FORRESTER®

# Cisco Duo: A Spotlight On Ease Of Use

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

Cisco commissioned Forrester Consulting to interview five representatives of four organizations and conduct a Total Economic Impact™ (TEI) study to better understand the benefits, costs, and risks associated with Duo. This abstract will focus on Duo's ease of use and its value to the interviewees' organizations.

Interviewees:

- Senior director of information security for a regional healthcare organization in North America with 11,000 Duo-protected accounts.
- Security technical lead for a global professional services organization based in North America with 6,800 Duo-protected accounts.
- IT support specialist for a global information services organization headquartered in North America with 1,225 Duo-protected accounts.
- Cybersecurity analyst and cyber defense operations center manager for a healthcare organization headquartered in North America with 12,000 Duo-protected accounts.

**2/3 less**
end-user time per authentication

**90% reduction**
in help desk cases

## INVESTMENT DRIVERS AROUND EASE OF USE

The interviewees said their organizations adopted Duo to reduce their security risks and improve ease of use. Prior to implementing Duo, these organizations struggled with challenges in their legacy environments, including:

- **Security analyst productivity around investigating suspicious login attempts.** With limited data readily available to support their organizations' investigations of suspicious login attempts, security analysts had to manually review logs for insights. A security technical lead at a professional services firm said: "In the past, our investigations of login attempts had to rely on super-generic logs. Analysts needed to log in to and then analyze each one of those. Tracking all these down, having the logins ready, and so on all took an hour or two for each case."

- **Poor end-user experience, including excessive time spent on each authentication.** Interviewees whose organizations previously used an authentication solution described end users' frustration with the time required to authenticate and the need to keep track of an additional device to do so.

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

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

## KEY RESULTS AROUND EASE OF USE

Interviewees reported the following ease-of-use benefits from implementing Duo:

**Security analyst productivity improvement.** Interviewees said Duo is easy to navigate and integrate with other applications and that it provides security analysts with detailed information about each authentication attempt. Analysts at the interviewees' organizations spent less time troubleshooting and investigating potential security issues that arose from suspicious login attempts.

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

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

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

→ READ THE FULL STUDY

**End-user time savings from streamlined authentication.** Interviewees said Duo saved end users time for each authentication request compared to their organizations' prior authentication solutions. A security technical lead at a professional services firm said: “With Duo, our end users spend less time on each authentication request. They no longer need to type in numbers and then wait for a response.”

Interviewees from organizations that opted to use Duo’s SSO functionality said their companies further improved end-user experiences by providing Duo users with a simplified and consistent login experience for all applications integrated with Duo whether the applications are on-premises or cloud-based. Cisco’s cloud-based SSO for Duo is designed to complement the Duo multifactor authentication solution, although Duo also integrates with dozens of third-party SSO and identity provider tools.

> **“It’s your easiest option for multifactor authentication in an enterprise environment.”**
>
> *IT support specialist, information services*

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

**Avoided costs for management and support of prior authentication solutions.** Interviewees said Duo is simpler to manage and support than their organizations’ previous solutions and that staff spend less time administering Duo, deploying additional functionality, adding new use cases, and optimizing its use. The organizations also eliminated expenses for professional services they previously needed to fill their internal expertise gaps.

- A security technical lead at a global professional services firm said: “Staff time savings have been a big benefit. Duo is very streamlined, and we were able to remove a lot of engineering hours that our team had spent to maintain the prior solution.”
- A cybersecurity analyst at a healthcare organization said: “Duo has been a great benefit to us in many ways — enrollment, provisioning, security, log activity, investigations, setting up policies, creating processes and standards to help internal teams. It’s all pretty easy. Some of the application owners I work with are not highly tech-savvy, but after working with them, explaining Duo to them, showing it to them, I don’t get a lot of them reaching out for help anymore. … With our prior product, we often had to contact the vendor for support because it was such a complicated system. Duo has helped our environment a lot.”
- An IT support specialist from an information services organization said: “We no longer pay for a professional services firm because we can manage Duo with our own security team. With the previous solution, we paid an external vendor on a constant basis to be available for us and help our dedicated engineers working on the solution. Now, instead of having to dedicate staff to supporting the solution, everybody on our security team is more or less trained to the level that they can operate Duo.”

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

**Help desk and end-user productivity improvement due to fewer authentication-related cases.** Interviewees said Duo simplified end users' authentication processes and eliminated the need for separate authentication devices. As a result, fewer authentication-related cases reached the help desk at interviewees' organizations, and this saved time for end users and help desk staff.

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

## TOTAL ECONOMIC IMPACT ANALYSIS

For more information, download the full study: "The Total Economic Impact$^{\text{TM}}$ Of Cisco Duo," a commissioned study conducted by Forrester Consulting on behalf of Cisco, February 2023.

## STUDY FINDINGS

Forrester interviewed five total representatives at four organizations with experience using Cisco Duo and combined the results into a three-year financial analysis for a composite organization. Risk-adjusted present value (PV) quantified benefits for the composite organization include:

- Savings of $671,000 from security analyst productivity improvement.
- End-user time savings from streamlined authentication, valued at $3.2 million.
- Savings of $326,000 from avoided costs for management and support of a prior authentication solution.
- Savings of $57,000 from help desk and end-user productivity improvements due to fewer authentication-related support cases.

**Return on investment (ROI)**

**159%**

**Net present value (NPV)**

**$3.23M**

## DISCLOSURES

The reader should be aware of the following:

- The study is commissioned by Cisco and delivered by Forrester Consulting. It is not meant to be a competitive analysis.
- Forrester makes no assumptions as to the potential ROI that other organizations will receive. Forrester strongly advises that readers use their own estimates within the framework provided in the report to determine the appropriateness of an investment in Cisco Duo.
- Cisco reviewed and provided feedback to Forrester. 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.
- Cisco provided the customer names for the interviews but did not participate in the interviews.

## ABOUT TEI

Total Economic Impact™ (TEI) 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. The TEI methodology consists of four components to evaluate investment value: benefits, costs, risks, and flexibility.

FORRESTER®