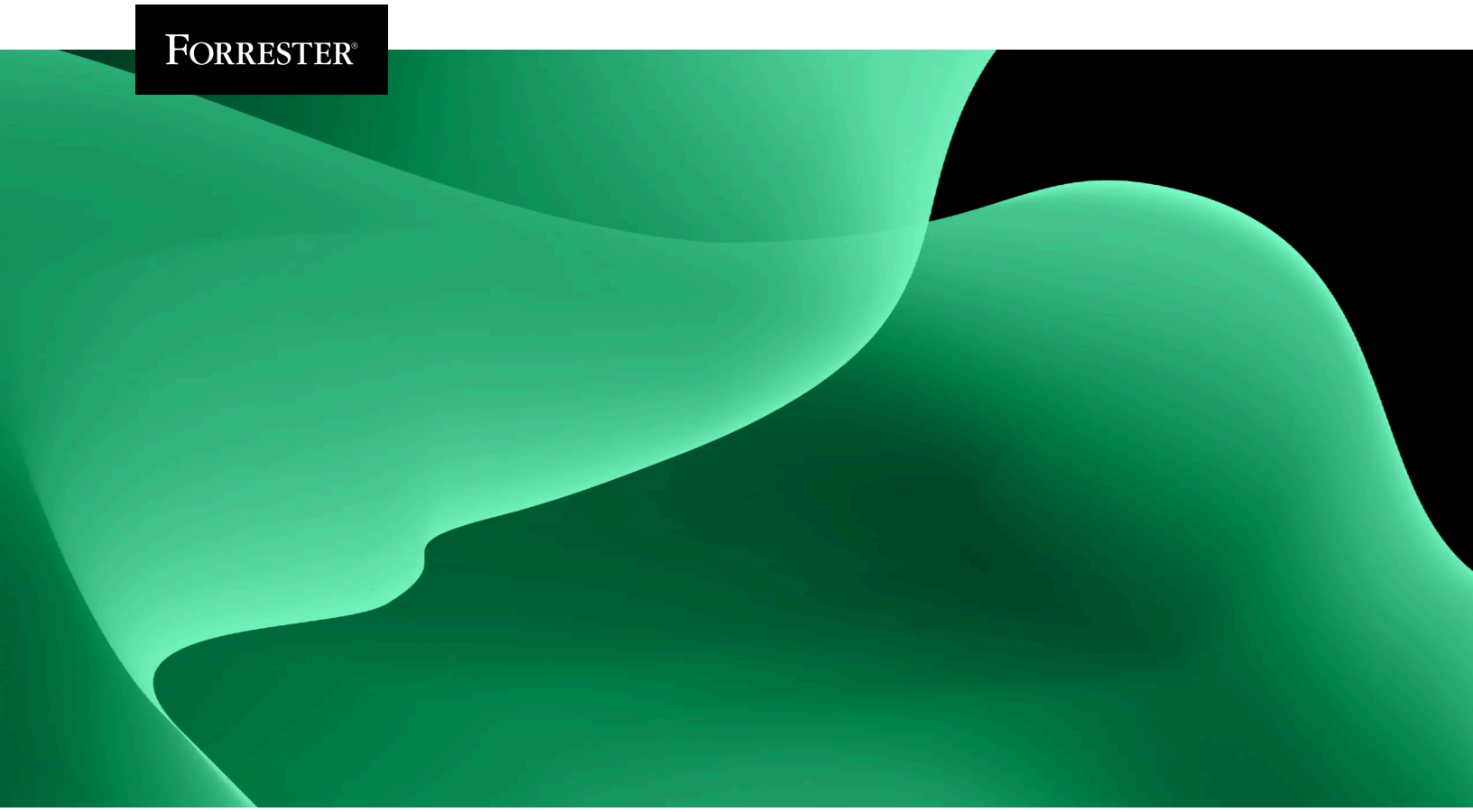
Total Economic Impact

The Total Economic Impact™ Of Cisco Duo

Cost Savings And Business Benefits Enabled By Cisco Duo

A FORRESTER TOTAL ECONOMIC IMPACT STUDY COMMISSIONED BY CISCO, JUNE 2025



Executive Summary

Today, identity and access management (IAM) is more critical than ever as organizations face rising threats from phishing, ransomware, and vulnerabilities from cloud misconfiguration. Businesses must balance security with agility, ensuring seamless access for employees, partners, and customers. A modern IAM solution enables phishing-resistant authentication, automates identity lifecycle management, and supports Zero Trust — boosting security, compliance, and operational efficiency.[1]

Cisco Duo is a leading IAM solution that takes a security-first approach to address modern identity-based threats without compromising usability. It delivers comprehensive protection through security-first identity, end-to-end phishing resistance, and unified identity intelligence. Organizations can use Duo as a stand-alone identity provider, with flexibility for it to serve as their primary directory or seamlessly integrate with existing identity infrastructures. This solution empowers organizations to safeguard their users, data, and systems with advanced security tools, all while ensuring an intuitive and efficient user experience.

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 Cisco Duo.[2] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Cisco Duo on their organizations.

198%

Return on investment (ROI)

$4.4M

Net present value (NPV)

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed seven decision-makers with experience using Cisco Duo. For the purposes of this study, Forrester aggregated the experiences of the interviewees and combined the results into a single composite organization, which is a global organization with 10,000 FTEs and $2.5 billion annual revenue.

Interviewees said that prior to using Cisco Duo, their organizations struggled with security gaps, operational inefficiencies, and compliance challenges. Without a solution for centralized IAM, the interviewees' organizations faced a range of persistent and costly security vulnerabilities, operational inefficiencies, and compliance burdens, creating a complex and often fragile environment for IT and security teams.

After the investment in Cisco Duo, the interviewees shared how it became a cornerstone of their identity-based cybersecurity strategies, helping their organizations strengthen security by closing identity gaps and improving visibility into user access across devices and locations. By providing visibility into who was logging in, from where, and with what device, Duo built resilience against unauthorized access and multi-factor authentication (MFA) targeting attacks, helping teams identify and address weak points in their authentication landscape across all applications. Operationally, Duo enabled the organizations to scale and improve their security posture without overburdening internal teams. By offloading authentication and simplifying infrastructure, Duo enabled scalable protection with efficiencies for teams across security operations; IAM; and governance, risk, and compliance (GRC), as well as a streamlined end-user experience resulting in significant productivity improvements.

Key Findings

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

- **Reduced costs of a credentials-related security breach by 60%.** Cisco Duo delivers measurable improvements in breach prevention, identity security, threat detection, and operational efficiency. Its layered approach to access

control and device verification helps the composite not only reduce the likelihood of a breach but also minimize the potential damage if one were to occur. The value of this reduced risk to the composite is $1.6 million.

- **Improved end-user productivity, saving FTEs 137,500 hours.** Duo helps reduce login friction and simplify onboarding for the composite organization, enabling consistent access across applications. End users who once had to manage numerous logins now enjoy a consistent, simplified experience across all clients, web-based apps, and browsers, empowering them to get to work faster and stay productive with fewer interruptions. The accumulated value of this improved productivity to the composite is $4.7 million.
- **Saved incident response time of more than 5,000 total hours.** Cisco Duo empowers incident response teams to work smarter, not harder. By automating identity risk assessments, reducing false positives, and providing actionable visibility, Duo allows teams to focus on real threats, respond faster, and maintain a stronger security posture across the board. Overall, Cisco Duo reduces the composite's authentication-related incident response effort by 50% for total time savings valued at $276,000.
- **Gained IAM efficiencies totaling more than 3,800 hours.** Cisco Duo enables the composite to simplify user provisioning, scale securely, and maintain strong administrative oversight — delivering measurable efficiencies across the IAM lifecycle. The value of these efficiencies to the composite is $205,000.
- **Optimized GRC with a 20% reduction in cyber insurance premiums.** Cisco Duo helps the composite organization navigate the complex compliance and cyber insurance landscape. By enabling MFA, providing audit-ready evidence, and supporting insurer confidence, Duo helps reduce cyber insurance premiums while improving GRC teams' ability to provide fast and comprehensive reporting. The value of these savings and efficiencies to the composite is $89,800.
- **Optimized IT help desk processes, eliminating 1,800 authentication-related support tickets.** Duo's streamlined process for granting application access, combined with the reduction in password resets and account unlocks, helps the composite organization ease pressure on its IT support function. Overall, adopting Duo leads to substantial time savings for the IT help desk. The value of this optimization to the composite is $28,000.

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

- Simplified ID and security environment.
- An identity-first security culture.
- Time savings reallocated to higher-value activities.

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

- **Cisco Duo.** The composite uses the Duo Advantage edition, charged on a flat, per user per month basis. These costs increase slightly year over year with organic growth in FTEs. Cisco Duo fees total $1,851,000 for the composite.
- **Implementation and management.** With Duo's moderate learning curve and the value of Duo Care premium support, the composite organization experiences low internal implementation and management costs**,** which total $357,000.

The financial analysis that is based on the interviews found that a composite organization experiences benefits of $6.6 million over three years versus costs of $2.2 million, adding up to a net present value (NPV) of $4.4 million and an ROI of 198%.

137,500 hours

Reduction in end-user time spent on authentication over three years with Cisco Duo

> *"Duo has definitely improved our efficiency in security administration. The enhanced visibility provided by Duo, especially when combined with Cisco Identity Intelligence, allows us to identify and address security gaps proactively. This has led to a significant reduction in false positives and faster investigation times, freeing up our security operations center (SOC) analysts to focus on more critical threats."*
>
> **Cybersecurity engineer, real estate**

Key Statistics

198%

Return on investment (ROI)

$6.6M

Benefits PV

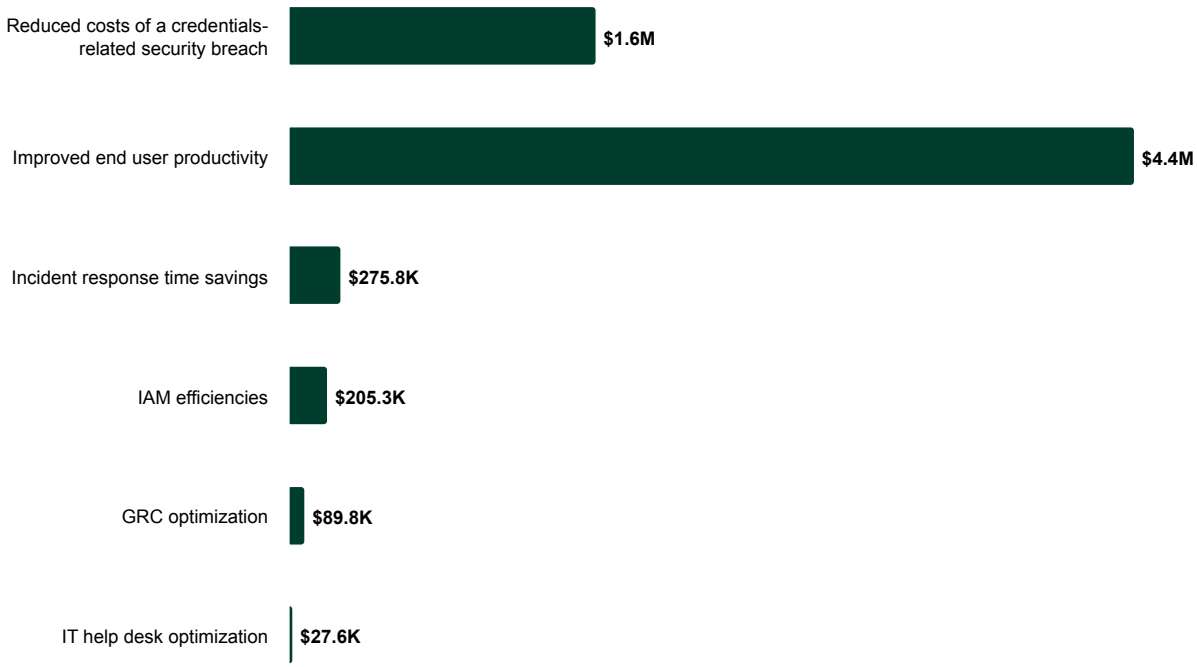
$4.4M

Net present value (NPV)

<6 months

Payback

Benefits (Three-Year)



The Cisco Duo Customer Journey

Drivers leading to the Cisco Duo investment

Interviews			
Role	**Industry**	**Region**	**Number of users**
Senior VP of IT	Healthcare	North America HQ and operations	15,000+
Cybersecurity leader	Healthcare	North America HQ and operations	5,000 to 9,999
Cybersecurity engineer	Real estate	North America HQ and operations	1,000 to 4,999
Infrastructure and security manager	Financial services	North America HQ, global operations	1,000 to 4,999
Information security leader	Retail	Europe HQ and operations	1,000 to 4,999
IT security manager	Transportation	North America HQ and operations	1,000 to 4,999
CISO	Technology services	North America HQ, global operations	>500

Key Challenges

The interviewees came from organizations facing a complex and evolving security landscape marked by credential theft, operational inefficiencies, and compliance failures. They shared how Cisco Duo helped their organizations address critical pain points across their environments. Interviewees' journeys reflected a common arc: from fragmented, high-risk systems to unified, secure, and efficient IAM postures with Cisco Duo.

Although they varied in industry, size, and region, interviewees noted how their organizations struggled with common challenges, including:

- **Credentials-related security risks and associated costs.** Interviewees who used an MFA provider in their prior environment discussed how their organizations inconsistently applied weak MFA processes, especially for critical systems like VPNs or administrative tools. They described how users were heavily reliant on passwords as the primary method of authentication, leaving them vulnerable to phishing attacks, credential theft, and brute-force intrusions. In many cases, the lack of robust authentication controls meant that a single compromised password could grant access to multiple systems, increasing the risk of lateral movement and costly data breaches. The financial exposure was significant, with potential breach costs estimated in the millions due to the sensitivity of the data involved — ranging from personal financial records to healthcare information.
    - The IT security manager in the transportation industry described their company's high level of risk due to lack of a centralized MFA: "Prior to Duo, [the risk of credential compromise] was pretty high. We've had close calls with business email compromise where accounting almost paid an invoice or somebody tried to change wire information. The risk is that it becomes much easier if you can get into the email system, and they definitely got into our environment on multiple occasions prior to Duo."
- **SecOps productivity impediments.** Security operations teams were often hampered by fragmented authentication systems and limited visibility into user activity. Logs were dispersed across platforms, making it difficult to detect anomalies or respond to threats in a timely manner. Manual processes dominated access control and incident response workflows, with a lack of centralized control and automation that created bottlenecks in threat detection and response.
- **User management complexity.** Managing user identities and access across a growing digital estate was a major operational burden for the interviewees' IAM teams. Interviewees noted that — depending on the application or department — their organizations often used a patchwork of authentication methods, ranging from passwords and SMS codes to hardware tokens and email-based verification. This inconsistency led to confusion among users and

inefficiencies for IT teams. Provisioning and deprovisioning users was largely manual, increasing the risk of error and misconfiguration. As organizations grew, the lack of a standardized approach to identity management became increasingly unsustainable, especially when onboarding new users or integrating new systems.

- The CISO at the technology services company shared: "[Prior to Cisco Duo,] software engineering would run and maintain a lot of their own infrastructure and would need to onboard [new developers]. ... When there's a new developer, [the team] would need to onboard them so [they could immediately start] to develop. It's important because they're picky, so if you don't solve [something] the way [the software engineers] like, they'll just do it themselves. ... They will bypass you at every turn."

- **Productivity drag for end users and slow onboarding for new users.** Interviewees discussed how their organizations were growing, but authenticating to access basic services was slow and cumbersome. Without streamlined provisioning and authentication workflows, new employees faced delays in gaining access to the tools and systems they needed to be productive.
  - The CISO at the technology services company noted: "[Prior to Duo,] it was not uncommon [to have] a dozen logins a day. ... If you were using a password manager, hopefully it [worked in] a couple of clicks. If you were not signed in to your password manager, at best you would have to hand-type out your password, [which would take] maybe 30 seconds, and then you would have differing degrees of MFA or login challenges."
- **GRC inefficiencies and cyber insurance challenges.** The lack of centralized visibility and control over user access hindered GRC teams. Organizations struggled to produce accurate audit trails, enforce consistent policies, and demonstrate compliance with regulatory requirements. Interviewees shared how cyber insurance providers increasingly demanded proof of strong authentication practices, and failure to meet these requirements led to higher premiums or reduced coverage. Manual reporting processes consumed significant time and introduced the risk of errors, making it difficult for organizations to stay ahead of evolving compliance standards.
- **IT help desk inefficiencies.** In their organizations' prior environments, support requests related to password resets, MFA setup issues, and access problems inundated help desks. These repetitive tasks consumed disproportionate time and resources, diverting attention from more strategic initiatives. The complexity of managing multiple authentication systems further compounded the problem. Users frequently encountered friction during login processes, leading to frustration and increased reliance on IT support. In environments with thousands of users, minor inefficiencies scaled into significant operational costs.

> *"[Our cyber] insurance cost was going to go up about 45%, and we would lose certain protections from insurance if we couldn't comply."*
>
> **Cybersecurity engineer, real estate**

Investment Objectives For Cisco Duo

The interviewees' organizations selected Duo due to its ease of use for end users and administrators and its high level of security. The interviewees described how their organizations deployed Cisco Duo across the security team for compliance, MFA, single sign-on (SSO) integration, and threat detection. The interviewees pointed to key drivers for their organizations' Cisco Duo investment, including its:

- **Advanced protections for credentials-related threats.** Duo gave organizations the ability to combine user and device context, helping move toward a Zero Trust security model. Duo's early support for device-based authentication and posture checks provided an additional layer of security beyond traditional MFA.
  - The cybersecurity engineer in the real estate industry discussed the importance of Duo's MFA and SSO capabilities as it related to their organization's use case: "The number one need was to have multi-factor authentication for desktop sign in, and Duo [not only] met that requirement, [but also] knocked it out of the park. ... We also use it for integrating with other applications with SSO and just for having ease of access and control over authentication methods for plenty of other applications as well."

- **Ease of use for end users.** The end-user experience was a key differentiator. Teams appreciated that Duo's design minimized disruption to users while maintaining strong security, which helped drive adoption across departments.
    - The senior VP of IT at the healthcare organization shared, "We looked at multiple different best-of-breed products at the time … and Duo was the easiest, both from an administrative and from an end-user perspective."
- **Time-saving integrations and automations across SecOps, IAM, and GRC-related roles.** Interviewees noted that Cisco Duo's user interface had a more intuitive design that was easier to use compared to other solutions they had decommissioned or tested. Organizations found Duo's interface to be clean and user-friendly, which made it easier to manage user enrollment and ongoing administration. Compared to other MFA solutions they evaluated, Duo was perceived as simpler to configure and faster to deploy.
    - The IT security manager in the transportation industry told Forrester that their organization chose Duo for its quick setup and flexible policy creation, allowing tailored MFA requirements based on application sensitivity and user access needs.
- **Ability to elevate standing with cyber insurers and compliance regimes.** Organizations used Duo to enforce policies based on device trust, ensuring that only secure and compliant endpoints could access sensitive systems. This capability was especially important for meeting cyber insurance requirements and reducing exposure to credential-based attacks.
    - The cybersecurity engineer in the real estate industry indicated that their primary driver for adopting Duo was to improve overall security with MFA and authentication to meet cyber insurance requirements, maintain coverage, and reduce premium costs: "The primary driver [of our Cisco Duo investment] was to bring down insurance costs and to also not lose any coverage from the insurance provider. … We wanted a more secure environment in general, including MFA for device sign in and enhanced analysis of those authentication actions."
- **Wide breadth of well-documented, easy-to-deploy integrations.** Interviewees also shared that Cisco Duo had a wide range of desired integrations with easy deployments, ensuring secure scaling into the cloud alongside organizational growth. Duo was selected for its ability to integrate seamlessly with a wide range of SaaS and on-premises applications and VPNs. The platform supported cloud and hybrid environments, allowing organizations to scale securely as they expanded. Teams valued the out-of-the-box support for many third-party tools, which reduced the need for custom development or complex configurations.
    - The cybersecurity engineer in the real estate industry reported that their organization selected Duo primarily for its desktop MFA functionality, which competitors either lacked at the time or would have been cost prohibitive when available: "The number one item we needed was to have MFA for desktop sign in. We needed an application that integrated with many different products for MFA that gave us visibility into how authentication was working."

> *"I really wanted to lay down a good MFA groundwork and strong identity [posture]. … From an MFA standpoint, Duo was the clear leader. They had the best UI/UX and [because] SSO was included, it just always made sense to start there. … Duo is a really nice turnkey way to establish both user and device context control and posture at [the same time]."*
>
> **CISO, technology services**

> *"We've used Cisco Duo to drive our Zero Trust [strategy]. If [it detects] odd logins or things that are abnormal, it requires more security, so that's been helpful. Cisco Duo has evolved, and security has gotten more important, [such] that they [have deployed] additional features that would help us lock down the environment."*
>
> **IT security manager, transportation**

Duo's Adaptive Roadmap: Leading-Edge Identity Security

Interviewees highlighted how Duo has evolved to include powerful new capabilities including Passwordless, Duo Passport, Duo Desktop, and Duo Push. These enhancements, combined with Duo's core MFA and SSO, helped ensure that only secure, managed devices could access company resources — while providing a consistent, mobile-friendly login experience across all applications.

- **Passwordless.** The interviewees that had deployed Passwordless Authentication highlighted how it boosted Duo's ease of access while being more secure than a traditional password.
    - The senior VP of IT at the healthcare organization highlighted the value of Duo Passwordless: "[Duo implementation and management] has gotten easier as we're able to do passwordless authentication. We were able to use biometrics and things like that, so that has helped. [It's just] a simple push; you respond to it and you're up and running."
- **Duo Desktop.** Interviewees discussed the value of deploying the Duo Desktop application for verifying the user's identity and their device's security posture before granting access.
    - The CISO at the technology services organization noted: "We were early adopters of their Duo Desktop. We're able to validate that [our endpoint threat detection] is there and that the device is corporate controlled."
- **Duo Passport.** Interviewees noted that Duo Passport streamlined application access by remembering device sessions between applications, which helped diminish login fatigue.
    - The cybersecurity engineer in the real estate industry shared that, following the Duo investment, end users at their organization benefited from centralized dashboards with Duo Passport. The interviewee described how it created a smoother, more efficient workflow for end users: "Duo Passport [has] essentialized dashboarding and SSO to click through pretty quickly [so] users don't have to type their password. … It's a few small wins that accumulate over time in your day that just make things a little easier."
- **Duo Push.** Duo's verified push feature helped some organizations eliminate MFA fatigue and unauthorized access, further enhancing productivity when deployed. Interviewees said that Duo Push stood out as a sleek, user-friendly alternative to clunky legacy tokens, offering seamless mobile access without the need for biometrics or hardware keys. Its built-in SSO tier eliminated the need for separate providers, simplifying identity management at scale. Unlike their legacy MFA tools with limited MFA controls, interviewees said that Duo delivered fine-grained customization that was elegant and easy.
    - The senior VP of IT at the healthcare organization shared: "We had experienced some account compromises because we had a few people respond to an MFA push when they didn't initiate the push. We were able to turn on Duo's Verified Push and eliminate that attack factor."
- **Cisco Identity Intelligence.** When paired with Cisco Identity Intelligence, Duo enabled real-time visibility into user login behavior and helped organizations improve their overall identity posture.
    - The information security leader in the retail industry said: "We've been heavily using Cisco Identity Intelligence alongside Duo and that's been helping us massively … in improving our identity posture, and we couldn't have done that without Duo."

> *"We run [Duo Desktop] on all of our endpoints so that we know not only is the user who they said they are but also that they're using the device they're supposed to be using, and it has our required security posture."*
>
> **Senior VP of IT, healthcare**

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 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 global organization generates $2.5 billion in annual revenue and maintains $150 million in cybersecurity insurance coverage. It has 10,000 FTE users, growing to 12,000 by Year 3. The composite has three FTEs dedicated to detection and response, two FTEs dedicated to IAM, and one FTE dedicated to GRC.
- **Deployment characteristics.** The composite organization deploys the Cisco Duo Advantage subscription with Duo Care to its 10,000 users in Year 1. This grows to 11,000 users in Year 2 and 12,000 users by Year 3.

KEY ASSUMPTIONS

- $2.5 billion annual revenue
- 10,000 users, growing to 12,000 by Year 3
- Duo Advantage subscription with Duo Care
- $150 million in cybersecurity insurance coverage

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 costs of a credentials-related security breach	$559,490	$683,822	$745,987	$1,989,299	$1,634,241
Btr	Improved end-user productivity	$1,599,994	$1,760,006	$1,920,000	$5,280,000	$4,351,615
Ctr	Incident response time savings	$90,575	$116,454	$129,393	$336,422	$275,799
Dtr	IAM efficiencies	$69,009	$86,261	$94,888	$250,159	$205,317
Etr	GRC optimization	$24,970	$39,493	$45,868	$110,331	$89,800
Ftr	IT help desk optimization	$8,460	$11,475	$13,860	$33,795	$27,588
	Total benefits (risk-adjusted)	$2,352,499	$2,697,511	$2,949,996	$8,000,005	$6,584,360

Reduced Costs Of A Credentials-Related Security Breach

Evidence and data. Although interviewees came from organizations across industries, all found significant value in using Cisco Duo to reduce the risk and potential cost of a material data breach. Duo's threat detection capabilities leveraged machine learning to improve security teams' ability to spot potential ongoing attack attempts. Furthermore, by blocking lateral movement and securing sensitive systems, Duo effectively disrupted the attack chain and enhanced overall cyber resilience. Interviewees shared how Duo decreased the likelihood of credentials-related cyberattacks by helping their organizations:

- **Combine user and device authentication for layered protection.** Interviewees discussed how Duo's layered defenses helped prevent unauthorized access to critical resources. These defenses included adaptive, phishing-resistant MFA using FIDO2 (WebAuthn); SSO; Passwordless; risk-based authentication; device verification; and conditional access policies. Duo helped interviewees' security teams protect against stolen credentials and account takeovers by enforcing strict access controls and allowing only secure, authorized devices to reach sensitive systems. Interviewees reported an estimated 60% improvement in their organizations' ability to mitigate these threats, while Duo's detailed logging enabled rapid detection of identity-based attacks, accelerating response to these incidents.
    - The cybersecurity engineer in the real estate industry said that Duo significantly strengthened identity security for their organization by drastically reducing the likelihood and potential impact of a breach. Its MFA made unauthorized access far less likely, even if credentials were compromised. This not only improved internal security assessments but also helped minimize potential breach-related costs like legal fees, data recovery, and reputational damage. They told Forrester: "With Duo, I estimate the probability of a successful breach has decreased substantially … [and] the cost of a potential breach would be significantly lower. Duo's MFA adds a strong layer of defense, making it much harder for attackers to gain unauthorized access, even if passwords are compromised. This is particularly crucial for our administrative accounts, which would be the most attractive targets for attackers."
- **Reduce their attack surface.** The interviewees discussed how Duo helped their IT team reduce the number of apps that were unmanaged or failing to meet security policies and standards.
    - The CISO at the technology services company highlighted how managing developer tools through the Duo environment helped ensure login security best practices, compared to the prior environment when they were managed outside of the IT organization: "From a security standpoint, Duo allows us to have some strict posture

checks for some of our most sensitive systems. We can guarantee that only compliant company devices can access the things that touch source code or build systems."

- **Eliminate key attack vectors and prevent lateral movement.** The interviewees noted that Duo helped prevent attacks and privilege escalation from common vectors by only allowing users with trusted endpoints to authenticate. It also played a critical role in defending against sophisticated threats like business email compromise and man-in-the-middle attacks, making it significantly harder for attackers to impersonate users or hijack sessions, even in scenarios involving help desk interactions or stolen tokens.
    - The cybersecurity engineer in the real estate industry explained that, by blocking privilege escalation from regular user accounts, Duo significantly disrupted the typical attack path. This made it much harder for attackers to reach sensitive systems and greatly reduced the likelihood of serious threats like ransomware or major breaches stemming from compromised user credentials.
    - The CISO at the technology services company explained how Duo automated critical identity security processes to prevent attacks from a variety of sources. By implementing SSO during onboarding, they reduced the likelihood of users reusing the same password for multiple applications. Their organization also implemented a 30-day patch cycle, blocking users who missed updates until they achieved compliance and ensuring all devices met security standards efficiently.

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- Based on Forrester Research's data for organizations with $2 billion to $5 billion in revenue, the average breach cost for the composite organization is $3.27 million.
- The estimated likelihood of experiencing a breach is 68%.
- Seventy percent of breaches are considered addressable by Cisco Duo.
- The reduction in risk exposure due to Duo improves from 45% in Year 1 to 60% in Year 3.

Risks. The following risks may impact this benefit:

- 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 leverages Duo's capabilities.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $1.6 million.

60%

Reduced risk of exposure to breach costs from addressable attacks with Cisco Duo

> *"Cisco Duo has led to a major improvement [in our identity security posture] across the board. Any time we do any kind of internal checks or scans or vulnerability assessments on ourselves, we always feel better knowing that people who have MFA-privileged accounts are not getting accessed, and if you want to access devices, especially servers that we have extra protections on, it's just not going to happen."*
>
> **Cybersecurity engineer, real estate**

Reduced Costs Of A Credentials-Related Security Breach					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
A1	Cumulative cost of breaches for the composite	Forrester research	$3,265,000	$3,265,000	$3,265,000
A2	Likelihood of experiencing one or more breaches for the composite	Forrester research	68%	68%	68%
A3	Percentage of breaches originating from external attacks targeting organizations or remote environments, internal incidents, attacks, or incidents involving the external ecosystem	Forrester research	70%	70%	70%
A4	Annual risk exposure addressable with Cisco Duo	A1*A2*A3	$1,554,140	$1,554,140	$1,554,140
A5	Reduced risk of exposure to breach costs from addressable attacks with Cisco Duo	Interviews	45%	55%	60%
At	Reduced costs of a credentials-related security breach	A4*A5	$699,363	$854,777	$932,484
	Risk adjustment	↓20%			
Atr	Reduced costs of a credentials-related security breach (risk-adjusted)		$559,490	$683,822	$745,987
	Three-year total: $1,989,299			**Three-year present value: $1,634,241**	

Improved End-User Productivity

Evidence and data. Across the interviewees' organizations, Cisco Duo emerged as a key enabler of smoother, faster end-user experiences. Rather than slowing users down with cumbersome login processes, Duo helped mitigate friction and streamline authentication in ways that directly improved productivity. This not only saved end users time but also reduced cognitive load and frustration. Whether it was reducing the time it took to log in, simplifying access across multiple applications, or minimizing disruptions during the workday, Duo allowed users to focus more on their tasks and less on navigating security barriers. This benefit had multiple value drivers, including:

- **Ease of use with SSO and other features.** The implementation of SSO, Duo Desktop, and passwordless authentication allowed users to access multiple applications with a single set of credentials and ensure quicker subsequent logins. Passwordless authentication provided additional savings and convenience, reducing the time spent on login processes. Duo's passwordless access eliminated the need to repeatedly enter credentials. Passport and Duo Desktop features also helped reduce repeated authentication prompts by leveraging secure tokens.
    - The cybersecurity engineer in the real estate industry shared that, following the Duo investment, end users experienced smoother, more efficient workflows, thus accumulating incremental time savings throughout the day.
- **A significant reduction in login time.** One of the most immediate Duo benefits reported was optimizing a secure end-user experience, which streamlined daily operations and enhanced productivity. Previously, users faced cumbersome login procedures that required multiple steps and considerable time. With Duo, the authentication process became swift and seamless, reducing the time spent on logins by 75%. This efficiency allowed users to

remain focused and eliminated the need to leave their workspace to retrieve authentication codes; thus, they could focus more on their tasks.

  - The information security leader in the retail industry said that their organization's end users previously spent 2 to 3 minutes authenticating in the prior environment. With Duo's push-based authentication, that time had dropped to just 30 seconds, allowing users to stay focused and get to work without unnecessary delays, even when multiple authentications were required throughout the day.
  - The CISO at the technology services company noted that their organization's prior login procedures were excessive and clunky. After deploying Duo, the interviewee shared that their organization experienced fewer disruptive authentications required of users and shorter login periods overall: "The logins would be [several steps totaling] 30 seconds in some cases, and [now with Duo,] they just go down to one click and 2 seconds. … I would say most people were signing in to anywhere from six to 20 applications a day. That just becomes one click: With SSO, you just click on your tile and it launches; you don't have to type anything. There are all these little things that add up."

- **Improved time to productivity for new users.** Duo also accelerated the onboarding period by decreasing the time it took for newly onboarded employees to become productive. The consistent onboarding experience across applications became a key enabler of business agility for the interviewees' organizations.
  - The CISO at the technology services company explained that implementing SSO simplified onboarding by reducing the need to set multiple passwords, making the process less daunting for new hires: "Now, even if we have to manually create the user accounts in some situations, on your first day, you get granted access to SSO, you set up your touch ID … and that's basically it. … A new hire doesn't have to set up 20 passwords."
  - The senior VP of IT at the healthcare organization noted that productivity for new users improved significantly, reducing the onboarding time from multiple weeks to just a few days. They also managed to cut down service desk hold times from 30 minutes to 2 minutes, enhancing user satisfaction. Additionally, the automated enrollment process for new devices and users streamlined workflows and reduced errors, making it easier for employees to get started: "The enrollment process is automated so that it is all self-service. … Every application that we deploy has the exact same login process. … As we bring on these new users, … it's very easy to get them trained and using applications over that authentication barrier."
- **Less end-user time spent waiting for support.** Interviewees described how Duo helped automate the user provisioning lifecycle (see IAM Efficiencies) leading to fewer manual errors in the process. This meant that new and existing users had fewer authentication-related issues requiring support, while improved authentication-related context meant support staff were able to shorten the time end users spent waiting for support.
  - The senior VP of IT at the healthcare organization explained that implementing Duo significantly reduced the need for extensive training and decreased service desk calls related to login issues. This streamlined approach allowed new users to access applications easily, improving overall efficiency and user satisfaction: "In the past, users would have 30-minute hold times, potentially longer. Now, we can keep those hold times down to 2 minutes or less."

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- The model assumes between 10,000 and 12,000 users, each performing 500 authentications per year.
- Before Duo, each authentication took 1.5 minutes; with Duo, this time drops to 0.5 minutes.
- End users recapture 50% of these time savings for productive work.
- The average fully burdened hourly rate for an end user is $48.

Risks. The following risks may impact this benefit:

- 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 20%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $4.4 million.

137,500 hours

Reduction in end-user time spent on authentication over three years with Cisco Duo

> *"[Before], it would take [end users] 2 to 3 minutes to authenticate, whereas now with Duo it's [down to] 30 seconds and the user is able to sit down and get their work done. That's what we want."*
>
> **Cybersecurity engineer, real estate**

Improved End-User Productivity					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
B1	Number of end users	Composite	10,000	11,000	12,000
B2	Average number of authentications per end user each year	Interviews	500	500	500
B3	End-user time spent on each authentication prior to Duo (minutes)	Interviews	1.5	1.5	1.5
B4	End-user time spent on each authentication with Duo (minutes)	Interviews	0.5	0.5	0.5
B5	**Subtotal: Total annual end-user time savings (hours)**	**(B1*B2*(B3-B4))/60**	**83,333**	**91,667**	**100,000**
B6	Fully burdened hourly rate for an end user	Composite	$48	$48	$48
B7	End-user productivity recapture	TEI methodology	50%	50%	50%
Bt	Improved end-user productivity	B5*B6*B7	$1,999,992	$2,200,008	$2,400,000
	Risk adjustment	↓20%			
Btr	Improved end-user productivity (risk-adjusted)		$1,599,994	$1,760,006	$1,920,000
	Three-year total: $5,280,000			**Three-year present value: $4,351,615**	

Incident Response Time Savings

Evidence and data. Organizations across industries reported that Cisco Duo significantly enhanced the productivity and responsiveness of their security operations teams. By improving visibility, reducing investigation time, and streamlining authentication processes, Duo enabled teams to act faster and more effectively when incidents occurred. In particular, interviewees reported how Cisco Duo helped their organizations:

- **Automate critical security steps.** Interviewees described how Duo significantly reduced the time required for security investigations by automating risk-based authentication assessments and providing better visibility into login activities. These automations allowed security teams to skip unnecessary steps and focus on critical issues, saving valuable time. Overall, these time-saving automations enabled security operations teams to work more efficiently and effectively, focusing on genuine threats and improving the organization's security posture.
  - The senior VP of IT at a healthcare organization described how Duo's automated escalation — such as flagging impossible logins from two distant locations — allowed their team to step up authentication requirements in real time. This proactive approach helped prevent unauthorized access and reduced the burden on analysts to detect anomalies manually.

- **Risk-based authentication.** Duo's risk-based authentication and visibility features were repeatedly highlighted as key enablers of faster, more confident decision-making based on rapidly changing risk factors.
    - The cybersecurity engineer in the real estate industry noted that Duo's risk-based assessments allowed their team to ignore low-risk logins and focus only on meaningful alerts, saying: "We could take off several people hours a month in terms of wasted time on looking at reports in areas that we didn't need to."
- **Lower false positives.** Another major area of improvement was reducing false positives and unnecessary escalations. With Duo's detailed authentication logs and integration with Cisco Identity Intelligence, service desks and SOC teams could quickly determine whether login issues were authentication-related or due to other system problems. The streamlined authentication process also minimized the occurrence of false positives, reducing the time spent on investigating nonissues.
    - The information security leader in the retail industry said: "Beforehand, we would have to manually look at logins and just see if there was anything suspicious, whereas now we can look at that risk-based assessment. … For us, that saves us time looking at detections and reports that are … just false positives in the end, helping us to improve the efficiency of the team when looking at investigations of different alerts."
- **Decrease investigation times.** Together, the impacts above led to a significant reduction in security investigation time. Teams that previously had to perform multiple manual steps to verify user activity — such as checking device logs or querying security information and event management (SIEM) systems — found that Duo provided near-instant answers.
    - The senior VP of IT at the healthcare organization shared how Duo reduced the time to investigate incidents by 50%, from 1 hour in the prior environment to 30 minutes with Duo. They added: "Cisco Identity Intelligence is an enhancement to that [time savings]. It gives us a lot more visibility into those identity incidents for sure."
- **Reduce account takeovers.** Interviewees shared that their teams also reported a significant drop in account takeover incidents. In their prior environment, their SecOps teams were handling a significant daily volume of account takeovers. With Duo's SSO, MFA, and other capabilities, however, account takeovers required minimal effort, if any at all.
    - The IT security manager in the transportation industry shared that before Duo, compromised accounts were a regular occurrence, often taking half a day to resolve. Since implementing Duo, they have had no successful account takeovers, even when credentials were phished — saving hours of work each week and reducing stress on a small security team. They told Forrester: "We went from pretty regularly having to deal with compromised accounts to none at all. We still have reports once in a while where we find out that somebody entered the username and password at a phishing site, but no bad guy has ever been able to take that account and do anything with it."

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- The composite organization dedicates 4,992 hours per year to incident response.
- With Duo, the composite reduces its incident response effort by 40% in Year 1, increasing to 55% in Year 3.
- Technical resources recapture 80% of time savings for productive work.
- The average fully burdened hourly rate for a technical resource is $72.

Risks. The following risks may impact this benefit:

- 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 leverages 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 (discounted at 10%) of $276,000.

>5,000 hours

Identity-related incident response time savings with Cisco Duo

> *"If you can just skip even two steps [with Duo], that saves 20 minutes per investigation, and that is a big deal."*
>
> **Cybersecurity engineer, real estate**

Incident Response Time Savings					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
C1	Total hours dedicated to incident response in the prior environment	Composite	4,992	4,992	4,992
C2	Percentage reduction in effort dedicated to incident response with Cisco Duo	Interviews	35%	45%	50%
C3	Fully burdened hourly rate for a technical resource	Composite	$72	$72	$72
C4	Productivity recapture	TEI methodology	80%	80%	80%
Ct	Incident response time savings	C1*C2*C3*C4	$100,639	$129,393	$143,770
	Risk adjustment	↓10%			
Ctr	Incident response time savings (risk-adjusted)		$90,575	$116,454	$129,393
	Three-year total: $336,422		**Three-year present value: $275,799**		

IAM Efficiencies

Evidence and data. Interviewees reported that their organizations had inconsistent, often manual IAM practices in their prior environments. They often distributed user management responsibilities across business users who were also app owners, rather than consolidate them through a secure IT function. Deploying Cisco Duo significantly streamlined their IAM processes, particularly in the areas of user provisioning, scalability, and administrative control. These efficiencies not only saved time but also improved security posture and operational agility. Interviewees pointed out how Duo IAM automations helped:

- **Improve administrative control and visibility.** Interviewees described how Duo's adaptive access policies gave IAM teams the ability to manage access privileges with newfound granularity based on role, device, location, and many other contextual factors.
  - The information security leader in the retail industry shared: "Duo has such a clean user interface. It really helps us to streamline our user enrollment, and I think that's been a big factor for us. … Setting up a new user in an application that's already in Duo could save 15% of your time just by putting them into one Duo group, and then boom, they have access."
- **Optimize user provisioning lifecycle.** Interviewees described how adding a user to a Duo group could instantly provision access to applications, eliminating the need to create and manage separate credentials, saving on per-user setup time and reducing the risk of forgotten passwords and the need for ongoing maintenance.
  - The information security leader in the retail industry said that Duo's integration with SSO and group-based access controls simplified the process of granting application access. The process of setting up authentication for a new employee decreased by 50% or more, from 20 minutes to just 5 to 10 minutes.

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- The composite organization dedicates 3,328 hours per year to IAM.
- Effort reduction improves from 40% in Year 1 to 55% in Year 3.
- Technical resources recapture 80% of time savings for productive work.
- The average fully burdened hourly rate for a technical resource is $72.

Risks. The following risks may impact this benefit:

- 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 leverages 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 (discounted at 10%) of $205,000.

55%

Percentage reduction in effort dedicated to IAM with Cisco Duo

> *"We're able to get a pretty good rate on [cyber insurance], and I think part of it is [seeing] Duo as part of our overall security program provides confidence to the cyber insurance companies."*
>
> **IT security manager, transportation**

IAM Efficiencies					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
D1	Total hours dedicated to IAM in the prior environment	Composite	3,328	3,328	3,328
D2	Percentage reduction in effort dedicated to IAM with Cisco Duo	Interviews	40%	50%	55%
D3	Fully burdened hourly rate for an IAM resource	Composite	$72	$72	$72
D4	Productivity recapture	TEI methodology	80%	80%	80%
Dt	IAM efficiencies	D1*D2*D3*D4	$76,677	$95,846	$105,431
	Risk adjustment	↓10%			
Dtr	IAM efficiencies (risk-adjusted)		$69,009	$86,261	$94,888
	Three-year total: $250,159			**Three-year present value: $205,317**	

GRC Optimization

Evidence and data. Interviewees noted how their organizations were under increasing pressure to demonstrate compliance with regulation requirements and governance policies. As cyber threats evolved, breaches occurred for some organizations in their prior environments, and insurers raised their standards across sectors. Interviewees

shared that Cisco Duo played a critical role in helping their organizations meet these rising expectations. They reported a range of ways in which this manifested, particularly in the areas of cyber insurance eligibility, cost savings, and compliance reporting, as well as meeting customer expectations on security. In particular, they highlighted their organizations':

- **Improved ability to provide evidence and reporting.** Duo helped organizations demonstrate compliance and provide evidence of security controls — a growing requirement as they noted insurers, regulators, and even customers were raising the bar on their standards. Compared to their prior environments, where gathering evidence and reporting was overly burdensome, interviewees noted how Duo made it easier to share SOC evidence on MFA.
    - The CISO at the technology services company shared that, prior to Duo, their teams would have to periodically audit out-of-date patches for users missing endpoint protection. They noted that Duo enabled real-time compliance enforcement, which mitigated the need for manual checks: "[Duo saves us] 2 hours per week [of] tedious, manual spreadsheet comparison and outreach to the help desk and … users. It allows us to enforce the major compliance bullet points in real time, so we don't have to try to figure out which laptops are missing [endpoint security agents]."
    - The senior VP of IT at the healthcare organization shared how their organization achieved regulatory and audit efficiencies: "We are spending less time [on reporting with Duo. It gives us] the ability to rapidly demonstrate how MFA is enabled for every user, for every authentication, both on the server side and the application side, which is our HIPAA regulatory requirement. We couldn't even produce a report [like that before], but in Duo we have it."
    - The IT security manager in the transportation industry said that having Duo at the center of their organizations' identity security strategy helped meet growing customer expectations on security: "Customers … were [always] very interested in what we had from a security standpoint, but nowadays we just get this long questionnaire with hundreds of questions that I have to fill out every year. … On the PCI side, I can just say 'not an issue; we're using Duo MFA.'"
- **Better standing with cyber insurers.** Although interviewees saw Duo as foundational to qualifying for cyber insurance, one of the most striking outcomes was its direct financial impact on cyber insurance premiums. Duo contributed to maintaining insurer confidence, and in some cases led to more favorable rates.
    - The cybersecurity engineer in the real estate industry reported that their organization saved 45% on cyber insurance costs after implementing Duo. Without Duo's MFA and privileged access controls, they were at risk of losing coverage altogether. Duo not only helped them retain coverage but also expanded it, making it a key factor in their insurance strategy. They told Forrester: "Through the Duo implementation, we were able to save 45% on the insurance cost, and we were going to lose some coverage without all the MFA and privileged access management, that ultimately, we were able to keep."

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- Cyber insurance premiums are set at $150,000 annually, with savings increasing from 10% to 20% over three years.
- GRC efforts total 1,664 hours annually, with a 15% to 25% reduction in effort for the composite.
- Technical resources recapture 80% of time savings for productive work.
- The average fully burdened hourly rate for a technical resource is $72.

Risks. The following risks may impact this benefit:

- 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 leverages 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 (discounted at 10%) of $90,000.

20%

Percentage reduction in cyber insurance premiums with Cisco Duo

> *"We're able to get a pretty good rate on [premiums because having] Duo as part of our overall security program provides confidence to the cyber insurance companies."*
>
> **IT security manager, transportation**

GRC Optimization					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
E1	Cyber insurance premiums in the prior environment	Composite	$150,000	$150,000	$150,000
E2	Percentage reduction in cyber insurance premiums with Cisco Duo	Interviews	10%	15%	20%
E3	**Subtotal: Savings on cyber insurance premiums with Cisco Duo**	**E1*E2**	**$15,000**	**$22,500**	**$30,000**
E4	Total hours dedicated to GRC in the prior environment	Composite	1,664	1,664	1,664
E5	Percentage reduction in effort dedicated to GRC with Cisco Duo	Interviews	15%	25%	25%
E6	Productivity recapture	TEI Methodology	80%	80%	80%
E7	Fully burdened hourly rate for a GRC resource	Composite	$72	$72	$72
E8	**Subtotal: GRC optimization**	**E4*E5*E6*E7**	**$14,377**	**$23,962**	**$23,962**
Et	GRC optimization	E3+E8	$29,377	$46,462	$53,962
	Risk adjustment	↓15%			
Etr	GRC optimization (risk-adjusted)		$24,970	$39,493	$45,868
	Three-year total: $110,331		**Three-year present value: $89,800**		

IT Help Desk Optimization

Evidence and data. Interviewees detailed how their IT help desk functions gained better visibility and clarity into authentication issues after adopting Duo. This lowered support costs and optimized productivity for end users and IT staff alike. Automated workflows in the provisioning lifecycle reduced the potential for errors and misconfigurations that often served as the bulk of support requests in the prior environment. Key value drivers for this benefit included:

- **Reduction in credentials-related support issues.** Organizations saw a reduction in the number of IT tickets related to authentication issues, with monthly ticket volumes dropping significantly.
  - The information security leader in the retail industry said that their organization reduced credentials-related ticket volume by up to 70%: "Per month, we'd have anywhere from 15 to 20 tickets in terms of authentication issues. Now [with Duo], we are down to maybe six [credentials-related tickets]."
- **Faster troubleshooting and resolution times.** Another key area of improvement was in the time taken to resolve IT tickets. The ability to check and unlock accounts quickly through Duo streamlined the process, reducing the burden on IT staff and minimizing downtime for users.
  - The CISO at the technology services company highlighted that their help desk saved half a day each week by streamlining user access to applications: "Not only is it easier [for the help desk] to give people access to

applications, but they're also not having to do password resets or unlock accounts across these dozens of SaaS applications. … No one's getting locked out [and] the whole process is streamlined."

- The information security leader in the retail industry said that their organization's support team took 15 to 20 minutes to resolve a credentials-related user issue in the prior environment. With Duo, the interviewee said that resolution time decreased by more than 67%, down to 5 minutes. The interviewee said that Duo helped support teams triage user issues better than in their prior environment: "We can immediately check Duo straight away to see if a user is locked out. … [Then,] we can just press a button, [and] they're unlocked; they can log in. That's definitely helped us decrease the amount of time that our IT help desk spends on these tickets and that our users are waiting to get on to the systems as well."

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- In the prior environment, the composite addresses 1,200 authentication-related help desk tickets per year, each taking 15 minutes to resolve.
- With Duo, the composite reduces ticket volume by 40% to 60% and reduces resolution time by 25% to 50%.
- The average fully burdened hourly rate for a help desk resource is $50.

Risks. The following risks may impact this benefit:

- The nature of the prior authentication solution.
- Help desk staff experience and capabilities.
- The extent to which an organization leverages 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 (discounted at 10%) of $28,000.

60%

Percentage reduction in annual authentication-related IT help desk tickets with Cisco Duo

> *"Duo has really helped us to identify issues … with user identities and authentication immediately and quickly, but also to stop them from happening again, so, it's worked in two ways, which has been grand for us."*
>
> **Information security leader, retail**

IT Help Desk Optimization					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
F1	Total annual authentication-related IT help desk tickets in the prior environment	Composite	1,200	1,200	1,200
F2	Percentage reduction in annual authentication-related IT help desk tickets with Duo	Interviews	40%	50%	60%
F3	Total annual authentication-related IT help desk tickets avoided with Duo	F1*F2	480	600	720
F4	Total hours to investigate authentication-related IT help desk tickets in the prior environment	Composite	0.25	0.25	0.25
F5	**Subtotal: Total IT help desk hours avoided from reduced volume of authentication-related tickets with Duo**	**F3*F4**	**120**	**150**	**180**
F6	Total IT help desk tickets with Duo	F1-F5	1,080	1,050	1,020
F7	Percentage reduction in time to resolve authentication-related IT help desk tickets with Duo	Interviews	25%	40%	50%
F8	Total IT help desk hours avoided from reduced time to resolve authentication-related IT help desk tickets with Duo	F6*(F4*F7)	68	105	128
F9	**Subtotal: Total IT help desk hours avoided with Duo**	**F5+F8**	**188**	**255**	**308**
F10	Fully burdened hourly rate for an IT help desk resource	Composite	$50	$50	$50
Ft	IT help desk optimization	F9*F10	$9,400	$12,750	$15,400
	Risk adjustment	↓10%			
Ftr	IT help desk optimization (risk-adjusted)		$8,460	$11,475	$13,860
	Three-year total: $33,795			**Three-year present value: $27,588**	

Unquantified Benefits

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

- **Simplified identity and security environment.** Duo simplified the technology stack for the interviewees' organizations by centralizing and streamlining authentication and log management technology. Duo replaced a fragmented mix of managed authentication tools and other unmanaged free solutions. This consolidation eliminated the complexity of supporting multiple tools and improved manageability and auditability.
    - The CISO at the technology services company highlighted how their IT teams consolidated a dozen on-prem services that were previously managed through their development organization. This allowed developers to focus on product innovation and gave IT more visibility and control over authentication.
    - The cybersecurity leader in the healthcare industry reported that, by consolidating authentication logs through Duo, organizations avoided needing to collect and manage logs from multiple disparate systems. This significantly reduced the volume of data sent to their SIEM, which is typically priced based on data ingestion volume. As a result, they achieved notable cost savings.
- **An identity-first security culture.** Interviewees described how their organization's underlying growth strategy and security culture reoriented around identity security following Duo adoption.
    - The information security leader in the retail industry said that Duo shifted their organization's culture toward a higher level of security maturity with identity and credentials at the center: "Using Duo has ingrained that mentality of checking for authentication issues upfront [as we scale], so it's ingrained within our teams."
- **Time savings reallocated to higher-value activities.** By recentering identity security and management with IT, business and technical users often applied the productivity gains to higher-value activities.

- The information security leader in the retail industry indicated that Duo obviated a significant volume of incidents, thus reducing the time security teams spent reviewing logs (see Incident Response Time Savings). They said that their teams reattributed these time savings to focusing on critical threats.
- The cybersecurity leader in the healthcare industry noted that the improved context from Duo provided upskilling opportunities for IT help desk staff. They noted that it empowered the teams with valuable knowledge about authentication processes to help further accelerate issue resolution.

> *"Duo helped us focus our attention on areas that really need it and keep our eyes on the screens that are most important at [any] given time."*
>
> **Information security leader, retail**

Flexibility

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

- **Secure scalability and growth.** Duo's robust support and roadmap guidance helped organizations deploy adaptive security models, allowing them to scale users and applications. Duo also enabled quick and secure user onboarding while maintaining compliance with MFA policies. This approach offered greater administrative control and visibility, standardized SSO and MFA processes, and reduced MFA fatigue, making it easier for IT teams to manage credentials, enforce security policies, and monitor access effectively as their organizations experienced rapid organic growth via mergers and acquisitions.
  - The infrastructure and security manager at a financial services firm shared how their organization grew from 750 to 2,700 FTEs during their investment period. They emphasized how Duo's support and roadmap guidance helped them stay ahead of their expanding needs. The interviewee noted that Duo gave their firm the ability to quickly and securely onboard users while maintaining compliance with MFA policies, which made growth more manageable and secure.
  - The CISO at the technology services company described how Duo helped their organization scale securely by offloading authentication management to IT, allowing technical teams to focus on development rather than maintaining infrastructure. With just-in-time provisioning, they could dynamically create new developer users and grant access through SSO, streamlining the onboarding process and enhancing scalability.
- **Faster time to value with mergers and acquisitions.** Multiple interviewees shared how the enhanced scalability and growth described above streamlined and accelerated their organizations' mergers and acquisitions activities. By implementing MFA for their VPNs and traditional logins, IT staff could onboard users faster and with more secure authentication.
  - The senior VP of IT at the healthcare organization shared how Duo enabled faster onboarding and smoother integration during rapid growth by standardizing the login process across all applications. This consistent SSO experience improved user adoption and supported business agility: "We're very much in growth mode. We just finished multiple acquisitions last month [and] have mandated everyone log in through this SSO method. ...That leads to that business agility [because] every application that we deploy has the exact same login process."

Flexibility would also be quantified when evaluated as part of a specific project (described in more detail in Total Economic Impact Approach).

> *"Everything moving forward has to meet [MFA policy] requirements [enforced by Duo]. That makes it easier to bring on users while being more secure, which makes us more scalable."*
>
> **Cybersecurity engineer, real estate**

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 Duo	$0	$680,400	$748,440	$816,480	$2,245,320	$1,850,524
Htr	Implementation and management	$14,256	$288,710	$51,110	$51,110	$405,187	$357,360
	Total costs (risk-adjusted)	$14,256	$969,110	$799,550	$867,590	$2,650,507	$2,207,884

Cisco Duo

Evidence and data. Factors that impacted the organizations' Cisco Duo fees included:

- **Cisco Duo edition.** Interviewees had various configurations of Duo enabled, including the Duo Essentials, Duo Advantage, and Duo Premier editions.
- **Organizational growth.** Interviewees noted licensing costs for Duo were charged on a flat, monthly, per user basis. Several organizations experienced organizational growth or had additional applications that they wanted to onboard to Duo following the initial implementation.
    - The cybersecurity engineer in the real estate industry shared: "We had some applications that didn't make the cut in the first year of deployment, so we actually just recently purchased a thousand more licenses. There are other applications we'll be adding, so we do expect to grow with Duo. ... In the future, we're looking to fill upward of 2,500 licenses."
- **Duo Care.** Some interviewees' organizations found value in their Duo Care services agreement with Cisco.
    - The cybersecurity engineer in the real estate industry shared: "Our Duo Care team was just incredible, from getting everything set up and keeping it going and avoiding [any] of the mistakes that we could have made or the headaches that we could have had. They have the best vendor [professional services team] I've ever worked with by a lot."

Pricing may vary. Contact Cisco for additional details.

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- Annual license fees start at $540,000 and increase to $648,000 by Year 3.
- Duo Care fees are 20% of Duo licensing, starting at $108,000 and growing to $129,600.

Risks. The following risks may impact this cost:

- Number of accounts Duo protects.
- Which edition 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 $1.9 million.

Cisco Duo						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
G1	Cisco Duo Fees	Composite		$540,000	$594,000	$648,000
G2	Duo Care	Composite		$108,000	$118,800	$129,600
Gt	Cisco Duo	G1+G2		$648,000	$712,800	$777,600
	Risk adjustment	↑5%				
Gtr	Cisco Duo (risk-adjusted)		$0	$680,400	$748,440	$816,480
	Three-year total: $2,245,320			**Three-year present value: $1,850,524**		

Implementation And Management

Evidence and data. Interviewees described Duo as quick and straightforward to deploy, with low administrative burden and IT costs compared to their prior environment. The 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., for remote users connecting into internal applications); then configuring, deploying, and testing the Duo solution; and integrating it with key applications. Interviewees described their organizations' implementation and management efforts, which included:

- **Deployment and integration processes.** Interviewees detailed their organization's rollout of Duo, the planning of which involved identifying all applications and setting up necessary infrastructure. Phased deployments allowed for testing and adjustments, leading to comprehensive organizational adoption with Duo at the center of a centralized, ID-based security strategy.
    - The information security leader in the retail industry said that their organization worked with a third party to integrate other apps into their Duo environment easily: "It was very easy for us to get it set up with our VPN, which is what our third party used. Cisco Duo's documentation is fantastic, and it provides really in-depth, step-by-step instructions on how to set it up and integrate it."
    - The senior VP of IT at the healthcare organization shared how their Duo Care team helped with their organization's phased deployment: "We were working very closely with the Duo customer success team. They stayed with us every step of the way, so that was extremely helpful. … We piloted from an administrative perspective on running on servers, just to get all of the people that were going to be administering and helping deploy this to become extremely comfortable with it. Then we started expanding that out into healthcare applications, [which took] us about a year to get fully deployed across all business units."
- **Training.** Templates and guidance from Cisco Duo documentation and Duo Care teams (when engaged) provided the foundation for organizationwide change-management processes. End users familiarized themselves with Duo through videos, reading materials, or training staff if needed and subsequently enrolled their devices with Duo. Newly hired end users educated themselves using the training materials and consulted help desk staff if needed.
- **Roadmap discussions with Cisco.** Many organizations engaged in regular roadmap discussions with their Cisco Duo team, fostering close relationships during and after implementation. Security-related IT staff managed and supported Duo, interfacing with Cisco to evaluate and optimize their use of Duo continually. They also handled projects such as onboarding new functions or exploring new use cases for Duo.

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- Technical deployment and management effort starts at 180 hours and increases to 312 hours annually.
- The average fully burdened hourly rate for a technical resource is $72.
- Each end user dedicates 30 minutes to Duo training and onboarding.
- The average fully burdened hourly rate for an end-user resource is $48.

Risks. The following risks may impact this cost:

- The number of end users.
- IT staff experience and capabilities.
- The maturity of an organization's security operations.
- The extent to which an organization leverages 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 (discounted at 10%) of $357,000.

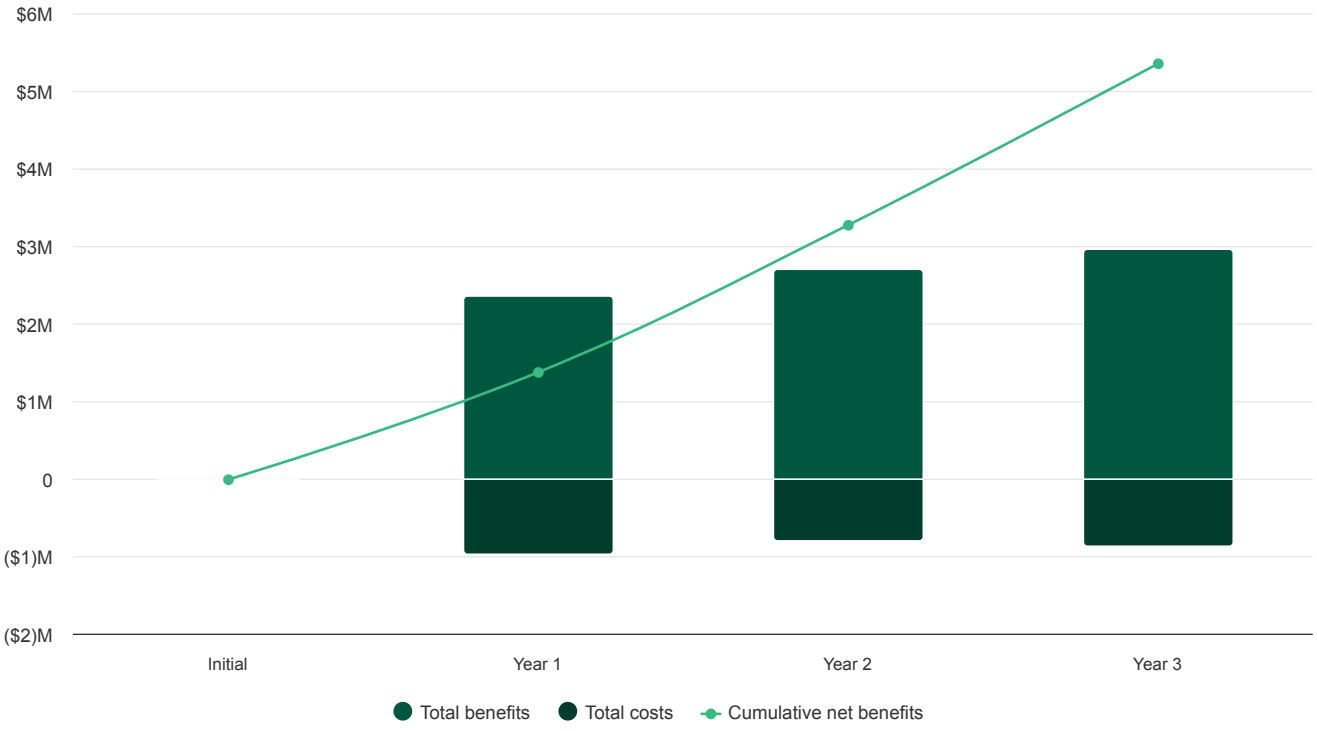
> *"Three [FTEs] focused on enrollment for Duo across the business, and then the rest of the team was focusing on business as usual. That just goes to show how simple Duo makes it to enroll users."*
>
> **Information security leader, retail**

Implementation And Management						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
H1	Total hours of Duo technical deployment and management effort per year	Interviews	180	312	312	312
H2	Fully burdened hourly rate for a technical resource	Composite	$72	$72	$72	$72
H3	**Subtotal: Deployment and scaling**		**$12,960**	**$22,464**	**$22,464**	**$22,464**
H4	Hours of Duo deployment effort per end user	Interviews	0	0.5	0.5	0.5
H5	Total end users adopted	Composite	0	10,000	1,000	1,000
H6	End-user hourly rate	Composite	$48	$48	$48	$48
H7	**Subtotal: Total end-user adoption costs**	**H4*H5*H6**	**$0**	**$240,000**	**$24,000**	**$24,000**
Ht	Implementation and management	H3+H7	$12,960	$262,464	$46,464	$46,464
	Risk adjustment	↑10%				
Htr	Implementation and management (risk-adjusted)		$14,256	$288,710	$51,110	$51,110
	Three-year total: $405,187			**Three-year present value: $357,360**		

Financial Summary

Consolidated Three-Year, Risk-Adjusted Metrics

Cash Flow Chart (Risk-Adjusted)



Cash Flow Analysis (Risk-Adjusted)						
	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	($14,256)	($969,110)	($799,550)	($867,590)	($2,650,507)	($2,207,884)
Total benefits	$0	$2,352,499	$2,697,511	$2,949,996	$8,000,005	$6,584,360
Net benefits	($14,256)	$1,383,388	$1,897,960	$2,082,405	$5,349,498	$4,376,476
ROI						198%
Payback						<6 months

Please Note

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.

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.

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 Cisco 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 Cisco Duo can have on an organization.

Due Diligence

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

Interviews

Interviewed seven decision-makers at organizations using Cisco Duo to obtain data about 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.

Glossary

Total Economic Impact Approach

Benefits

Benefits represent the value the solution delivers to the business. The TEI methodology places equal weight on the measure of benefits and costs, allowing for a full examination of the solution's effect on the entire organization.

Costs

Costs comprise all expenses necessary to deliver the proposed value, or benefits, of the solution. The methodology captures implementation and ongoing costs associated with the solution.

Flexibility

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

Risks

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."

Financial Terminology

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

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

Appendixes

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 solution providers in communicating their value proposition to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of business and technology initiatives to both senior management and other key stakeholders.

APPENDIX B

Endnotes

[1] Source: The Top Trends Shaping Identity And Access Management In 2025, Forrester Research, Inc., March 6, 2025; Making The Business Case For Identity And Access Management, Forrester Research, Inc., March 20, 2025.

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

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 Cisco Duo. For any interactive functionality, the intent is for the questions to solicit inputs specific to a prospect's business. Forrester believes that this analysis is representative of what companies may achieve with Cisco Duo based on the inputs provided and any assumptions made. Forrester does not endorse Cisco or its offerings. Although great care has been taken to ensure the accuracy and completeness of this model, Cisco and Forrester Research are unable to accept any legal responsibility for any actions taken on the basis of the information contained herein. The interactive tool is provided 'AS IS,' and Forrester and Cisco make no warranties of any kind.

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

Consulting Team:

Courtenay O'Connor

Alyssa Dolan

PUBLISHED

June 2025