Access Management

Buyer's Guide

CISCO DUO

Defending against today's threats requires the right kind of MFA, device trust, ease of use, and more. Learn what it takes to protect everything that matters—and how to choose the access management solution that's right for you.

Table of Contents

© 2023 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Access management in a changing world

That phone in your hand is a vulnerability. So is your laptop, your colleague's home computer, and every other device an employee, customer, or partner may use to access your network, applications, or data.

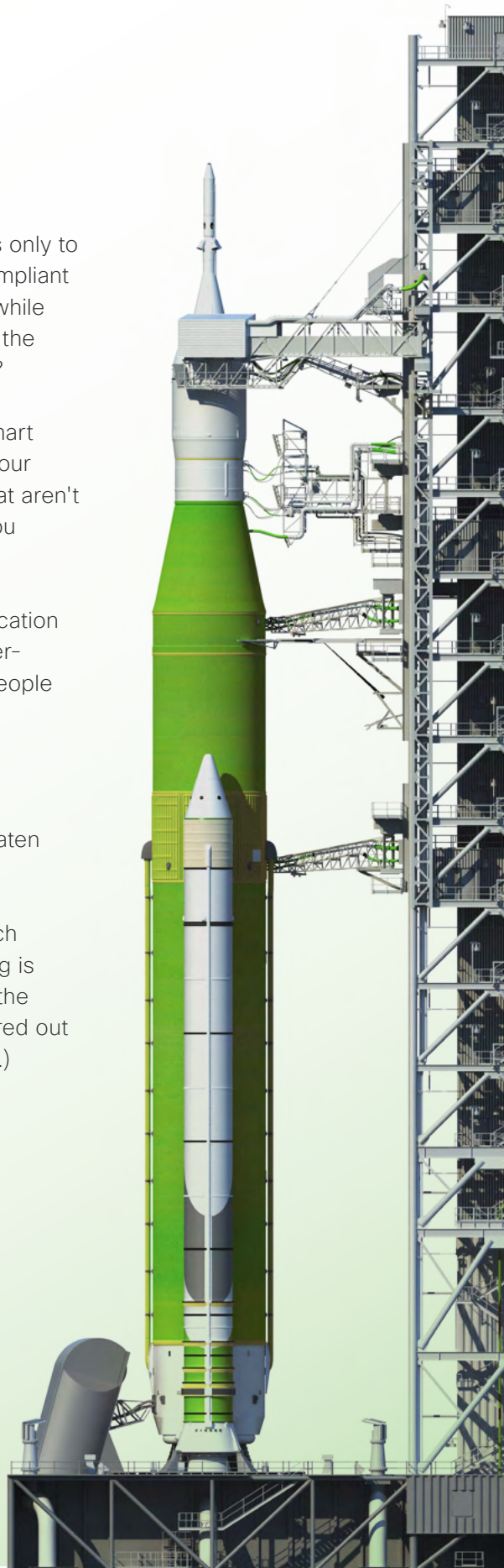
The environment your security team works hard to defend is changing constantly. Employees are no longer bound to desktop systems. They're working from everywhere, at any hour, and on virtually any device.

So too are threat actors who want to gain access to your networks, applications, and data. These attackers are constantly innovating to find weak spots in your existing defenses, such as recent efforts to bypass weaker multifactor authentication (MFA) systems. Anything less than strong security will leave you and your organization unnecessarily open to attacks.

For security and IT teams, the questions this changing environment poses are many.

- How can you extend access only to those endpoints that are compliant with your security policies, while also verifying the identity of the people who are using them?
- How can you ensure that smart phones and other devices your employees use daily—but that aren't managed by IT—won't put you at risk?
- How can you make authentication and security protections user-friendly enough to ensure people will be willing participants in securing your enterprise?
- How can you ensure that strong security doesn't threaten productivity?
- Lastly, how can you tell which access management offering is right for you? (That may be the hardest part, but we've figured out how to make that easier too.)

This eBook aims to answer all those questions.



Today's threats call for strong security

Cyber attacks continue to grow in volume and sophistication. And access has become its own valuable currency for threat actors. Take ransomware attacks, which infiltrate systems or data and hold them hostage until the victim pays money to get its digital property returned. The 2022 Verizon Data Breach Investigations Report (DBIR) finds that ransomware attacks grew more last year than in all five previous years combined.

It only makes sense. If you can lock down your perimeter–if you can control who and what enters your network and all it contains–you'll be in a better position to protect your applications and data.

But network perimeters aren't what they used to be; today, they're built around people, not sites. So access must be adaptive, and managing it must involve more than enforcing strong password policies. You need to protect employees wherever they are, even as their location changes or they switch devices, and as they move from one application to the next. And you need to achieve all this without compromising the user experience or productivity, because security that's difficult to use makes you less safe.

"Ransomware by itself is just a model of monetizing an organization's access."

2022 Verizon Data Breach Investigations Report

MFA bypass attacks prey on weaker solutions

Achieving trusted access has become a bigger challenge than ever, thanks to a new generation of attacks targeting gaps in weaker MFA solutions and counting on busy employees' impatience with difficult-to-use authentication platforms. MFA bypass attacks deploy techniques such as push bombing, in which attackers armed with stolen user credentials (such as a username and password) repeatedly push authentication notifications to the victim's smartphone. These attacks, also called MFA fatigue attacks, can result in users confirming the MFA access request just to end the notification bomb.

Attackers also are buying phishing kits and stealing session cookies (or tokens) that are created on endpoints when legitimate users successfully authorize a device via MFA systems. Token theft is popular because MFA session cookies have become as valuable as passwords among cybercriminals, who use them to bypass less robust MFA platforms.

Governments mandate strong MFA and zero trust, but are organizations equipped?

It's no wonder governments are increasingly requiring strong MFA, including phishing-resistant MFA, as part of a zero trust security model for organizations needing to comply with regulations to do business. The regulations require organizations to have awareness and visibility into the health and security posture of all the devices used to access their critical applications and data.

Access management is the foundation of zero trust

With a zero trust security model, you never assume trust–you always verify it. Here, access management plays a crucial role by enabling essential elements of zero trust:

- **Establish trust** for users and devices requesting access to your applications or network.
- **Enforce trust-based access** so access is granted explicitly, based on the need-to-know principle of least privilege.
- **Continuously verify trust** even after initial access is granted (because change is inevitable).
- **Respond to changes in trust** by denying access, prompting the user to remediate, or by granting additional access once trust has been rebuilt.

Unfortunately, most organizations aren't equipped to address these challenges or fully meet these mandates. According to Cisco's 2023 Cybersecurity Readiness Index report, "There is significant progress to be made to meet the challenge of identity verification." Just one in five organizations have a mature identity verification implementation.

Being unprepared invites significant risks, including:

- Increased risk of compromise and security incidents.
- Greater risk of compromise for weaker MFA implementations.
- Increased liability, including exposure to fines due to non-compliance, costly lawsuits, higher insurance premiums, and even ineligibility for cybersecurity insurance.
- Eroding user productivity from poor adoption of crucial security and authentication measures.
- An inability to properly ensure the safety of hybrid work.
- Onerous IT administration and help desk time and resources required to handle cumbersome access tools and cover special use cases such as authenticating endpoints not managed by IT.

The vital task before security professionals is to implement a mature access solution that provides robust protection against evolving threats, but doesn't threaten productivity, exhaust users, or break the budget. To achieve all that, you need an access management system that's simple, adaptive, and phishing-resistant.

"Just 1 in 5 organizations have a mature identity verification implementation."

2023 Cybersecurity Readiness Index Report

What are your primary THREATS?

A threat is a weapon or tactic that can lead to a potential attack on your network or data.

MFA bypass attacks

Attacks designed to take advantage of gaps in weaker MFA solutions by deploying various techniques, including:

- Push bombing, in which attackers take advantage of MFA fatigue by inundating users with so many push notifications that they finally approve access just to silence the notifications.
- Token theft, in which attackers steal session cookies created when legitimate users authenticate a device.
- Machine-in-the-middle attacks, which use phishing schemes to lure users into clicking a malicious link that leads them to a proxy server designed to intercept traffic between the user and the real server, stealing credentials and tokens in the process.

Malware

Software that infiltrates your environment can exploit vulnerabilities in systems and applications to steal passwords, access data, and take control of systems.

Phishing

Emails, programs or push notifications impersonate legitimate sources to fool users into giving up their credentials, visit malware-infested web pages, or download malicious programs.

Ransomware

A specialized malware attack that takes control of systems or data and demands money to release it.

Where are your biggest RISKS?

A risk is an element in your environment that increases the chances of a successful exploit.

Devices

Mobile phones and other personal devices are often not managed by IT admins. That means you can't be sure their OS or app versions are up to date, or whether they meet your secure trusted access requirements. This leads to potential vulnerabilities—and opens a door for bad actors.

People

Your workforce is your No. 1 asset. They're also the No. 1 target of attackers. Threat actors count on busy employees to adopt careless habits like using recycled or easily guessed passwords, using the same passwords for both personal and work accounts, and storing them unprotected on devices. In fact, most breaches result from stolen credentials or weak passwords.

Hard-to-use security

Security that's difficult to use or administer achieves the opposite of what you want. Complicated access apps that throw up roadblocks for both users and admins can threaten adoption and limit your ROI. Solutions unable to dynamically adjust to changing context leave you vulnerable.

Insufficient security

MFA systems that are bundled free as part of larger security offerings tend to leave dangerous gaps that attackers know how to target. Insufficient MFA fails to cover all users, devices, and applications, lacks the ability to verify endpoints not managed by IT, is difficult to use and administer, burdens help desks, and more.

What to look for in access management solutions

When selecting the right access management solution for your organization, it's important to acknowledge where your risks are—where your organization is exposed to threats—and then determine how an access management solution can help close those gaps. You don't necessarily need to implement a full zero trust environment from day one—that is a journey. Instead, it's wise to establish a foundation built around proven zero trust elements such as phishing-resistant MFA, trusted endpoints, and single sign-on (SSO), and then expand from there. Access management is the perfect starting place.

But the process can be confusing. Different solution providers make similar-sounding claims about what their products do, even though what they offer is often not comparable to competing solutions. Some bundle access management with unrelated products in packages that simply don't prioritize security, leaving customers with solutions that leave them at risk.

As too many organizations are learning firsthand, today's threats can't be neutralized by "check the box" access management solutions that provide substandard protection. Fortunately, there's no reason to compromise.

Robust and adaptive access management solutions are available today. The best will meet three core requirements—the three pillars of modern access management: security, productivity, and value.

Security

It's simple: Strong security is now a must. Attackers are finding ways around defenses that once stopped them cold. It makes no sense to invest time and resources in solutions designed to protect you against last year's threats.

To find an access management solution capable of delivering strong security, look for:

- **Strong authentication with phishing-resistant MFA options.** You'll want a solution that's designed specifically to foil attackers no matter how they come at you, including and especially attempts to bypass your MFA processes. Your access management solution should be able to detect and respond to MFA bypass attacks in real time. Anything less leaves you at risk.
- **Adaptive, risk-based authentication.** Adaptive, risk-based authentication allows you to respond instantly to changing context, such as location, device role, and other factors. You should be able to customize your security policies, defining which roles can gain access to which applications or data. And you should be able to deploy risk-based methods like identifying anomalous access that could indicate an unauthorized attempt; when this happens, your solution should allow you to adjust authentication requirements to require additional verification.
- **Endpoint trust.** Access management involves more than just verifying identities. You need visibility into every device that attempts to access your applications—even if that device is not managed by IT—and enforce access control based on your own policies. Look for solutions that can assess mobile devices, computer systems, and other endpoints in real time by answering crucial questions. *Is the device's software up to date? Does it meet your compliance goals and device access policies? Is the device logging in from a location you've restricted?* Some solutions even provide dynamic updates, which takes the heavy lifting out of keeping devices trustworthy.
- **Early detection of potential attacks.** Keeping a step ahead of attackers is a priceless advantage for security teams. Look for solutions capable of alerting you to attacks as they are emerging—not after they've happened.

Productivity

Complex security makes your organization less productive while also making it less safe. When security systems are hard to use and administer, people come up with workarounds and administrators get overwhelmed by cumbersome configurations and help desk requests from frustrated users.

“182 Days

Is what overly complex security costs large U.S. organizations in productivity every year.”

– IS Decisions

Among users, access management solutions are often the point of the spear for corporate security. This puts a premium on features that won't hinder productivity, and an even greater value on those that actually help improve it. The good news is that there's no longer any reason to sacrifice productivity for security (or vice versa)—so long as you choose an access management solution that offers:

- **Seamless, consistent user experience.** Ease of use is everything, as it drives adoption which in turn lowers your risk profile. It's important for users to have the same experience across all platforms and applications. Don't settle for anything less, because you'll feel the productivity impact down the line.

- **Single sign-on (SSO).** The average organization manages 300 applications. That's a lot of logging in. Single sign-on enables users to authenticate their identity once, and then access all the applications they need to work without having to log in again. SSO complements MFA by pairing added security with seamless convenience.

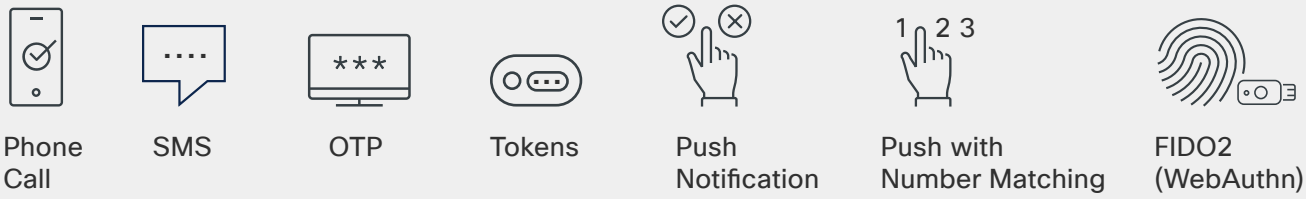
- **Self-service remediation.** When device or user authentication fails, many MFA solutions present users with confusing, even meaningless error messages that urge them to contact their IT administrator. Seek solutions that tell users why they're blocked and how they can fix it. This allows them to get back to work sooner and reduces changes of MFA fatigue.

- **Comprehensive coverage.** With hybrid work here to stay and IT infrastructures in a constant state of flux, comprehensive coverage is essential to meet your organization's evolving need to manage access. Prioritize solutions that offer support for all types of applications (cloud, on-premises, and private and public apps), endpoints (corporate-owned, BYOD, Windows, MacOS, iOS, and Android), and users (employees, contractors, third parties, remote or on-premises).

Remember: Limitations impede productivity.

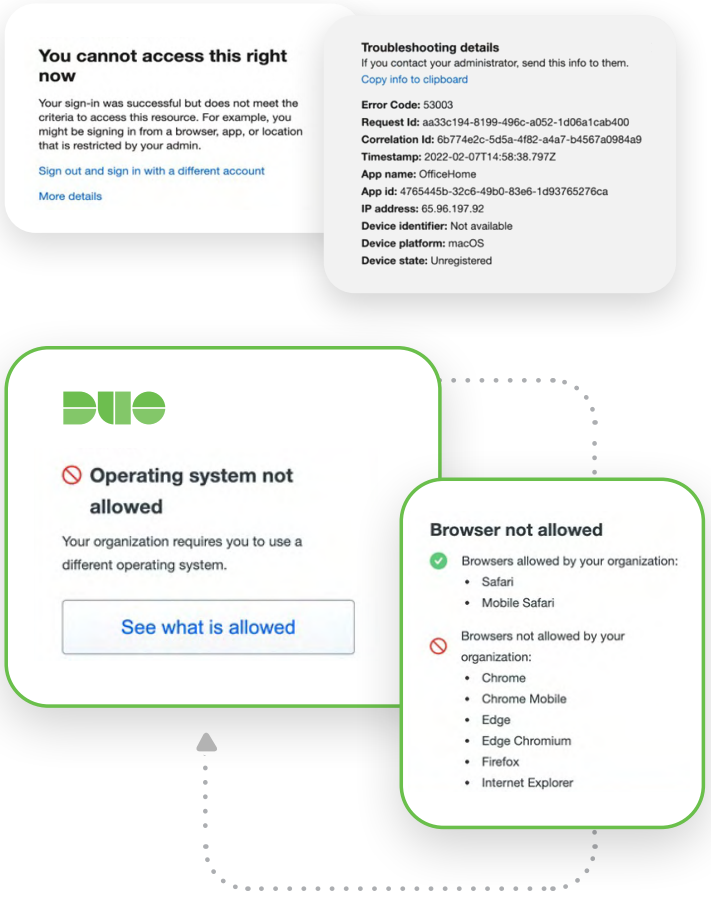
Support for an array of authentication factors. To help all users get to work as quickly as possible, a robust authentication environment will support a broad range of authentication factors, from phone calls (necessary for some populations), text messages, and push notifications all the way to strong FIDO2 authentication. Be sure your solution supports passwordless authentication, including biometric factors like fingerprint and facial recognition, for even greater security and efficiency.

Authentication factors can vary widely



What does self-service look like? Less friction and easy answers.

If you think "self-service security" sounds like extra work for users, it actually means the opposite. Take the example of blocked access. An employee tries to sign into an application and is denied. Some device trust solutions simply tell the user they can't access the app and supply an error code that's meaningless and frustrating to users. Their next step? Either sign in with different account or contact IT. With a solution designed for self-service, like the app pictured on the right, users find out why they're not allowed access, and what changes they can make to gain access. Self-service security saves time and avoids headaches for users—and saves on support costs.



Value

Determining value is perhaps the hardest piece of this puzzle. Access management solutions can differ in pricing and features, and so-called "free" bundles can muddy the waters further. But it helps to approach this pillar by acknowledging both upfront costs, such as per-seat subscription costs, as well as add-on fees that, if not properly vetted, can add up fast.

To assess the value of any access management solution, consider what it costs (in dollars, time, and resources) to not only deploy the system but also to administer it and evolve it as your needs change. Look for solutions that offer:

- **Fast, easy implementation.** Some access management solutions can take six months or longer to deploy. And many require paid consultants to configure and even maintain the solution. Waiting, however, is a poor security strategy. Look for solutions that can be deployed in days, even hours—and with minimal burden on IT. Insist on out-of-box integrations for major applications and APIs that make it easy to integrate with custom applications. The solution you want will provide value up front, will work with both modern and legacy systems, and will work across multiple siloed apps. Keep in mind that proprietary solutions can be inherently expensive because they limit your options, not just for security tools but for enterprise software in general.

- **Simple administration.** Be sure your solution is flexible enough to configure policies at various granular levels to accommodate a range of use cases and user roles. In addition, seek solutions that can generate comprehensive reports so you'll always know where your access management progress stands.

- **Accessible pricing.** Some providers charge premium prices for essential access management features like SSO, passwordless, and trusted endpoint support. These providers may market their solutions as affordable—especially if they're bundled at no extra charge with other offerings—but add-on costs can quickly mount, especially as you equip yourself to defend against MFA bypass attacks and other emerging threats.

- **Reliable service and global support.** This seems like a no-brainer, but we all know what it's like when vendors don't deliver it. Be sure your provider has a meaningful, fully supported presence everywhere you do business. And ask hard questions about the extent of real-world technical and customer success support—and what you're really getting for your money.

- **Comprehensive compliance.** Another key factor is ensuring that your new solution will help you meet major regulations (including NIST, FIPS, and EPCS) and accessibility guidelines (such as WCAG, HIPAA, SOX, PCI, GDPR, and GLBA). Make sure your access management solution makes compliance easier, not harder.

- **Measurable impact on security.** It's one thing to check a compliance box. But if you're going to go through the effort of implementing an access management solution, make it count. Look for solutions that demonstrably reduce the risk of unauthorized access. Does it give you visibility to all users and devices in your environment? Does it allow you to apply access policies to both managed and unmanaged devices? Will it let you block access by geographic region? Will you be alerted to suspicious login activity? Can you track success metrics?

10 metrics for measuring success

How do you know your access management protections are working? These metrics would be a good starting point. Make sure your solution lets you track them.

Lower is better

Password reset requests. When helpdesk staff find they spend a lot of time fielding these calls, it could be a sign that your password management system is poorly designed or even malfunctioning. Lowering these requests should be a goal.

Access creep. The policy of least privilege aims to grant users access to only what they absolutely need to do their jobs—and nothing more. But a rise in the number of users with access to sensitive data potentially signals sloppy policy management. Careful monitoring of accounts, especially as employees leave or change roles, can keep this metric manageable.

Time to provision user accounts. The sooner accounts are provisioned, the faster employees can get to work. This is a vital metric for measuring the effectiveness of your access management program and can flag potential areas of improvement.

Offboarding flaws. Departed employees who still retain access to systems represent a security risk. Tracking and closing those accounts is crucial. It's another metric you'll want to see reduced over time. (The same goes for inactive or orphan accounts, which can belong to active employees but aren't in use: they're a vulnerability.)

Stepped-up security incidents. Risk-based authentication gives you an added layer of defense. Understanding how often it's deployed and in what circumstances (by region, user role, endpoint type, etc.) provides insights that tell you more about how your access management solution is protecting you.

MFA bypass incidents. Tracking attempts to bypass your MFA system, and the details around those attempts, will help you understand how threat actors are targeting your networks and applications—and can provide insights to help you shore up your defenses with user training, risk-based authentication, and more.

Higher is better

Authentication factor types. The number of authentication factor types you support (such as passcodes, tokens, and biometric authenticators)—and their use—can be indications of your environment's maturity. Among Duo customers, app-based Duo Push authentication is the most used method.

Growth indicators. Several metrics can help you gain insight into your organization's relative growth. New accounts provisioned usually tracks the number of people who join your ranks, while expansion rates (of data, apps, locations, or users) can provide monthly snapshots into growth within various parts of the business. So long as your organization can manage that expansion, increases in these metrics can be viewed as a positive.

Admin time. Freeing up time spent administering access management (thanks to fewer help desk calls and streamlined configuration and management) leaves more time for other tasks and drives down TCO.

User satisfaction. Understanding how user sentiment changes over time can give you a sense of how well your access management program is working—and where to course correct if necessary.

Stronger **Security**

Increased **Productivity**

Unmatched **Value**

Most IT environments are complex, and they will only get more so. Organizations rely on hundreds of applications and cloud services, which host their most valuable information. To protect these multi-environment systems, you can only allow access to those users and devices who are known to be trusted. And you always must remain a step ahead of threat actors who aim to outmaneuver the very protections you've put in place to stop them.

That's where Cisco Duo comes in. Duo provides strong security with multi-layered defenses and advanced capabilities that thwart sophisticated malicious access attempts—and all in a way that frustrates attackers, not users.

If it's connected, it's protected.

When attackers attempt to bypass MFA authentication, Duo doesn't give them a way in.

Duo protects against malicious attacks, including and especially push-phishing attacks, with multi-layered defenses that detect and block suspicious login attempts in real time.

In fact, Duo provides strong protections like device verification as a standard feature across all of its paid editions. (Duo even enables organizations to verify or block devices that aren't managed by IT.)

All Duo paid editions include strong MFA with push phishing-resistant options, single sign-on (SSO), passwordless authentication, and trusted endpoint protection.

Duo is a core part of Cisco's assurance that "if it's connected, it's protected." Duo delivers peace of mind through strong security, increased productivity, and unmatched value. This makes Duo the smart access management choice for every organization, regardless of their size, IT infrastructure, or security expertise. Quick to set up and easy to use, Duo provides trusted access while driving down support costs and ramping up user productivity.

Only Duo delivers access management that is this user friendly, this secure, and this cost-effective. It achieves this by helping you:

- **Reduce your risk of breaches** with strong user authentication and device verification combined with dynamic risk-based access policies to prevent sophisticated identity-based attacks.
- **Easily prove compliance** with regulatory requirements and data privacy standards using Duo's robust policy engine and comprehensive reporting for IT audits.
- **Improve workforce productivity** by frustrating only attackers, not users. Minimizing user friction delivers a delightful user experience and ensures adoption of security best practices.
- **Safely enable hybrid work** by allowing users to be productive from any location—without compromising security—using SSO, passwordless, risk-based authentication and device verification.
- **Reduce administrative burden and IT costs** with Duo's self-service, ease of use and broad coverage of use cases that results in fewer help desk tickets, less time spent administering or supporting existing solutions, and simplified yet stronger access management.
- **Maintain operations with world-class support,** which Duo delivers to more than 40,000 customers in over 100 countries. That global reach and scale allows Duo to process 1.3 billion authentications a month and analyze the health telemetry of 26 million endpoints. More than nine out of 10 customers recommend Duo.

Solution Comparison Worksheet

Use the chart below to make your own comparisons between Cisco Duo and other solutions.

Security	DUO	Option 1	Option 2
Prevent unauthorized access with strong and adaptive MFA, including phishing-resistant FIDO2 (WebAuthn) options	✓		
Strengthen authentication in real-time when signal risk rises	✓		
Rich, broad range of active security threat signals	✓		
Extend access policies to personal & 3rd-party devices	✓		
Identify anomalous/risky authentications	✓		
Establish device trust through security posture assessment	✓		
Defend against push-phishing and MFA targeted attacks	✓		
Get granular visibility into users & devices	✓		
Protect macOS & Windows devices with offline MFA	✓		
Machine Learning-based detection of potential attacks in progress	✓		
Protect legacy & homegrown applications	✓		
Ability to identify and block/allow devices without an MDM	✓		
Productivity	DUO	Option 1	Option 2
Easily deploy secure access policies to all users & devices	✓		
Enable VPN-less secure remote access for private & other on-premises services	✓		
Simplify user experience & device management	✓		
Notify users when and how to self-remediate their devices to limit helpdesk burden	✓		
Accelerate risk assessment & login experience	✓		
Easy to configure advanced policies	✓		
Simple and accurate troubleshooting & reporting	✓		
Value	DUO	Option 1	Option 2
Unlimited application integrations	✓		
Features and reporting that support compliance & insurance requirements	✓		
Reduce helpdesk call volume for login issues, password resets and device updates	✓		
IT can rapidly deploy & easily manage secure access policies	✓		
Support hybrid work, partners, and contractors	✓		
Straightforward and simple license costs	✓		
Protect access for entire workforce more efficiently	✓		
Integrate with existing security & identity solutions	✓		
Quickly protect new mergers and acquisitions within their existing IT environments	✓		

© 2023 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

Learn More

Learn how Duo's access management solutions can help you protect your environment–and achieve peace of mind through strong security, increased productivity, and unbeatable value.

Resources

The Latest Cisco Trusted Access Report

The Multi-Factor Authentication Evaluation Guide

The Life and Death of Passwords

Visit Duo.com to learn more and start a free 30-day trial.

Start a Free Trial

Duo Security, now part of Cisco, is the leading multi-factor authentication (MFA) and secure access provider. Duo is a trusted partner to more than 40,000 customers globally.

Try it for free at duo.com.

cisco SECURE

Cisco Secure delivers a streamlined, customer-centric approach to security that ensures it's easy to deploy, manage, and use. We help 100 percent of the Fortune 100 companies secure work – wherever it happens – with the broadest, most integrated platform.

Learn more at cisco.com/go/secure.

© 2023 Cisco Systems, Inc. and/or its affiliates. All rights reserved.