security and compliance, transportation*



Global access remediation time savings: 62% of total benefits

FORRESTER®

- The composite only attempts to remediate global access on the 1% of folders that pose a major security risk.
- The average hourly compensation for a security analyst responsible for this task is $60.

The following risks may affect this benefit category:

- The number of folders with global access in a company's file systems prior to deploying Varonis.
- The amount of sensitive data stored in a company's file system.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year risk-adjusted total PV of $4,795,188.

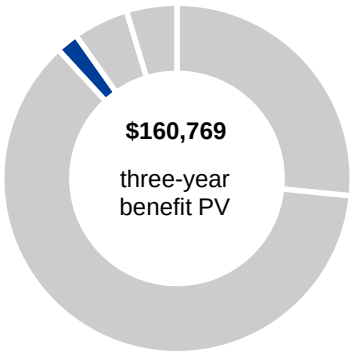
Global Access Remediation Time Savings: Calculation Table

REF.	METRIC	CALCULATION	INITIAL	YEAR 1	YEAR 2	YEAR 3
B1	Folders with global access remediated with Varonis	Interviews	500,000	1,100,000	300,000	300,000
B2	Percentage of folders containing sensitive information	Interviews	1%	1%	1%	1%
B3	Time required to identify and remediate global access without Varonis (hours)	Interviews	4.5	4.5	4.5	4.5
B4	Hourly compensation of security analysts responsible for global access remediation	Assumption	$60	$60	$60	$60
Bt	Global access remediation time savings	B1*B2*B3*B4	$1,350,000	$2,970,000	$810,000	$810,000
	Risk adjustment	↓10%				
Btr	Global access remediation time savings (risk-adjusted)		$1,215,000	$2,673,000	$729,000	$729,000

Data Restoration Process Efficiencies

Interviewees highlighted several ways in which using the Varonis Data Security Platform creates efficiencies in data restoration processes:

- Prior to investing in the Varonis Data Security Platform, organizations frequently ran into situations where employees were unexpectedly moving or deleting files. With minimal ability to track where these files were moved, employees would submit requests to have their data restored from a previous backup. Security admins would initiate a lengthy restoration process to restore a user's data from their last backup. However, often the files were not deleted but simply moved to a different location. "Back before we started using Varonis to do this, somebody would be missing data, and they would open up a ticket, and they would look for it and say, 'We don't know what happened; somebody deleted it.' Well, nine times out of 10, it wasn't deleted; it was moved," explained one interviewee. These unnecessary restores were not only a waste of resources, but they also created duplicate files in the system, confusing users and increasing the attack surface of the data environment.
- Data restoration could also lead to lost productivity for employees. One customer described the inefficiencies in this process that led to significant amounts of downtime: "Admins may not have seen that request for 24 hours since they're not working in a queue, and they're working tickets as they come in. So, I'll say anywhere from 2 to 24 hours later, they're seeing it, and then spending time to do the



Data restoration process efficiencies: 2% of total benefits

FORRESTER®

research. Then it must go over to the guys who do the data restore. That could take another half a day to a day before they see it. You're talking a potential of a day to two days later before that data is restored if it's not an emergency." Once data was restored, employees would then have to recreate work that was lost between the time of the most recent backup and the time when the file was moved, further limiting their productivity and adding to the cost of these events.

- Varonis enables customers to track data movement and identify situations where a user moves a folder to a new location. This allows them to point employees to the correct place without going through the restore process. An added benefit of this increased visibility is that organizations have been able to shift the burden of investigating help desk tickets of this nature to more junior staff. A security analyst for a healthcare organization said: "We were able to push that level of research to the tech zone. Now when someone calls up and says, 'Hey, I got an issue; these files aren't there anymore; they were there a couple of days ago; today they're not,' the service desk can look into it and say, 'Bob Smith moved them into this folder a day and a half ago; you might want to talk to him about it.' It's an immediate response."

For the composite analysis, Forrester assumes that:

- The composite organization generates 350 tickets annually where employees are reporting missing or deleted data.
- Prior to investing in Varonis, these situations involved a significant amount of waiting and downtime. The actual time spent on the investigation and restoration process was approximately 2 hours per request. The security analyst team investigated these requests. The average hourly compensation for a security analyst is $60.
- With Varonis, the composite organization reduces the time it spends on these requests to only the time it takes to locate the missing file. On average, this process takes approximately 30 minutes. More junior employees complete these investigations. The average hourly compensation for junior employees responsible for these tasks is $34.
- In legacy workflows where a ticket reporting missing data was solved by restoring a user's data from their latest backup, users had to make up an average of 4 hours' worth of work per incident.
- Many of the requests to restore data involve documents that are being collaborated on by multiple users. As a result, these events affect 400 employees annually.
- The average hourly compensation for an employee affected by these incidents is $40.
- Not all saved time is repurposed for additional work. To capture the value of repurposed time, Forrester conservatively assumes a 50% productivity capture.

The following risks may affect this benefit category:

- Company polices on data restoration processes and the frequency at which users back up their data.
- Organization's abilities to find and locate data that has been moved by users.

To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year risk-adjusted total PV of $160,769.

"We were able to push that level of research to the tech zone. Now when someone calls up and says, 'Hey, I got an issue; these files aren't there anymore; they were there a couple of days ago; today they're not,' the service desk can look into it and say, 'Bob Smith moved them into this folder a day and a half ago; you might want to talk to him about it.' It's an immediate response."

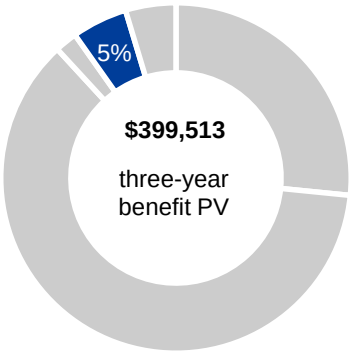
Security analyst, healthcare

Data Restoration Process Efficiencies: Calculation Table						
REF.	METRIC	CALCULATION	INITIAL	YEAR 1	YEAR 2	YEAR 3
C1	Requests to restore data annually	Interviews		350	350	350
C2	Time to restore data prior to Varonis (hours)	Interviews		2	2	2
C3	Hourly compensation of security admins responsible for data restoration	Assumption		$60	$60	$60
C4	Cost to restore data without Varonis	C1*C2*C3		$42,000	$42,000	$42,000
C5	Time to restore data with Varonis (hours)	Interviews		0.5	0.5	0.5
C6	Hourly compensation of junior employees responsible for data restoration	Assumption		$34	$34	$34
C7	Cost to restore data with Varonis	C1*C5*C6		$5,950	$5,950	$5,950
C8	Reduced cost to restore lost data	C4-C7		$36,050	$36,050	$36,050
C9	Employees affected annually	Interviews		400	400	400
C10	Average hours of lost productivity recovered per request	Interviews		4	4	4
C11	Average employee hourly compensation	Assumption		$40	$40	$40
C12	Productivity capture	Assumption		50%	50%	50%
C13	Reduced cost of end user downtime	C9*C10*C11*C12		$32,000	$32,000	$32,000
Ct	Data restoration process efficiencies	C8+C13	$0	$68,050	$68,050	$68,050
	Risk adjustment	↓5%				
Ctr	Data restoration process efficiencies (risk-adjusted)		$0	$64,648	$64,648	$64,648

Security Incident Investigation Time Savings

Interviewees highlighted several ways that the Varonis Data Security platform improves their threat detection workflows:

- Organizations use the Varonis DatAlert Suite to improve their threat detection processes. Varonis tracks the actions of individual users to build out a profile of expected user behavior. When a user does something that does not match their usual behavior, an alert is triggered and sent to security teams. One interviewee shared the following anecdote to describe the effectiveness of this process: “We had somebody who had just moved from the US to Europe, and they were copying all their old files. They just wanted access to their old file server. In the process, they were accessing a bunch of stuff that they don’t really need to be accessing. So, we were able to quickly identify this alert and shut that down.”
- In addition to increased threat detection capabilities, Varonis makes it easier to investigate the security incidents that it provides to customers. In cases where an unknown entity is deleting or accessing significant amounts of files, security analysts can quickly see what files are being affected, compare these actions to expected behavior patterns, and respond accordingly. One interviewee described: “Varonis allows us to do investigations and analysis of things that we could not do previously. Our old system for investigating threats was fine, but Varonis is so much better. They are so much faster, so much more responsive. It’s easier to pivot and look at that data. You don’t have to rerun reports; the data is just queried live, which is a large time saver for us.”



Security incident investigation time savings: 5% of total benefits

FORRESTER®

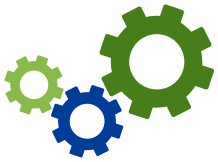
For the composite analysis, Forrester assumes that:

- Prior to investing in Varonis, the security analyst team would collectively spend approximately 12 hours investigating a security incident to determine if was a legitimate threat or a false positive.
- With the insights provided by the DatAlert Suite, the team needs just 90 minutes to investigate and understand an incident.
- The organization receives 300 security incidents through Varonis annually.
- The average hourly compensation for a security analyst is $60.

The following risks may affect this benefit category:

- Additional security solutions that organizations have in place.
- The number of security analysts required to investigate an alert.

To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year risk-adjusted total PV of $399,513.



Customers reduce alert investigations by 10.5 hours per alert.

Security Incident Investigation Time Savings: Calculation Table

REF.	METRIC	CALCULATION	INITIAL	YEAR 1	YEAR 2	YEAR 3
D1	Security incidents investigated annually	Interviews		300	300	300
D2	Average time spent investigating security incidents without Varonis (hours)	Interviews		12	12	12
D3	Average time spent investigating security incidents with Varonis (hours)	Interviews		1.5	1.5	1.5
D4	Hourly compensation of security analysts responsible for alert investigation	Assumption		$60	$60	$60
Dt	Security incident investigation time savings	D1*(D2-D3)*D4		$189,000	$189,000	$189,000
	Risk adjustment	↓15%				
Dtr	Security incident investigation time savings (risk-adjusted)		$0	$160,650	$160,650	$160,650

Data Access Provisioning Efficiency

Interviewees highlighted several ways in which using the Varonis Data Security Platform creates efficiencies in data access provisioning:

- Prior to investing in Varonis, provisioning access to data was a very manual and time-consuming activity. The workflows around these requests required lengthy investigations by security analysts and would often lead to incorrectly provisioning data to users or mistakenly turning off access for users with a legitimate need.
- One interviewee highlighted these inefficiencies: “Prior to Varonis, you would actually have to not only give access to the folder in question but then go up that tree to figure out where the inheritance is turned on. We would be stuck trying to figure out who may need access to a folder three levels down, but then you find out they can’t access a folder on level 2, and they only need read access on the third level. You had to provision all those separately, and you needed to wait for one to finish before the other one even starts. So, depending on the size of the folder, it could take hours or overnight to set up the top level, then you had to go back to fix the bottom level. So, we’re talking about hours if not days for this kind of process.”

› Additionally, this process no longer requires extensive investigation by the security team to complete. Organizations can relieve their security analysts of data provisioning responsibilities, allowing them to focus on higher-priority security initiatives.

For the composite analysis, Forrester assumes that:

› The composite organization processes 1,000 data provisioning access requests annually.

› Prior to using Varonis, organizations spent an average of 3 hours per request manually provisioning access to data and remediating any issues that arose during the process. The security team completed these requests; the average hourly compensation for a security team member is $60.

› With Varonis, the time to complete an access request decreases to 15 minutes, and data owners are responsible for completing these requests. The average hourly compensation for a junior employee is $34.

The following risks may affect this benefit category:

› The number of provisioning requests an organization fields each year.

› The amount of automation organizations had in their data access provisioning workflows prior to investing in the Varonis Data Security Platform.

› The fully loaded compensation of security team members and junior employees.

To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year risk-adjusted total PV of $362,521.

Using Varonis to provision data access saves organizations 2.75 hours per request.

Data Access Provisioning Efficiencies: Calculation Table

REF.	METRIC	CALCULATION	INITIAL	YEAR 1	YEAR 2	YEAR 3
E1	Number of data provisioning requests per year	Interviews		1,000	1,000	1,000
E2	Time to provision data prior to investing in Varonis (hours)	Interviews		3	3	3
E3	Hourly compensation of security analysts responsible for data provisioning	Assumption		$60	$60	$60
E4	Cost to provision data without Varonis	E1*E2*E3		$180,000	$180,000	$180,000
E5	Time to provision data with Varonis (hours)	Interviews		0.25	0.25	0.25
E6	Hourly compensation of junior employees responsible for data provisioning	Assumption		$34	$34	$34
E7	Cost to provision data with Varonis	E1*E5*E6		$8,500	$8,500	$8,500
Et	Data access provisioning efficiencies	E4-E7	$0	$171,500	$171,500	$171,500
	Risk adjustment	↓15%				
Etr	Data access provisioning efficiencies (risk-adjusted)		$0	$145,775	$145,775	$145,775

Unquantified Benefits

The interviewed organizations experienced the following benefits, which are not quantified for this study:

- **Increased employee satisfaction.** Automating manual processes and transferring work to the help desk allows the security team to focus on more pressing and strategic priorities. Additionally, Varonis makes the average user's experience better. Employees spend less time waiting to get access to the data they need to complete their jobs, allowing them to be more efficient and productive. One interviewee noted: "We are not sending access requests over to somebody just to be stuck waiting in their queue. With Varonis, we send the ticket to the queue and are getting almost an immediate resolution."
- **Cost and performance efficiencies.** Customers identify and eliminate significant amounts of stale data by deploying Varonis across their file systems. Organizations either delete a large portion of this data or move it to less expensive storage options before deleting it. One interviewee described this process: "We were able to flush out a lot of old stale data, especially data that was eight to 10 years old. While we were not able to retire any hardware, we did regain some space on our servers, which was a large benefit." Freeing up space on file servers allows organizations to perform backups faster and restore data in a timelier manner when necessary.
- **Increased peace of mind for security teams.** The increased security provided by Varonis brings organizations peace of mind as they know even in the event of a breach, Varonis allows them to quickly understand the scope of the breach and recover affected data more quickly. One interviewee noted: "For me, Varonis brings peace of mind. I know that if somebody tries to delete a bunch stuff or somebody tries to affect a bunch of files, we're going to be able to quickly identify them and stop them thanks to Varonis."

> "We are not sending access requests over to somebody just to be stuck waiting in their queue. With Varonis, we send the ticket to the queue and are getting almost an immediate resolution."
>
> *IT security engineer, energy*

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 the Data Security Platform and later realize additional uses and business opportunities, including:

- **Using Varonis for managing data in the cloud.** All interviewed customers were still early in their migrations to the cloud but stated that Varonis would be an integral part of their migrations and ongoing monitoring. They expect the efficiencies they experience using Varonis on-premises to translate to the cloud and in certain circumstances to increase. One interviewee noted: "In the cloud, Varonis will give us the same capabilities that we have with our current file system. The only difference is that our cloud provider does not give any visibility into how data is being shared or what kind of permission it has. So, Varonis will be providing us that information."
- **Detecting more threats across the kill chain.** Varonis Edge enhances DatAlert by analyzing metadata from perimeter technologies like DNS servers, VPN concentrators, and web proxies to spot signs of attack at the perimeter. It detects attacks like malware, APT intrusion, and exfiltration in context with activity and alerts on core data stores and infrastructure.

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.

- **Automating threat response.** Some users are beginning to utilize Varonis not only to receive security alerts but to also automate the response to these alerts. Automating responses to alerts enables security analysts to become increasingly efficient, and they can focus on the highest-level threats and let the Data Security Platform respond to lower-priority security alerts.
- **Streamlining entitlement reviews.** DataPrivilege ensures that access to groups, distribution lists, and business data is consistently reviewed by the right people. Entitlement reviews are delivered directly to data owners, which lets them see who currently has access to their data and make changes without any involvement from IT. Machine learning algorithms flag users that probably shouldn't have access anymore, making reviews quick and easy.
- **Using Varonis to automate and enforce classification policies.** Customers plan to use Varonis' data classification capabilities to automate their data classification processes. Automatically restricting sharing and access to certain files will further increase the overall security of data systems and will also reduce the amount of time organizations will spend remediating access to folders.

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 AS APPLIED TO THE COMPOSITE

Total Costs

REF.	COST	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Ftr	Varonis software cost	$0	$474,128	$474,128	$474,128	$1,422,384	$1,179,086
Gtr	Implementation and management of Varonis	$2,728	$2,904	$2,904	$2,904	$11,440	$9,950
	Total costs (risk-adjusted)	$2,728	$477,032	$477,032	$477,032	$1,433,824	$1,189,036

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 composite organization expects risk-adjusted total costs to be a PV of nearly $1.2 million.

Varonis Software Cost

The composite participates in the Varonis Risk Assessment as part of the proof of concept. Upon completion of the proof of concept, the composite deploys Varonis across its entire file system.

The composite deploys the Varonis base product DatAdvantage as well as the DatAlert Suite, Data Classification Engine, Automation Engine, and DataPrivilege. The composite pays $474,128 each year for the license fees to use these products. This price includes a fee paid to Varonis to connect its various data storage platforms and to pull events and other metadata into the main Varonis platform server.

The investment made by the composite is reflective of a customer attempting to maximize its Varonis investment in Year 1. Many Varonis customers stated they started their investment with a portion of the platform and expanded their investment to additional products over time.

Forrester did not apply a risk adjustment to the cost of software costs as Varonis provided the cost of the product suite the composite deploys. They are representative of costs other organizations can expect to incur for a similar configuration of products.

The three-year total PV for the Varonis software license is $1,179,086.

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.

Varonis Software Cost: Calculation Table

REF.	METRIC	CALCULATION	INITIAL	YEAR 1	YEAR 2	YEAR 3
Ft	Varonis software cost		$0	$474,128	$474,128	$474,128
	Risk adjustment	0%				
Ftr	Varonis software cost (risk-adjusted)		$0	$474,128	$474,128	$474,128

Implementation And Management Of Varonis

The composite incurs costs for implementation and operationalization of the Varonis Data Security Platform.

- The composite dedicates two employees to lead the implementation of Varonis. These employees spend 16 hours planning for and implementing Varonis. They spend an additional 15 hours upfront training to use the solution and preparing training materials for their colleagues.

- In Year 1, 25 employees receive training on the Varonis platform. This includes a mixture of both security analysts and IT help desk administrators. Each employee spends approximately 2 hours training in Year 1 and attends 2 hours of training in subsequent years to learn about new platform capabilities and other solution improvements.
- The average hourly compensation for employees involved in the implementation and training process is $40.
- The composite organization relies on two employees for the ongoing management of the Varonis Data Security Platform. These employees spend approximately 8 hours of their time monitoring the platform each year.

This cost will vary based on the following risk factors.

- The complexity of the deployment.
- The level of expertise required to successfully deploy the solution.
- The number of employees who are trained to use the Varonis Data Security Platform.

To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year risk-adjusted total PV of $9,950.

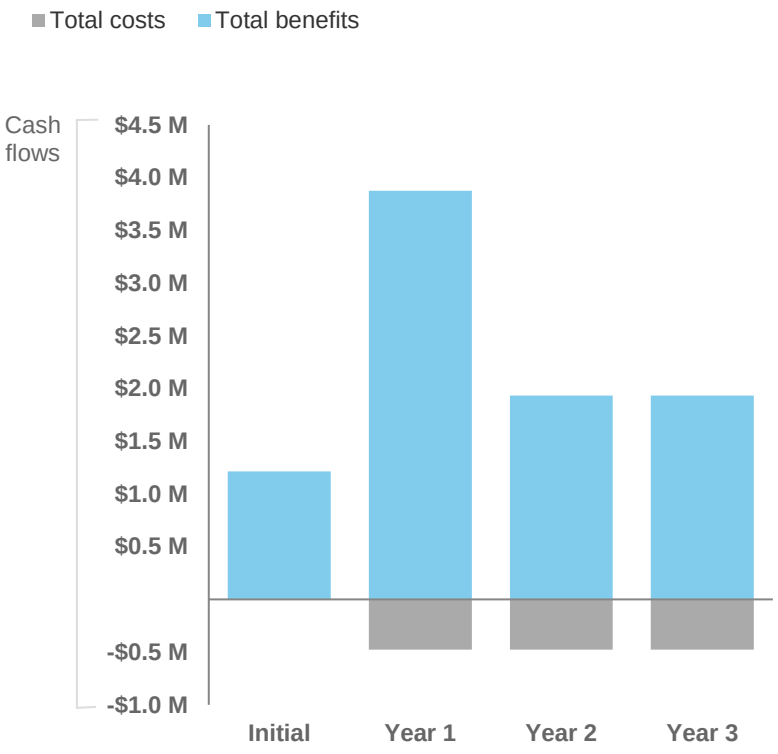
Implementation And Management Of Varonis: Calculation Table

REF.	METRIC	CALCULATION	INITIAL	YEAR 1	YEAR 2	YEAR 3
G1	FTEs dedicated to managing system		2			
G2	Total time spent implementing Varonis (hours)		16			
G3	Hourly compensation of dedicated FTE		$40			
G4	Cost to implement Varonis	G1*G2*G3	$1,280			
G5	Hours spent training to use Varonis		15	2	2	2
G6	Number of FTEs involved in training		2	25	25	25
G7	Cost to train employees on Varonis	$G3_{Initial}$*G5*G6	$1,200	$2,000	$2,000	$2,000
G8	FTEs dedicated to managing system			2	2	2
G9	Hours spent managing system annually			8	8	8
G10	Cost to manage Varonis	$G3_{Initial}$*G8*G9		$640	$640	$640
Gt	Implementation and management of Varonis	G4+G7+G10	$2,480	$2,640	$2,640	$2,640
	Risk adjustment	↑10%				
Gtr	Implementation and management of Varonis (risk-adjusted)		$2,728	$2,904	$2,904	$2,904

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 composite 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 Analysis (risk-adjusted estimates)

	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Total costs	($2,728)	($477,032)	($477,032)	($477,032)	($1,433,824)	($1,189,036)
Total benefits	$1,215,000	$3,876,793	$1,932,793	$1,932,793	$8,957,378	$7,788,843
Net benefits	$1,212,272	$3,399,761	$1,455,761	$1,455,761	$7,523,554	$6,599,807
ROI						555%

FORRESTER®

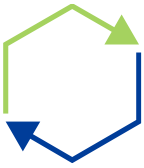
Appendix A: Total Economic Impact

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.

FORRESTER®

VARONIS

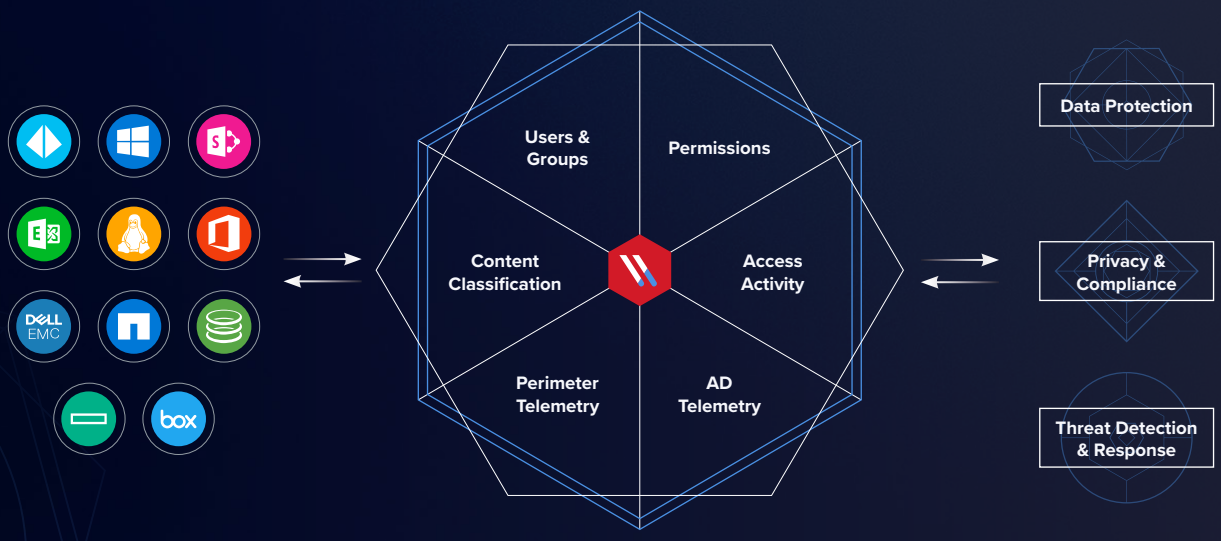
Data Security Platform

The most powerful way to find, monitor, and protect sensitive data on premises and in the cloud

Gain visibility into your critical data and infrastructure

Combine multiple data streams to discover security risks

Solve board-level data security problems at scale with automation



Rapidly reduce risk, detect advanced threats, and prove compliance

"We completely eradicated our global access problem (over 40,000 sensitive folders open to everyone) in 17 days without breaking anything. I couldn't believe it."

CISO
Major Online Retailer

"Detection, prevention, and investigation are all inter-related. **No other solution does all three as well as Varonis."**

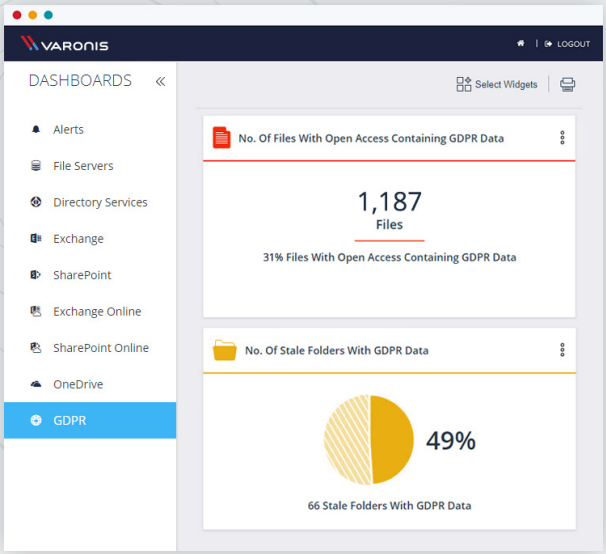
SECURITY ENGINEER
Major U.S. Energy Provider

"Varonis helps our team identify incidents faster when users gain access to files to which they shouldn't have access. Before Varonis, no one knew which users had permission to which data."

TECHNICAL ENGINEER
Rabobank

Data Protection

- Prioritizes and fixes permissions exposures
- Tracks all data access activity
- Automates authorization, migration, and deletion
- Visualizes risk across hybrid environments

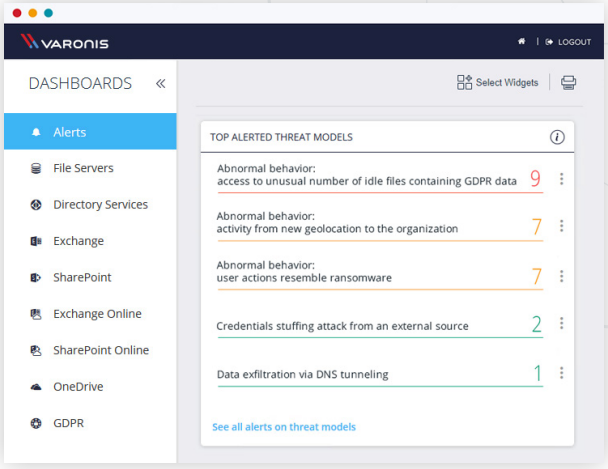


Privacy & Compliance

- Finds and classifies data with hundreds of built-in rules
- Prioritizes based on sensitivity, exposure, and activity
- Labels or quarantines sensitive data
- Enables Data Subject Access Request (DSAR) for unstructured data

Threat Detection & Response

- Analyzes the right telemetry from data, directory services, DNS, and edge devices
- Builds the right context about users, roles, devices, and data
- Makes forensics intuitive and conclusive
- Decreases time to detect and time to respond



Appendix B: Endnotes

[1] Source: “Business Technographics Global Security Survey,” Forrester Research, Inc., 2019.