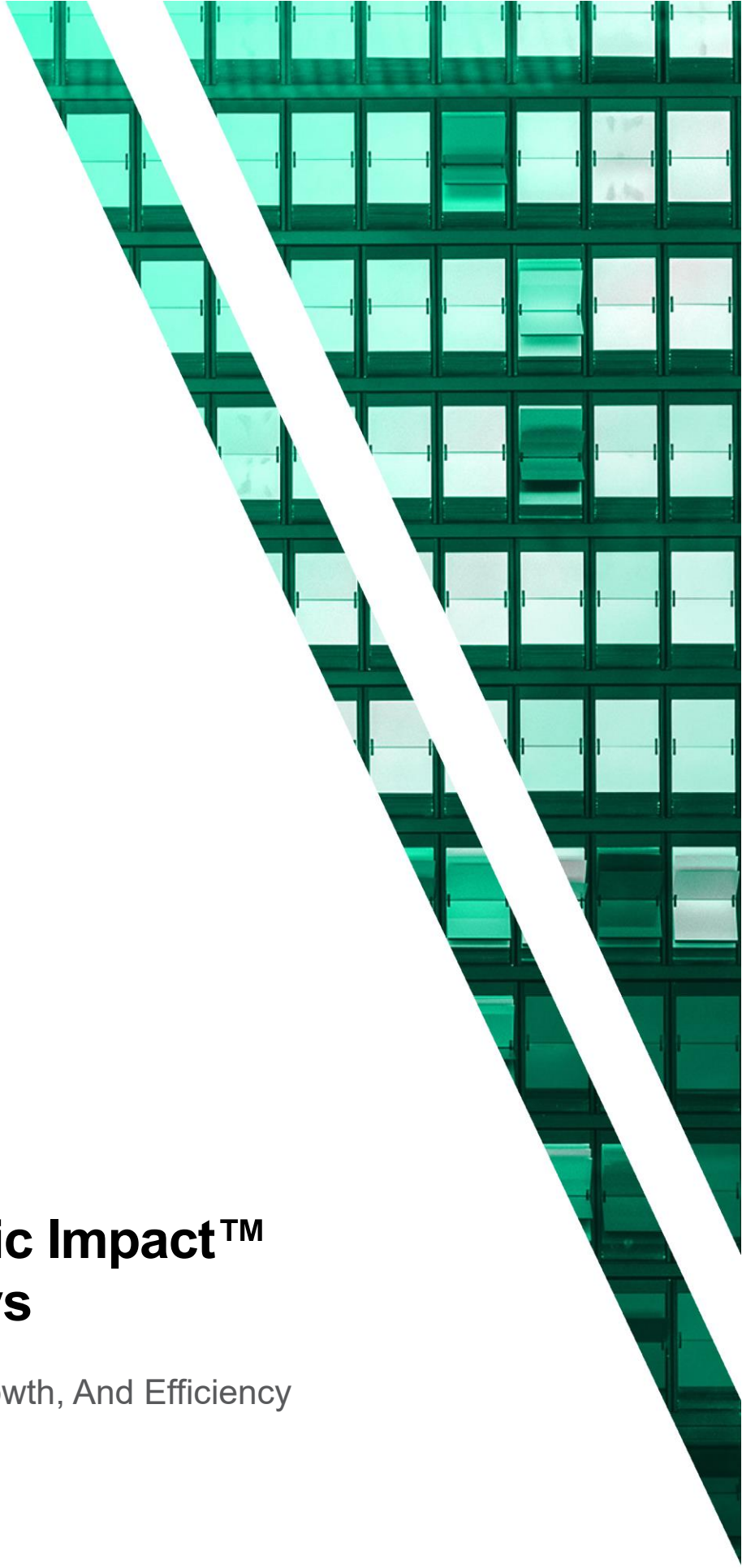
FORRESTER®



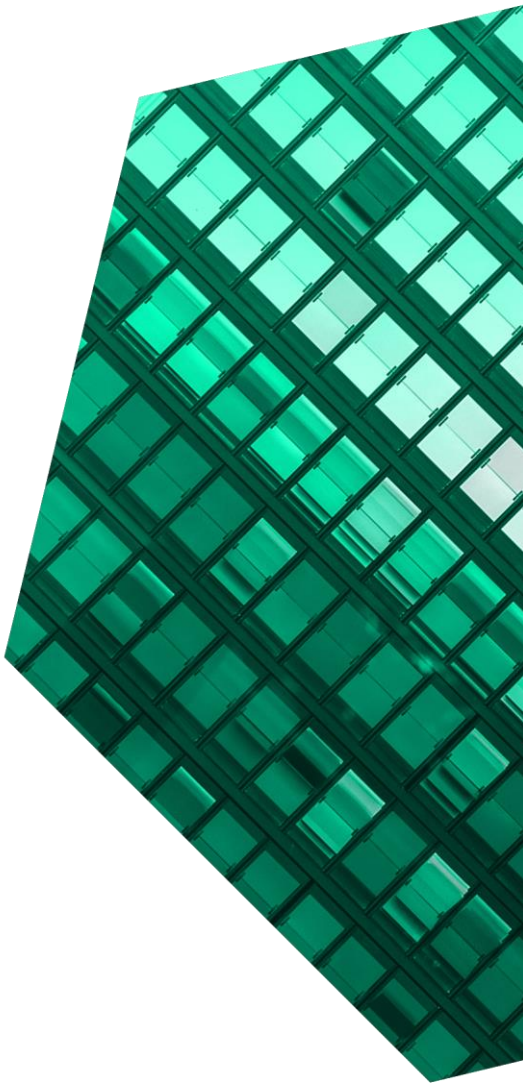
The Total Economic Impact™ Of Yubico YubiKeys

Risk Reduction, Business Growth, And Efficiency Enabled By YubiKeys

SEPTEMBER 2022

Table Of Contents

Project Lead: *Benjamin Brown*



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

Security leaders must deploy strong multifactor security solutions to protect their organizations, users, and customers. Forrester interviewed security leaders from five enterprises using YubiKeys and found that YubiKeys slashed exposure to security breaches from phishing and credential thefts by 99.9% while driving business growth through improved reputation and access to high-security contracts. Further, YubiKeys reduced administrative overhead while providing a flexible, dependable user experience.

YubiKeys are hardware-based, phishing-resistant multifactor authentication (MFA) solutions based on open standards that are produced by Yubico. YubiKeys support a vast range of authentication protocols and come in a wide variety of form factors and connectors, such as USB-A, USB-C, Lightning, and NFC, ensuring that they can be used by almost any organization and user on almost any device.

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

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed five security leaders from organizations that use YubiKeys across their user bases. 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 based in North America with 5,000 users and revenue of $2.5 billion per year.

Fewer successful phishing and credential theft attacks

99.9%

KEY STATISTICS

Return on investment (ROI)

203%

Net present value (NPV)

$3.24M

Prior to using YubiKeys, interviewees' organizations — particularly those not yet using any form of MFA — faced excess and unacceptable exposure to security risks. Security teams expended excess effort on setting and managing password policies while users struggled with frustrating, time-consuming password updates and resets. Organizations with legacy MFA solutions also struggled with poor user experiences, outdated code, lock-in to proprietary technology, and expensive, low-quality hardware.

Interviewees' organizations adopted modern, phishing-resistant MFA security by deploying YubiKeys and simplified password policies across their systems on the ultimate journey to becoming passwordless. YubiKeys virtually eliminated risk of phishing and credential theft, drove business growth due to improved security levels and reputation, and improved productivity and user experience across the organizations.

KEY FINDINGS

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

- **Strengthened security and reduced risk exposure of $2.2 million.** By deploying YubiKeys across its user base, the composite reduces the risk of successful phishing and credential theft attacks by 99.9%.
- **Improved reputation and ability to win security-related contracts and projects, driving business growth of $1.2 million.** The improved security reputation from using YubiKeys drives a higher deal conversion rate. Additionally, YubiKeys meet the strict security requirements to bid on new opportunities, resulting in more won deals.
- **Security operations efficiency labor savings worth $765,000.** The composite reallocates three FTEs by using YubiKeys to eliminate work related to phishing and credential theft investigation and password management.
- **Help desk support savings of $51,000.** Simplifying password policies with YubiKeys reduces help desk tickets by up to 75%.
- **Improved end user productivity worth $596,000.** End users save 30 minutes per avoided password update and 2 hours per password reset. After adjustments, the organization recaptures almost $57 in annual labor per user by Year 3.

Unquantified benefits. Benefits that are not quantified in this study include:

- **Labor and cost savings from legacy hardware authentication elimination.** YubiKeys replace outdated hardware solutions with burdensome IT administration and poor user experiences.
- **Improved security and data protection for end customers and partners.** YubiKeys benefit both direct users and other parties including customers, clients, and partners.
- **Strong and trusted partnership with Yubico.** Security leaders see Yubico as a trusted brand with dependable hardware and great support.
- **Improved employee experience.** Users find YubiKeys easy to use with convenient form factors and connection options, reducing password and hardware frustration.
- **Extensive partner and vendor ecosystem.** Services from Yubico and its partners help customers be successful in their MFA journeys.

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

- **YubiEnterprise Subscription costs of $361,000, based on 5,000 users.** The composite enjoys predictable costs, consistent supplies, replacements, and technical support. YubiEnterprise Subscription begins at 500 users.
- **YubiEnterprise Delivery costs of $52,000.** The composite distributes YubiKeys to its users globally using Yubico's turnkey delivery program.
- **Deployment costs of $494,000.** The composite deploys YubiKeys during a one-year period with the work of security engineers, IT staff members, cross-functional leaders, and pilot testers.
- **Ongoing management costs of $165,000.** After deploying YubiKeys, the composite requires ongoing management for updates, maintenance, support, training, distribution, and more.
- **End-user training and setup costs of $522,000.** End users typically require up two hours of training, setup, and familiarization when getting a YubiKey and learning to use MFA.

Synopsis. The composite organization invests $1.6 million in costs and experiences $4.8 million in benefits over three years, adding up to a net present value (NPV) of $3.2 million and an ROI of 203%.

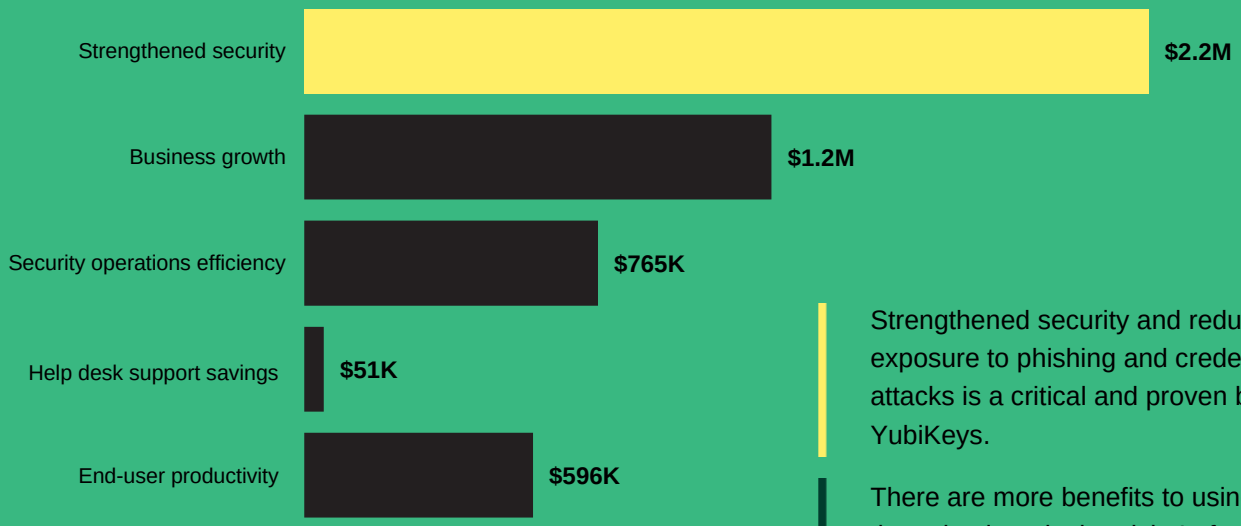
ROI
203%

BENEFITS PV
$4.83M

NPV
$3.24M

PAYBACK
11 months

Benefits (Three-Year)



Strengthened security and reduced risk exposure to phishing and credential theft attacks is a critical and proven benefit of YubiKeys.

There are more benefits to using YubiKeys than simply reducing risk. In fact, the sum of all other benefits outweighs the costs alone.

“We run our environment through various penetration tests and simulated attacks and, of course YubiKeys stand up against all that.”

— Director of security engineering, energy

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 YubiKeys.

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 YubiKeys 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 Yubico 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 YubiKeys.

Yubico 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.

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

The Yubico YubiKeys Customer Journey

Market overview and drivers leading interviewees to invest in YubiKeys

MARKET OVERVIEW

Passwords have long protected digital resources and data; however, they are "easy pickings for cybercriminals and the culprit behind many cyberattacks" while "administrative costs and user productivity losses add insult to injury."[2] Passwords are no longer adequate to protect organizations, their employees, nor their customers. According to Forrester Research, single-factor passwords are the weakest form of user authentication.[3]

Passwords are "phishable, crackable, stuffable, and snoopable."[4] Between 2018 and 2020, the number of stolen usernames and passwords available in the dark web increased 300%, with 15 billion stolen logins from 100,000 breaches."[5] Infrastructure and staffing to maintain passwords and investigate incidents can be significant. Password resets are expensive and hurt productivity, costing many enterprises more than $1 million per year in support costs alone.[6] Further, passwords are difficult to remember, particularly when regular resets are required. Even despite firm password requirements, more than half of users frequently reuse passwords.[7] Users often revise the same base password with only minor changes, such as different numbers at the end.

Forrester advises "to use enterprise MFA and modern passwordless approaches to protect against brute force attacks, phishing, credential stuffing, and other techniques that exploit compromised user credentials." [8] "MFA thwarts such attempts by requiring two or more factors for identity claims before granting a given user access to your organization's networks and sensitive corporate data."[9] Enterprise MFA can "eradicate embarrassing password-related security breaches," "show auditors and regulators you are serious about workforce access control," and "reduce dependence on cumbersome and expensive password policy management."[10]

Many organizations are beginning to require that technology vendors offer MFA. For example, the United States Department of Defense's Cybersecurity Maturity Model Certification (CMMC) Level 3 requires multifactor authentication for local and network access to privileged accounts and for network access to nonprivileged accounts.[11] Similarly, the EU's revised Payment Services Directive (PSD2) mandates MFA for banking transactions.[12]

Further, Forrester advises organizations try to move away from passwords entirely while deploying MFA.[13] Passwordless authentication lowers cost and improves security and business efficiency of adopting firms.[14] Despite restrictive technology environments, passwordless MFA adoption is growing.

There are many ways to approach multifactor or two-factor authentication, many of which are passwordless factors such as biometrics, tokens, keys, or open authorization (OAuth)-related solutions. These greatly reduce the attack surface of man-in-the-middle attacks, and vendors of these solutions can help organizations kill the password.[15]

"Multifactor is not an option anymore. Organizations need to do it, and they need to do it now. YubiKeys specifically support so many functions. They're durable. We have good user acceptance of the form factor. We've had just one physical failure in the 50,000 or so keys we've gone through. It's a testament to the quality."

General director of information assurance, transportation

Any out-of-band second factor (i.e., using a distinct channel) will significantly improve security; however, Forrester recommends to use stronger methods than one-time passwords (OTP) delivered via SMS text messages because they are vulnerable to SIM swapping attacks.[16] Although adding SMS two-factor authentication (2FA) is a major improvement over single-factor authentication (SFA), it only stops 76% of narrowly targeted attacks.[17]

For stronger authentication, organizations have a variety of available solutions.[18] Hardware tokens are one of the most secure options available. Because physical presence of the key is required, they are essentially only susceptible to physical theft or malicious insider usage of the key when phishing-resistant protocols are used. Even then, attackers would still have to cross further hurdles from other security solutions to access an account.

Best-in-class hardware tokens can meet the demands of protocols and open standards, thus ensuring wide support across devices and vendors. Further, best-in-class hardware tokens come in many form factors and with many connector options to prevent potential frustration or limitations for users.

QUANTIFYING SECURITY BREACH EXPOSURE

Forrester's 2021 Business Technographics Security Survey found that 63% of organizations had at least one security breach in the past 12 months, with 51% having two or more breaches.[19] Of those breaches, 44% cost less than $1 million, 42% cost between $1 million and $5 million, and 14% cost more than $5 million.[20]

Similarly, third parties currently estimate the cost of a typical breach anywhere from $21,659 (Verizon) to $140,000 (CISA) to $4.2 million (IBM), and the frequency of breaches from many times per month to as low as one or two breaches every few years.[21]

Despite varying data, sources agree on one thing: Security breaches are a major material threat to organizations' top and bottom lines. Estimating the reduction in security risk exposure is consequently critical when evaluating the business case for a security solution such as Yubico YubiKeys.

In July 2020, Forrester Consulting's Total Economic Impact practice fielded an independent survey to further evaluate the frequency and severity of breaches for the purposes of improving financial analyses of security solutions regardless of vendor.[22] This survey of 342 respondents involved in security at US firms found that the average organization experiences 1.8 material breaches per year that incur labor, costs, and other losses.[23] This includes:

- **A total of 3,437 labor hours.**[24] This figure includes approximately 837 hours for security operations, 871 hours for IT/network operations, 895 hours for development operations, and 835 hours for external resources (rounded). Assuming an average fully burdened salary of $58 per hour, this equates to $199,346 in labor costs.
- **Direct costs of $269,550.**[25] This figure includes approximately $104,799 for response and notification, $27,036 for regulatory fines, $54,004 for customer compensation, $45,706 for customer lawsuits and punitive damages, and $38,006 for additive audit and security compliance costs (rounded).
- **Business losses of $385,296.**[26] This includes approximately $63,849 in lost revenue due to downtime, $89,895 in lost revenue from customer attrition, $80,436 in cost to rebuild brand equity, and $151,116 in customer churn and additional cost to acquire new customers.

These frequency, labor, and cost estimates form one component of this TEI financial analysis.[27] Although actual risk reduction can never be perfectly estimated nor would it be the same for all organizations, this data yields a conservative, reasonable representation of the risk exposure for a typical enterprise.

Interviews

Role	Industry	Region	YubiKey Users
Product owner of authentication	Manufacturing	Global, based in Europe	More than 100,000 users
Director of security engineering	Energy	Global, based in Europe	More than 50,000 users
General director of information assurance	Transportation	North America	15,000 to 50,000 users
IT product manager	Media and communications	Global, based in North America	5,000 to 15,000 users
Senior director of IT	B2B technology	Global, based in North America	1,000 to 5,000 users

KEY CHALLENGES

Before using YubiKeys, interviewees' organizations used a mix of usernames and passwords, software MFA, and hardware MFA tokens and cards to secure their businesses. These solutions did not fully meet their security needs, particularly due to the following common challenges:

- **Organizations faced excess, unacceptable exposure to security risks.** Interviewees' organizations faced threats including phishing, social engineering, malicious insiders, stolen credentials, weak passwords, and more. The risk of breaches was high, and, in fact, some organizations were hit by successful material breaches in their legacy environments. Security teams saw increasing risks, particularly those that targeted high-profile figures or employees with access to critical, sensitive data. In an internal test, one company found that it could have employee accounts accessed via a password spray attack. Another company experienced a major newsworthy attack forcing phishing-resistant MFA adaptation.
- **Password policies provided inadequate protection while causing wasted labor and poor user experiences.** Interviewees mentioned the weaknesses and inefficiencies of passwords. They observed employees sharing, reusing, and creating simple passwords. Interviewees also acknowledged industry reports about the danger of lost and stolen credentials and spoke about the unnecessary time spent on password management, resets, and help desk support.
- **Existing MFA solutions had major downsides.** Some interviewees' organizations previously used or tested hardware solutions like legacy tokens and smart cards. However, these options often broke and had limited battery life, leading to excessive cost and replacements. They also yielded poor user experiences requiring frequent, frustrating reauthentication and leading to mindless approval of authentications and subsequent security risks. Interviewees also expressed concerns with software MFA options such as SMS codes that can be prone to phishing attacks and SIM swaps.

> **"The major push was after [we had a security breach], and so we made the decision that we need to make a huge investment in securing YubiKeys for both our customers and our internal employees."**
>
> *— Anonymous interviewee*

- **Other MFA options struggled to or could not meet unique business requirements.** Employees in dangerous work environments like factory floors may not be able to access phone-based authentication or use a keyboard to type a one-time code or password. Often, these environments also do not have cell reception to receive push/SMS messages. Legacy MFA options could not endure the rigors of the environments which led to breakages, or they could not meet the limitations of the machine interfaces and how workers could interact with them. Air-gapped critical systems were difficult or impossible to protect with other forms of MFA that relied upon some form of network access.
- **Organizations needed to prove satisfactory security protection to external audiences.** Interviewees noted a need to demonstrate seriousness about security to stakeholders, customers, clients, shareholders, and regulators. Meeting these expectations was a requirement to win and retain business, maintain valuation, and avoid excessive regulatory scrutiny or even fines. One interviewee from the energy company mentioned that customers now consistently ask about MFA and security certifications during their vendor selection process, while another interviewee from the transportation company pointed out the importance of proving satisfactory security to third parties with oversight of their operations.

Voice Of The Customer

"With our [legacy hardware], once the battery life expired, the token was never useful ever again. It became a bottle opener at that point. The YubiKey was selected for obvious advantages without expirations or batteries."
— Product owner of authentication, manufacturing

"We've caught people sharing passwords. You can't share geographically because people can't share multifactor tokens — not YubiKeys, at least — because it's one physical thing."
— General director of information assurance, transportation

"We operate a Zero Trust environment that is 100% in the cloud. It's just super important for us to protect identities, because if one account is taken over, then they can single sign-on across our environment and do a whole bunch of different things from there. It's just really scary."
— Senior director of IT, B2B technology

"Today, it's the customers that are asking us about two-factor authentication and security certifications. [With Yubico,] we are ready and willing to respond to that. We actually appreciate getting those questions now instead of dreading them."
— Director of security engineering, energy

INVESTMENT OBJECTIVES

The interviewees' organizations sought a phishing-resistant MFA solution based on open standards that could help them achieve the following goals:

- **Strengthen security to reduce risk and improve brand reputation.** Organizations needed to reduce the probability of phishing incidents, social engineering attacks, and insider risk. They hoped to avoid costly investigations, breaches, and losses along with the potential for negative impacts to reputation that might lead to lost sales and market valuation. Conversely, they hoped that strong security would improve their reputations to grow their businesses.

  The general director of information assurance for a transportation organization shared: "[We want to show] that we are taking [security] seriously and that we have a robust and ever-improving mature program."

- **Leverage open standards to avoid lock-in and ensure portability, interoperability, and flexibility for current and future industry standards.** After some interviewees' organizations experienced or researched MFA solutions with proprietary standards, they hoped to invest in an option that could meet shared, open security standards like FIDO2. Their investments would allow them the flexibility to use the same solution across different systems for the foreseeable future with the option to evolve with open standards.

  The product owner of authentication for a manufacturing company stated: "We've improved usability, flexibility, granularity, and — to some extent — security from our tokens. With those rotating passcodes, there was no alternative use case for it like how the YubiKey can be used as a U2F token, a FIDO token, an HOTP token, or as a smart card if we want. It was really the granularity and flexibility that are offered with the YubiKey [that led to our deployment]."

- **Protect all corporate systems regardless of vendor, infrastructure, or region.** Decision-makers needed an MFA solution that could work for their organizations' entire environments to ensure functionality, avoid complexity of multiple devices or solutions, and avoid risk of a failed rollout. The solution needed to support the many technical standards and support the physical demands of the authentication, even for dangerous or high-impact work environments with limited user interfaces or worker equipment.

  The product owner of authentication in the manufacturing industry spoke of their organization's varied systems with different security level needs, while the general director of information assurance in the transportation industry told Forrester about their organization's thousands of employees distributed extensively and individually across North America. A director of security engineering with an energy company described how their organization needed MFA in both office environments and intense physical environments. They said, "Many times, these servers are in network closets out in the middle of the plant floor, like in an industrial environment."

  Enable smooth, fast rollout with flexible architecture plus first- and third-party deployment and distribution options. To accelerate implementation, interviewees' teams wished to have the option to partake in a vendor's distribution program or collaborate with knowledgeable and supportive partners. YubiEnterprise Delivery met this goal, simplifying the distribution of YubiKeys to users in both domestic and international locations including residential addresses. The product owner of authentication in the manufacturing industry said their company used a partner for a similar goal. They explained: "[The distributor] took the orders, processed them, worked directly with Yubico, and handled [complications such as] customs, tariffs, or import fees from the various different

countries. We used to literally have [an employee] stuff an envelope full of [our previous solution], stick [an address label on an] envelope, and [bring it] down to our internal post office."

- **Ensure trust, quality, and consistent supply.** The selected MFA solution needed to be from a vendor decision-makers could trust to limit risk of intrusion through product weaknesses or back doors. Hardware needed to be traceable, have high quality to avoid breakages or failures, and needed to have a consistent and fast supply to avoid disruption to the business.
- **Offer positive end-user experiences.** Security leaders wanted to avoid disrupting end users and provide them value in the process. The MFA solution needed to support a variety of form factors, ports, and systems. Solutions that could be used by employees to secure their personal lives were desirable, effectively turning a security requirement into an employment benefit.
- **Enable the ability to sell offerings to customers with high security demands.** Interviewees' organizations needed authentication capabilities that met the highest levels of security requirements for government clients and customers in other critical industries. It was important both that their own organizations could demonstrate security of customers' data in their solutions and that they could bundle YubiKeys with their software and hardware offerings for customers themselves to use when interacting with the system.

"I haven't seen any supply chain issues with Yubico, which is pretty impressive considering almost every other vendor we deal with has insanely long lead times this year. The keys are manufactured in the US and Sweden, so we feel very comfortable. Their hardware is reliable, the keys are available, and the [YubiEnterprise Delivery] service has been really good."

Senior director of IT, B2B technology

SELECTION CRITERIA

After evaluating a variety of authentication options, interviewees' organizations ultimately selected Yubico's YubiKeys for the following reasons:

- Ability to provide a high level of security via phishing-resistant MFA.
- Brand recognition, reputation, trust, and market adoption.
- Build quality, durability, and trusted supply chain including production of the hardware in the United States and Sweden.
- Positive user experience with easy-to-use form factors and multiple connectors including USB-A, USB-C, Lightning, and NFC that work with major desktop and mobile operating systems.
- Flexibility with open standards to support current and future protocols like FIDO2, WebAuthn U2F, PIV, OATH TOTP/HOTP, and OpenPGP, including two custom configurable slots, and enabling passwordless logins.
- Professional services from Yubico and its partners for implementation, deployment, and ongoing management, as well as enterprise services such as YubiEnterprise Delivery and YubiEnterprise Subscription programs.
- Yubico's supportiveness and flexibility to assist with customers' unconventional situations, such as systems without connectivity, air-gapped systems, or unique software requirements.

Voice Of The Customer

"We chose Yubico for a few reasons. … We like the flexibility of the various tokens with USB-A, USB-C, [Lightning, and NFC]. ... We like that they have a lot of different ways you can utilize them. We can utilize them as an event-driven token, an HOTP token with a button press, or basically as a static password similar to a security card."
— Product owner of authentication, manufacturing

"Our decision to go with YubiKeys was the enterprise distribution platform and the ability to do sort of point-to-point distribution. We chose a model that met our needs and could do the fulfillment."
— IT product manager, media and communications

"[We] decided that the YubiKey would be acceptable for the highest-level protection but that the smartphone would not."
— Product owner of authentication, manufacturing

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, and it is used to present the aggregate financial analysis in the next section.

The composite organization has the following characteristics:

- **A global company based in North America with 5,000 users.** The composite company has an annual revenue of $2.5 billion with an average operating margin of 13.6%.[28]
- **Embracing MFA to simplify and eventually eliminate password policies.** The composite company hopes to eliminate passwords where possible, simplify existing password policies, and reduce policy management. Before implementing YubiKeys, the organization did not use MFA and enforced quarterly password changes with strict password requirements. With these prior policies, the composite company averaged one password reset per user per year.
- **Selecting the YubiEnterprise Subscription and YubiEnterprise Delivery programs.** The composite company utilizes Yubico's subscription model for purchasing keys, replacements, and professional services and the delivery model for distribution.

Deployment characteristics. The composite organization employs Yubico's YubiEnterprise Delivery program to manage the distribution of security keys to its global users. Sixty percent of the company's users work at or near a bulk distribution point such as an office, while 40% work remotely. The composite manages the implementation and user training itself with advice and support from Yubico.

Reference table. The following reference table lists key metrics for the composite organization that are used throughout this financial analysis. In addition to the metrics described elsewhere in this section:

- The average fully burdened hourly salaries for DevSecOps and cross-functional leaders are based on TEI standards for common roles at interviewees' organizations that are involved in the YubiKeys investment.
- The average fully burdened hourly salary for private industry FTEs is the rounded US average from the Bureau of Labor Statistics.[29]
- Risk exposure for the composite in rows R7 through R12 is calculated using data from the Forrester Consulting Cost Of A Cybersecurity Breach Survey, Q1 2021, as described in the Quantifying Security Breach Exposure section.

Key Assumptions

- **$2.5 billion in annual revenue**
- **Employs 5,000 global users**
- **Exposed to $1.5 million in material breach risk per year**
- **Deploys YubiKeys for phishing-resistant MFA on the journey to passwordless MFA**

Reference Table

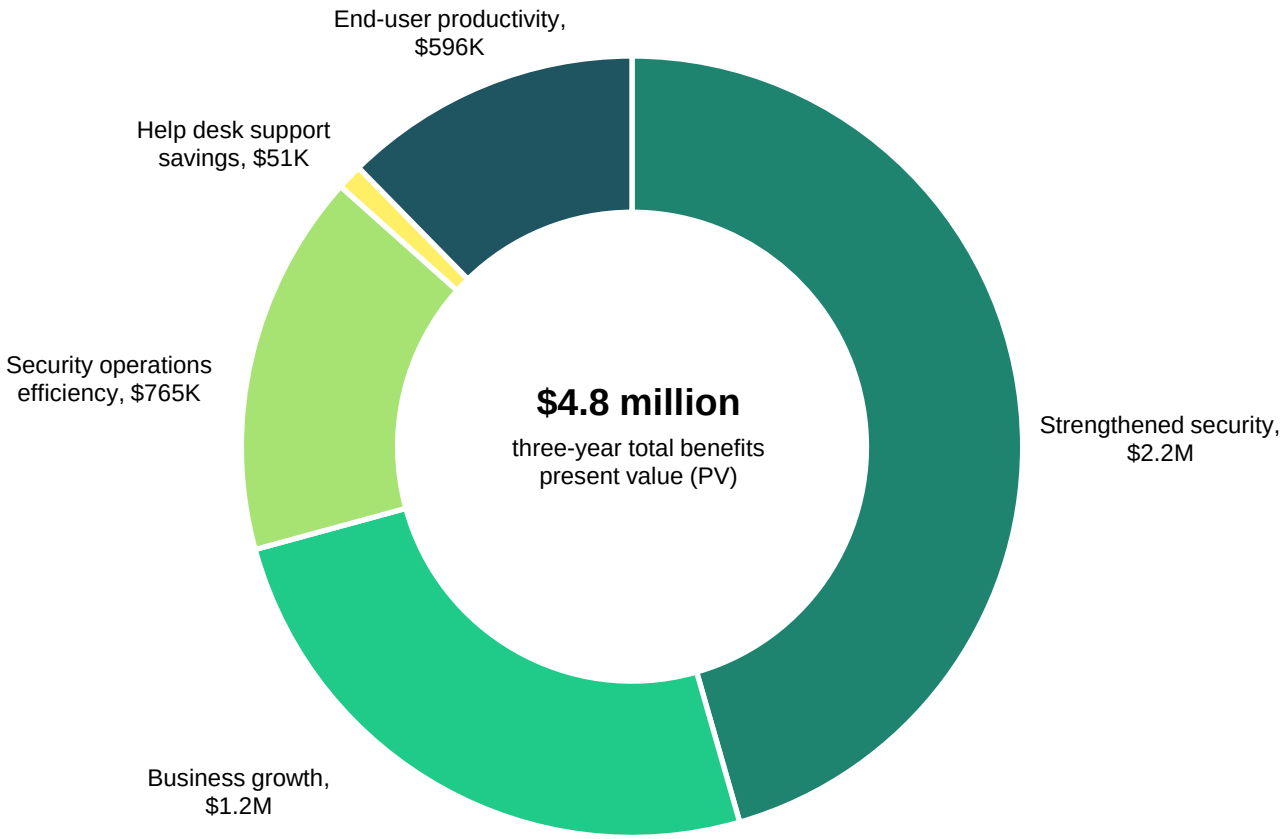
Ref.	Metric	Source	Metric
	Composite		
R1	Annual revenue	Composite	$2,500,000,000
R2	Average pre-tax, pre-stock compensation operating margin	Stern School of Business at NYU, January 2022	13.6%
R3	Number of users	Composite	5,000
	Salaries		
R4	Average fully burdened hourly salary for DevSecOps employees	TEI standard	$58
R5	Average fully burdened hourly salary for cross-functional leaders	TEI standard	$100
R6	Average fully burdened hourly salary for private industry FTEs	Bureau of Labor Statistics	$38
	Risk Exposure		
R7	Average remediation and reporting labor cost per material breach	Forrester Consulting	$199,346
R8	Average costs of response and notification, fines, damages, compliance costs, and customer compensation per material breach	Forrester Consulting	$269,550
R9	Average lost business revenues and additional costs to acquire customers per material breach	Forrester Consulting	$385,296
R10	Total estimated cost of a significant material breach	R7+R8+R9	$854,192
R11	Average incidence of significant material breaches per year	Forrester Consulting	1.8
R12	Annualized risk exposure to significant material breaches	R10*R11	$1,537,546

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	Strengthened security	$884,741	$884,741	$884,741	$2,654,222	$2,200,219
Btr	Business growth	$0	$522,750	$1,045,500	$1,568,250	$1,217,524
Ctr	Security operations efficiency	$307,632	$307,632	$307,632	$922,896	$765,035
Dtr	Help desk support savings	$10,625	$21,250	$31,875	$63,750	$51,169
Etr	End-user productivity	$201,875	$242,250	$282,625	$726,750	$596,070
	Total benefits (risk-adjusted)	$1,404,873	$1,978,623	$2,552,373	$5,935,868	$4,830,017



STRENGTHENED SECURITY

Evidence and data. Since deployment of YubiKeys, the interviewees' organizations have had no breaches or failed penetration tests. Interviewees firmly stated that Yubico's YubiKeys virtually eliminated the risk of breaches involving phishing or stolen credentials, driving interviewees' organizations to widely deploy security keys.

- The general director of information assurance for a transportation company shared, "We have a risk-acceptance curve with a predicted cost of risk, and YubiKeys lowered our risk profile significantly." They cited other industry research, noting the importance of multifactor and said: "[To win budget for YubiKeys,] I sell YubiKeys as a huge risk reduction."
- An IT product manager for a media and communications organization said: "[YubiKeys] give us peace of mind where we know that there is a certain range of phishing attacks [and] that when they happen, [they] are less risky now. … For me, the biggest benefit of Yubico is just knowing that these identities are safe from phishing. In general, even if someone steals an employee's password, they can't do anything with it. So even if people reused their same common password from their [personal life] and their password gets leaked, it doesn't matter because the attacker who has the credentials also physically needs the key [to access our environment]."
- The director of security engineering at an energy company shared: "Ransomware typically gets onto systems via social engineering. Having [YubiKeys as] a second factor of authentication makes social engineering extremely difficult to almost near impossible. That's where this becomes so important."

> **"We're safe from 99.9% of [credential theft and phishing] attacks."**
>
> *Senior director of IT, B2B technology*

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

- The composite organization faces phishing and credential theft attacks, representing 64% of its $1.5 million in annualized risk exposure.[30]
- YubiKeys prevents 99.9% of these attacks from succeeding.

Risks. Risk reduction may vary based on:

- The presence and efficacy of other security tools.
- The company size, industry, region, sensitivity and volume of data, workforce composition, and other unique factors affecting risk exposure.
- The scale of the YubiKey deployment and the decisions made by security teams regarding password and authentication policies.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $2.2 million.

Strengthened Security					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
A1	Annualized risk exposure to significant material breaches	R12	$1,537,546	$1,537,546	$1,537,546
A2	Percent of breaches involving phishing or credential theft paths	Verizon	64.0%	64.0%	64.0%
A3	Reduced credentials or phishing attack successes with YubiKeys	Interviews	99.9%	99.9%	99.9%
At	Strengthened security	A1*A2*A3	$983,045	$983,045	$983,045
	Risk adjustment	↓10%			
Atr	Strengthened security (risk-adjusted)		$884,741	$884,741	$884,741
	Three-year total: $2,654,222			**Three-year present value: $2,200,219**	

BUSINESS GROWTH

Evidence and data. Deploying YubiKeys offered organizations new business opportunities due both to improved security reputations (and avoided losses) and the ability to meet stringent customer security requirements. All five interviewees' organizations promoted the use of YubiKeys during discussions with clients and customers. Two interviewees actively marketed their use of YubiKeys publicly to drive interested and improve reputation. Interviewees noted how specific deals were won because YubiKeys were supported as an authentication protocol for the buyer. With YubiKeys, several organizations could now bid on (and win) deals by meeting CMMC L3 MFA requirements. YubiKeys met many various high-security requirements, enabling access to new potential buyers and offerings.

- The IT product manager in the media and communications industry said, "We've definitely seen [YubiKeys'] positive impact on reputation and positive feedback." A senior director of IT of a B2B technology firm said: "We're protecting [critical] systems from bad actors [with YubiKeys]. If a breach happened and it was audited and disclosed, the impact to our company's reputation and potential stock price could be super, super expensive."
- When asked the following: "Is there potentially a business value there like you need that key to be able to win that business and do that business with the government?", the senior director of IT for a B2B technology company responded affirmatively. He explained, "Engineers are required to use a fixed certain security key from Yubico [to meet regulations]."
- The director of security engineering for an energy company shared: "We were able to make at least two very big sales because the [enterprises] already use YubiKeys. During the presentation, we told them that we supported YubiKey, and they got big smiles on their faces because it was a familiar technology."

"Yubico has driven revenue. We can help customers meet strong cybersecurity requirements and we can help them support and implement those requirements. [YubiKeys] are driving value."

Director of security engineering, energy

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

- The composite organization has $2.5 billion in annual revenue.
- The composite organization's security reputation and customer convenience improve over time, resulting in increased deal conversion rates.
- The composite attributes 50% of revenue from better deal conversions driven by security reputation and customer convenience to Yubico.
- The composite now meets CMMC Level 3 MFA security requirements with YubiKeys, allowing it to bid on government contracts with high security requirements. It bids on and wins a total of 12 deals with an average size of $1 million and a tighter profit margin due to aggressive negotiation needed to win the government contracts.

Risks. Business growth may vary based on:

- The annual revenue and operating margin.
- The security reputation and perception and the level of promotion done regarding MFA.
- The industry and types of products offered and, subsequently, the value of protecting those offerings and associated data with MFA.
- The ability to bid on deals with high security requirements and the associated size and win rate for those deals.

Results. To account for these risks, Forrester adjusted this benefit downward by 25%, yielding a three-year, risk-adjusted total PV of $1.2 million.

Business Growth

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Annual revenue	R1	$2,500,000,000	$2,500,000,000	$2,500,000,000
B2	Increased deal conversion rate from security reputation and customer convenience with YubiKeys	Interviews	0.00%	0.25%	0.50%
B3	Attribution of YubiKeys to identified business growth	Assumption	50%	50%	50%
B4	Operating profit margin	R2	13.6%	13.6%	13.6%
B5	Incremental profit from improved security reputation	B1*B2*B3*B4	$0	$425,000	$850,000
B6	Deals identified and won with YubiKeys that required CMMC Level 3 MFA security to bid	Interviews	0	4	8
B7	Average deal size for high-security business opportunities	Composite	$1,000,000	$1,000,000	$1,000,000
B8	Profit margin reduction for competitive contracts	Assumption	50.0%	50.0%	50.0%
B9	Incremental profit from winning high-security clients	B4*B6*B7*(1-B8)	$0	$272,000	$544,000
Bt	Business growth	B5+B9	$0	$697,000	$1,394,000
	Risk adjustment	↓25%			
Btr	Business growth (risk-adjusted)		$0	$522,750	$1,045,500
	Three-year total: $1,568,250			**Three-year present value: $1,217,524**	

SECURITY OPERATIONS EFFICIENCY

Evidence and data. By deploying YubiKeys, organizations gained substantial labor efficiency. DevSecOps employees no longer had to investigate phishing and credential theft attacks due to their reduction or spend as much time on password-related tasks due to the elimination of password policies and related complexity. This allowed security personnel to dedicate time to other tasks. YubiKeys were widely usable out of the box with major open standards and most third-party solutions. For third parties that do not currently support YubiKeys or an associated open standard, Yubico offers integration support for technology partners.

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

- Security operations personnel are saving portions of workloads team-wide totaling three FTEs.
- The composite vastly simplifies and eliminates password policies on the road to passwordless.

Risks. Efficiency savings may vary based on:

- Unique business complexities including technology and data environment, security tooling, and the labor spent managing passwords and investigating attacks.
- The decisions made regarding password policies and potential passwordless future.
- The number of DevSecOps employees and their average salaries.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of $765,000.

> **"When we get notifications [about compromised passwords], we know that the accounts are safe because they're protected by security keys. ... If we weren't using security keys, we'd have a totally different security response process that's really intense."**
>
> *Senior director of IT, B2B technology*

Security Operations Efficiency

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Security personnel reallocated to other value-add tasks by avoiding investigation of phishing or credential theft attacks	Interviews	2	2	2
C2	Security personnel reallocated to other value-add tasks by simplifying password policies and reducing policy management	Interviews	1	1	1
C3	Security operations FTEs reallocated to other security tasks	C1+C2	3	3	3
C4	Average fully burdened annual salary for DevSecOps employees	R4*2,080	$120,640	$120,640	$120,640
Ct	Security operations efficiency	C3*C4	$361,920	$361,920	$361,920
	Risk adjustment	↓15%			
Ctr	Security operations efficiency (risk-adjusted)		$307,632	$307,632	$307,632
	Three-year total: $922,896		**Three-year present value: $765,035**		

HELP DESK SUPPORT SAVINGS

Evidence and data. Simplifying password policies with YubiKeys enabled interviewees' organizations to significantly reduce or eliminate password reset and related support tickets. They also reduced device authentication tickets. For example, the IT product manager in the media and communications industry shared: "There usually was a surge in tickets in [whenever phonemakers] release new phones. We've actually eliminated that class of tickets completely because we no longer need people to repair their own authenticator when setting up a new device." Although organizations did gain tickets related to YubiKeys, the net result was a significant overall reduction in tickets that improved over time.

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

- The composite organization has 5,000 users.
- Passwords are reset once per year at an average cost of $10 per ticket. Note: User productivity savings are shown separately in the next section.
- YubiKeys eliminate password tickets as the composite simplifies password policies, but also generate new security key-related tickets. By Year 3, the composite reduces tickets by 75%.

Risks. Support savings may vary based on:

- The number of users and company size.
- The number of password resets per user per year and the cost of a password reset ticket. Ticket costs vary significantly depending on availability of self-service and regional agent costs.
- The decisions made regarding password policy.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of $51,000.

> **"The number of help desk tickets is down closer to 25% with YubiKeys versus tickets for password issues before implementing MFA."**
>
> *General director of information assurance, transportation*

Help Desk Support Savings

Ref.	Metric	Source	Year 1	Year 2	Year 3
D1	Number of users	R3	5,000	5,000	5,000
D2	Typical password resets per user, per year	Assumption	1	1	1
D3	Typical number of password resets	D1*D2	5,000	5,000	5,000
D4	Average cost per ticket	Assumption	$10	$10	$10
D5	Percent reduction in tickets by replacing password resets with tickets for hardware keys	Interviews	25%	50%	75%
Dt	Help desk support savings	D3*D4*D5	$12,500	$25,000	$37,500
	Risk adjustment	↓15%			
Dtr	Help desk support savings (risk-adjusted)		$10,625	$21,250	$31,875
	Three-year total: $63,750			**Three-year present value: $51,169**	

END-USER PRODUCTIVITY

Evidence and data. Interviewees whose organizations eliminated quarterly password resets and simplified password rules said users saved significant time and frustration by no longer having to repeatedly update their passwords, meet stringent password rules, repeatedly memorize new passwords, and occasionally go through password reset processes. Furthermore, they said users also loved the experience and time savings of tapping a YubiKey compared to entering a code from a mobile application or other legacy hardware MFA options.

The product owner of authentication in the manufacturing industry stated: "Users like the simplicity of the key. They like just plugging it in and pushing the button, and most just leave it plugged in all day long. It's a lot simpler and faster than having to read [and input] a code."

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

- The composite organization has 5,000 users.
- The composite organization did not use MFA prior to using YubiKeys. It previously enforced strict password requirements with quarterly changes, which are eliminated with YubiKeys.
- Not all time saved for users will lead to additional value-add work. Forrester's standard for Total Economic Impact studies estimates that 50% of time saved will be returned to productive work.

Risks. End-user productivity may vary based on:

- The prior security and password policies.
- The number of users and company size.
- The habits of users and the nature of their work.
- The average fully burdened hourly salaries.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of $596,000.

End-User Productivity

Ref.	Metric	Source	Year 1	Year 2	Year 3
E1	Number of users	R3	5,000	5,000	5,000
E2	Hours saved per user per password update	Interviews	0.5	0.5	0.5
E3	Total hours saved for quarterly password updates	E1*E2*4	10,000	10,000	10,000
E4	Number of avoided password resets per year	D3*D5	1,250	2,500	3,750
E5	Hours of end user disruption avoided per password reset	Interviews	2	2	2
E6	Hours saved by end users from prevented password resets	E4*E5	2,500	5,000	7,500
E7	Total hours saved by end users	E3+E6	12,500	15,000	17,500
E8	Average fully burdened hourly salary for private industry FTEs	R6	$38	$38	$38
E9	Productivity recapture rate	TEI standard	50%	50%	50%
Et	End-user productivity	E7*E8*E9	$237,500	$285,000	$332,500
	Risk adjustment	↓15%			
Etr	End-user productivity (risk-adjusted)		$201,875	$242,250	$282,625
	Three-year total: $726,750		**Three-year present value: $596,070**		

UNQUANTIFIED BENEFITS

Additional benefits that customers experienced but were not able to quantify include:

- **Labor and cost savings from legacy hardware authentication elimination.** Some interviewees' organizations used legacy physical authentication methods before using YubiKeys. These interviewees said that before making the transition, the downsides to these legacy tokens and cards included physical damage, drained batteries, mindless authentication, and poor user experiences.

  Although moving to YubiKeys from a legacy MFA solution may not have yielded as great of a risk reduction as compared to a company not yet using MFA, the benefits were still evident to the interviewees. These organizations instead made strong business cases around savings from no longer managing and using legacy physical authentication solutions alongside improved user experiences and other benefits.

- **Improved security and data protection for end customers and partners.** Interviewees highlighted how their organizations' clients, customers, and partners benefited from their improved security in addition to their direct users and employees.

- **Strong and trusted partnership with Yubico.** Interviewees found solace not only in Yubico's hardware, but also in their supply chain and support. Yubico manufactures its security keys in the United States and Sweden, and interviewees' organizations never experienced supply issues. This was critical when committing to a new solution. Furthermore, interviewees spoke highly of Yubico's flexibility and assistance with their organizations' unique use cases.

  The IT product manager for a media and communications company emphasized the trust they placed in Yubico and its supply chain: "The other value for me was brand trust. I started working with Yubico, and we were writing out on a napkin how this could work. Once I realized I could really trust this company and that [Yubico is] really just top of its class, that's when I went to [my leadership] and said that YubiKeys could probably help us with our supply chain security."

- **Improved employee experience.** Interviewees shared stories of improved user experiences with less password and hardware frustration. They said they and end users valued the diverse form factor and connection options, which helped protect devices and accounts both in the office and at home. Further, users were encouraged to use YubiKeys to protect their personal accounts as an added employee benefit. This helped prevent frustrating, time-consuming, and potentially costly breaches in their personal lives.

  The product owner of authentication for a manufacturing company said: "The users like just plugging [their YubiKey] in and [touching the sensor]. They don't even take it out of their USB port. For them, it's a lot simpler [and] faster than [legacy options]." Similarly, the B2B technology company's senior director of IT shared, "[Once users] know how to use [YubiKeys], it's faster [than other MFA methods] because all they have to do is tap it."

"[With YubiKeys], we're saying that we care about employees and protecting their data. We provide these keys as a service to help people protect their personal identities as well."

Senior director of IT, B2B technology

- **Strong partner and vendor ecosystem.** Interviewees' organizations advocated for the value and capabilities of the partners that helped them deploy and manage their YubiKeys. The transportation company's general director of information assurance received valuable support from Yubico and one of its partners, remarking: "Yubico will let you implement however you want. They're not going to restrict you. They're not going to mandate for you. I look to Yubico and [our partner] as a huge part [of our success]. We wouldn't be successful without Yubico."

"Reputation matters. Yubico has almost immediate support follow-up and they always are willing to work outside the box."

Director of security engineering, energy

FLEXIBILITY

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

- **Securing and tracking internal processes.** Interviewees spoke of novel uses for YubiKeys like requiring a valid security key authentication to approve payments, submit code commits, and grant data access.

  The senior director of IT for a B2B technology company discussed how their organization creatively used YubiKeys to sign code commits and create a chain of proof. They said: "By using [a data encryption program with] the security key, we are actually signing commits to code [with YubiKeys] which helps us to ensure the security of the software supply chain from computer to deployment."

- **Leveraging open standards.** Choosing an MFA solution based on open standards enabled interviewees' organizations to adopt current standards and adapt to new, modern standards like FIDO2. Already-deployed YubiKeys could be used for new authentication protocols without disruptive redistribution and could support multiple functions simultaneously during a phased rollout. Additionally, interviewees valued the interoperability and portability to authenticate in virtually any environment from any vendor without the lock-in that comes from using an open standards-based solution. YubiKeys could even be used in novel ways, such as securing an air-gapped system.

  The general director of information assurance for a transportation company discussed the flexibility of YubiKeys' open standards, saying: "YubiKeys save us from buying an additional token [for different environments] and managing that additional token separately. Further, FIDO is still our end goal, and it's still the direction that cybersecurity world seems to be going. When we get there, we can leverage the YubiKeys that are already in our customers' and employees' hands to make that change with no additional cost or logistics. We already did the work, and we will get to reap the benefits."

- **Deployment flexibility with subscription or perpetual purchase models.** Yubico customers can purchase keys individually or in bulk as perpetual purchases or use the YubiEnterprise Subscription. The subscription model provides budget predictability and control, shifting from capital expenditure-based (capex) to operating expenditure-based (opex) to lighten the blow to initial budgets and adding agility for evolving

business needs. The subscription model also includes key replacements, which could simplify processes during employee turnover with just-in-time inventory and management. Evaluating which model will be better for an organization will depend on the organization's priorities, the size of its user base, the unique behaviors and needs of users, and the length of time included in the financial analysis to compare costs.

- **Supporting a passwordless future.** With multiprotocol support, YubiKeys offer a bridge to passwordless authentication, enabling a smooth transition to a passwordless future. YubiKeys were a critical part of interviewees' plans to move beyond passwords and improve their security.

  The IT product manager of a media and communications organization said: "[YubiKeys] have helped us prepare to move away from a traditional VPN toward externally accessible applications. We are a lot more likely to adopt a security scope similar to Zero Trust with a key-based U2F (universal 2nd factor). It is a lot more interesting and compelling because YubiKeys are there as one of the bedrock pieces."

- **Choosing the keys users need.** YubiKeys come in many form factors with connectors that ensure they work across various devices and operating systems, including mobile and desktop, giving interviewees' organizations the flexibility to adapt to the needs of their users.

- **Improving planning with better visibility to inventory and demand.** Using YubiEnterprise Delivery, interviewees' organizations could more easily monitor inventory and demand for YubiKeys, which helped to better predict, control, and plan for their users' needs. Using YubiEnterprise Subscription, they could also potentially minimize the need for bulk purchases to avoid the risk of purchasing excess inventory versus demand, purchasing the wrong form factors for their users, or needing to store and track large amounts of on-site inventory.

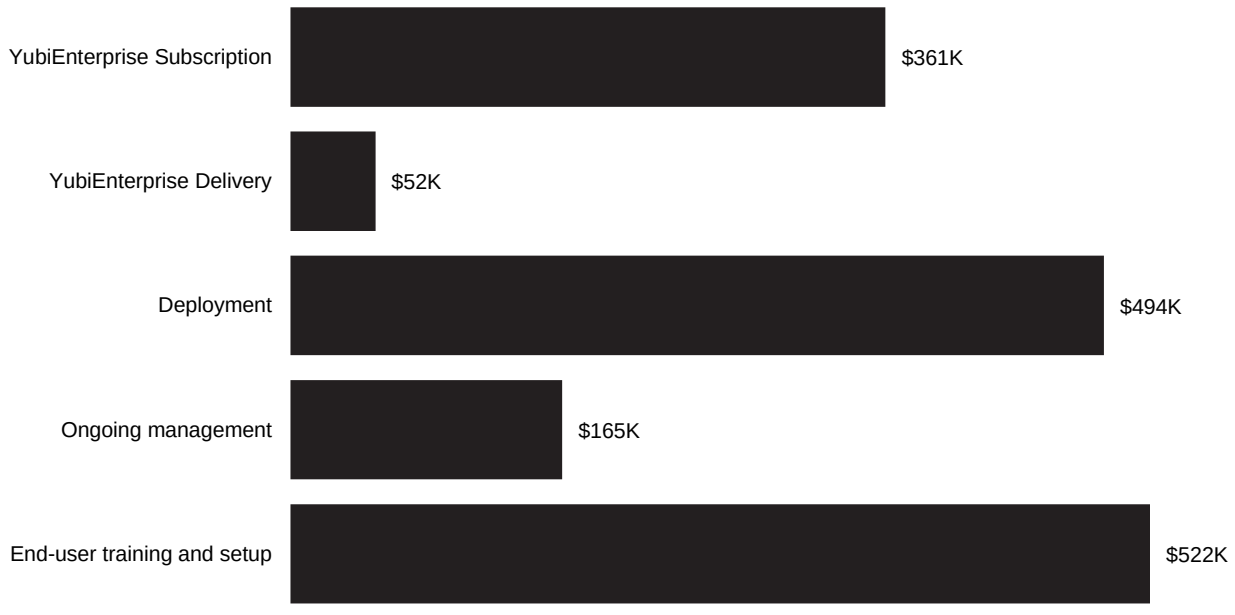
Flexibility would also be quantified when evaluated as part of a specific project (described in more detail in Appendix A).

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	YubiEnterprise Subscription	$33,000	$132,000	$132,000	$132,000	$429,000	$361,264
Gtr	YubiEnterprise Delivery	$34,500	$6,900	$6,900	$6,900	$55,200	$51,659
Htr	Deployment	$493,944	$0	$0	$0	$493,944	$493,944
Itr	Ongoing management	$0	$66,352	$66,352	$66,352	$199,056	$165,008
Jtr	End-user training and setup	$418,000	$41,800	$41,800	$41,800	$543,400	$521,950
	Total costs (risk-adjusted)	$979,444	$247,052	$247,052	$247,052	$1,720,600	$1,593,825

Costs (Three-Year)



YUBIENTERPRISE SUBSCRIPTION

Evidence and data. Interviewees' organizations purchased YubiKeys via both perpetual and subscription models. The capex perpetual model includes one-time purchases of YubiKeys with lifetime use. When keys are lost or new employees are hired, new keys must be purchased. In contrast, the opex subscription model incurs recurring charges per user per year with included key replacements, even as users leaving the company take their keys with them. The YubiEnterprise Subscription program can provide predictable annual costs, reliable supplies with buffer, replacements, flexibility, and technical support from Yubico.

- The IT product manager for a media and communications organization spoke about the benefits of the subscription model and the exchange of capex for opex. They said: "People are used to exchanging [costs like this] via capex. But now, for things like the actual operational flow when people … need a replacement, we are seeing the benefits of the [YubiEnterprise Subscription] program."
- The same IT product manager also discussed the flexibility of the subscription program. They said: "[YubiEnterprise Subscription] lets us choose. Over time, we went with a YubiKey 5C NFC, which is what we were looking for to get the combination. But if we were to branch it out into other types of keys we were offering [to users], it would be very easy for us to add that then."

Modeling and assumptions. Forrester modeled the cost for the composite organization assuming:

- The composite organization uses Yubico's YubiEnterprise Subscription program at the advanced tier and pays list pricing rates. This tier includes YubiKey 5 NFC and nano options with USB-A and USB-C port options.
- The composite organization has 5,000 users. Subscription costs start an average of three months prior to launch day to allow time for distribution and training.
- Subscription pricing may vary by company size and needs. For organizations considering perpetual purchases, list pricing is publicly available on Yubico's website and from other retailers. Contact Yubico for additional details.

Risks. YubiEnterprise Subscription fees may vary based on the number of users and the desired models of YubiKeys to meet user needs.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $361,000.

YubiEnterprise Subscription

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
Ft	YubiEnterprise Subscription	Yubico	$30,000	$120,000	$120,000	$120,000
	Risk adjustment	↑10%				
Ftr	YubiEnterprise Subscription (risk-adjusted)		$33,000	$132,000	$132,000	$132,000
	Three-year total: $429,000			**Three-year present value: $361,264**		

YUBIENTERPRISE DELIVERY

Evidence and data. Security key distribution has grown more complex in recent years as remote work has increased. To deliver YubiKeys to their employees whether at home or at work, most interviewees' organizations participated in Yubico's YubiEnterprise Delivery program, taking advantage of efficient outsourced distribution and a cloud-based ordering and APIs.

Aside from minimum purchase requirements, the only associated cost was shipping. Shipping costs would be incurred regardless of whether an organization uses this service or does it themselves, though costs may vary. Interviewees reported saving significant labor effort and frustration by using this service.

The senior director of IT of a B2B technology company told Forrester: "We've fully automated the process that programmatically ships [new hires] their laptop and interacts with Yubico through their APIs to ship them security keys. [YubiEnterprise Delivery] will ship the keys to users and provide tracking information."

Modeling and assumptions. Forrester modeled the cost for the composite organization assuming:

- The composite organization takes advantage of Yubico's YubiEnterprise Delivery program.
- The composite organization has 5,000 users.
- Around 40% of the composite organization's workforce is remote, and the remaining 60% can get YubiKeys from offices.
- The composite ships YubiKeys globally at an average cost of $15 per key, based on interview-reported costs for sample locations in North America and Europe.

Risks. Distribution costs may vary based on:

- The number of users and company size.
- The global locations of workers and offices.
- The shipping speed and priority for keys.
- The habits of workers and the nature of their work, which may lead to more lost keys.
- Potential shipping rate increases.

Results. To account for these risks, Forrester adjusted this cost upward by 15%, yielding a three-year, risk-adjusted total PV of $52,000.

YubiEnterprise Delivery

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
G1	Number of users	R3	5,000	5,000	5,000	5,000
G2	Percent of total users receiving a new key in the calendar year	Interviews	100%	20%	20%	20%
G3	Percent of keys shipped to users rather than distributed in bulk	Composite	40%	40%	40%	40%
G4	Average global shipping cost per key sent directly to users	Interviews	$15	$15	$15	$15
Gt	YubiEnterprise Delivery	G1*G2*G3*G4	$30,000	$6,000	$6,000	$6,000
	Risk adjustment	↑15%				
Gtr	YubiEnterprise Delivery (risk-adjusted)		$34,500	$6,900	$6,900	$6,900
	Three-year total: $55,200		**Three-year present value: $51,659**			

DEPLOYMENT

Evidence and data. After selecting Yubico YubiKeys, interviewees' organizations took steps to build, test, deploy, and evangelize the new solution. The keys themselves supported many standards and required minimal labor. However, in many cases, organizations needed to update or deploy solutions to enable MFA for systems that did not use MFA in the past or used outdated standards.

- Interviewees emphasized the importance of gaining buy-in from management and users before and during deployment. Lack of understanding regarding hardware keys and MFA led to early resistance; having top leaders such as the CEO on board helped change hearts and minds to make deployment successful.
- Deployment effort varied significantly by organization due to the vast range technology environments and physical workplaces ranging from offices, remote workers, or even air-gapped systems. All deployments required some technical labor to integrate YubiKeys.
- Interviewees' organizations often ran a pilot or deployed in stages, prioritizing users with access to the most critical information first. After early successes, the organizations rolled out YubiKeys to the rest of their teams. Positive feedback from early adopters and business groups helped get other leaders and teams to support the initiative.

"The key stakeholder that probably made us successful was our CEO. He was supportive both financially and very willing to talk to people and share with them that he supports our rollout to MFA. That took a lot of the friction away for our project."

General director of information assurance, transportation

"[When we started implementing YubiKeys], we had a person that was ripping on our project. I ran into them a year later, and the first thing they said was: 'I have to apologize to you. This is really easy to use.'"

General director of information assurance, transportation

Modeling and assumptions. Forrester modeled the cost for the composite organization assuming:

- The composite organization insources deployment, committing three technical resources over the one-year deployment
- Cross-functional leaders commit 780 hours to deployment and pilot users commit 240 hours to testing and feedback during the deployment.
- The composite organization takes advantage of Yubico's YubiEnterprise Subscription program and implements YubiKeys with guidance from Yubico team members.

Risks. The deployment costs may vary based on:

- The option to insource or outsource deployment work with support from Yubico or a partner.
- Unique business complexities and needs.
- The average fully burdened hourly salaries.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $494,000.

Deployment						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
H1	Internal labor hours for security, IT, and network engineers	Interviews	6,240			
H2	Average fully burdened hourly salary for technical employees	R4	$58			
H3	Technical labor cost	H1*H2	$361,920			
H4	Internal labor hours for cross-functional leadership and change management	Interviews	780			
H5	Average fully burdened hourly salary for cross-functional leaders	R5	$100			
H6	Cross-functional labor cost	H4*H5	$78,000			
H7	Internal labor hours for pilot users	Interviews	240			
H8	Average fully burdened hourly salary for private industry FTEs	R6	$38			
H9	Pilot user labor cost	H7*H8	$9,120			
Ht	Deployment	H3+H6+H9	$449,040	$0	$0	$0
	Risk adjustment	↑10%				
Htr	Deployment (risk-adjusted)		$493,944	$0	$0	$0
	Three-year total: $493,944		**Three-year present value: $493,944**			

“Our CISO was an advocate of YubiKeys [and] our CTO was using one on their personal accounts. They were into [MFA], they understood it, and so we understood the value of it.”

— Senior director of IT, B2B technology

ONGOING MANAGEMENT

Evidence and data. Interviewees discussed ongoing management requirements beyond the initial deployment of YubiKeys to their organizations' users. Ongoing work included technical tasks like patching, updates, and implementations along with management labor for security key distribution and user training.

- When asked about ongoing management costs, the general director of information assurance for a transportation company with tens of thousands of users answered: "It's typically between 15 minutes and an hour every day. … In our headquarters, we go through the neighborhood of 60 lost keys a month, and then onboarding depending on the hiring cycle. We distribute those through HR when we can."
- The product owner of authentication of a manufacturing corporation discussed technical workloads over time. They said: "We are going to shut the [legacy] system off. We are at the very end of the migration project now. … It took about three to four years to reach our worldwide user base. Much of that was just the time of getting these applications [migrated] over."
- The senior director of IT for a B2B technology organization spoke about continuous costs, saying: "People lose keys. People travel without their keys and get locked out of their accounts. There is definitely some element of help desk support that comes in."

Modeling and assumptions. Forrester modeled the cost for the composite organization assuming:

- The composite organization uses YubiEnterprise Delivery to reduce ongoing management needs.
- Half of an FTE's time is being devoted to security labor hours for ongoing management.

Risks. Management costs may vary based on:

- Diverse technical environments and workforces which could necessitate extra labor hours.
- Selecting the right key form factors, running effective training, and following best practices can help to mitigate costs or disruption.
- The average fully burdened hourly salaries of the DevSecOps employees.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $165,000.

Ongoing Management

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
I1	Security labor hours for updates, maintenance, and support of authentication environment	Interviews		520	520	520
I2	Security labor hours for running trainings and distributing keys	Interviews		520	520	520
I3	Average fully burdened hourly salary for DevSecOps employees	R4	$58	$58	$58	$58
It	Ongoing management	(I1+I2)*I3	$0	$60,320	$60,320	$60,320
	Risk adjustment	↑10%				
Itr	Ongoing management (risk-adjusted)		$0	$66,352	$66,352	$66,352
	Three-year total: $199,056			**Three-year present value: $165,008**		

END-USER TRAINING AND SETUP

Evidence and data. After purchasing and distributing YubiKeys, interviewees and their teams concentrated on user training and setup. Many users had not used any form of MFA in the past, so early education helped leaders and end users understand MFA and learn how to use Yubikeys. Once executives and users got over the hump, they quickly saw the value and came to prefer YubiKeys more than their prior environments. Users typically received up to an hour of formal training on MFA and Yubikeys and spent a small amount of time reading instructional articles and setting up devices and account logins. Total time requirement was typically up to 2 hours per user.

- The manufacturing company's product owner of authentication shared: "It was an hour or two of writing up an article, taking some screenshots, and then publishing that to our internal documentation where the help desk can get this information and relay it to the end user."
- The B2B technology company's senior director of IT shared, "There is some level of help desk tickets or challenges with [users learning to use YubiKeys], but it's so minimal, and the benefit greatly outweighs the pain."

Modeling and assumptions. Forrester modeled the cost for the composite organization assuming:

- The composite organization has 5,000 users.
- The composite did not use MFA prior to YubiKeys. Users need to learn about and get used to MFA and beyond simply using Yubikeys.
- Only first-time users undergo training and setup. Some retraining or further support could be needed, but it is likely to be minimal and is reflected in the risk adjustment.

Risks. End-user labor costs may vary based on:

- The number of users and company size.
- End users' knowledge and familiarization with MFA, which can differ by company, industry, and role and could necessitate extra training.
- Lost YubiKeys, which could require extra setup, reauthentication, and retraining time.
- The average fully burdened hourly salaries.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $522,000.

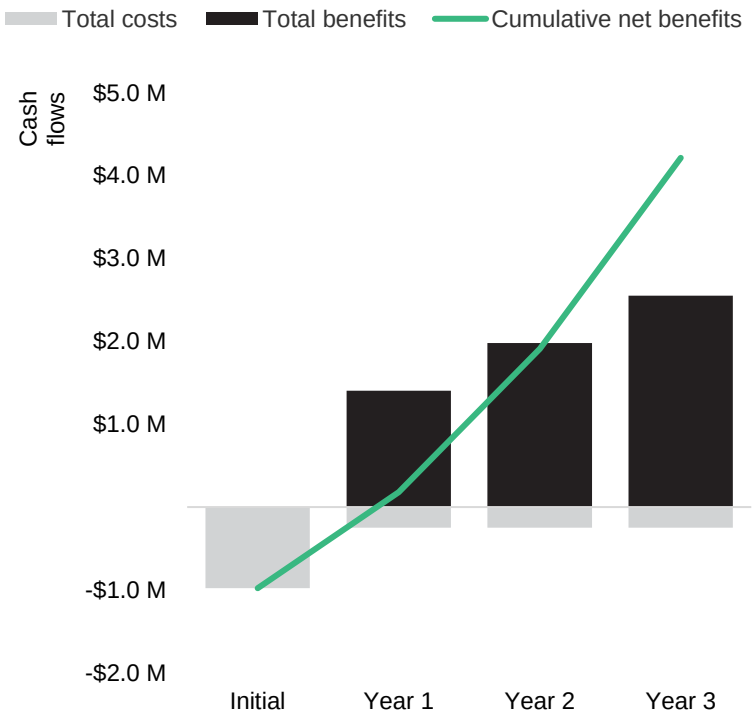
End-User Training And Setup

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
J1	New key deliveries	G1*G2	5,000	1,000	1,000	1,000
J2	Percent of keys going to first-time YubiKey users	Interviews	100%	50%	50%	50%
J3	Number of trainees	J1*J2	5,000	500	500	500
J4	Hours of training, setup, and familiarization per first-time user	Interviews	2.0	2.0	2.0	2.0
J5	Average fully burdened hourly salary for private industry FTEs	R6	$38	$38	$38	$38
Jt	End-user training and setup	J3*J4*J5	$380,000	$38,000	$38,000	$38,000
	Risk adjustment	↑10%				
Jtr	End-user training and setup (risk-adjusted)		$418,000	$41,800	$41,800	$41,800
	Three-year total: $543,400			**Three-year present value: $521,950**		

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	($979,444)	($247,052)	($247,052)	($247,052)	($1,720,600)	($1,593,825)
Total benefits	$0	$1,404,873	$1,978,623	$2,552,373	$5,935,868	$4,830,017
Net benefits	($979,444)	$1,157,821	$1,731,571	$2,305,321	$4,215,268	$3,236,192
ROI						203%
Payback						11 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: "Using Zero Trust To Kill The Employee Password," Forrester Research, Inc., August 2, 2021.

[3] Source: "Now Tech: Enterprise Multifactor Authentication Solutions, Q1 2022," Forrester Research, Inc., February 3, 2022.

[4] Source: "The Top Trends Shaping IAM In 2020," Forrester Research, Inc., January 29, 2020.

[5] Source: "Now Tech: Enterprise Multifactor Authentication Solutions, Q1 2022," Forrester Research, Inc., February 3, 2022.

[6] Source: "Optimize User Experience With Passwordless Authentication," Forrester Research, Inc., March 2, 2020.

[7] Source: "The State Of Customer Authentication, 2022," Forrester Research, Inc., June 2, 2022.

[8] Source: "Now Tech: Enterprise Multifactor Authentication Solutions, Q1 2022," Forrester Research, Inc., February 3, 2022.

[9] Source: Ibid.

[10] Source: Ibid.

[11] Source: "CMMC Practice IA.L2-3.5.3 – Multifactor Authentication: Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.," Defense Industrial Base Sector Coordinating Council.

[12] Source: "The Top Trends Shaping IAM In 2020," Forrester Research, Inc., January 29, 2020.

[13] Source: Sean Ryan, "Two-Factor Authentication (2FA) Or Multifactor Authentication (MFA)? That Is The Question," Forrester Blogs.

[14] Source: "Optimize User Experience With Passwordless Authentication," Forrester Research, Inc., March 2, 2020.

[15] Source: "A Practical Guide To A Zero Trust Implementation," Forrester Research, Inc., August 2, 2021.

[16] Source: Sean Ryan, "Two-Factor Authentication (2FA) Or Multifactor Authentication (MFA)? That Is The Question," Forrester Blogs.

[17] Source: "Remote Workers Turning To SMS-Based Two-Factor Authentication Is Much Better Than Passwords, But It Won't Stop Targeted Attacks," Forrester Research, Inc., September 22, 2020.

[18] Source: "The Current State Of Enterprise Passwordless Adoption," Forrester Research, January 19, 2022.

[19] Source: "Forrester Analytics Business Technographics Security Survey, 2021," Forrester Research, Inc., September 2021.

[20] Source: Ibid.

[21] Source: "2021 Data Breach Investigation Report," Verizon, May 2021; "Cost of a Cyber Incident: Systematic Review and Cross-Validation," Cybersecurity & Infrastructure Agency, October 26, 2021; "How much does a data breach cost in 2022?," IBM, 2021. The high degree of variance in this data across sources is expected. The likelihood and cost of a given breach varies based on many factors. Many breaches are never reported and those that are reported often only have limited data. Estimates must usually rely upon self-reporting, which may not be an accurate representation of real costs. Investigation and measurement methodology significantly affects analysis.

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

[23] Source: Ibid.

[24] Source: Ibid.

[25] Source: Ibid.

[26] Source: Ibid.

[27] The Forrester TEI survey data is the primary source of risk exposure in this study's financial analysis because: 1) It is one of the only available sources that samples all organizations regardless of whether they have had a breach rather than biasing to only measure breaches; 2) It therefore can measure the frequency of breaches per organization; 3) It also pairs this breach frequency with an average cost estimate per breach (most sources do only one or the other); 4) It further breaks down cost beyond a single number into specific categories (most available sources do not do so), exposing more insight and increasing confidence in the data; and 5) Its' breach frequency and cost estimates both fall conservatively within the range of estimates from other notable third-party sources.

[28] Source: "Margins by Sector (US)," NYU Stern School of Business, January 2022.

[29] Source: "Employer Costs For Employee Compensation — March 2022," Bureau of Labor Statistics, June 16, 2022.

[30] Source: "2022 Data Breach Investigation Report," Verizon, June 2022.


FORRESTER®