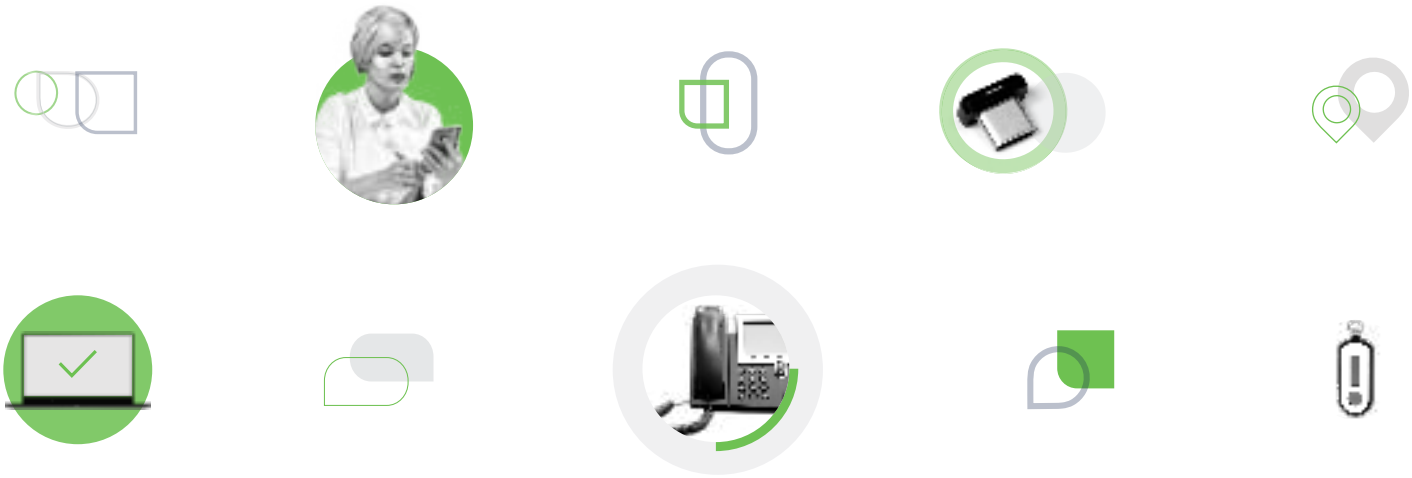


Multi-Factor Authentication Evaluation Guide

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

cisco SECURE

Multi-Factor Authentication
Evaluation Guide

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

cisco SECURE

Over 80% of the breaches categorized under web application attacks can be attributed to stolen credentials, allowing attackers to login rather than break-in.

VERIZON 2022 DATA BREACH INVESTIGATIONS REPORT

Multi-factor authentication is the simplest, most effective way to make sure users really are who they say they are.

It protects your applications and data against unauthorized access due to credential theft by verifying your users' identities before they access your data. Multi-factor authentication works by requiring multiple factors to be confirmed before permitting access versus just an email and a password. Authentication factors can be something you know, like a password; something you have, like your device or a security key; something you are, like your personal fingerprint (biometrics); somewhere you are, like your location; and your level of access based on adaptive policies.

But, not every MFA 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 maintenance. Plus, many traditional solutions are clunky, error-prone and require extensive user training and support – costing your employees time and productivity.

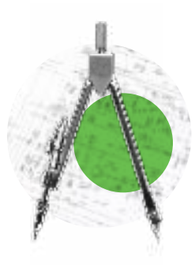
IN THIS GUIDE, YOU'LL GET:

+ A comprehensive set of criteria to customize your evaluation to your organization's needs
+ An overview of the hidden costs of an MFA solution 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

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

Security Impact

Can your solution protect against unauthorized access and provide visibility of 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?



Strategic Business Initiatives

Is your solution compatible with other business initiatives such as enabling remote work or onboarding cloud applications? Does it fulfill 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?

Time to Value

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

Required Resources

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

These are some of the big questions you want to ask to find out if an MFA solution is truly the best solution for your business. Let's dig in deeper into these questions.

Security Impact

The most critical security 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

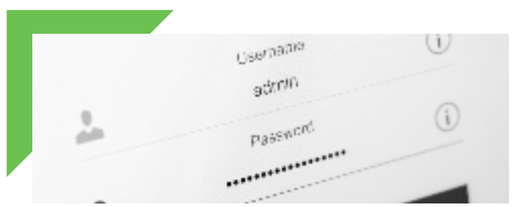
Before you implement a new security solution, take full inventory of your organization's applications, networks and data that can be accessed remotely. If you can log into an application or a system over the internet, you should protect it with more than just a username and password. VPN, SSH and RDP connections are gateways to your corporate networks and therefore require added layers of protection to prevent unauthorized access. Wherever possible, use **FIDO-based** (Fast IDentity Online, an open industry standard for strong authentication) security keys that leverage **WebAuthn** and provide the highest level of assurance for authentication.

With a modern MFA solution built on **zero trust principles**, you can get a clearer picture of the users and devices that are trying to access your network. It is no longer enough just to verify the user before granting access. Consider verifying the device status as part of the authentication workflow. Ensure your solution can integrate with any custom software, VPNs, cloud-based applications and device management tools.

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.

For end users, SSO provides access to multiple applications with a single login (using one master set combination of username and password) – and reducing the number of passwords eliminates bad password habits such as 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.

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

SECURE SENSITIVE DATA

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 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

VERIFY DEVICE STATE

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

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

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.

Examples of adaptive policies and controls include:

+ Require admins and IT staff to perform 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

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.

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

VISIBILITY & ANALYTICS

Ask your provider if your solution gives you 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 devices in your environment, letting you take action to 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.

Ensure your solution comes 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, phone callback, 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 MFA 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.

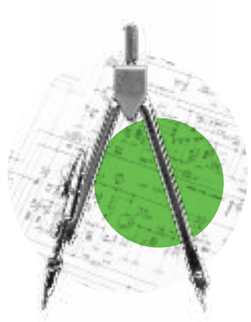
To protect against downtime, your provider's service should be distributed across multiple geographic regions, providers and power grids for seamless failover. Reliable vendors should demonstrate **99.99% uptime**, guaranteed by strong service level agreements (SLA).

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

Ensure your solution comes with detailed logs about your users, devices, administrators and authentication methods.

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

Most of your applications and servers might be on-premises, but some may migrate to the cloud in the near future. 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 of the different types of 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 and control into 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).

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

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 from another location around the world, your security team will know.

Every organization's environment is unique. Check if the solution provider offers advanced machine learning-based behavioural analytics that can create a risk profile for your specific organization and notify administrators of any unusual login activity.

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.

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 (TCO) 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 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 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, and more

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.

Upfront Costs

(continued)

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.

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 solution will typically include these costs in the licensing model.

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 troubleshoot 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 helpdesk 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.

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

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 SaaS and 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.

You should also consider the frequency of updates — 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 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 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 helpdesk staff, including troubleshooting time.

Gartner estimates that password reset inquiries comprise anywhere between 30% to 50% of all helpdesk calls. And according to Forrester, 25% to 40% of all helpdesk 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.

Modern Solutions

High value, upfront costs

+ Simple subscription model
+ Free authentication mobile app
+ No fees to add new apps or devices
+ No data center/server maintenance
+ High availability configuration
+ 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

Traditional Solutions

Potentially 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 and server maintenance
– High availability configuration
– Administrative support
– Patches, maintenance and upgrades
– Helpdesk 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 a 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.

Cloud-based services deploy faster because 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 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 (SSO) 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 amount 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.

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?

The Duo Advantage

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

Security Impact

TRUSTED USERS

Duo's authentication is built on the foundation of **zero trust**. Duo verifies the identity of users and protects against breaches due to phishing and other password attacks with an advanced MFA solution, verifying trust in multiple ways before granting access. Duo's contextual **user access policies** let you create custom controls to further protect access to your applications based on type of users, devices and apps.

Learn more about **Trusted Users**.

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.

Learn more about **Trusted Devices**.

SECURE EVERY APPLICATION

To secure **every type of application**, 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.

Learn more about **Every Application**.

Duo verifies the identity of your users with two-factor authentication, and the security health of their devices before they connect to your applications.

Security Impact

(continued)

START YOUR PASSWORDLESS JOURNEY

Going passwordless means establishing a strong assurance of a user's identity without relying on passwords, allowing them to authenticate using biometrics, security keys or a mobile device. Duo will help you get to a passwordless future starting with reducing the number of logins. With Duo's secure cloud-based **single sign-on** (SSO), 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.

Duo's **passwordless authentication** solution will improve user experience, reduce IT overhead, and strengthen security posture. Duo uniquely takes its **passwordless solution** a step further by enabling organizations to implement a **passwordless authentication** that's secure and usable. Duo ensures that a risky device (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.

Learn more about **Passwordless**.

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.

"We are a very open organization and want employees to work from anywhere. Box manages highly sensitive data for some of the largest organizations in the world. As a result of this, 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

VISIBILITY & ANALYTICS

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.

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's MFA can work. You can use a smartphone, landline (such as your office or home phone), tablet or hardware token. **Authentication methods** include mobile push, biometrics, time-based one-time passcodes, bypass codes, security tokens, SMS passcodes and callback.

Learn about **User Provisioning**.

AVAILABILITY

Duo's Service Level Agreements (SLA) guarantees a **99.99% uptime** and is distributed across multiple geographical locations for a seamless failover. Duo is maintained independently from your systems keeping you safe even if your systems are breached.

Duo gives you insight into the security posture of both corporate and personal devices used to connect to company applications and services.

Strategic Business Initiatives

CLOUD ADOPTION

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 it's easy to scale with your growing users and applications. Duo also supports SAML cloud apps via secure single sign-on, including Google Apps, Amazon Web Services, Box, Salesforce and Microsoft Office 365.

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 **remembered device**. Duo is focused on enabling users to be productive without compromising on security thereby achieving the right balance for your organization.

BRING YOUR OWN DEVICE (BYOD) - REMOTE WORK PROTECTION

The **Duo Mobile app** (iOS, Android) and the **Device Health app** (Windows, MacOS) 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 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. In addition, **Duo Trust Monitor** employs machine learning–behavioral analytics to simplify risk detection in case of anomalous login activity.

VALIDATION AND COMPLIANCE

Duo's full-time security team is experienced in running large-scale systems security, and comprises top mobile, app and network security experts. Duo's operational processes are SOC 2 compliant. Duo's multi-factor authentication cryptographic algorithms are also validated by NIST and FIPS. Duo has achieved ISO (the international security standard) 27001:2013, 27017:2015 & 27018:2019 Certification.

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, while Duo's one-time passcodes meet FIPS 140-2 compliance for government agencies.

Duo **Federal Editions** are built to enable customer compliance with FIPS 140-2 compliant authentication standards and align with National Institute of Standards and Technology (NIST) SP 800-63-3 guidelines. Duo Federal editions meet Authentication Assurance Level 2 (AAL2) with Duo Push or Duo Mobile Passcode for both iOS and Android devices out of the box and by default with no additional configuration required. Duo also supports AAL3 authenticators such as the FIPS Yubikey from Yubico.

Duo **Device Trust** enables organizations to check and enforce the device security and compliance posture prescribed by standards such as PCI-DSS, HIPAA and the NIST cybersecurity framework.

Learn more about **Security & Reliability**

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 (TCO)

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.

NO UPFRONT COSTS

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. Duo offers a simple subscription model priced per user, billed annually, with no extra fees for new devices or applications.

+ 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, with patch management, maintenance and live support at no extra cost
+ Advanced features that let you customize policies and controls, as well as get detailed device health data
+ Conext leveraged from endpoint security agents and device management systems
+ Self remediation to ensure devices meet your security requirements
+ Insight on user login behavior in your environment and the ability to flag anomalous login attempts
+ First steps on the journey to eliminate passwords and improve security with passwordless authentication
+ A secure single sign-on (SSO) and authentication solution in one

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.

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

ADMINISTRATIVE SOFTWARE/HARDWARE

Duo's subscription-based model eliminates hefty software licensing fees and includes administrator management tools, meaning there's no need to pay for top-dollar management software to use it.

AUTHENTICATORS

Users can download the Duo Mobile app to any device, eliminating the need to shell out for a fleet of devices to deploy to your workforce. Duo also offers several authentication methods based on specific use cases; along with Duo Push, Verified Duo Push, end users can authenticate via U2F, biometrics, tokens, passcodes and more.

NO DATA CENTER COSTS

Because Duo is cloud-based, you don't need to buy servers and absorb all of the costs that come with running a data center.

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.

DEPLOYMENT & CONFIGURATION

Duo makes deployment and configuration a snap. Your in-house resources can install, test and troubleshoot Duo in just minutes.

END USER ENROLLMENT

With Duo, end user enrollment is a breeze — end users can simply download the Duo Mobile app for free, enrolling themselves to get started with Duo in seconds.

ADMINISTRATIVE SUPPORT

Duo offers easy deployment with the help of drop-in integrations for all major apps and APIs, and an administrative panel for user and solution management.

PATCHES, MAINTENANCE & UPGRADES

Duo offers automatic application updates, with patch management, maintenance and live support at no extra cost.

ADMINISTRATIVE MAINTENANCE

Duo makes routine tasks like adding new users, revoking credentials or replacing tokens quick and easy, meaning your administrative resources won't have to do another full-time job to maintain your Duo deployment.

SUPPORT & HELPDESK

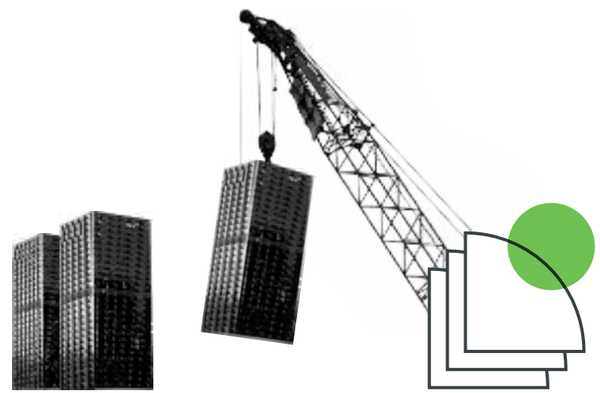
Duo has an extensive library of free resources to answer any and all questions you may have. Duo also offers live support at no extra cost, and with **Duo Care** premium support, you can receive 24/7 white glove service for a small fee.

BUDGET CONSOLIDATION

With Duo, you can replace the need for multiple different hardware and software security solutions that solve for isolated use cases, like authentication, network access control, endpoint security, vulnerability assessment tools, etc. with a single cloud service that provides multi-factor authentication, device trust, single sign-on and adaptive policies and controls.

Duo's trusted access solution provides a comprehensive security platform that eliminates the need — and budget — for many disparate 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. MFA is one step in securing access, and as we've grown and developed, we've built on that to cover more steps.

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. **View Duo's documentation**.

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 **provision new users** with bulk enrollment, self-enrollment, Microsoft Active Directory synchronization, or with the use of **Duo Access Gateway** for cloud-based applications.

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.

Required Resources

APPLICATION SUPPORT

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 into 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.

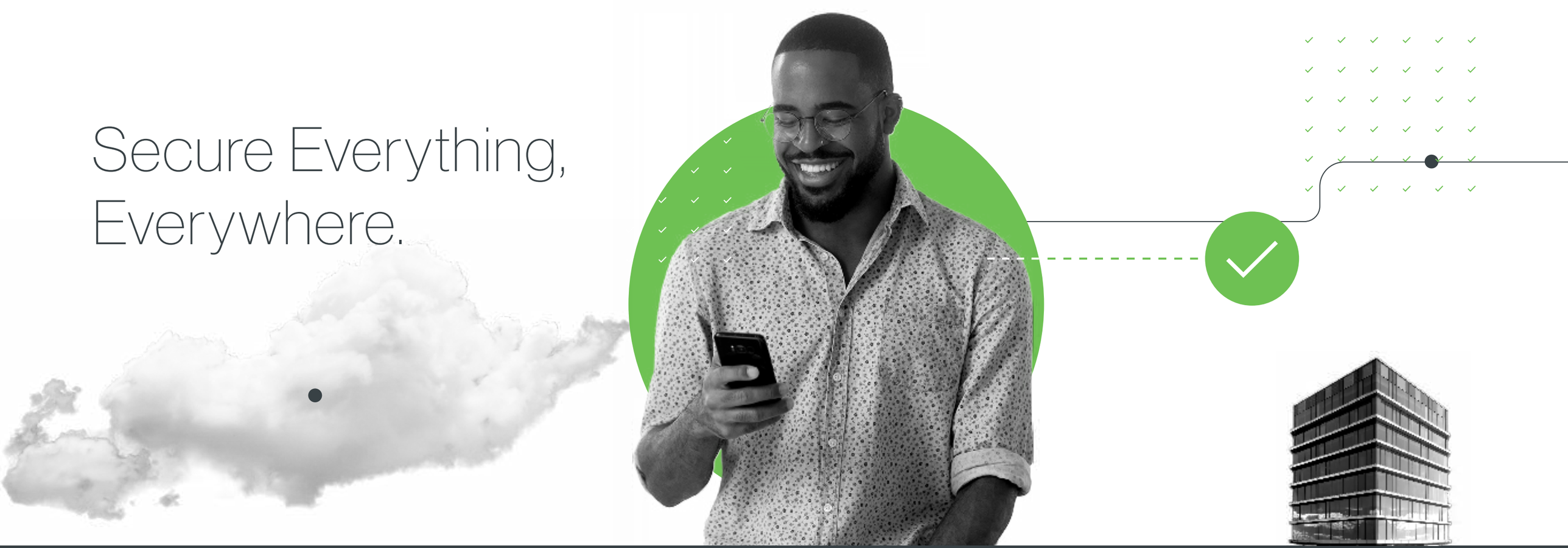
The Duo Customer Success team equips you with everything you need to roll out your Duo deployment, including a customized launch kit to help with security policies, user training, solution architecture design and more.

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

> “Duo increased our security and was an easy tool to deploy; every organization should consider it immediately.”

Chad Spiers
Director of Information Security, Sentara Healthcare

Secure Everything, Everywhere.



At Duo, we combine security expertise with a user-centered philosophy to provide 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.

Duo is built on the promise of doing the right thing for our customers and each other. This promise is as central to our business as the product itself. Our four guiding principles are the heart of the sensibility: Easy, Effective, Trustworthy, Enduring.

Duo Security makes security painless, so you can focus on what's important. Duo's scalable, cloud-based trusted access platform addresses security threats before they become a problem, by verifying the identity of your users and the health of their devices before they connect to the applications you want them to access.

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 MFA.

Duo Security, now part of Cisco, is the leading multi-factor authentication (MFA) and secure access provider. Duo comprises a key pillar of Cisco Secure's Zero Trust offering, the most comprehensive approach to securing access for any user, from any device, to any IT application or environment. Duo is a trusted partner to more than 25,000 customers globally, including Bird, Facebook, Lyft, University of Michigan, Yelp, Zillow and more. Founded in Ann Arbor, Michigan, Duo also has offices in Austin, Texas; San Francisco, California; and London.

Duo.com