
# Two-Factor Authentication
# Evaluation Guide

What to look for when assessing and comparing two-factor authentication solutions.

A helpful guide from

DUO

**Over 95%** of security incidents involve harvesting credentials from customer devices, then logging into web applications with them.

***Verizon 2015 Data Breach Investigations Report***

**Two-factor authentication defends against account takeovers and data theft** by verifying your users' identities before they access your data. Using a device, like a smartphone, prevents attackers from remotely accessing your networks, servers and on-premises and cloud applications protected only with a password.

**But, not every two-factor solution is the same.** Some vendors only provide the bare minimum needed to meet compliance requirements – and lots of hidden costs required for deployment, operation and maintainence. Make sure you take your ROI (return on investment) into account when you evaluate different two-factor authentication solutions.

**This guide provides a comprehensive set of criteria to help you customize your evaluation using the aspects most important to your organization.**

# Consider the following criteria when evaluating different two-factor authentication solutions:

## SECURITY IMPACT

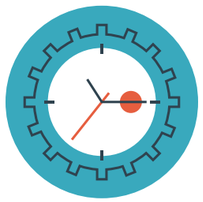
Can your solution protect against threats and provide visibility into your environment? How effectively does the solution reduce the risk of a data breach?

## STRATEGIC BUSINESS INITIATIVES

Is your solution compatible with other business initiatives? Does it fulfill compliance requirements?

## TOTAL COST OF OWNERSHIP

Does your solution provide more upfront value, or more hidden costs to your organization?



## TIME TO VALUE

How quickly can you get the solution up and running in your environment?

## RESOURCES REQUIRED

What kind of resources are required to deploy and provision users? Is the solution architected to reduce ongoing administration tasks?

# Security Impact

The most critical aspects of an authentication solution are 1) effectiveness against threats related to credential theft, and 2) underlying security and reliability. The primary goal is to reduce the risk of a data breach to your organization. If a solution is easily bypassed or doesn't provide comprehensive protection, it's not worth implementing (at any cost!).

## Secure Everything, Everywhere

### FOCUS ON REMOTE LOGINS

Before you implement a new security solution, take full inventory of your organization's applications, networks and data that can be accessed remotely.

If you can log into it over the Internet, you should protect it with more than just a username and password! Ensure your solution can integrate with any custom software, VPNs, cloud-based applications and devices.

### SECURE SENSITIVE DATA

Check that the solution allows you to create advanced policies and controls that you can apply to environments with sensitive data – whether it is Internet-accessible or on your private network. Examples include:

+ Define how users access sensitive systems, such as servers containing financial data
+ Set a stricter policy for servers with customer payment data vs. public file servers

### DETECT COMPROMISED DEVICES

Consider a solution that offers more advanced detection and protection from compromised devices – whether laptops, desktops, or mobile devices.

Check that the solution doesn't require an agent to run on every device, which can compromise user privacy.

> If you can log into it over the Internet, you should protect it with more than a username and password.

## Policies and Controls

An advanced two-factor authentication solution lets administrators define rules based on users, groups, devices, networks and applications. Examples include:

+ **Create a policy** that requires admins and IT staff to perform two factor every time they log in to protect privileged access
+ **Require less privileged users** to authenticate less often when using the same device
+ **Block login attempts** from foreign countries you don't do business in, and block access from anonymous networks, like Tor

While traditional solutions such as firewalls and intrusion prevention systems (IPS) can do this, they're typically limited to protecting your on-premises data center.

But by focusing only on the local network perimeter, these solutions leave many security gaps and zero coverage for cloud applications.

## Flexibility

It's expensive to rip and replace a solution, so choose one that can grow to support new users, integrations and devices – no matter where they are, including on-premises and in the cloud.

Check that your provider offers different authentication methods, including smartphone apps, phone callback, SMS passcodes and hardware tokens to fit every user's need.

## Availability

A security solution is only as valuable as it is available, and resilient against security incidents and downtime. A cloud-based two-factor provider should maintain their solution independent from your systems. That way, even if you're breached, access to your applications is still securely managed by your provider.

To protect against downtime, your provider's service should be distributed across multiple geographic regions, providers and power grids for seamless failover. Reliable vendors should demonstrate 99.995% uptime, guaranteed by strong service level agreements (SLA).

## Visibility

Ask your provider if your solution gives you insight into your users and their devices used to access your organization's apps and data. An advanced authentication solution should give you an at-a-glance picture of your security profile, letting you take action to protect against known vulnerabilities.

Ensure your solution comes with detailed logs about your users, administrators and telephony so you can create custom reports, ideal for security analysts and compliance auditors.

Choose a solution that gives you visibility into authentication attempts, including data on IP addresses, anonymous networks, blacklisted countries and more – useful for determining where and when certain attacks may occur.

> Check that your provider offers different authentication methods to fit every user's need.

# Strategic Business Initiatives

When evaluating a new security solution, consider how it may integrate with ongoing or future business initiatives, including Bring Your Own Device (BYOD), mobile enablement or the adoption of cloud applications. Other business drivers to consider include compliance regulation requirements, which vary by industry.

## Cloud Adoption

Today, most of your applications and servers might be on-premises, but some may migrate to the cloud over the next five years. Check that the authentication solution can easily integrate with your cloud applications.

Additionally, if you're moving away from managing software and hardware on-premises, then you should consider adopting a cloud-based authentication solution that can scale as needed.

Make sure your authentication solution protects what's important both today and in the future.

## Bring Your Own Device (BYOD)

Many organizations are considering or already allowing employees to use their personal computers, smartphones, and tablets to get work done. When evaluating authentication solutions, be sure to consider how compatible they are with your BYOD environment.

**Can users use their own devices to complete authentication?** This eliminates the need to carry around an extra device for authentication, allowing employees to conveniently use their smartphones.

**Can your authentication solution detect potential vulnerabilities and threats to your environment?** Ask your provider how you can get greater visibility and control into your cloud and mobile environment, without the need to download an extra agent on personal devices.

## Mobile-First

Are your employees accessing data and using mobile devices for work? If so, you'll want to make sure that your authentication solution is also "mobile-first."

Check that your authentication solution provides a mobile app that works with all of the different types of mobile devices used by your employees, including iOS, Android, Blackberry and Windows Phone. For flexibility, ensure the solution works with other phone-based methods, like SMS and phone callback.

If it's not easy to use, your users won't use it – evaluate the usability of your mobile app, for both your users (enrollment, activation and daily authentication) and administrators (user and solution management).

> If it's not easy to use, your users won't use it.

## Logging & Reporting

Ensure your solution comes with detailed logs about your users' activity so you can create custom reports, ideal for security analysis and compliance auditors.

Armed with details about jailbroken statuses, patch levels, browsers and more, you can also take action to prevent opening your network up to known vulnerabilities.

Logging also gives you insight into any user behavior anomalies or geo-impossible logins – if your user logs in from one location, and then logs in from another location around the world, your security team will know.

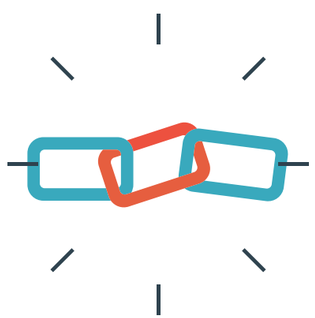
## Validation & Compliance

If you deal with any type of sensitive data, like personally identifiable data (PII), protected health information (PHI), customer payment data, etc., you need to ensure your two-factor solution can meet any compliance regulation requirements.

Additionally, your two-factor provider must be able to provide an up-to-date proof of compliance report for your auditors. Ask your provider if their company and solution is audited annually or regularly by an independent third-party auditor.

Check that the vendor's cloud-based service uses PCI DSS (Payment Card Industry Data Security Solution), ISO (International Organization for Standardization) 270001 and SOC (Service Organization Controls) 2 compliant service providers.

Remember, It only takes one weak link in the security chain of contractors for a breach to affect your organization.



Remember, It only takes one weak link in the security chain for a breach to affect your organization.

# Total Cost of Ownership

The total cost of ownership (TCO) includes all direct and indirect costs of owning a product – for a two-factor solution, that may include hidden costs, such as upfront, capital, licensing, support, maintenance, operating and many other unforeseen expenses over time.

**How can you be sure you're getting the best security return on your investment? Consider:**

## Upfront Costs

See if your vendor's purchasing model requires that you pay per device, user or integration – this is important if your company plans to add new applications or services in the future. Estimate how much it will cost to deploy two-factor authentication to all of your apps and users.

### ADMINISTRATIVE SOFTWARE/HARDWARE

**Is this included in the software license?** Additional management software is often required – without this, customers can't deploy two factor.

### AUTHENTICATORS

**Do you have to purchase dedicated end-user devices?** While tokens can add up, a mobile authentication app is typically free for any number of users.

### DATA CENTER COSTS

**Do you have to purchase servers?** Server hosting costs can add up: power, HVAC (heating, cooling and air conditioning), physical security, personnel, etc. A cloud-based vendor will cover those costs.

### HIGH AVAILABILITY CONFIGURATION

**Is this also included in your software license?** By setting up duplicate instances of your software and connecting a load balancer with the primary instance, you can end up tripling your software costs. Setting up a redundant or disaster recovery configuration can also increase costs significantly, and some vendors charge additional licenses for business continuity.

Look for vendors with simple subscription models, priced per user, with flexible contract times.

# Deployment Fees

## DEPLOYMENT & CONFIGURATION

Find out if you can deploy the solution using your in-house resources, or if it will require more resources and time to install, test and troubleshoot integration.

## END USER ENROLLMENT

Estimate how long it will take each user to enroll, and if it requires any additional administrative training and helpdesk time. Look for an intuitive end user experience and simple enrollment process that doesn't require training. Token-based solutions are often more expensive to distribute and manage than they are to buy.

## ADMINISTRATOR SUPPORT

To make it easy on your administrators, look for drop-in integrations for major apps, including APIs, to cut time and resources needed for implementation. See if you can set up a pilot program for testing and user feedback – simple integrations should take no longer than 15 minutes.

# Ongoing Costs

## PATCHES, MAINTENANCE & UPGRADES

Annual maintenance can raise software and hardware costs, as customers must pay for ongoing upgrades, patches and support.

It's often the responsibility of the customer to search for new patches from the vendor and apply them. Look for a vendor that automatically updates the software for security and other critical updates, saving the cost of hiring a team.

One of the benefits of cloud-hosted services is that servers, maintenance and monitoring are covered by the provider's network and security engineers, lightening the load for your team.

Depending on your solution, you may have to manually upgrade to the latest version. Some vendors may only update a few times a year, which can leave you susceptible to new vulnerabilities and exploits. Choose a vendor that updates often, and rolls out automatic updates without any assistance from your team.

## ADMINISTRATIVE MAINTENANCE

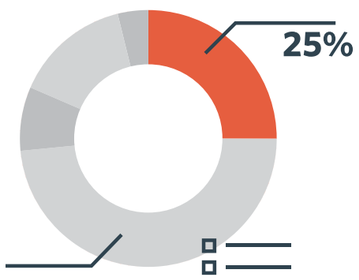
Consider the costs of employing full-time personnel to maintain your two-factor solution. Does your provider maintain the solution in-house, or is it up to you to hire experts to manage it?

Estimate how long it takes to complete routine administrative tasks – is it easy to add new users, revoke credentials or replace tokens? Routine tasks, like managing users, should be simple – sign up for a trial and take it for a test run before deploying it to all of your users.

## SUPPORT & HELP DESK

Live support via email, chat, and/or phone should also be included in your vendor's service – but sometimes support costs extra. Consider how much time is required to support your end users and help-desk staff, including troubleshooting time. For enterprises with large IT departments, it's not uncommon for help desk tickets related to tokens to account for 25 percent of the overall IT support workload.

If a solution requires extensive support from your IT or infrastructure teams, will you get charged for the time spent supporting your on-premises two-factor solution? Estimate that cost and factor it into your budget.




Token-related help desk tickets can account for 25% of the IT support workload.

## Modern Solutions

### High value, higher upfront costs

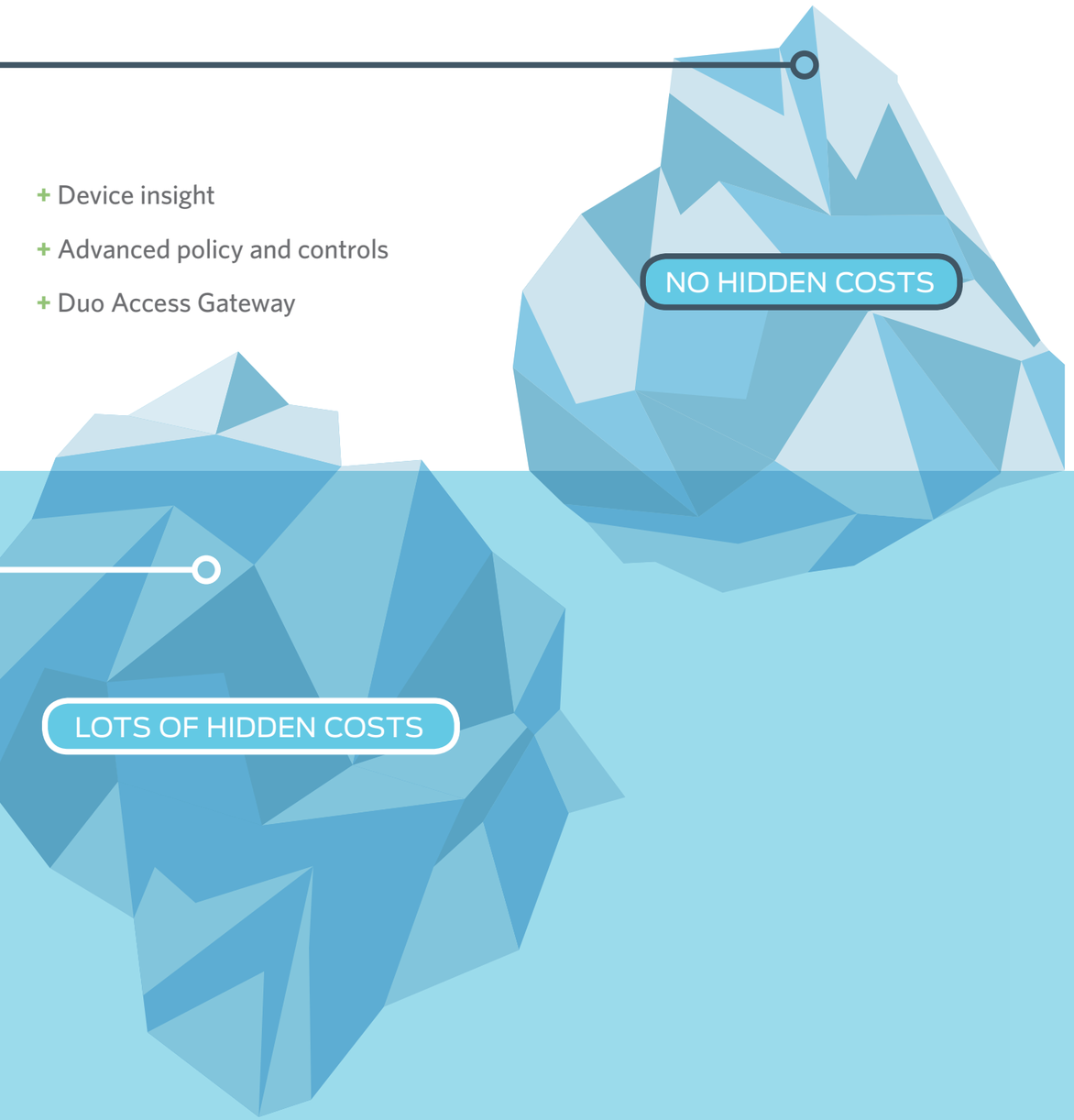
+ Simple subscription model
+ Free authentication mobile app
+ No fees to add new users or apps
+ No data center/server maintenance
+ High availability configuration
+ Automatic security and app updates
+ Administrative panel included
+ User self-service portal included
+ Device insight
+ Advanced policy and controls
+ Duo Access Gateway

## Traditional Solutions

### Low upfront costs, not much value

LOTS OF HIDDEN COSTS:

- **Additional cost to add new apps or users**
- **Administrative software/hardware**
- **Authenticators – tokens, USB, etc.**
- **Data center & server maintenance**
- **High availability configuration**
- **Administrative support**
- **Patches, maintenance & upgrades**
- **Help desk support**



# Time to Value

Time to value, or time to security, refers to the time spent implementing, deploying, and adapting to the solution. Determine how long it takes before your company can start realizing the security benefits of a two-factor authentication solution – particularly important after a recent breach or security incident.

## Proof of Concept

Setting up a two-factor pilot program lets you test your solution across a small group of users, giving you the ability to gather valuable feedback on what works and what doesn't before deploying it to your entire organization.

> Cloud-based services deploy faster since they don't require hardware or software installation.

## Deployment

Walk through likely implementation scenarios so you can estimate the time and costs associated with provisioning your user base. Cloud-based services provide the fastest deployment times since they don't require hardware or software installation, while on-premises solutions tend to take more time and resources to get up and running.

Most security professionals don't have time to write their own integration code. Choose a vendor that supplies drop-in integrations for all major cloud apps, VPNs, Unix and MS remote access points. You'll also want to look for a vendor that enables you to automate functionality and export logs in real time.

Also, to save on Single Sign-On (SSO) integration time, check that your two-factor solution supports the Security Assertion Markup Language (SAML) authentication standard that delegates authentication from a service provider or application to an identity provider.

## Onboarding & Training Users

A vendor's enrollment process is often a major time sink for IT administrators – make sure you walk through the entire process to identify any potential issues.

For enterprises, bulk enrollment may be a more time-efficient way to sign up a large amount of users. To support your cloud apps, ensure your two-factor solution lets you quickly provision new users for cloud apps by using existing on-premises credentials.

See if the solution requires hardware or software for each user, or time-consuming user training. Token deployment can require a dedicated resource, but easy self-enrollment eliminates the need to manually provision tokens.

With a mobile cloud-based solution, users can quickly download the app themselves onto their devices. A solution that allows your users to download, enroll and manage their own authentication devices using only a web browser can also save your deployment team's time.

# Required Resources

Consider the time, personnel and other resources required to integrate your applications, manage users and devices, and maintain/monitor your solution. Ask your provider what they cover, and where you need to fill in the gaps.

## Application Support

Some two-factor solutions require more time and personnel to integrate with your applications, whether on-premises or cloud-based.

Check that they provide extensive documentation, as well as APIs and SDKs so you can easily implement the solution into every application that your organization relies on.

## User & Device Management

Like any good security tool, your two-factor solution should give administrators the power they need to support users and devices with minimal hassle.

Look for a solution with a centralized administrative dashboard for a consolidated view of your two-factor deployments, and enables admins to:

+ Easily generate bypass codes for users that forget or lost their phones
+ Add and revoke credentials as needed, without the need to provision and manage physical tokens

Ask your provider if they offer a self-service portal that allows users to manage their own accounts, add or delete devices, and other simple tasks.

## Maintenance

Make sure that your solution requires minimal ongoing maintenance and management for lower operating costs – cloud-hosted solutions are ideal since the vendor handles infrastructure, upgrades and maintenance.

Can you use your existing staff to deploy and maintain this solution, or will you need to hire more personnel or contractors to do the job? Ask your vendor if monitoring or logging is included in the solution.

A solution that requires many additional resources to adapt and scale may not be worth the cost and time. Evaluate whether your solution allows you to easily add new applications or change security policies as your company needs evolve.

> Can your staff deploy and maintain the solution, or will you need to hire more personnel or contractors?

# The Duo Advantage

Duo Security's two-factor solution combines intuitive usability with advanced security features to protect against the latest attack methods - and to provide a frictionless authentication experience.

## Security Impact

### SECURE EVERYTHING, ANYWHERE

Duo's two-factor solution supports a wide variety of applications and systems, including VPNs, RDP, on-premises apps and more. Duo also provides APIs and mobile SDK to protect your custom applications and any proprietary systems.

» Learn about Supported Applications

Secure access to enterprise cloud apps like Google Apps, Amazon Web Services, Box, Salesforce and Microsoft Office 365. With Duo Access Gateway, you can use your users' existing credentials stored in Microsoft Active Directory, making provisioning faster and more accurate.

### POLICY AND CONTROLS

Duo's advanced two-factor authentication solution, Duo Platform Edition, gives you the ability to set custom policies and controls to protect your assets based on type of users, apps and devices – all without installing an extra agent on your users' devices.

» Learn more about Policy and Controls

### FLEXIBILITY

As a cloud-based solution, it's easy to provision new users and protect new applications with Duo as your company grows. There are no limits or additional charges per application protected. Onboard new users with self-enrollment, bulk enrollment or Active Directory synchronization.

» Learn about User Provisioning, and explore everything that can be protected with Duo

### AVAILABILITY

Duo protects against downtime, ensuring high availability with distribution across multiple geographic regions, providers and power grids for seamless failover. Duo has had 99.995% uptime since 2010 and is backed by the best SLA in the industry, ensuring your security is always available. Duo also takes its own service security very seriously.

» Learn more about Security & Reliability

### VISIBILITY

With Duo's Device Insight, IT admins can gain insight into the security configuration of mobile and PC devices used to connect to company applications and services, without the use of agents.

Duo's solution also provides detailed security logs that track events related to users, administrators and telephony activity, you can quickly create custom reports, ideal for security analysis and compliance auditors.

» Learn more about Reporting

# Strategic Business Initiatives

## CLOUD ADOPTION

As a cloud-based solution, Duo's two factor doesn't require any hardware or software to install or manage, and it's easy to scale with your growing users and applications.

Duo supports single sign-on (SSO) solutions, such as Okta, OneLogin, Ping Identity and Microsoft ADFS. Duo also supports SAML (Security Assertion Markup Language) cloud apps via Duo Access Gateway, including Google Apps, Amazon Web Services, Box, Salesforce and Microsoft Office 365.

## BRING YOUR OWN DEVICE

Duo's authentication mobile app, Duo Mobile is BYOD-friendly and can be used on many different devices, with no additional hardware required. Users can download the free app on their personal device without the use of an agent, ensuring user privacy.

## MOBILE-FIRST

As an authentication app, Duo was built for mobile from the start, and supports other mobile apps, such as LastPass, a popular password management solution. Duo also supports logging into Windows and Unix servers (using iOS/Android) with ease by using push notifications, Duo Push for authentication.

## LOGGING AND REPORTING

Duo's detailed user, administrator and telephony security logs can be easily imported into a security information and event management (SIEM) tool for log analysis, or viewed via Duo's Admin API for real-time log access.

Duo's Device Insight also provides data on your users' authentication devices, helping you identify outdated or vulnerable devices, as well as any anomalous user behavior.

## VALIDATION AND COMPLIANCE

Duo's security team includes some of the world's foremost experts in modern mobile, application and network security research and technologies. With regular security training, Duo's people work full-time to support large-scale security deployments.

Duo's cloud-based service uses PCI DSS, ISO 270001 and SOC (Service Organization Controls) 2 compliant service providers. Duo also offers protection for Epic applications, ideal for healthcare clients that use the system for electronic prescriptions.

Duo's two-factor authentication cryptographic algorithms have been validated by NIST, and Duo also complies with the U.S.-E.U. and U.S.-Swiss Safe Harbor frameworks for data privacy. Duo is serious about security – learn more about our Security and Reliability.

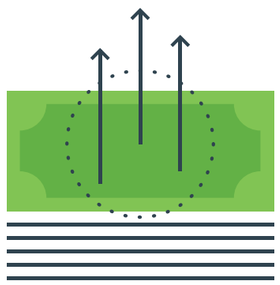
Duo's security team includes some of the world's foremost experts in modern mobile, application and network security research and technologies.

# Total Cost of Ownership

While traditional security products require on-premises software or hardware hosted in a data center, Duo offers security in a software as a service (SaaS) model through a cloud-based platform.

With Duo's two factor, you get the most upfront value with no hidden costs, including:

+ Easy deployment with the help of Duo's drop-in integrations for all major apps and APIs, and an administrative panel for user and solution management
+ A simple subscription model priced per user, billed annually, with no extra fees for new devices or apps
+ A free authentication mobile app that users can download themselves
+ A high availability configuration, disaster recovery and data center management
+ Automatic application updates, with patch management, maintenance and live support at no extra cost
+ Advanced features that let you customize policies and controls, as well as get device data



Other solutions may appear to come with a lower price tag, but the layers of hidden costs can add up fast, rapidly tripling TCO and offering less value overall.

# Time to Value

## PROOF OF CONCEPT

Duo lets you try before you buy, helping you set up pilot programs before deploying it to your entire organization, with extensive documentation and knowledge articles to help guide you through the evaluation stage.

## DEPLOYMENT

For faster and easier deployment, Duo provides drop-in integrations for all major cloud apps, VPNs, Unix and Microsoft remote access points, as well as support for web SDK and APIs. Quickly provision new users with bulk enrollment, self-enrollment, Microsoft Active Directory synchronization, or with the use of Duo Access Gateway.

Duo's solution lets you quickly provision new users for cloud apps by using existing on-premises credentials, including those for Microsoft Active Directory or cloud-based apps (OneLogin and Okta).

## ONBOARDING & TRAINING USERS

Duo's authentication app, Duo Mobile allows users to download the app onto their devices, while a self-service portal also lets users manage their own accounts and devices via an easy web-based login, reducing help desk tickets and support time.

# Required Resources

## APPLICATION SUPPORT

Integrate easily with your on-premises or cloud-based applications, with no need for extra hardware, software or agents. Duo's extensive documentation, APIs and SDKs makes for seamless implementation, reducing the need for a dedicated IT or security team.

## USER & DEVICE MANAGEMENT

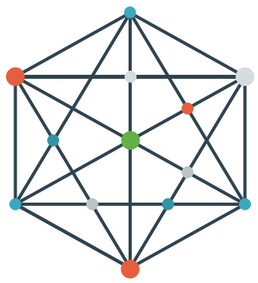
Duo's administrative panel allows admins to support users and devices using a centralized dashboard. Use the web-based portal to manage user accounts and devices, generate bypass codes, add phones to users and more.

Duo's self-service portal enables users to easily manage their own devices, reducing help desk tickets and support time for simple tasks.

## MAINTENANCE

As a cloud-hosted solution, Duo covers the infrastructure and maintenance, letting you focus on your core business objectives. Since security and other updates are rolled out automatically, you don't need to hire a dedicated team to manage the solution.

Plus, Duo's solution is flexible enough to scale quickly, letting you easily add new applications, users, or change security policies as needed.



Duo is flexible enough to scale quickly, letting you easily add new apps, users, or change security policies as you grow.

## ABOUT DUO SECURITY

Duo Security provides cloud-based two-factor authentication to thousands of organizations worldwide, including Facebook, Etsy, Random House, Paramount Pictures, Box, Toyota, Yelp, Threadless and more. In as little as fifteen minutes, Duo Security's innovative and easy-to-use technology can be deployed to protect users, data, and applications from breaches, credential theft and account takeover.

Try it Free

Learn More

## CONTACT


Toll Free +1 (866) 760-4247
International +1 (734) 330-2673

info@duosecurity.com