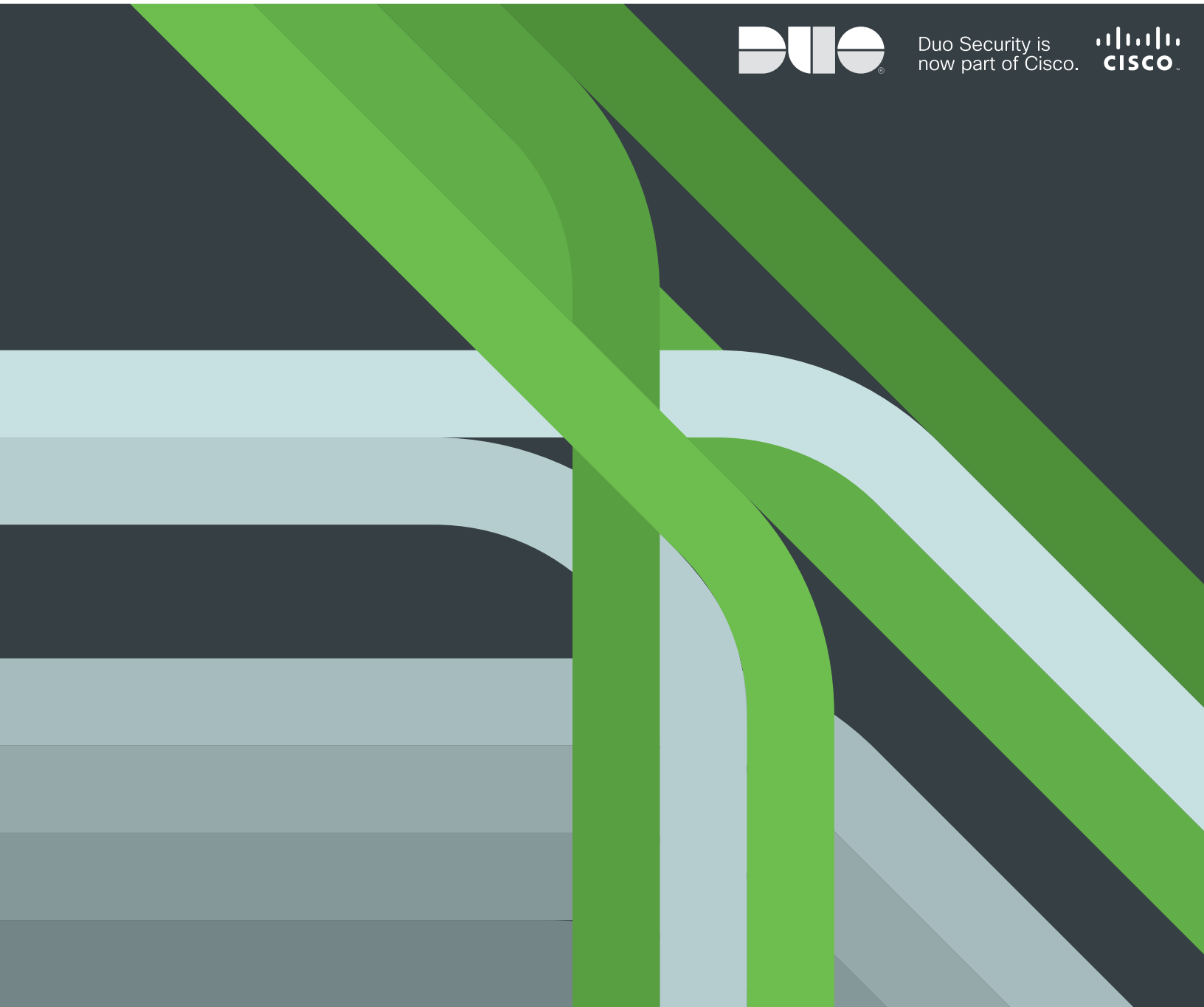
Infinit Technology Solutions

Cisco Partner

Zero Trust Evaluation Guide

For the Workforce



The Different Zero-Trust Models

The concept of zero trust can be seen in **Gartner's CARTA** model – continuous adaptive risk and trust assessment. This calls for a shift away from one-time, binary access decisions and toward contextual, risk and trust-based decisions. This model is about giving just enough trust to users, even after authentication, to complete the action requested.

Forrester's Zero Trust eXtended (ZTX) refers to breaking down "monolithic perimeters" into a series of micro-perimeters or network segments to apply granular security controls around them. But they also acknowledge that it's much more than just network segmentation – it's a holistic approach to securing data, network, device, workloads and workforces.

Google's BeyondCorp is their implementation of a zero-trust architecture that requires securely identifying the user and device, removing trust from the network, externalizing apps and workflow, and implementing inventory-based access control.

Introduction User Trust Device Visibility Device Trust Adaptive Policies Access to All Apps Duo's Zero Trust

All of these models require more controls around identity as the new perimeter – users and their devices as they access applications and services. There are many different components of a zero-trust model that require securing different workflows:

Workforce

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

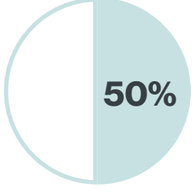
Workload

Secure all connections within your apps, across multi-cloud.

Workplace

Secure all user and device connections across your network, including IoT.

One approach is to start by ensuring only the right users and secure user devices are accessing applications; your workforce – the foundation of a zero-trust model. This guide is focused on evaluating the criteria required to adopt a trust-centric security approach for the workforce.



Gartner predicts security as a service will represent at least 50 percent of security software delivery by 2020.

01.

Establish User Trust

The first step toward architecting zero trust for your workforce is verifying your users' identities when they log into your cloud and on-premises work applications, services and platforms.

Can you trust your users are who they say they are? And how do you reduce the threat of compromised credentials and devices caused by phishing, malware and other vectors – while also meeting data regulatory compliance requirements for access security?

Multi-Factor Authentication

Verify your users' identities with a scalable, frictionless multi-factor authentication (MFA) solution.

Support Every User

Does your MFA solution provide flexible authentication options to fit a broad range of users, security profiles and technical backgrounds? Make sure your solution supports employees, frequent travelers, contractors, vendors, customers, partners, etc.

You should be able to customize and enforce which MFA methods can be used. For more secure access to high-risk applications, require the use of:

- Easy-to-use, out-of-band mobile push notifications
- Phishing-proof **Universal 2nd Factor (U2F)** security keys
- Biometric-based **WebAuthn**

Ease of Administration

Is your MFA solution easy for administrators to deploy? Choose a cloud-based solution that requires minimal infrastructure and staff to roll out to reduce the burden on your team.

Does it provide user enrollment and provisioning options to scale as your organization grows? For example:

- Auto-enrollment
- Administrative APIs for scalable user provisioning
- Option to synchronize users from existing directories, such as Active Directory and Azure AD

Save on training, support and ongoing help desk tickets with user self-enrollment and self-service – let your users enroll in MFA and manage their own authentication devices without administrative assistance.

> Reduce risk with a flexible, easy-to-use and easy to deploy multi-factor authentication solution.

Support BYOD & Mobile

The extended perimeter presents new challenges around securing BYOD (bring your own device). A zero-trust model should both work well with your existing infrastructure without causing friction, and support any type of device.

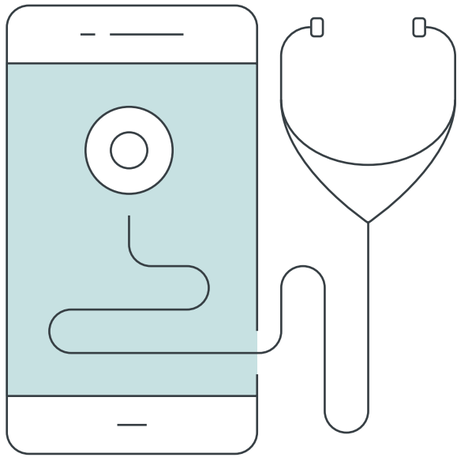
You should be able to get insight into personal and corporate-owned devices, including mobile devices. BYO devices may not meet security requirements or may be running older software versions prone to vulnerabilities.

A comprehensive device visibility solution should let you identify mobile devices with certain security features enabled or disabled, as well as their security posture:

Device Logs & Reports

Many compliance regulations and auditors require user activity and device security logs and reports. Can your device visibility solution give you access to detailed reports on user behavior and risky devices – all in one dashboard? Does it integrate nicely with any existing SIEM (security information and event management) software?

Make sure your admins have easily accessible and exportable reports for auditors, with insight into authentications, users, admins, policies and more.



OPERATING SYSTEM
iOS or Android version

DISK ENCRYPTION

SCREEN LOCK

BIOMETRICS
Fingerprint, Touch or Face ID

DEVICE STATUS
Jailbroken, rooted or tampered with

03.

Establish Device Trust

At login, check the security health of all user devices attempting to access your applications. Establishing trust extends beyond managing the status of the device to include inspecting and controlling access based on mobile and personally-owned devices.

Can you enforce endpoint controls for risky devices or corporate-owned devices? How are you establishing mobile device trust? Are you able to automatically notify users of out-of-date software to reduce your help desk tickets?

Introduction User Trust Device Visibility Device Trust Adaptive Policies Access to All Apps Duo's Zero Trust

Enforce Endpoint Controls

By leveraging the visibility of devices connecting to your applications (as discussed previously), you should be able to establish device-based access policies to prevent any risky or untrusted devices from accessing your applications.

Risk-Based Device Access

For access to high-risk applications, you may require a device to be corporate-owned or managed by your organization's IT team. High-risk applications may include electronic health record (EHR) systems like Epic that contain patient health information; cloud infrastructure like Microsoft Azure and Google Cloud Platform; and many others.

Can you enforce access policies based on the application risk or whether the device is corporate or personally-owned? And can you do this without requiring endpoint certificates?

Additionally, you may require MFA for access to more sensitive applications for a higher level of assurance of your users' identities. Can you require your users to use push notifications, U2F security keys, or biometric-based WebAuthn before granting them access to certain applications?

Establish Mobile Device Trust

Make sure your solution allows you to establish mobile device trust with or without the use of mobile device management (MDM) software.

Users may object to installing MDMs on their personal devices due to privacy concerns, resulting in lower overall adoption and reduced insight into their device security. And sometimes it's outside of your IT team's control to install an agent on the personal devices of third-party providers that may need access to your applications.

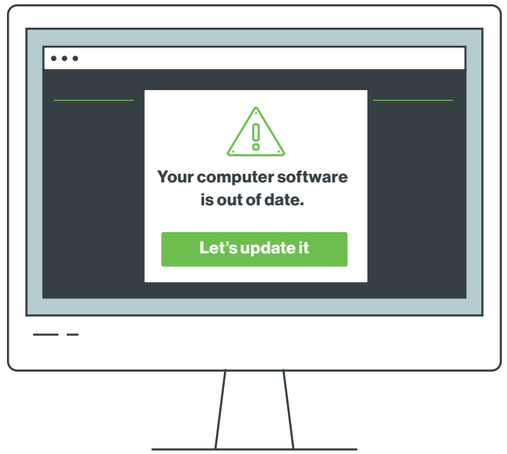
Whether or not you have an MDM solution, you should be able to block devices from accessing your applications based on:

+ 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)

Notify Users to Update Risky Devices

Does your solution enable your users to manage their own devices? Choose a solution that can detect older software versions, then notify users when their device software is out of date.

To relieve the burden on your help desk support team, prompt users to update the software on their own devices at login. A self-service portal also allows them to easily manage their own authentication devices without submitting a help desk ticket.



> Enforce controls and policies to keep risky endpoints from accessing your applications.

04.

Enforce Adaptive Policies

Enforce contextual access policies allowing access to your applications with user, device and location-based controls. The context includes different aspects of their login attempt – where they're located, what role they have in your organization, what type of device they're using, etc.

Limit access to only what your users need to do their jobs and add stricter controls for access to more sensitive applications – without negatively impacting user workflows. Can you customize policies based on users, user groups or user location? Or challenge users with a more secure MFA method, based on what application they're accessing?

Contextual Access Policies

Customize policies to allow, deny or require stricter security based on user-specific roles and responsibilities, devices and applications – all while balancing security with usability.

Role-Based Access Policies

Not all users need access to every application – can you customize access based on the type of user group? Give contractors or third-party providers temporary and restricted access to non-sensitive applications or systems.

You should be able to enforce policies to grant a higher level of access to admins and privileged users, while ensuring only developers have access to your production environments and cloud infrastructure.

Check that your admins can:

+ Customize policies based on the user, group, or their specific roles and responsibilities
+ Set custom policies based on authentication method
+ Only allow users to authenticate using certain methods
+ Easily use Active Directory or Azure AD user groups to apply policy

App-Specific Policies

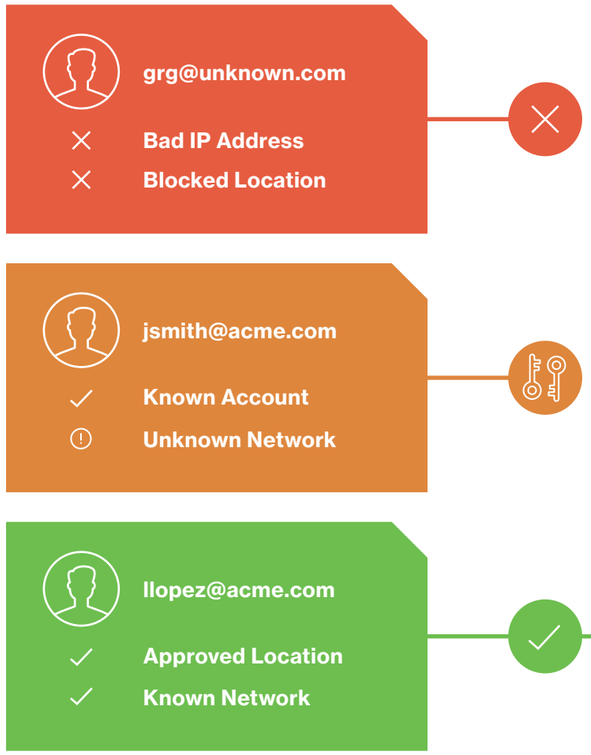
Enforce the use of more secure MFA methods for access to business-critical applications and services to reduce the risk of unauthorized access.

Your admins should be able to configure app-specific policies to require only the use of push-based or U2F security keys to verify your users' identities before granting access to these applications. The required use of only more secure methods provides a higher level of assurance of user identity; strengthening access control to your more sensitive applications and data.

User Location

Prevent unauthorized access from any geographic location with user-based access policies. If you don't do business in certain countries, you should be able to block access attempts originating from those regions.

Admins should also be able to block authentication attempts based on a set of IP address ranges or those coming from anonymous networks like Tor or proxies. However, non-blocked IP addresses do not imply that access is allowed – this is only one attribute to consider in the broader context of an access request.



> "Shift from 'good' versus 'bad' macro decisions, toward a context-based set of smaller decisions. Give just enough trust to entities like users – even once they've been authenticated – to complete the action being requested."
>
> **—Gartner's Continuous Adaptive Risk & Trust Assessment (CARTA)**

05.

Enable Secure Access to All Apps

Give users secure and consistent access to all applications, services and platforms, no matter where they're hosted.

Introduction User Trust Device Visibility Device Trust Adaptive Policies Access to All Apps Duo's Zero Trust

Protect Your Investments

You may be a cloud-forward organization, or a large enterprise with a complex mix of both cloud and legacy on-premises infrastructure and applications. Whatever it is, make sure you can protect access to all of it with MFA, contextual access policies, and device visibility and controls.

Remote Access

The shift to cloud infrastructure has made it challenging for organizations to apply stronger access controls across hybrid and multi-cloud environments.

Your solution should simplify and keep the user login experience consistent, no matter where users are located, when they're connecting to various systems and applications hosted in different cloud environments.

Make sure you can secure access to:

- Multi-cloud environments, such as Azure, AWS and Google Cloud Platform
- Infrastructure, dev/DevOps environments and internal Linux servers
- HTTPS web applications and SSH servers
- Virtual private network (VPN) and remote access applications

Enforce stronger security controls to only allow managed, up-to-date devices access to infrastructure and developer environments.

Cloud/Identity Access

Secure access to all of your cloud apps such as Office 365, Google, Box, Dropbox, Slack, and more, as well as access to any existing single sign-on (SSO), identity providers and federation services. Make sure your solution provides secure access to any SAML 2.0-enabled cloud application.

Best practices recommend securing access to these apps by separating your primary authentication method from your secondary (using MFA). Shift away from depending solely on a primary authentication provider to avoid a vendor-based breach that can risk exposing both primary and secondary authentication.

Secure Single Sign-On (SSO)

For a consistent login experience, let your users log in once to access all of their cloud and internal work applications with a secure single sign-on (SSO) solution.

Protect your SSO with MFA and contextual access policies, and check the security of your users' devices each time before granting access.

> Secure access to all applications, services and platforms – whether multi-cloud, on-prem, custom, remote access or VPN.

Duo's Zero Trust for the Workforce

Duo provides the foundation for a zero-trust security model by providing user and device trust before granting access to applications – ensuring secure access for any user and device connecting to any application, from anywhere.

Each time a user logs into an application, the trust of their identity and security of their device is checked by Duo, before granting access to only the applications they need. Duo gives you adaptive policies and controls to make access decisions based on user, device and application risk.

Establish User Trust

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

Multi-Factor Authentication

Eliminate the threat of attacks that stem from compromised credentials with Duo's easy and effective **multi-factor authentication**. Duo's intuitive MFA makes enrollment and secure logins easy for users, reducing friction to their workflow. Users can quickly tap a button on a **Duo Push** notification sent to their smartphone via the **Duo Mobile** authentication app to verify their identity.

For All Types of Users

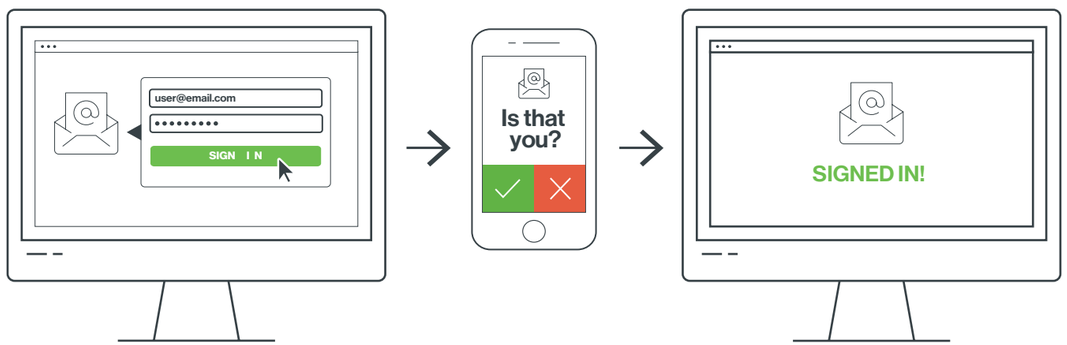
Duo's MFA works well for all user groups in the enterprise, including employees, contractors, vendors, customers, partners, etc., supporting user group-specific access policies.

Designed to support every user login scenario from offline to limited cell service and internet connectivity, Duo offers many different **MFA methods**, including mobile apps, push notifications, offline options, **biometric-based WebAuthn**, security keys and more.

Plus, using Duo's access policies, your admins can require the use of certain methods for access to more sensitive applications for higher assurance of your users' identities.

Easy to Deploy

Admins benefit from Duo's native integrations, easy cloud-based setup and low maintenance solution. Duo's automated sign-up options such as **user self-enrollment** and Active Directory sync options allow for scalable user provisioning. To reduce help desk tickets and management, Duo's **self-service portal** 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.

Across Every Platform

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 to get insight into their security posture.

Centralized Dashboard

Admins get one centralized, intuitive interface to easily manage users, devices and policies globally, as well as security reports and logs for compliance audits.

Duo's **detailed reports** give admins data on user behavior and risky devices, as well as user, admin and telephony data – all easily integratable with existing security information and event management (SIEM) systems.

Support BYOD & Mobile

Get greater BYOD insight and control with Duo's platform that detects and tracks every device accessing protected applications, including desktop, laptop and mobile – without using an agent.

Identify both corporate IT-managed and personally-owned devices with Duo's **Trusted Endpoints**. 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 without the need to deploy and manage a complex PKI certificate infrastructure.

Establish Device Trust

Duo provides administrators with visibility into user and device risks and provides the ability to apply controls that prevent threats and risky devices from gaining access to sensitive applications and data.

Risk-Based Device Access

Admins can support BYOD policies by marking endpoints as **trusted or untrusted**, while enforcing policies that require stronger security or limit access by untrusted devices.

Establish Mobile Device Trust

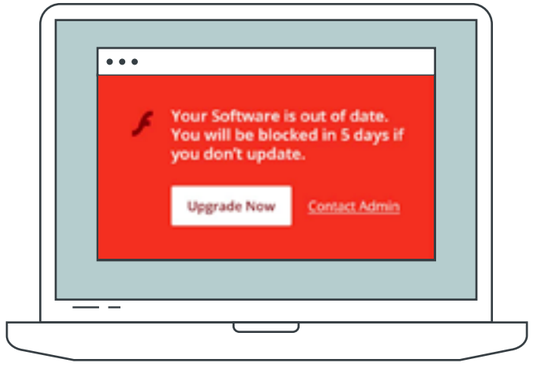
Using **Duo Mobile for Trusted Endpoints**, you can block devices from accessing your applications based on:

+ 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)

The Duo Mobile app installed on your users' phones can serve as your Android/iOS managed device verification tool.

Notify Users to Update Risky Devices

To ease the burden on your help desk team and reduce support tickets, Duo's **Self-Remediation** notifies and assists users to update any out-of-date devices. Inform users they'll be denied access in a certain number of days unless they update, and provide a direct link to update their software to close security gaps faster.



Enforce Adaptive Policies

Duo gives you the controls to limit access by risky endpoints and users to applications based on conditional risk (adaptive authentication).

Role-Based Access Policies

The principle of least privilege means limiting access to data and applications by only those people that need access to do their job. Duo allows you to set role-based access controls and restrict access to applications based on users' roles and job responsibilities.

For example, you can use Duo's policy framework to ensure only developers have access to critical infrastructure hosted in AWS – and that they can only access it using corporate-issued devices running the latest operating system, using the secure MFA method Duo Push.

App-Specific Policies

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.

User Location

To comply with regional data privacy laws, you may need to enforce access policies based on location. To enable you to do that, Duo lets you set policies to grant or deny access to your applications based on where the user/device is coming from (a set of IP address ranges).

You can also require MFA for certain locations. Plus, Duo enables you to block authentication attempts to your applications from anonymous networks like Tor and proxies.

Introduction User Trust Device Visibility Device Trust Adaptive Policies Access to All Apps Duo's Zero Trust

Enable Secure Access to All Apps

Duo provides **broad coverage across every application**, with out-of-the-box integrations for ease of setup with all types of apps – from legacy to modern to custom tools. For custom applications, Duo also offers APIs, WebSDKs and support for other protocols to allow you to extend Duo's security platform to protect proprietary services.

Duo provides flexible, frictionless access to hybrid and multi-cloud environments, allowing you to apply a zero-trust security approach for remote access to cloud infrastructure and corporate applications.

Remote Access

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.

Cloud/Identity Access

As organizations migrate their applications and infrastructure to the cloud, Duo can fully protect both a hybrid and multi-cloud environment. Duo provides users with consistent remote access to multi-cloud and hybrid environments, including cloud infrastructure providers, as well as on-premises and cloud applications.

Duo supports cloud access use cases, such as developers accessing Amazon Web Services (AWS) and contractors who need remote access to internal applications. Duo's MFA also integrates with other SSO provides like Ping, Azure, Okta, Oracle and Shibboleth; providing identity integration with AD and SAML.

Secure Single Sign-On (SSO)

Users get a consistent login experience with Duo's single sign-on that delivers centralized access to both on-premises and cloud applications. Reduce password fatigue and increase user productivity by enabling your users to log in just once to Duo's **single sign-on (SSO)** to access all of their apps. Duo's secure SSO checks device security every time before granting access to each application

Tech Partnerships

Duo's **technology and security partnership** ecosystem makes it easy for you to eliminate complexity while protecting your existing IT investments. Our tech partners (Microsoft, Cisco, Workday, Citrix, VMware and many others) include identity and access management; network and remote access; endpoint management and security; detection and response; as well as popular business applications.

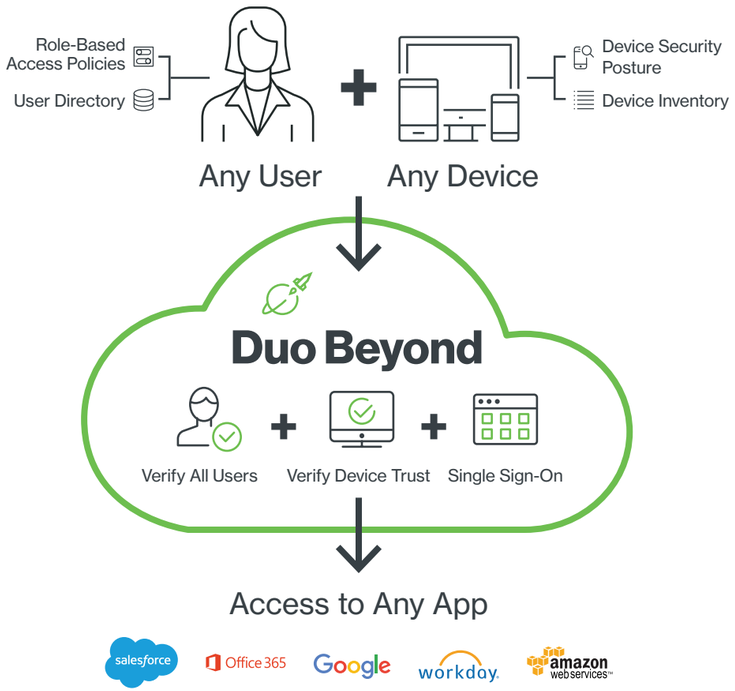
Begin your zero-trust journey with

Duo Beyond

In the **Duo Beyond edition**, you'll receive:

Full-featured two-factor authentication for every organization:

+ Protect logins with **Duo's MFA**
+ Insight into an overview of **device security hygiene**
+ Manage Duo's solution with **Admin APIs**
+ Duo's secure **single sign-on (SSO)** provides a consistent user login workflow across all applications
+ Protect access to both **on-premises and cloud applications**



Essential access security suite to address cloud, BYOD and mobile risks:

+ Complete visibility into both mobile and desktops, including **corporate-managed and unmanaged** (personally-owned) devices to support BYOD policies
  + Mobile device breakdown with visibility into enabled **security features and tampered or unencrypted devices**
+ Enforce rules on who can **access which applications, under what conditions** (adaptive authentication)
+ Enforce a policy to **allow only managed devices** access to sensitive applications
+ Provide modern **remote access to multi-cloud environments** (on-premises, Azure, AWS, Google Cloud Platform) while enforcing zero-trust security principles
+ **Notify users** to update their devices based on device access policies
+ Identify users vulnerable to phishing through **phishing campaigns**
+ Full-featured dashboards and custom reports for **compliance audits** and ease of administrative management

Learn more about Duo Beyond in our **documentation**.

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.

Get a **free trial for 30 days** and quickly protect all users, devices and applications. Or, **contact us**.

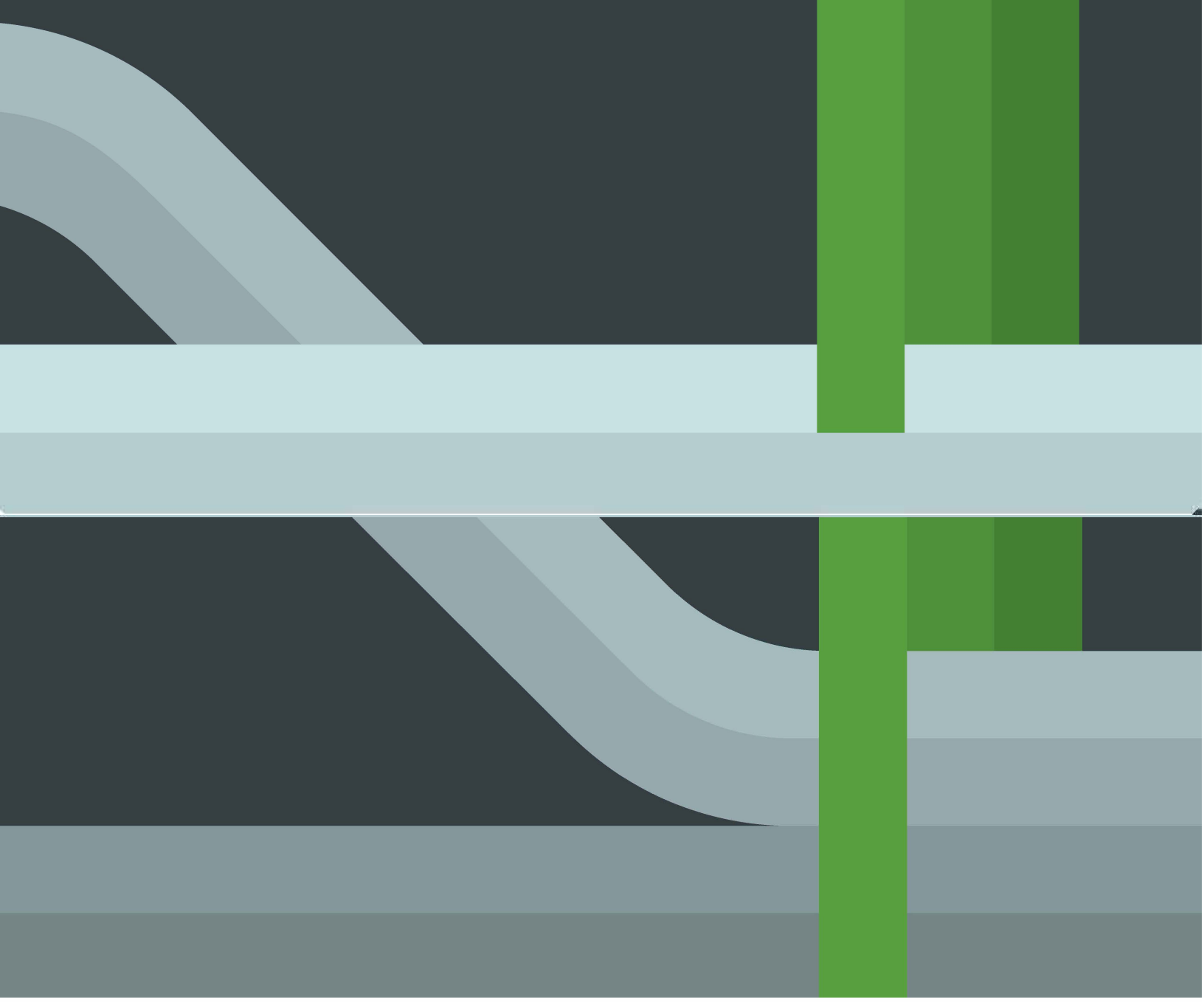
Cisco Zero Trust

Cisco Zero Trust provides a comprehensive approach to securing all access across your applications and environment, from any user, device and location. It protects your workforce, workloads and workplace.

+ To protect the workforce, Cisco ensures only the right users and secure devices can access applications.
+ To protect workloads, Cisco secures all connections within your apps, across multi-cloud.
+ To protect the workplace, Cisco secures all user and device connections across your network, including IoT.

This complete zero-trust security model allows you to mitigate, detect and respond to risks across your environment.

Learn More About
Cisco Zero Trust



Infinit is an engineering company providing Advanced IT Services and hardware solutions. We partner with world-class manufacturers to assess, plan and develop solutions that work best for a particular environment.

Contact us today for a Cisco Duo Free trial.

Infinit Technology Solutions

www.infinit-tech.com
contact@infinit-tech.com
877-825-8340 ext.3144

Cisco Partner