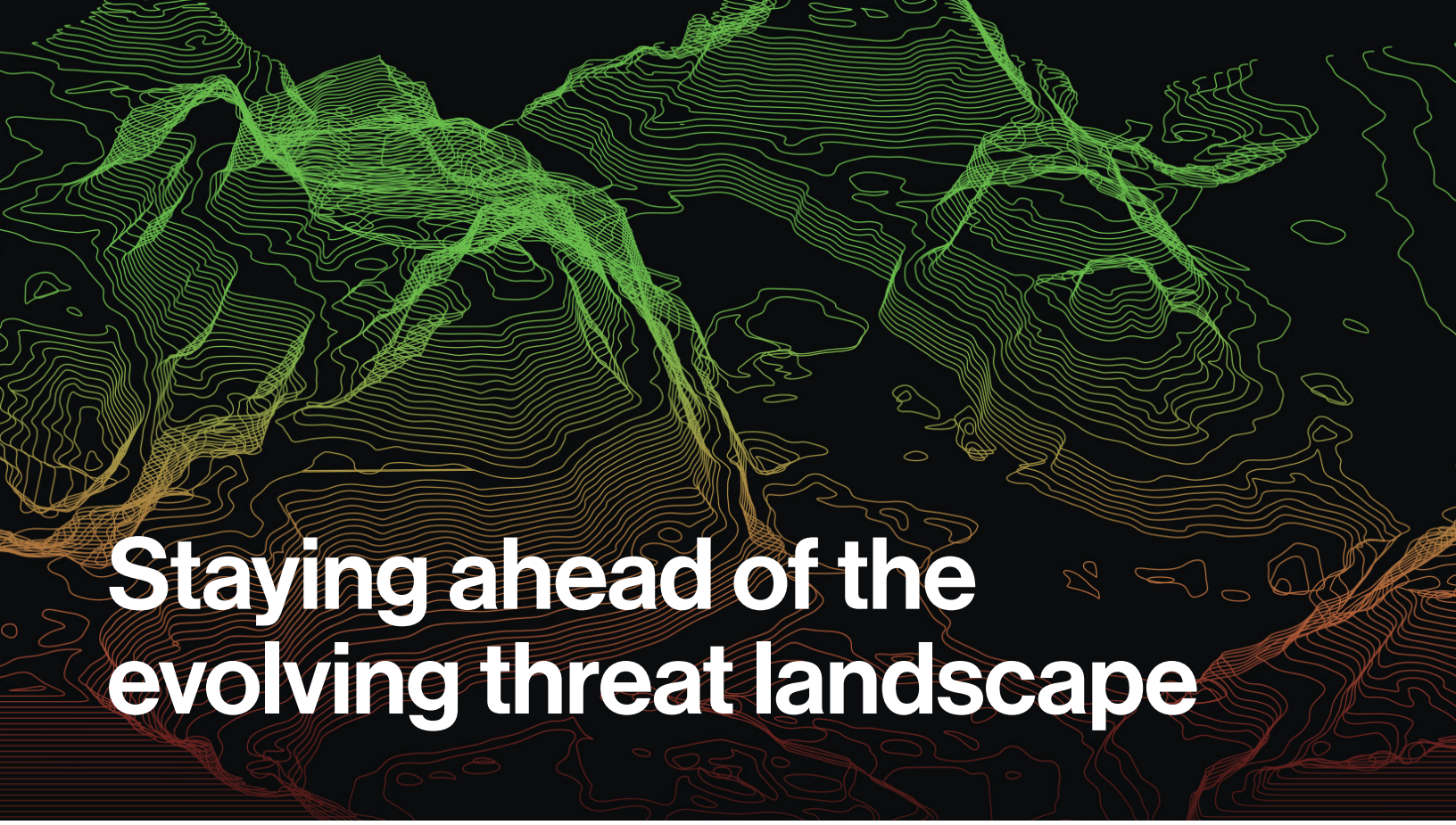
Fortifying Identity Security

CISCO DUO

Multi-factor Authentication

Buyer's Evaluation Guide



Staying ahead of the evolving threat landscape

In recent years, multi-factor authentication (MFA) has become a necessary defense for any cybersecurity strategy. By requiring multiple factors to be confirmed before permitting access, MFA protects your applications and data and helps to ensure only authorized users can log in to company networks.

However, with the emergence of new threat types such as push-bombing, social engineering, and spear phishing, organizations need to do more than rely on MFA alone. For as powerful and necessary as MFA is, it cannot be the only tool in your arsenal to identify, detect, and respond to these new threat types accordingly.

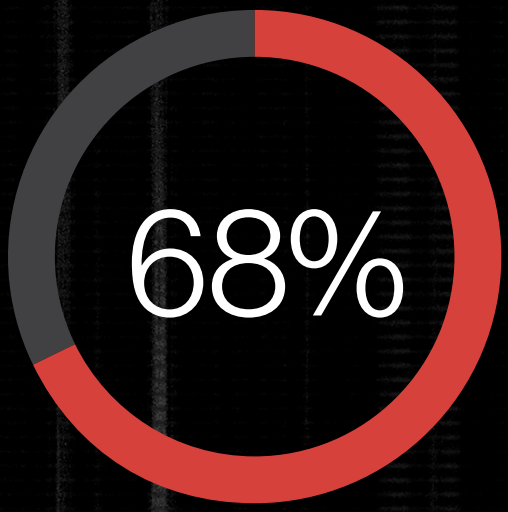
So, what are those new tools and why are they important?

Passwordless Logins

Risk-Based Authentication

Adaptive Access Policies

Identity Visibility Tools



68% of breaches involved a non-malicious human element, like a person falling victim to a social engineering attack or making an error.

Verizon 2024 Data Breach Investigations Report

To stay protected, organizations need to increase the effectiveness of MFA with powerful next-generation solutions such as passwordless logins, risk-based authentication (RBA), adaptive access policies, and identity visibility tools. These new improvements and additions to your security all serve the same purpose: fending off even the most sophisticated attacks.

But not every solution is the same. Some vendors only provide the bare minimum needed to meet compliance requirements, and often include hidden costs required for deployment, operation, and maintenance. Many traditional solutions are clunky, error-prone, and require extensive user training and support – costing your employees time and productivity. Security tools can be a tradeoff between efficacy and employee efficiency, with smooth end-user experience being a necessary consideration.

In this guide, you'll get:

- A thorough look at expanding your identity security posture beyond MFA minimums
- An overview of the hidden costs of identity security solutions and how to determine your return on investment (ROI)
- What to look for to ensure your solution can protect against the risk of a data breach
- A list of resources needed to deploy, provision, and integrate your solution
- An overview of the different strategic business initiatives, and how your solution fits into them

Going beyond MFA: Consider the following criteria when evaluating different solutions

Security Impact

Can your solution protect against unauthorized access and provide visibility into users and devices in your environment? How effectively does the solution reduce the risk of a data breach? Can your solution provide access control for managed and unmanaged devices? Does your solution alert you to unusual or suspicious login activities? How will the solution stay up-to-date on novel attack methods?

Strategic Business Initiatives

Is your solution compatible with other business initiatives such as zero trust, enabling remote work, or onboarding cloud applications? Does it fulfill industry-specific compliance requirements?

Total Cost of Ownership

Does your solution provide upfront value, or incur hidden costs to your organization? Can it work with modern and legacy systems? Can the solution help consolidate multiple siloed tools? What are the predicted help desk costs or potential savings from password-related cases?

Time to Value

How quickly can you get the solution up and running in your environment? How easily can you onboard end-users? How much planning is required before deployment?

Required Resources

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

Suggested KPI for MFA and Identity Security

- % of user accounts configured to use multi-factor authentication
- % of user accounts using strong forms of MFA (FIDO2, passwordless, passkeys, number-matching)
- % of guest accounts with MFA
- % authentication-related help desk tickets
- # risky authentication events triaged per time frame

Security Impact

The most critical security aspects of an authentication solution are:

1. effectiveness against threats related to credential theft or account takeover, and
2. underlying security and reliability

The primary goal is to reduce the risk of a breach to your organization. If a solution is easily bypassed or doesn't provide comprehensive protection that keeps up with and responds to novel threat data, it's not worth implementing.

Protecting All Applications

For end users, single sign-on (SSO) provides access to multiple applications with a single login (using one master set combination of username and password) – and reduces the number of passwords, eliminating bad password habits such as poorly-constructed passwords and password reuse. For administrators, SSO serves as a unified point of visibility for authentication and access logs, and an effective policy enforcement point to apply security policies for each application depending on its risk profile.

Reduce Dependency On Passwords

Passwords are a thorn in the side of enterprise security. An average enterprise uses more than 1,000 cloud apps today. That's too many passwords for IT to manage securely, and for users to remember. This results in password fatigue, and it's no surprise that weak and stolen passwords are among the leading causes of a breach. Eliminating passwords from authentication sounds very attractive; however, as with any new technology, it is wise to take a thoughtful approach to adopting passwordless authentication.

Passwordless is a journey that requires incremental changes for both users and IT environments. Ask security vendors how their products can help you embrace a passwordless future without creating security gaps or causing IT headaches.

Enabling a single sign-on (SSO) option along with MFA is a great way to start the passwordless journey without compromising on security.

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

Adaptive Policies & Controls

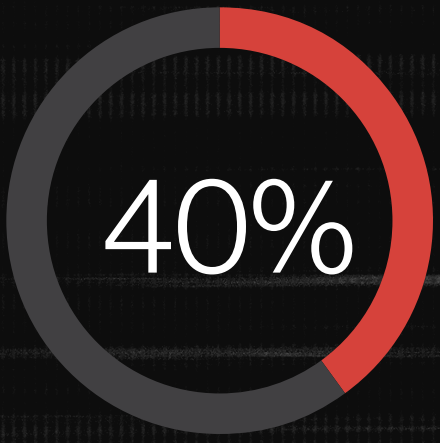
An advanced multi-factor authentication solution lets administrators define rules and levels of access with adaptive controls, balancing security and ease-of-use based on the users, groups, devices, networks, and applications involved. One tenant of zero trust security, granular policies limit access to critical data to only those who need it.

Check that the solution allows you to create and enforce advanced policies and controls that you can apply to environments with sensitive data – whether it is internet-accessible or a private network.

Examples of adaptive policies and controls include:

- Require admins and IT staff to perform a more secure two-factor authentication using biometrics or a FIDO-based security key every time they log in to protect privileged access
- Allow users to authenticate less often when using the same device
- Block login attempts from foreign countries where you don't do business, and block access from anonymous networks, like Tor
- Allow users to only access critical applications from corporate managed devices
- 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

While traditional solutions such as firewalls and network access control (NAC) can do this, they're typically limited to protecting your on- premises resources. But by focusing only on the local network perimeter, these solutions leave many security gaps and zero coverage for cloud applications. Look for a solution that offers protections beyond a traditional network-based perimeter and truly protects access from any device and from any location.



On average, over 40% of accounts do not have strong forms of MFA enabled.

Duo Trusted Access Report

Implement Risk-Based Authentication

In addition to reducing reliance on passwords, risk-based authentication is a very effective policy method to block attackers from getting unauthorized access – especially when risk decisions are based on organization benchmarks and industry best practices.

An access solution should continuously assess access risk by examining signals such as the user's location, device, browser, and access behavior on each login attempt. Having this context enables an automated and dynamic response to the login request, "stepping-up" authentication when necessary, using the zero trust principle of "never trust, always verify."

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

Verify Device State

Consider a solution that offers comprehensive device verification capabilities across laptops, desktops, and mobile devices. The solution should ensure that devices accessing your environment comply with your organization's security criteria. This includes verifying that the devices have critical software patches installed and enabling end-user self-remediation where applicable.

Check that the solution can leverage telemetry from your endpoint security agents and device management tools as part of posture assessments.

Visibility & Analytics

Ideally, your new solution would give insight into your users and the devices they use to access your organization's apps and data. An advanced authentication solution should give you an at-a-glance picture of the security profile of all identities and devices in your environment, ensuring all users are set up with MFA and letting you protect against known vulnerabilities. Because data is only as useful as it is accessible, make sure your dashboard provides a comprehensive bird's-eye view along with the ability to quickly zoom or filter into more granular information.

Your identity solution should come with detailed logs about your users, devices, administrators, and authentication methods. The solution should allow these logs to easily export to your SIEM tools and help 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. Ask if the provider can detect and automatically alert administrators in case of risky login behavior or suspicious events, such as new device enrollment for authentication or login from an unexpected location.

Flexibility

It's expensive to rip and replace a solution, so choose one that can scale 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, biometrics, smart wearable devices, phone callback, passcodes, and hardware tokens 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 legacy systems, bring your own device (BYOD), remote work or the adoption of cloud applications. Other business drivers to consider include compliance regulation requirements, which vary by industry and location.

Cloud Adoption Today

While many of your applications and servers might be on-premises, cloud implementations proliferated over the past few 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) — Remote Work Protection

Many organizations are allowing employees to use their personal devices to get work done. When evaluating authentication solutions, consider how compatible they are with your BYOD environment. Can users use their own devices to complete authentication?

Check that your authentication solution provides a mobile app that works with all the different mobile and remote devices your employees use, including Windows, Apple iOS and Android. For flexibility, ensure the solution works with other methods like security keys, mobile push, code generators, and phone callback.

Can your authentication solution detect potential vulnerabilities in the devices your employees use? Ask your provider how you can get greater visibility into and control over your cloud and mobile environment, without requiring users to enroll their personal devices in enterprise mobility solutions (like mobile device management/MDM).

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).

Monitoring & 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 up your network to known vulnerabilities. Monitoring 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 with the same credentials from another location around the world, your security team will know.

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

Validation & Compliance

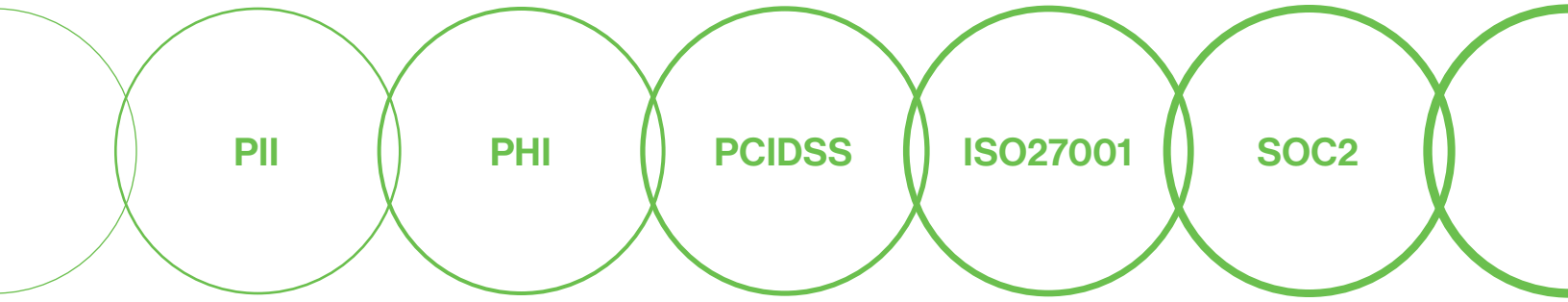
If you deal with any type of sensitive data, like personally identifiable information (PII), protected health information (PHI), customer payment data, etc., you need to ensure your two-factor solution can meet any compliance regulation requirements.

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

Additionally, your MFA 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. 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 includes all direct and indirect costs of owning a product – for a multi-factor solution, that may include hidden costs, such as upfront, capital, licensing, support, maintenance, operating, and many other unforeseen expenses over time, like professional services and ongoing operation and administration costs.

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 scale and add new applications or services in the future. Many hosted services provide a per-user license model, with a flat monthly or annual cost for each enrolled user. When investigating licensing costs, make sure to confirm whether licenses are named (locked to a single user ID) or transferable, whether there are add-on charges for additional devices or integrations configured, or delivery charges for different factor methods. Estimate how much it will cost to deploy multi-factor authentication to all 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 MFA. Does the service require the purchase and configuration of hardware within your environment? Confirm the initial and recurring costs for this equipment, and research the typical time and labor commitment necessary to set up these tools. For administrative access with tiered permissions based on license version, confirm all functionality you depend on is available, or collect a complete list of necessary upcharges.

Vendor Consolidation

While network environments with a traditional perimeter defense model rely on a handful of key services to maintain visibility and enforce security standards, the growth of SaaS adoption has resulted in many piecemeal solutions to cover the expanded needs of securing cloud-based data and assets. Secure access includes strong authentication through MFA to validate users and may also include:

- Endpoint management or mobile device management tools for defending against device compromise threats
- Single sign-on portals to centralize and simplify login workflows for users
- Log analysis tools to identify and escalate potential security threats
- Multiple dashboards to manage disparate services and cover unsupported applications

Along with the redundant costs that can accrue from these overlapping services, each added tool increases complexity and the chances of human error or oversight. Finding a solution with comprehensive utility for secure access can reduce both initial and ongoing management labor costs.

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

Authenticators

Do you have to purchase hardware authentication devices? Physical tokens add inventory, management, and shipping costs to consider. For mobile authenticators, confirm if there is any per-device cost for soft tokens, or if an unlimited number of enrolled devices is permitted for each user license.

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 licensing fees for business continuity.

Deployment Fees

Deployment & Configuration

Find out if you can deploy the solution using your in-house resources, or if it will require professional services support and time to install, test, and trouble-shoot all necessary integrations.

End User Enrollment

Estimate how long it will take each user to enroll, and if it requires any additional administrative training and help desk time. Discuss with your vendor the typical deployment timeframe expected with your use case and seek feedback from peers to validate how this aligns with their experience. Look for an intuitive end-user experience and simple enrollment process that doesn't require extensive 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, to cut time and resources needed for implementation. Also confirm the availability of general-purpose integrations for the most common authentication protocols to cover edge use cases, along with APIs to simplify integration for web applications. 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

Security 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, requiring time and resources.

Look for a vendor that automatically updates the software for novel security breaches and other critical updates, saving the cost of hiring a team. Choose a vendor that updates often, and ideally rolls out automatic updates without any assistance from your team.

Administrative Maintenance

Consider the costs of employing full-time personnel to maintain your MFA 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 users.

Support & Help Desk

Gartner estimates that password reset inquiries comprise anywhere between 30% to 50% of all help desk calls. And according to Forrester, 25% to 40% of all help desk calls are due to password problems or resets. Forrester also determined that large organizations spend up to $1 million per year on staffing and infrastructure to handle password resets alone, with labor cost for a single password reset averaging $70.

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

High value, upfront costs

- Simple subscription model
- Free authentication mobile app
- No fees to add new apps or devices
- No data center/server maintenance
- Automatic security and app updates
- Administrative panel included
- User self-service portal included
- User, device, and application access policies and controls
- Device health and posture assessments
- Device context from third-party security solutions
- Passwordless authentication
- User behavior analytics
- Single sign-on (SSO) and cloud support

Modern Solutions

Traditional Solutions

Many Hidden Costs

No Hidden Costs

Potentially low upfront costs, not much value

- Additional cost to add new apps or users – administrative software/hardware
- Authenticators – tokens, USB, etc.
- Data center and server maintenance
- High availability configuration
- Administrative support
- Patches, maintenance, and 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 multi-factor authentication solution. This is particularly important after a recent breach or security incident.

Proof of Concept

Setting up an MFA 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.

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 because 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 integration time, check that your MFA 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 number of users. To support your cloud apps, ensure your MFA solution lets you quickly provision new users for cloud apps by using existing on-premises credentials and simple identity provider (IdP) syncing.

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 MFA 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 MFA 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 because 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?

How Duo Can Help

Duo's MFA solution, built with zero trust security as a priority, combines intuitive usability with advanced identity security features to protect against unauthorized access and the latest attack methods, while still providing a frictionless authentication experience.

Security Impact

Stop identity-based threats and boost user productivity. Duo provides the best access management experience across all users, devices, and applications – and adds a powerful security layer for any identity infrastructure.

Secure Every Application

Remote access is a growing IT norm. Duo's solution easily and quickly integrates with virtual private networks (VPNs) and remote access gateways like CA SiteMinder, Juniper, Cisco, Palo Alto Networks, Citrix, and more; enterprise cloud apps like Microsoft O365, Salesforce, Google Apps, AWS, and Box; and on-premises and web apps like Epic, Splunk, Confluence, Shibboleth, and more. Duo provides APIs and client libraries for everything else, including your custom and proprietary software.

For Microsoft Windows environments, Duo integrates with Microsoft Windows client and server operating systems to add two-factor authentication to Remote Desktop and local WinLogon and credentialed User Access Control (UAC) elevation prompts.

With Duo's secure cloud-based single sign-on, you can leverage your existing identity provider for faster provisioning and improved accuracy whether in the cloud or on-premises, allowing your users to log in just once to securely access your organization's applications.

Learn more about securing Every Application and see how easy it is to set up Duo SSO.

"One of the reasons we continue to invest and further our implementation with Duo is because it isn't just an MFA tool. The risk-based challenges are something we enabled very early on to get ahead of the MFA fatigue attacks that we were seeing."

Mark Rodrigue
Senior Network Engineer, Room & Board

Room&Board

Start Your Passwordless Journey

Duo Passwordless authentication improves user experience, reduces IT overhead, and strengthens security posture. With security in mind, risky devices (unknown, jailbroken or out of date) cannot be used to authenticate without a password. In addition, Duo continually monitors logins and new enrollments to automatically detect anomalies and alerts the administrators in case your environment is compromised.

Duo Passport further enables your organization's continuous identity security by eliminating subsequent authentication interruptions without compromising on security – a true and secure single sign-on experience starting at the device level.

Learn more about Passwordless and Duo Passport.

Real-Time Risk-Based Authentication

Traditional "block or allow" policies and risk signals like IP addresses can be too blunt for today's attack landscape. Duo's Risk-Based Authentication takes baseline authentication behavior and evaluates contextual signals to dynamically adjust security requirements in real time, protecting trusted users and frustrating attackers. If context changes when a trusted user is attempting access, for example if a login in an active session is coming from a new location such as a coffee shop or the user has a new smartphone or laptop, Duo will respond dynamically with a more secure authentication method based on the potential risk level it determines. If the risk level is determined to be low, the user seamlessly continues with their work.

Learn more about Risk-Based Authentication.

Verify Device State With Trusted Devices

When organizations deploy Duo, device trust becomes a part of the authentication workflow during the user login process for protected applications. This enables Duo to provide in-depth visibility across managed and unmanaged devices, however and from wherever the users connect to these applications. Duo also verifies the security health and management status of endpoints before granting access to your applications, and blocks access if the device is unhealthy or does not meet your security requirements.

You can easily ensure that users maintain appropriate device hygiene, whether by updating the OS patch levels or browser versions, checking for presence of device certificates, or enabling security features such as enterprise antivirus (AV) agents and disk encryption.

With Duo Trusted Endpoints, included in every Duo edition, allows administrators to define a trust policy for every endpoint – whether managed or unmanaged, company-issued, contractor-owned, or personal – and stop attacker's unknown devices even if they can bypass MFA.

Learn more about Trusted Devices.

In one month, using Duo, Cisco performed 2.6 million health checks and users self-remediated 48,000 devices. That's 48,000 times a potential vulnerability was patched without any effort from IT or impact on the help desk.

Read the full Cisco case study here

Adaptive Policies & Controls

Security policies for every situation. Duo's granular advanced policy controls provide zero trust protection to environments with sensitive data, whether on-premises or in the cloud. With Duo, you can create custom access policies based on role, device, location, and many other contextual factors that are the bedrock of a strong zero trust security framework.

Duo verifies the identity of your users with multi-factor authentication and the security health of their devices before they connect to your applications. With Duo, IT administrators may also create complex policy rules that continuously monitor logins to identify and flag unusual activity.

Learn more about Adaptive Access Policies and demo setting up a policy in Duo.

Visibility, Analytics, & Remediation

Duo's dashboard, reports, and logs make it easy to monitor every user, on any device, anywhere, so you can identify security risks before they lead to compromised information. Get visibility into authentication attempts, including data on IP addresses, anonymous networks, blacklisted countries, and more from Duo's admin panel.

Duo gives you complete visibility and helps you inventory every endpoint accessing your applications and provides data on operating system, platform, browser, and plugin versions, including passcode, screen lock, full disk encryption, and rooted/jailbroken status. You can easily search, filter, and export a list of devices by OS, browser, and plugin, and refine searches to find out who's susceptible to the latest iOS or Android vulnerability.

Duo Trust Monitor is a security analytics feature that identifies and surfaces risky, potentially insecure user behavior in a customer's Duo deployment. If a user significantly deviates from their individualized behavioral profile, Duo Trust Monitor will surface the case as behaviorally anomalous.

Identity Threat Detection and Response (ITDR) is a growing security focus. With Duo and Cisco Identity Intelligence, you get powerful detection of identity-based risk from all relevant identity sources – with insight to take the right remediation action. Identify MFA gaps, dormant accounts, and privilege creep to reduce the risk of a breach.

Learn more about the Duo Admin Panel and Cisco Identity Intelligence.

"We need to ensure the highest level of protection for all user interactions with our services. We also need to meet an extremely high bar for security standards while making it easy for users to be productive. Duo helps us do just that."

Mark Schooley
Senior Director, IT Operations & Engineering, box

box

"We have deployed Duo across several domains and the product easily scales to all my users without additional overheads. I am able to save my company up to 30,000 USD a year in licensing costs."

Clint McWilliams
Network Security Administrator, Globe Life

Flexibility

As a cloud-based solution, it's easy to provision new users and protect new applications with Duo as your company grows, because there are no limits or additional charges per application. We believe that if you're protecting a user's access to your most important applications, you shouldn't be penalized or charged more to protect them everywhere. Easily onboard new users with Duo's self-enrollment, bulk enrollment or Active Directory synchronization options.

There are a variety of ways Duo MFA can work, though not all factors provide the same level of security. While FIDO2-based phishing resistant passwordless is an ideal end-goal, Duo meets organizations at their level of need. You can use a smartphone, landline (such as your office or home phone), tablet, or hardware token. Authentication methods include mobile push, biometrics including Touch ID or Windows Hello, passwordless, smart watches, roaming authenticator tokens, and more.

Learn about User Provisioning.

Strategic Business Initiatives

Cloud Adoption

Duo meets organizations at any stage of digital transformation by providing the widest coverage of applications. By leveraging a scalable cloud-based platform rather than relying on on-premises hardware requiring setup and costly maintenance, Duo can be deployed rapidly and easily scales with your growing users and applications. Duo protects SAML cloud apps via secure single sign-on, and partners with other technology providers to provide deep integration with Microsoft and Google apps, Amazon Web Services, Epic, and Salesforce. See our full list of partnerships and integrations.

Workforce Productivity

Duo provides a better end-user experience for accessing applications by reducing workflow friction and increasing workplace productivity.

Duo offers low-friction authentication methods such as Duo Push, biometrics, and FIDO security keys. Duo also offers the ability to apply intelligent policies to reduce how often a user is prompted to authenticate, using features such as risk-based authentication and custom remembered device policies. With Duo Passport, combine MFA, SSO, RBA, and device trust to implement a truly secure and seamless user sign-in experience while lowering the administrative burden for IT. Duo is focused on aligning with your organization's goals by enabling users to be productive without compromising on security.

Bring Your Own Device (BYOD) – Remote Work Protection

The Duo Mobile app (iOS, Android) and the Duo Desktop app (Windows, macOS, Linux) are BYOD-friendly for remote access and can be used on many different devices. Duo can maintain your device inventory, so you have clear visibility into what device is connecting, when, and from where. Users can download the app on their personal device without enrolling in device management solutions, ensuring user privacy.

Monitoring & 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. In addition, Duo Trust Monitor employs machine learning – behavioral analytics to simplify risk detection in case of anomalous login activity. Having detailed logs at hand can help add context for IT and security teams without having to manually sift through.

Validation & Compliance

Duo's full-time security team is experienced in running large-scale systems security, and comprises top mobile, app, and network security experts. Cisco Duo has been independently certified with the ISO/IEC 27001, 27017 and 27018, SOC 2 Type II, as well as certified by FIDO2 and NIST 800-63-3 (Digital Identity Guidelines) and PCI-DSS v 4.0.

Duo can also help your business meet various compliance requirements and regulatory framework guidelines. Duo Push satisfies Electronic Prescription of Controlled Substance (EPCS) requirements for two-factor authentication in the healthcare industry, and Duo's one-time passcodes meet FIPS 140-2 compliance for government agencies.

Duo enables organizations to check and enforce the MFA, device security, and compliance posture prescribed by insurance and industry standards.

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.

Duo's full-time security team is experienced in running large-scale systems security. Duo's diverse research and engineering teams comprises top mobile, app and network security experts and have worked at Fortune 500 companies, government agencies and financial firms.

Total Cost of Ownership

No Hidden Costs

Duo offers a simple subscription model priced per user, billed annually, with no extra fees for new devices or applications. With Duo's multi-factor authentication, you get the most upfront value with no hidden costs such as upfront, capital, licensing, support, maintenance, operating and many other unforeseen expenses over time.

Get the most upfront value with no hidden costs, including:

- Wide range of secure authentication methods to fit your organization's needs
- 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
- Automatic application updates that keep up with latest attack trends, with patch management, maintenance, and live support at no extra cost
- Advanced features that let you customize granular policies and controls, as well as get detailed device health data
- End user self-remediation to ensure accessing devices meet organization security requirements, reducing burden on your help desk
- Insight on user login behavior in your environment and the ability to flag anomalous login attempts, with navigable and reportable logs
- Support on the journey to eliminate passwords and improve security with passwordless authentication
- No data center costs with a fully cloud-delivered software

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.

Read Forrester's Total Economic Impact of Cisco Duo report.

ISO + SOC2

99.99%

High-Availability Configuration

Where some vendors require you to purchase additional licenses for business continuity and high availability, Duo offers high availability configuration, disaster recovery and data center management tools without busting your budget.

Duo provides a high-availability service split across multiple geographic regions, providers, and power grids for seamless failover, and our multiple offsite backups of customer data are encrypted.

Duo's nine international data centers are ISO27001 and SOC2 compliant and maintain 99.99% target service availability goal.

Read Duo's Guide to Business Continuity Preparedness and SLA.

Support & Help Desk

Duo has an extensive library of free resources to answer all questions. Duo also offers live support at no extra cost and provides four kinds of paid support options, providing you with the opportunity to choose the best fit for your organization. With Duo Care premium support, you can receive 24/7 tailored, white glove subject matter expert involvement.

See Duo's support resources.

Budget Consolidation

Modern-day heterogenous IT environments can create complex security infrastructures and reveal edge cases in protection. This requires adaptable solutions that offer more coverage and higher value.

An identity visibility, secure single sign-on, device trust, and modern authentication solution in one, Duo's continuous identity security solution provides comprehensive platform-agnostic security that eliminates the need — and budget — for many disparate identity security and access management tools that may prove difficult to fully integrate. The value is in consolidation, filtering out as much of the noise as possible and giving a comprehensive dashboard that gives a birds-eye view, and the ability to quickly zoom in to the granular details where attention is needed.

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

Time to Value

Proof Of Concept

Duo lets you try before you buy, helping you set up pilot programs before deploying 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 MS remote access points, as well as support for web SDK and APIs. Quickly provide new users with bulk enrollment, self-enrollment, or easy-to-use Microsoft Active Directory synchronization.

Onboarding & Training Users

Duo's authentication app, Duo Mobile, allows users to quickly 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. Duo also provides ready-to-use resources for end-users.

DENVER
THE MILE HIGH CITY

The City and County of Denver leveraged Duo's end-user email communication templates that detail step-by-step enrollment instructions. This helped to successfully roll out Duo MFA to over 18,000 users within three months, which resulted in less than 100 help desk tickets.

Read the full case study here

Required Resources

Duo integrates 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 make 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 one centralized dashboard. Log in to 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 manage their own devices, reducing administrative 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 frequently and automatically to patch for the latest vulnerabilities, you don't need to hire a dedicated team to manage the solution. Duo's solution is flexible enough to scale quickly, letting you easily add new applications, users or change security policies as needed.

Dedicated, Responsive Support

To answer your questions before, during and after your Duo deployment, you can count on our fully staffed, in-house Duo Support team.

Our responsive support team members have the security expertise to quickly assist you with any specific integration needs. Duo's customer support service is included with your solution at no extra charge, with no support contracts required. In addition, we offer extensive knowledge base articles to help troubleshoot and quickly fix known issues. Our end-user guide and detailed documentation are frequently updated and helpful resources available on Duo.com.

For more advanced deployments and specific SLA requirements, we provide Duo Care, a premium customer support service with extended coverage and a dedicated Customer Success team. Other options include Duo Quick Start, a high-touch 60-day program to accelerate your Duo deployment, and Software Support Service (SWSS) Enhanced Support for Duo.

The Duo Customer Success team equips you with everything you need to roll out your Duo deployment, including a customized launch kit to help with security policies, user training, executive business reviews (EBR), solution architecture design, and support for identifying security gaps or deploying new features.

"The Customer Success team continues to check in with us on a monthly basis. That commitment to excellence is rare and not present with every organization that we do business with. We are now asking others to be as committed to their product as Duo has been."

Nicholas Pelczar
Director of Information Security and Business Continuity, Stinson Leonard Street

STINSON

Get Stronger Identity Security Today

At Duo, we combine security expertise with a user-centered philosophy to provide identity visibility and security, advanced multi-factor authentication, endpoint remediation, and secure single sign-on tools for the modern era. It's so simple and effective, you get the freedom to focus on your mission and leave protecting it to us.

Cisco Duo's continuous identity security solution provides a strong access management experience across all users, devices, and applications – and adds a powerful security layer for any identity infrastructure. Its platform incorporates context from all identity sources and uses AI to assess and dynamically respond to identity-related threats before, during, and after login. Duo's SSO and Device Trust offerings additionally reduce user login friction without compromising security for the widest range of applications.

A trusted security partner to over 100K organizations across the globe, Duo stops identity-based threats and boosts user productivity while dramatically decreasing TCO with 159% average ROI and payback in less than six months.

Experience advanced multi-factor authentication, endpoint visibility, custom user policies, and more with your free 30-day trial. You'll see how easy it is to secure your workforce, from anywhere on any device with Duo.

Start your free 30-day trial and quickly protect users, devices, and applications at duo.com.

duo.com