Zero Trust for the Workforce

Ensure only the right users and secure devices can access applications.

Duo offers zero-trust security for the workforce – users and the devices they use to access work applications. A zero-trust approach for the workforce is the foundation for a zero-trust security model that ensures users and devices are trusted before granting them access.

Duo enables secure access to applications from anywhere. It gives organizations the ability to evaluate and make access decisions based on specific risk-based context, including:

Is their device secure and trusted?

Is the user who they say they are?

Do they have access to the right apps?

Zero trust for the workforce is a component of the Cisco Zero Trust framework; a three-pronged zero-trust platform that comprises the **workforce**, **workloads** and **workplaces**.

Duo Security is now part of Cisco.

Establish User Trust

Verify the identity of your users with strong multi-factor authentication (MFA) that provides flexible, broad coverage for every type of user.

- Eliminate the threat of attacks that stem from compromised credentials with Duo's easy and effective MFA
- Simplify enrollment and secure logins for users and reduce friction to their workflow – users verify their identity with a quick tap on a Duo Push notification sent to their smartphone via the Duo Mobile app
- Support group-specific access policies for all user groups, including employees, contractors, vendors, customers, partners, etc.
- Support every user login scenario with different MFA methods (mobile apps, push notifications, offline options, biometric-based WebAuthn, security keys and more)
- Scale user provisioning with automated sign-up options such as user self-enrollment and Active Directory sync
- Reduce help desk tickets and management with a self-service portal that lets users quickly and easily manage their own authentication devices

Gain Visibility Into User Devices

Get a detailed overview of your users' devices with Duo's endpoint visibility and a single view of overall security status with Duo's Admin Panel that flags risky devices.

- Get complete visibility into mobile, laptop, desktop and PC devices across every platform (Windows, Mac, iOS, Android and Chrome)
- Identify and monitor corporate and personally-owned devices and get insight into their security posture with Duo's Trusted Endpoints
- Gain greater insight and control over BYOD with Duo's platform that detects and tracks every device accessing protected applications, including desktop, laptop and mobile – without using an agent
- Use existing device management infrastructure to establish and enforce device trust with Duo's integrations with Active Directory, AirWatch, Google, Jamf, Landesk, MobileIron and Sophos and without the need to deploy and manage a complex PKI certificate infrastructure
- Easily manage users, devices and policies globally, as well as security reports and logs for compliance audits from one centralized, intuitive interface
- Get detailed data and reports on user behavior and risky devices; and user, admin and telephony data – all easily integratable with existing security information and event management (SIEM) systems

Establish Device Trust

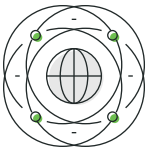
Gain visibility into user and device risks and apply controls that prevent threats and risky devices from gaining access to sensitive applications and data.

- Support BYOD policies by marking endpoints as trusted or untrusted, while enforcing policies that require stronger security or limit access by untrusted devices
- Verify managed Android and iOS devices with the Duo Mobile app on your users' phones
- Close security gaps faster, ease the burden on your helpdesk and reduce support tickets with Duo's Self-Remediation, which notifies users to update out-of-date devices; informs them they'll be denied access in a certain number of days if they don't update; and provides a direct link to update their software
- Block devices from accessing your applications based on:
  - OS, browser and plugin versions and how long they've been out of date
  - Status of enabled security features (configured or disabled):
    - Full disk encryption
    - Mobile device biometrics (Face ID/Touch ID)
    - Screen lock
    - Tampered (jailbroken, rooted or failed Google's SafetyNet)

Enforce Adaptive Policies

Limit access by risky endpoints and users to applications based on conditional risk (adaptive authentication).

- Set role-based access controls and restrict access to applications based on users' roles and job responsibilities
- Enforce the use of more secure MFA methods (Duo Push, U2F, etc.) for access to high-risk applications and services (like those with financial, health, HR or other sensitive data) for a higher level of assurance of your users' identities
- Require users to authenticate for every new session, prompting users after a set amount of time
- Set location-based policies to grant or deny access to your applications based on where the user/device is coming from (a set of IP address ranges); and require MFA for certain locations
- Block authentication attempts to your applications from anonymous networks like Tor and proxies



Enable Secure Access to All Apps

Use out-of-the-box integrations to easily set up all types of apps – from legacy to modern to custom tools – with Duo's broad coverage across every application.

- Extend protection to custom applications and proprietary services with APIs, WebSDKs and support for other protocols to extend Duo's security platform to protect proprietary services
- Apply a zero-trust security approach for remote access to cloud infrastructure and corporate applications with flexible, frictionless access to hybrid and multi-cloud environments
- Secure against compromised credentials and protect access to your remote access gateway providers with Duo's integrations for virtual private networks (VPNs), virtual desktop infrastructure (VDI) and proxies such as Cisco AnyConnect, Juniper, F5, Citrix and more
- Protect hybrid and multi-cloud environments, cloud infrastructure providers and on-premises and cloud applications with Duo's consistent remote access
- Support cloud access use cases, such as developers accessing Amazon Web Services (AWS) and contractors who need remote access to internal applications
- Give users a consistent login experience, reduce password fatigue and increase user productivity by enabling them to log in just once to access all of their apps with Duo's single sign-on (SSO), which also checks device security every time before granting access to each app
- Easily integrate with other SSO provides like Ping, Azure, Okta, Oracle and Shibboleth; providing identity integration with AD and SAML with Duo's MFA
- Protect your existing IT investments and reduce complexity with Duo's technology and security partnership ecosystem, which includes partners (Microsoft, Cisco, Workday, Citrix, VMware and many others) that provide identity and access management; network and remote access; endpoint management and security; detection and response; and popular business applications

"Duo is the partner we rely on in our journey towards a zero-trust model."

Andrew Spenceley
Cyber Security Architect, University of Sunderland

"Duo Beyond has enabled us to push our zero-trust strategy faster."

Mike Johnson
CISO, Lyft

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

Duo Security

Duo is a cloud-based security platform that protects access to all applications, for any user and device, from anywhere. It's designed to be both easy to use and deploy, while providing complete endpoint visibility and control.

Duo verifies users' identities with strong multi-factor authentication. Paired with deep insights into your users' devices, Duo gives you the policies and control you need to limit access based on endpoint or user risk. Users get a consistent login experience with Duo's single sign-on that delivers centralized access to both on-premises and cloud applications.

With Duo, you can protect against compromised credentials and risky devices, as well as unwanted access to your applications and data. This combination of user and device trust builds a strong foundation for a zero-trust security model.