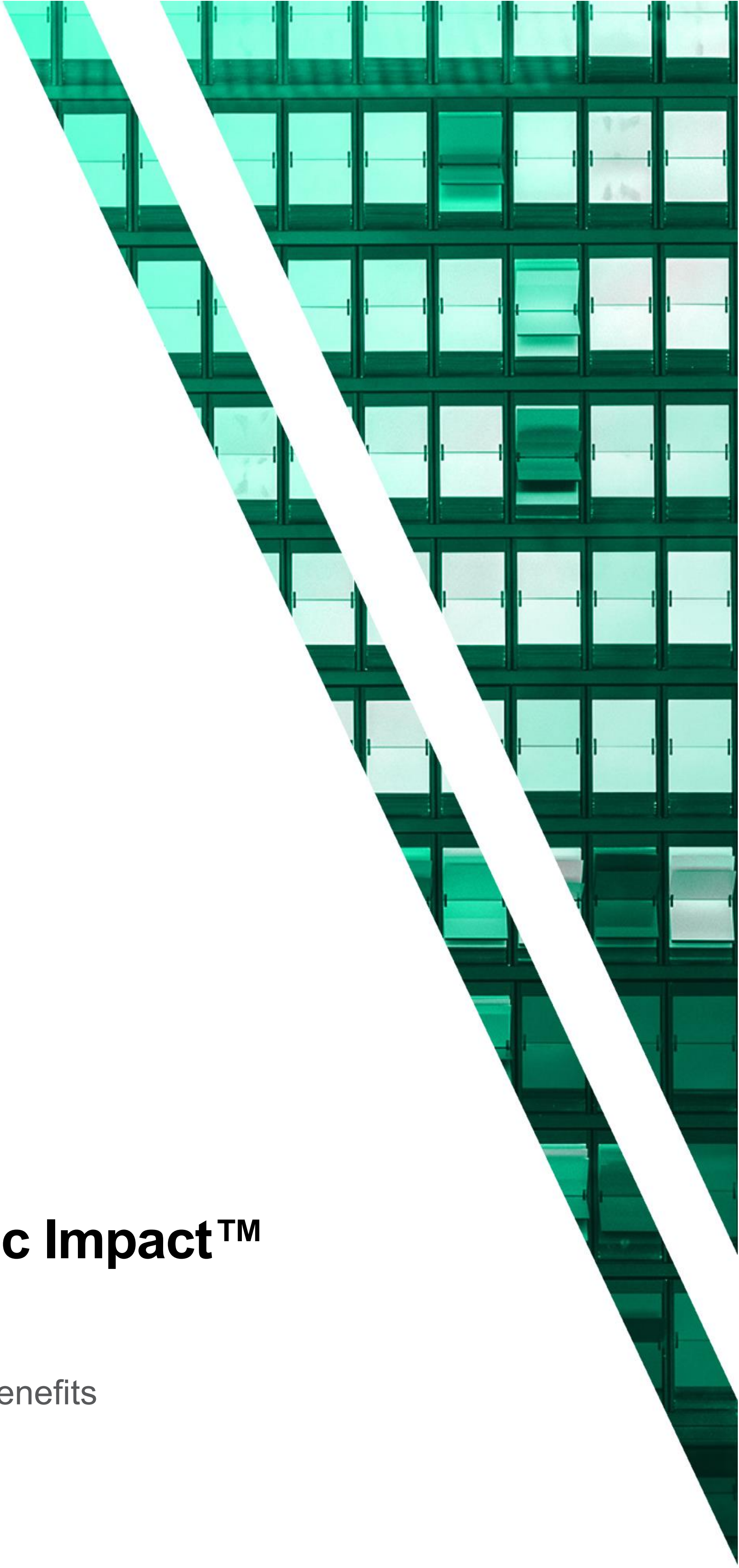
FORRESTER®



The Total Economic Impact™ Of Cisco Duo

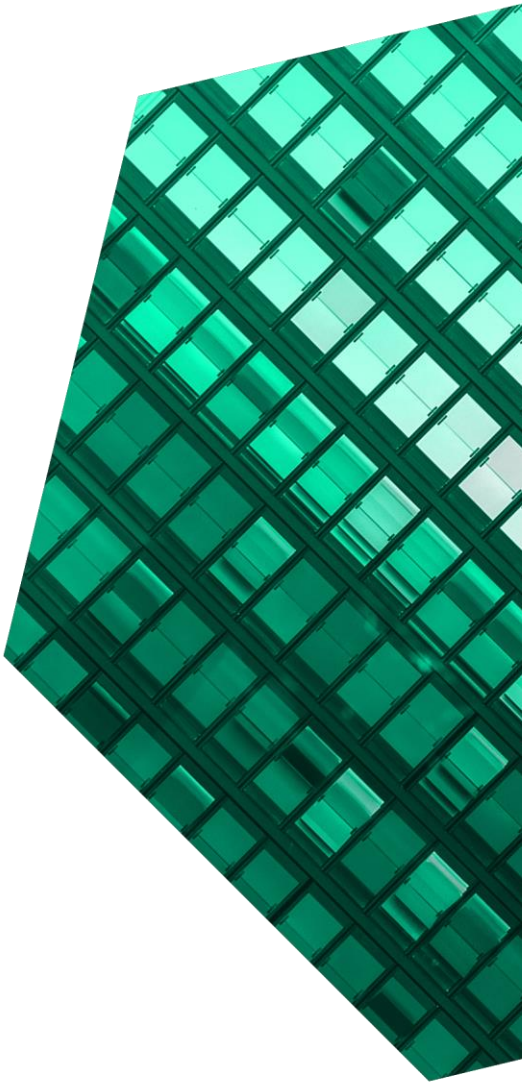
Cost Savings And Business Benefits Enabled By Duo

FEBRUARY 2023

A FORRESTER TOTAL ECONOMIC IMPACT™ STUDY COMMISSIONED BY CISCO

Table Of Contents

Consultant: *Mary Anne North*



ABOUT FORRESTER CONSULTING

Forrester provides independent and objective research-based consulting to help leaders deliver key transformation outcomes. Fueled by our customer-obsessed research, Forrester's seasoned consultants partner with leaders to execute on their priorities using a unique engagement model that tailors to diverse needs and ensures lasting impact. For more information, visit forrester.com/consulting.

Executive Summary

Implementing Duo produced time savings for end users, help desk staff, security analysts, and other IT staff compared to the organizations' prior solution. Duo also decreased those organizations' risk of a credentials-related security breach by providing better intelligence around all authentication attempts, simplifying the comprehensive and consistent application of security policies, and enabling proactive identification of authentication vulnerabilities.

Cisco Secure Access by Duo secures access to applications in the cloud or on-premises by using multifactor authentication (MFA), passwordless authentication, single sign-on, and device posture checks to authenticate the identity of end users seeking to access those applications. This provides visibility into each authentication attempt, including the security status of the multiple devices that may be associated with each end user's account. Duo also simplifies an organization's enforcement of access security policies across the enterprise while adapting to user, device, and application risk.

Cisco commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Duo.[1] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Duo on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed five representatives at four organizations with experience using Duo. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization that is a global company with annual revenue of $3 billion and 10,000 user accounts protected by Duo.

KEY STATISTICS

Return on investment (ROI)
159%

Net present value (NPV)
$3.23M

Prior to deploying Duo, the interviewees' organizations either addressed credentials-related security (including authentication) with another solution, or protected access to applications using only static passwords. However, these prior approaches produced inadequate intelligence around access attempts, didn't sufficiently protect against data losses from a credentials-related security breach, and created additional costs in the form of productivity drags on end users, help desk staff, security analysts, and other IT staff.

After the investment in Duo, the interviewees' organizations saved time for end users, help desk staff, security analysts, and other IT staff. They also reduced their risk of a credentials-related security breach because of the intelligence Duo provided and their more rigorous application of access-related security policies.

KEY FINDINGS

Quantified benefits. Three-year, risk-adjusted present value (PV) quantified benefits for the composite organization include:

- **Reduced risk of a credentials-related security breach, valued at $792,000.** By deploying Duo, the composite organization reduces its risk of a credentials-related security breach because of the intelligence Duo delivers around authentication attempts, Duo's extensive capabilities around authentication-related security and security policies, and the ease of applying those authentication-related security policies across the organization.
- **Savings of $671,000 from security analyst productivity improvement.** Because of Duo's easy navigation, integration with other applications, and detailed information about each authentication attempt, security analysts at the composite organization spend less time troubleshooting and investigating potential security issues arising from suspicious login attempts.
- **End-user time savings from streamlined authentication, valued at $3.2 million.** For the composite organization's end users, Duo saves time on each authentication request compared to their prior authentication solution.
- **Savings of $235,000 from avoided costs of a prior authentication solution.** Moving to Duo eliminates the composite organization's ongoing expenses for annual maintenance and support fees on the previous solution, and its costs to purchase new replacement devices at periodic intervals for end users.
- **Savings of $326,000 from avoided costs for management and support of a prior authentication solution.** Since Duo is simpler to manage and support than the composite organization's previous solution, the organization's staff spends less time administering the solution, deploying additional functionality, adding new use cases, and optimizing Duo's use. It also eliminates expenses for professional services it previously needed to fill internal expertise gaps.
- **Savings of $57,000 from help desk and end-user productivity improvements due to fewer authentication-related support cases.** Duo simplifies end users' authentication process and eliminates their need for a separate authentication device. As a result, fewer authentication-related cases reach the composite organization's help desk, saving time for end users and help desk staff.

Unquantified benefits. Benefits that provide value for the composite organization but are not quantified in this study include:

- **Better end-user experience.** Interviewees noted end users found Duo easy to use and saved time and frustration on each authentication compared to their prior authentication solutions.
- **Ease of further improving the user experience with Duo's single sign-on (SSO**). Interviewees' organizations that opted to use an SSO provided Duo users with a simplified and consistent login experience for all applications integrated with Duo**.**
- **Audit and regulatory compliance efficiencies.** Duo's auditing data and user activity reports enabled automation of some audit reports.
- **Enhanced ability to acquire new customers or partners.** Duo brand recognition provided a comfort level for customers and partners.
- **Vendor rationalization**. Interviewees whose organizations had already used other Cisco products valued not having to add and manage another vendor.

- **Duo's moderate learning curve and the value of Duo Care premium support**. End users and IT staff alike found Duo easy to use, and Duo Care a helpful resource.

Costs. Three-year, risk-adjusted PV costs for the composite organization include:

- **Cisco fees of $1.7 million.** Cisco fees include subscription fees for the Access version of Duo, and Duo Care fees for additional services beyond the standard support included with Duo.
- **Internal effort of $340,000 for implementation, management, and support.** The composite organization implements Duo and manages and optimizes it on an ongoing basis using an internal IT team along with guidance from a Duo Care team.

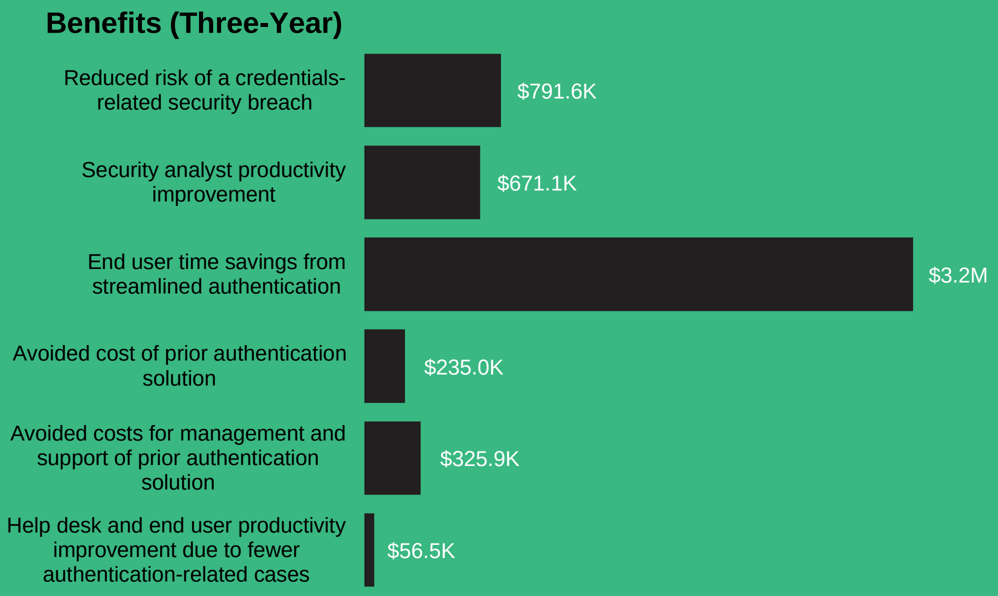
The representative interviews and financial analysis found that a composite organization experiences benefits of $5.26 million over three years versus costs of $2.03 million, adding up to a net present value (NPV) of $3.23 million and an ROI of 159%.

ROI
159%

BENEFITS PV
$5.26M

NPV
$3.23M

PAYBACK
<6 months



> **“Duo’s layered approach to security and security policies provides capabilities that our previous product just didn’t have. The much richer data we can analyze now is of course improving our security by far.”**
>
> — Security technical lead, professional services

TEI FRAMEWORK AND METHODOLOGY

From the information provided in the interviews, Forrester constructed a Total Economic Impact™ framework for those organizations considering an investment in Duo.

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 Duo can have on an organization.

Forrester Consulting conducted an online survey of 351 cybersecurity leaders at global enterprises in the US, the UK, Canada, Germany, and Australia. Survey participants included managers, directors, VPs, and C-level executives who are responsible for cybersecurity decision-making, operations, and reporting. Questions provided to the participants sought to evaluate leaders' cybersecurity strategies and any breaches that have occurred within their organizations. Respondents opted into the survey via a third-party research panel, which fielded the survey on behalf of Forrester in November 2020.

DISCLOSURES

Readers should be aware of the following:

This study is commissioned by Cisco 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 study to determine the appropriateness of an investment in Duo.

Cisco 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.

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

DUE DILIGENCE

Interviewed Cisco stakeholders and Forrester analysts to gather data relative to Duo.

INTERVIEWS

Interviewed a total of five representatives at four organizations using Duo to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION

Designed a composite organization based on characteristics of the interviewees’ 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 interviewees.

CASE STUDY

Employed four fundamental elements of TEI in modeling the investment impact: benefits, costs, flexibility, and risks. Given the increasing sophistication of ROI analyses related to IT investments, Forrester’s TEI methodology provides a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

The Cisco Duo Customer Journey

Drivers leading to the Duo investment

Interviews

Role	Industry	Region	Duo-Protected Accounts
Senior director of information security	Healthcare	Headquartered in North America; regional operations	11,000
Security technical lead	Professional services	Headquartered in North America; global operations	6,800
IT support specialist	Information services	Headquartered in North America; global operations	1,225
Cybersecurity analyst	Healthcare	Headquartered in North America; national operations	12,000
Cyber defense operations center manager	Healthcare	Headquartered in North America; national operations	12,000

KEY CHALLENGES

Prior to deploying Duo, the interviewees' organizations either addressed credential-related security with another authentication solution or protected access to applications using only passwords.

The interviewees noted how their organizations struggled with common challenges, including:

- **High risk of a credentials-related security breach.** Before Duo, the interviewees' organizations had a heightened risk of a credentials-related security breach because they lacked multilayered protection, found it difficult to consistently implement and update security policies, and captured only limited intelligence around authentication attempts and the security status of their end users' devices.
- **Security analyst productivity around investigating suspicious login attempts.** With limited data readily available to support their investigations of suspicious login attempts, security analysts at the interviewees' organizations had to manually review logs for insights.

  A security technical lead at a professional services firm said: "In the past, our investigations of login attempts had to rely on super-generic logs. Analysts needed to log in to and then analyze each one of those. Tracking all these down, having the logins ready, and so on, all took an hour or two for each case."
- **Poor end-user experience, including time spent on each authentication.** Interviewees whose organizations previously used an authentication solution described end users' frustration with the time required to authenticate and the need to keep track of an additional device to do so.

> **"Before Duo, we were operating without much intelligence around access attempts. It was difficult to determine if someone actually authenticated or from which region they did so."**
>
> *Cybersecurity analyst, healthcare*

- **Effort required for security admins and other IT staff to manage and support a prior authentication solution.** Interviewees said that their prior solutions were complex and time-consuming to maintain and optimize, e.g., to add a new employee, protect additional applications, or establish and update security policies. A security technical lead at a professional services firm said: “Maintaining what we had and onboarding new functionality was a big effort with our prior solution. Integrating that solution with other applications was possible only with external help and very secret knowledge about the solution and so on. It wasn’t straightforward.”

  A cybersecurity analyst at a healthcare organization said: “Our previous solution was just so complicated — ‘You can’t forget to do this, and you can’t forget to do that.’ And when we ran into issues, it seemed like it took a long time or we had to reach out to the more senior engineers at the vendor.”

- **Productivity drags on help desk staff and end users due to authentication-related cases.** End users’ more complex login processes and need for a separate device prompted a significant number of help desk cases at organizations that used other types of authentication solutions. Resolving those cases disrupted end users and required time from help desk staff and end users alike.

- **Technical issues with prior authentication solutions.** Interviewees mentioned downtime, instability, problematic integrations with other applications, and other technical issues with their prior solutions.

COMPOSITE ORGANIZATION

Based on the interviews, Forrester constructed a TEI framework, a composite company, and an ROI analysis that illustrates the areas financially affected. The composite organization is representative of the five interviewees’ organizations, and it is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics:

Description of composite. The composite organization is a $3 billion global company with 10,000 Duo-protected accounts. It deploys Duo on any account used to remotely access applications. Most of those accounts are associated with employees, with the rest used by contractors or other third parties who need to access the organization’s systems. The devices used to access these applications are a mix of mobile devices, laptops, or desktops. The mobile devices and laptops are frequently used remotely. The composite organization’s applications are a mixture of cloud-based and on-premises, with the cloud-based percentage increasing over time. Prior to deploying Duo, the composite organization used another multifactor authentication system.

Key Assumptions

- **$3 billion annual revenue**
- **Global operations**
- **10,000 accounts protected by Duo**
- **Both cloud-based and on-prem applications**
- **Applications accessed via mobile, laptop, and desktop**
- **Frequent remote access**

Deployment characteristics. The composite organization purchases the Access version of Duo and selects Duo Care, a premium level of Cisco support. It implements Duo using a combination of professional services from its Duo Care team and internal resources from its IT staff. As part of implementation, it provides brief training to all who use accounts with Duo deployed. Once Duo's functionality is implemented and fully available, the organization's IT staff invests time on an ongoing basis to expand usage and adoption including new features as they are introduced.

Analysis Of Benefits

Quantified benefit data as applied to the composite

Total Benefits

Ref.	Benefit	Year 1	Year 2	Year 3	Total	Present Value
Atr	Reduced risk of a credentials-related security breach	$267,943	$331,579	$364,737	$964,259	$791,649
Btr	Security analyst productivity improvement	$240,259	$282,872	$291,368	$814,499	$671,105
Ctr	End-user time savings from streamlined authentication	$1,243,120	$1,280,307	$1,318,557	$3,841,985	$3,178,866
Dtr	Avoided cost of prior authentication solution	$94,500	$94,500	$94,500	$283,500	$235,008
Etr	Avoided costs for management and support of prior authentication solution	$128,845	$131,184	$133,588	$393,616	$325,914
Ftr	Help desk and end-user productivity improvement due to fewer authentication-related cases	$22,094	$22,757	$23,437	$68,288	$56,502
	Total benefits (risk-adjusted)	$1,996,760	$2,143,199	$2,226,187	$6,366,147	$5,259,044

REDUCED RISK OF A CREDENTIALS-RELATED SECURITY BREACH

Evidence and data. The interviewees said that by deploying Duo, their organizations reduced their risk of a credentials-related security breach. They attributed that risk reduction to Duo capabilities that go beyond the authentication method itself and to the intelligence Duo provided for each authentication, Duo's extensive capabilities around authentication-related security and security policies, and the ease with which they could consistently and comprehensively apply authentication-related security policies across their organizations.

Specific to the Access version of Duo that all interviewees used, organizations that had a prior authentication solution did not simply change the way their end users authenticated, but also added new capabilities that reduced their risk of a credentials-related security breach. Duo enabled the interviewees' organizations to better identify systems vulnerable to credential threat attacks (e.g., through context analysis and continuous inspection of the security posture of each device at every access attempt) and implement more granular authentication policies, such as setting up additional detail around who accessed what and how (e.g., restricting access from certain locations or limiting access from noncompliant devices).

A security technical lead at a professional services firm said: "The more data you have, the more things you can detect. We now have better intelligence around each multifactor authentication, and we leverage that. We can detect from where somebody is issuing a multifactor authentication, we can detect which device they are using, and we can detect odd behaviors — things that are not adding up."

That security technical lead also said: "Even our service desk interactions are more secure now. If somebody contacts our service desk, we have a default procedure where the service desk will send you a Duo push and you must verify that you are you with this multifactor authentication. This wasn't possible with our prior solution."

An IT support specialist at an information services company said: "Now, we have a single pane of glass through which we can look at all our protected applications and monitor trends. That saves some time, but more importantly we have new relevant information that we just didn't have before Duo … And Duo has a cool feature that enables us to identify and address vulnerabilities like someone running an out-of-date operating system or using an end-of-life browser or one that needs a patch. While we have other portals that show some of that, Duo shows it all in one place."

Interviewees partially attributed their reduced risk to other security measures they implemented simultaneous to their Duo deployment, such as better security training of end users, improved security policies and processes, and expanded use of multifactor authentication for a broader set of applications and use cases.

> **"Duo has wonderful information and capabilities in addition to authentication. We can determine the current software version on the device from which authentication was requested, and if it has outdated security patches. We can form our policies and say, 'Okay, if you haven't updated your device, you can no longer authenticate from it.'"**
>
> *Security technical lead, professional services*

Modeling and assumptions. For the composite organization, Forrester assumes:

- Organizations experience an average of three security breaches each year.[2]
- Thirty percent of security breaches are due to compromised credentials.
- The estimated cost to remediate a data breach (sized to the number of end users in the composite organization) is $605,274 in Year 1 and increases by 10% each year due to new regulations and other evolving factors.[3]
- After deploying Duo, the risk of a credentials-related security breach decreases by 80% in Year 1 and 90% in each of Years 2 and 3.
- Seventy percent of that reduction is attributable to Duo.

Risks. Reduced risk of a credentials-related security breach will vary based on:

- The prevalence, nature, and average cost of data breaches in an organization's industry.
- The volume and type of data breached.
- The geographic scope of operations.
- The regulatory and compliance measures an organization is required to follow.
- An organization's prior state and maturity level for security operations.
- The prior authentication software.
- The extent to which an organization has leveraged Duo's capabilities.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $792,000.

Reduced Risk Of A Credentials-Related Security Breach

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Average total number of security breaches experienced in a year	Forrester research	3	3	3
A2	Percentage of total that is due to compromised credentials	Forrester assumption	30%	30%	30%
A3	Estimated cost to remediate a single data breach	Forrester research	$605,274	$665,801	$732,382
A4	Subtotal: Total average annual cost of credentials-related breaches	A1*A2*A3	$562,905	$619,195	$681,115
A5	Reduction in risk of a credentials-related security breach after Duo is deployed	Interviews	80%	90%	90%
A6	Percentage of that reduction attributed to Duo	Interviews	70%	70%	70%
At	Reduced risk of a credentials-related security breach	A4*A5*A6	$315,227	$390,093	$429,102
	Risk adjustment	↓15%			
Atr	Reduced risk of a credentials-related security breach (risk-adjusted)		$267,943	$331,579	$364,737
	Three-year total: $964,259		**Three-year present value: $791,649**		

SECURITY ANALYST PRODUCTIVITY IMPROVEMENT

Evidence and data. For security analysts at the interviewees' organizations, Duo saved time troubleshooting and investigating potential security issues around login attempts. Interviewees attributed these time savings to Duo's easy navigation, integration with other applications, and capture of detailed information around each authentication attempt.

A cybersecurity analyst at a healthcare organization said: "Duo is a really big help for our 24/7 team because they rely on Duo to help them determine if a user has authenticated or not, if the user is actually in that certain [internet protocol] (IP) region or not, or if the user is in a certain permitted group when it comes to authentication and accessing an application. Duo is one of their primary resources for investigating authentications. Because so much is sitting in Duo and they don't have to look at many different tools, it's easy for them to read log activity and determine where the issue lies and then readily articulate that to other teams."

An IT support specialist at an information services company said: "Before Duo, we had to look at the logs of individual applications to verify what was going on. Duo saves a lot of time compared to that, because we can look at all our protected applications within a single pane of glass and see when an employee accesses something, how long they were there, and what they were doing there."

> **"Now when our [security operations center] (SOC) gets an alert, they have much more granular data to work with and they get it in a way that saves time. So, from hours to investigate, we went down to minutes."**
>
> *Security technical lead, professional services*

A security technical lead at a professional services firm said their security analysts saved investigation time because of the ease (via APIs) of pulling Duo logs into the organization's security information and event management (SIEM) to provide more context for security analysts.

Modeling and assumptions. For the composite organization, Forrester assumes:

- Each year, 3,500 authentication-related alerts need investigation.
- Before Duo, a security analyst spends an average of 90 minutes investigating each alert.
- With Duo, a security analyst spends an average of 20 minutes investigating each alert in Year 1, and 10 minutes in each of Years 2 and 3.
- Security analysts productively apply 90% of the time that they save.

Risks. Security analyst productivity improvement will vary based on:

- The nature of an organization's security incidents and the resulting per-incident analyst time to address.
- An organization's prior state.
- The nature of the prior authentication solution.
- How other systems are integrated with Duo.
- The volume of authentication alerts.
- Security analyst experience and capabilities.
- The maturity of an organization's security operations.
- The extent to which an organization has leveraged Duo's capabilities.
- Prevailing local compensation rates.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of $671,000.

Security Analyst Productivity Improvement

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Number of authentication-related alerts needing investigation each year	Interviews	3,500	3,500	3,500
B2	Security analyst time to investigate each alert before Duo (minutes)	Interviews	90	90	90
B3	Security analyst time to investigate each alert with Duo (minutes)	Interviews	20	10	10
B4	Subtotal: Annual time savings (hours)	(B1*(B2-B3))/60	4,083	4,667	4,667
B5	Productivity recapture	TEI standard	90%	90%	90%
B6	Security analyst fully burdened hourly compensation	TEI standard	$76.92	$79.23	$81.61
Bt	Security analyst productivity improvement	B4*B5*B6	$282,658	$332,790	$342,786
	Risk adjustment	↓15%			
Btr	Security analyst productivity improvement (risk-adjusted)		$240,259	$282,872	$291,368
	Three-year total: $814,499		Three-year present value: $671,105		

END-USER TIME SAVINGS FROM STREAMLINED AUTHENTICATION

Evidence and data. Interviewees said their end users saved time from Duo's streamlined authentication processes compared to what they previously used for authentication.

A security technical lead at a professional services firm said: "With Duo, our end-users spend less time on each authentication request. They no longer need to type in numbers, and then wait for a response."

Modeling and assumptions. For the composite organization, Forrester assumes:

- Each of its 10,000 end users authenticate an average of 500 times each year.
- Before Duo, an end user spends 1.5 minutes on each authentication.
- With Duo, an end user spends 0.5 minutes on each authentication.
- End users productively apply 50% of the time they save.

Risks. End-user time savings from streamlined authentication will vary based on:

- The number of end users.
- The average number of authentications per end user each year.
- The nature of the prior authentication solution.
- Prevailing local compensation rates.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of $3.2 million.

End-User Time Savings From Streamlined Authentication

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Number of end users	Composite	10,000	10,000	10,000
C2	Average number of authentications per end user each year	Interviews	500	500	500
C3	End-user time spent on each authentication prior to Duo (minutes)	Interviews	1.5	1.5	1.5
C4	End-user time spent on each authentication with Duo (minutes)	Interviews	0.5	0.5	0.5
C5	Subtotal: Total annual end-user time savings (hours)	(C1*C2*(C3-C4))/60	83,333	83,333	83,333
C6	End user blended fully burdened hourly rate	TEI standard	$35.10	$36.15	$37.23
C7	End-user productivity recapture	TEI standard	50%	50%	50%
Ct	End-user time savings from streamlined authentication	C5*C6*C7	$1,462,494	$1,506,244	$1,551,244
	Risk adjustment	↓15%			
Ctr	End-user time savings from streamlined authentication (risk-adjusted)		$1,243,120	$1,280,307	$1,318,557
	Three-year total: $3,841,985		**Three-year present value: $3,178,866**		

AVOIDED COST OF PRIOR AUTHENTICATION SOLUTION

Evidence and data. By moving to Duo, interviewees' organizations that previously used another authentication solution eliminated their ongoing expenses for those solutions. This is a net benefit, however, since the organizations now pay for Duo.

Modeling and assumptions. For the composite organization, Forrester assumes:

- The prior solution provider charges a $2.50 annual maintenance and support fee for each end-user authentication device in use.
- Each year, 25% of end-user authentication devices are replaced.
- A new end-user authentication device costs $25.
- The average cost to send a new device to an end user is $7.

Risks. Avoided infrastructure cost of prior authentication solutions will vary based on:

- The number of end users.
- The organization's prior approach to authentication.
- Vendor fees for initial cost and subsequent maintenance and support.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $235,000.

Avoided Costs Of Prior Authentication Solution

Ref.	Metric	Source	Year 1	Year 2	Year 3
D1	Number of end users	Composite	10,000	10,000	10,000
D2	Annual maintenance and support fee paid to solution provider per end-user authentication device	Interviews	$2.50	$2.50	$2.50
D3	Subtotal: Annual maintenance and support fees to authentication vendor	D1*D2	$25,000	$25,000	$25,000
D4	Percentage of end-user authentication devices replaced each year	Interviews	25%	25%	25%
D5	Cost per new device	Interviews	$25	$25	$25
D6	Cost to send new device to end user	Interviews	$7	$7	$7
D7	Subtotal: Annual costs to replace devices	D1*D4*(D5+D6)	$80,000	$80,000	$80,000
Dt	Avoided costs of prior authentication solution	D3+D7	$105,000	$105,000	$105,000
	Risk adjustment	↓10%			
Dtr	Avoided cost of prior authentication solution (risk-adjusted)		$94,500	$94,500	$94,500
	Three-year total: $283,500		Three-year present value: $235,008		

AVOIDED COSTS FOR MANAGEMENT AND SUPPORT OF PRIOR AUTHENTICATION SOLUTION

Evidence and data. Because interviewees' organizations found Duo simpler to manage and support than their previous solutions, they paid less to do so compared to their prior solutions. It reduced the time staff spent ensuring the solution was working, answering questions, deploying additional functionality, adding new use cases, and generally optimizing its use, and also created savings from the elimination of professional services fees formerly paid to fill internal expertise gaps.

Management and support activities included enacting and adjusting authentication policies; adding new users and managing end-user credentials; integrating the authentication solution with other security investments and with all applications; enrolling and activating new users; and fine-tuning the user experience.

An IT support specialist at an information services company said, "It's your easiest option for multifactor authentication in an enterprise environment." A security technical lead at a global professional services firm said: "Staff time savings have been a big benefit. Duo is very streamlined, and we were able to remove a lot of engineering hours that our team had spent to maintain the prior solution."

That IT support specialist also said: "We no longer pay for a professional services firm because we can manage Duo with our own security team. With the previous solution, we paid an external vendor on a constant basis to be available for us and help our dedicated engineers working on the solution. Now, instead of having to dedicate staff to supporting the solution, everybody on our security team is more or less trained to the level that they can operate Duo."

A cybersecurity analyst at a healthcare organization said: "Duo has been a great benefit to us in many ways — enrollment, provisioning, security, log activity, investigations, setting up policies, creating processes and standards to help internal teams. It's all pretty easy. Some of the application owners I work with are not highly tech-savvy, but after working with them, explaining Duo to them, showing it to them, I don't get a lot of them reaching out for help anymore … With our prior product, we often had to contact the vendor for support because it was such a complicated system. Duo has helped our environment a lot."

> **"Duo has been really easy to learn, navigate, and work with, compared to our prior solution. It requires less management."**
>
> *Cybersecurity analyst, healthcare*

Duo also saved staff time because of:

- **The simplicity of setting up authentication policies.** A cybersecurity analyst at a healthcare organization said: "Duo benefits us because it's very easy to set up a policy and implement it in one of our applications within Duo, and then everyone's on the policy. With our prior product it was more complicated."
- **The ease of integrating Duo with other applications.** A security technical lead at a professional services firm said: "Duo has great documentation for nearly all the [software-as-as-service] (SaaS) vendors. Whatever you need to call in the internet, you can nearly guarantee that Duo has well-documented and straightforward integration that we can just use, and the simplicity of the onboarding processes is quite good for us. … We enforce Duo authentication on all our cloud SaaS vendors and appreciate the excellent documentation that's provided for all these integrations."

> An IT support specialist at an information services company said: “These days, a lot of third-party applications have an integration with Duo. They already recognized Duo as one of the top MFAs. So, ‘You’re using Duo? Here’s your Duo MFA integration.’ You don’t have to go hunt and peck — it’s just right there.”

Modeling and assumptions. For the composite organization, Forrester assumes:

- To manage and support the prior authentication solution, two IT staff FTEs work a combined total of 4,160 hours each year.
- To manage and support Duo, varied IT staff work a combined total of 312 hours each year.
- IT staff productively apply 50% of the saved time.

Risks. Avoided costs for management and support of prior authentication solutions will vary based on:

- The nature of the prior authentication solution.
- IT staff experience and capabilities.
- The maturity of an organization’s security operations.
- The extent to which an organization has leveraged Duo’s capabilities.
- Prevailing local compensation rates.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of $326,000.

Avoided Costs For Management And Support Of Prior Authentication Solution

Ref.	Metric	Source	Year 1	Year 2	Year 3
E1	Number of IT staff FTEs needed for ongoing management and support of prior authentication solution	Interviews	2	2	2
E2	Number of hours each FTE works each year	TEI standard	2,080	2,080	2,080
E3	IT staff time needed for ongoing management and support of Duo (hours)	Interviews	312	312	312
E4	Subtotal: IT staff time saved with Duo (hours)	(E1*E2)-E3	3,848	3,848	3,848
E5	Productivity recapture	TEI standard	50%	50%	50%
E6	IT staff blended fully burdened hourly compensation	TEI standard	$47.60	$49.03	$50.50
E7	Avoided professional services fees	Interviews	$60,000	$60,000	$60,000
Et	Avoided costs for management and support of prior authentication solution	(E4*E5*E6)+E7	$151,582	$154,334	$157,162
	Risk adjustment	↓15%			
Etr	Avoided costs for management and support of prior authentication solution (risk-adjusted)		$128,845	$131,184	$133,588
	Three-year total: $393,616		**Three-year present value: $325,914**		

HELP DESK AND END-USER PRODUCTIVITY IMPROVEMENT DUE TO FEWER AUTHENTICATION-RELATED CASES

Evidence and data. Because Duo simplifies an end user's authentication process and eliminates the need for a separate device, fewer authentication-related cases reached help desks at the interviewees' organizations. This saved time for help desk staff and end users.

A security technical lead at a professional services firm said: "We went from 20 calls each week to maybe one or two. The number of calls dropped because the app is more intuitive and less problematic for end users. The old app was not that straightforward, people sometimes missed the code, and so on. And we have very good feedback from the service desk that the Duo verification they're doing from their end on incoming calls is working without any issues for them."

> **"Users have fewer issues with authentication, and the Duo logs are a huge help in resolving user issues that do reach our service desk."**
>
> *Cybersecurity analyst, healthcare*

Modeling and assumptions. For the composite organization, Forrester assumes:

- Before Duo, the help desk handles 1,500 authentication-related cases each year.
- With Duo, 90% of those cases are eliminated.
- Help desk staff spend 0.4 hours to resolve each authentication-related case.
- Help desk staff productively apply 100% of the time they save.
- End users spend 0.4 hours to resolve each authentication-related case.
- End users productively apply 50% of the time they save.

Risks. Help desk and end-user productivity improvement due to fewer authentication-related cases will vary based on:

- The nature of the prior authentication solution.
- Help desk staff experience and capabilities.
- The extent to which an organization has leveraged Duo's capabilities.
- Prevailing local compensation rates.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $57,000.

Help Desk And End-User Productivity Improvement Due To Fewer Authentication-Related Cases

Ref.	Metric	Source	Year 1	Year 2	Year 3
F1	Annual number of authentication-related help desk cases before Cisco Duo	Interviews	1,500	1,500	1,500
F2	Percentage reduction in those cases after deploying Duo	Interviews	90%	90%	90%
F3	Subtotal: Reduction in cases with Duo	F1*F2	1,350	1,350	1,350
F4	Help desk time per case (hours)	Interviews	0.4	0.4	0.4
F5	Help desk fully burdened hourly rate	TEI standard	$27.91	$28.75	$29.61
F6	Help desk productivity recapture	TEI standard	100%	100%	100%
F7	Subtotal: Help desk productivity improvement	F3*F4*F5*F6	$15,071	$15,525	$15,989
F8	End-user time per case (hours)	Interviews	0.4	0.4	0.4
F9	End user blended fully burdened hourly rate	TEI standard	$35.10	$36.15	$37.23
F10	End-user productivity recapture	TEI standard	50%	50%	50%
F11	Subtotal: End-user productivity improvement	F3*F8*F9*F10	$9,477	$9,761	$10,052
Ft	Help desk and end-user productivity improvement due to fewer authentication-related cases	F7+F11	$24,548	$25,286	$26,041
	Risk adjustment	↓10%			
Ftr	Help desk and end-user productivity improvement due to fewer authentication-related cases (risk-adjusted)		$22,094	$22,757	$23,437
	Three-year total: $68,288		**Three-year present value: $56,502**		

UNQUANTIFIED BENEFITS

Interviewees mentioned the following additional benefits that their organizations experienced but were not able to quantify:

- **Better end-user experience.** End users found it easy to begin using Duo, and they subsequently saved time (on each authentication and from downtime) and frustration.

  A security technical lead at a professional services firm said: “The usability of Duo is very well accepted in our organization. With Duo, you get the push and just do a one-touch thing on your device. Compare this with the previous method, where they all had little tokens, and they needed to dial up a number within a certain amount of time. … And since we onboarded Duo, we’ve had no downtime due to authentication-related security incidents.”

  A senior director of information security at a healthcare organization said: “Moving to Duo improved the end-user experience 100%. First, you’re not having to carry a physical device and keep track of it versus a phone that I already have with me. And second, instead of having to try to read some numbers from the token and then type them into the device, I just hit ‘Accept.’” A cybersecurity analyst at a healthcare organization said, “Even our self-enrollment is pretty simple for end users.”

- **Ease of further improving the user experience with Duo's single sign-on (SSO).** Organizations that opted to use Duo's SSO functionality further improved the end-user experience by providing Duo users with a simplified and consistent login experience for all applications that are integrated with Duo, whether on-premises or cloud-based. Cisco's cloud-based SSO for Duo is designed to complement the Duo multifactor authentication solution, although Duo also integrates with dozens of third-party SSO and identity provider tools.

  A cybersecurity analyst in a healthcare organization that uses Duo's SSO said: "Duo SSO is easy to set up and manage. Most employees I've talked to love how easy it is to use. Duo SSO saves end users time because now after signing into one application, they don't have to multifactor into every subsequent application."

- **Audit and regulatory compliance efficiencies.** A security technical services lead at a professional services firm said: "With Duo's better auditing data and user activity reports, we can run fully automated audit reports. That wasn't possible with our prior solution."

- **Enhanced ability to acquire new customers or partners.** An IT support specialist at an information services company said: "I think using Duo does help us acquire new customers and partners, or more revenue from our current customers, once they know we're using Cisco Duo. It has brand recognition in some of the markets we're in, and that gives them a comfort level."

- **Vendor rationalization.** A senior director of information security at a healthcare organization said, "It made sense to go with a company we already worked with, so we could limit the number of people we have to pick up the phone and call." An IT support specialist at an information services company said, "The ease of integrating Duo with our existing security products from the same vendor was attractive."

- **Duo's moderate learning curve and the value of Duo Care premium support.** A security technical lead at a professional service firm said: "Our learning curve was low. The product is self-explanatory, and the customer support is excellent." An IT support specialist at an information services firm said, "Cisco made our onboarding and everything else that much easier."

  A cybersecurity analyst at a healthcare organization said: "Our Duo Care team has been very supportive about how to do things or providing us with the resources we need to resolve our issue. Or if we're looking to implement a certain design, they've been very helpful in our figuring that out."

FLEXIBILITY

The value of flexibility is unique to each customer. There are multiple scenarios in which a customer might implement Duo and later realize additional uses and business opportunities, including:

- **Further capitalizing on Duo's capabilities.** Interviewees mentioned the broad scope of Duo's capabilities and their intent to leverage more of that functionality. A cybersecurity analyst at a healthcare organization said: "There's a lot more we can get from Duo. It definitely has more features that we can't wait to try."

- **Protecting additional applications with Duo.** Interviewees' organizations typically deployed Duo initially to their top-priority applications (especially those that are frequently accessed remotely) and then continued to extend Duo to additional applications over time, including internal applications and services. An IT support specialist at an information services company said: "Adding another application doesn't change what we pay for Duo. The more applications I can protect with Duo, the more value I'm getting from it."

- **Readily expanding Duo use to acquired entities.** A cybersecurity analyst at a healthcare organization said, "We'll have a lot more employees joining us soon because of an acquisition, but Duo makes that easy."

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
Gtr	Cisco fees	$0	$680,400	$680,400	$680,400	$2,041,200	$1,692,054
Htr	Internal effort for implementation, management, and support	$218,691	$47,596	$49,023	$50,489	$365,798	$340,408
	Total costs (risk-adjusted)	$218,691	$727,996	$729,423	$730,889	$2,406,998	$2,032,462

CISCO FEES

Evidence and data. Duo fees reflected subscription fees for the Access version of Duo, and Duo Care fees for additional services beyond the standard support included with Duo.

Since customer-specific factors determine subscription and Duo Care fees, consult with Cisco for likely costs specific to your organization when conducting your analysis. Your organization’s fees may differ from the composite organization’s fees.

Modeling and assumptions. For the composite organization, Forrester assumes:

- The organization deploys the Access version of Duo for 10,000 accounts.
- The organization opts for Duo Care.

Risks. Cisco fees will vary based on:

- Number of accounts Duo protects.
- Which version of Duo an organization chooses.
- Whether an organization selects Duo Care.

Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $1.7 million.

Cisco Fees

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
G1	Duo Access subscription fees	Composite		$540,000	$540,000	$540,000
G2	Duo Care fees	Composite		$108,000	$108,000	$108,000
Gt	Cisco fees	G1+G2	$0	$648,000	$648,000	$648,000
	Risk adjustment	↑5%				
Gtr	Cisco fees (risk-adjusted)		$0	$680,400	$680,400	$680,400
	Three-year total: $2,041,200			**Three-year present value: $1,692,054**		

INTERNAL EFFORT FOR IMPLEMENTATION, MANAGEMENT, AND SUPPORT

Evidence and data. Interviewees described Duo deployment as relatively straightforward. The interviewees' organizations implemented Duo using internal resources that included a project leader, network and server admins, and security admins, and guidance from their Duo Care team. Technical setup included determining requirements (e.g., around remote users connecting into internal applications), and then configuring, deploying, and testing the Duo solution and integrating it with key applications.

The interviewees' organizations' internal training staff developed documentation and training materials for end users based on templates and guidance their Duo Care team provided, and then supported end users during the initial rollout of Duo across their organizations. End users got familiar with Duo by reading materials or watching a video and consulting with training staff if needed and, subsequently, enrolled their devices with Duo.

On an ongoing basis, security-related IT staff managed and supported Duo (including interfacing with Cisco and continually evaluating how to further optimize their use of Duo) and handled projects like onboarding new functions or new use cases to Duo. Newly hired end users educated themselves using the training materials and consulted help desk staff if needed.

Modeling and assumptions. For the composite organization, Forrester assumes:

- IT staff spends a combined total of 180 hours over one month on technical implementation.
- Training staff spends a combined total of 340 hours during implementation developing and distributing materials and guiding end users.
- IT staff spends a combined total of 312 hours on management and support each year.
- Help desk staff spend a combined total of 75 hours each year onboarding new Duo end users.
- All end users are trained during implementation; new hires are trained as they are hired.
- Each end user spends 0.5 hours learning about Duo and enrolling their device.
- Annual turnover is 15%.

Risks. Internal effort for implementation, management, and support will vary based on:

- The number of end users.
- IT staff experience and capabilities.
- The maturity of an organization's security operations.
- The extent to which an organization has leveraged Duo's capabilities.
- Prevailing local compensation rates.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $340,000.

> **"Moving to Duo was easy. Duo made that really simple – just plug and play. Documentation, updates, and support are all good."**
>
> *Cybersecurity analyst, healthcare*

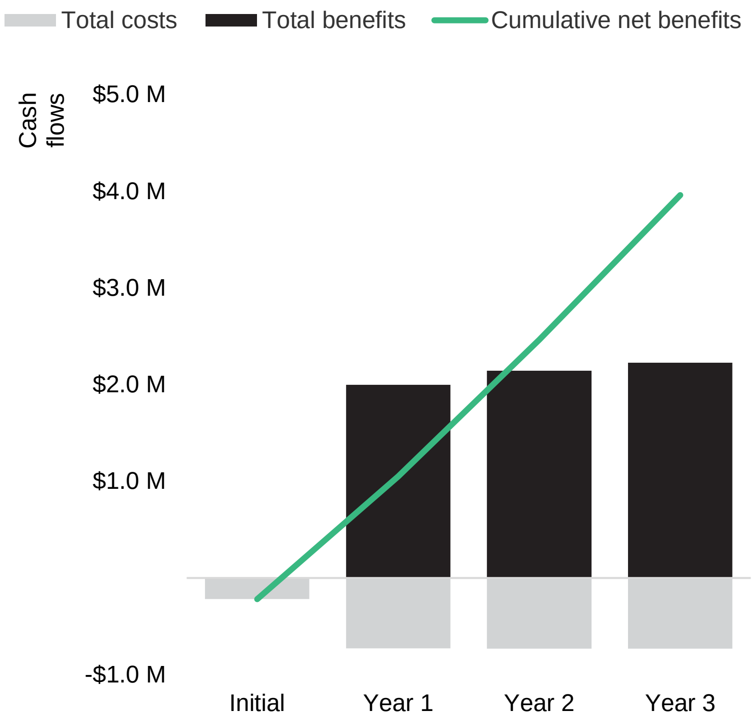
Internal Effort For Implementation, Management, And Support

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
H1	IT team combined total hours required for initial technical implementation and ongoing management and support of Duo	Interviews	180	312	312	312
H2	IT staff blended fully burdened hourly compensation	TEI standard	$47.60	$47.60	$49.03	$50.50
H3	Trainer combined total hours required for initial training	Interviews	340			
H4	Trainer fully burdened hourly compensation	TEI standard	$43.36			
H5	Help desk time to help onboard end users to Duo (hours)	Interviews		75	75	75
H6	Help desk fully burdened hourly compensation	TEI standard		$27.91	$28.75	$29.61
H7	Number of end users new to Duo	Composite	10,000	1,500	1,500	1,500
H8	Time each end user new to Duo spends learning about it and enrolling their devices (hours)	Interviews	0.5	0.5	0.5	0.5
H9	End user blended fully burdened hourly compensation	TEI standard	$35.10	$35.10	$36.15	$37.23
Ht	Internal effort for implementation, management, and support	(H1*H2)+(H3*H4)+(H5*H6)+(H7*H8*H9)	$198,810	$43,269	$44,566	$45,899
	Risk adjustment	↑10%				
Htr	Internal effort for implementation, management, and support (risk-adjusted)		$218,691	$47,596	$49,023	$50,489
	Three-year total: $365,798		**Three-year present value: $340,408**			

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	($218,691)	($727,996)	($729,423)	($730,889)	($2,406,998)	($2,032,462)
Total benefits	$0	$1,996,760	$2,143,199	$2,226,187	$6,366,147	$5,259,044
Net benefits	($218,691)	$1,268,765	$1,413,777	$1,495,298	$3,959,148	$3,226,582
ROI						159%
Payback						<6 months

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.

Appendix B: Endnotes

[1] 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.

[2] Source: Forrester Consulting Cost Of A Cybersecurity Breach Survey, Q1 2021.
[3] Source: Ibid.

FORRESTER®