Solution Guide
Cisco Public

Your zero trust roadmap

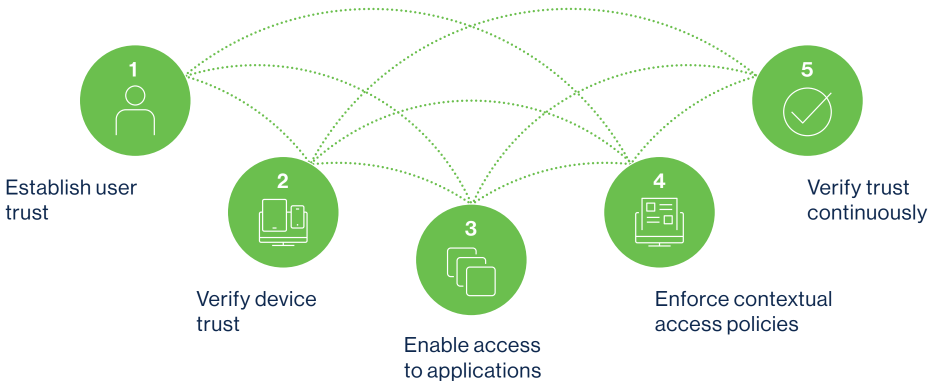
A five-phase plan for securing user and device access to applications

Adopting zero trust architecture offers a new way of securing user access to applications. By implementing a zero trust strategy, organizations eliminate the assumption of trust by constantly verifying trust at each access attempt–for users, devices, apps, networks, and clouds. By never assuming trust, continuously verifying it, and applying least privilege to each access decision, organizations can reduce risk systematically without impacting productivity or operations.

What are the steps needed to make meaningful progress toward zero trust?

This guide lays out a practical five-phase approach for implementing zero trust architecture for securing user and device access to applications. Keep in mind that a complete zero trust architecture extends beyond this use case to protect app-to-app access, access to multicloud and hybrid IT environments, and much more.

5 steps from MFA to zero trust


1
Establish user trust
2
Verify device trust
3
Enable access to applications
4
Enforce contextual access policies
5
Verify trust continuously

Phase 1

Establish user trust using strong or phishing-resistant multi-factor authentication (MFA) to verify users truly are who they say they are. Make it easy for users to authenticate while providing flexibility and a choice of strong authentication options, whether they're employees or contractors (e.g., BYOD).

Key activities:

Evaluate the use of passwordless for strong authentication; gather use case details and adoption targets and expand the use of MFA to the most visible applications.

Critical capabilities:

- Duo MFA

Phase 2

Verify device trust with posture checks and block unwanted access with a trusted endpoint policy. Guide users in fixing device trust issues on their own before gaining access to apps without having to call the helpdesk.

Key activities:

Go beyond managed devices to include BYOD and personally-owned devices in a secure manner. At the same time, evaluate the option of automatically denying login access to any untrusted or unmanaged devices for sensitive applications and environments.

Critical capabilities:

- Duo’s Trusted Endpoints
- Duo Desktop

Phase 3

Enable access to applications with passwordless SSO and VPN-less access (e.g., ZTNA). Shrink the attack surface by reducing password usage with passwordless SSO to make it faster and more convenient for users to get to the apps they need – whether SaaS-based, on-premises, or private.

Key activities:

Rank and prioritize applications based on their criticality to the business and the sensitivity of their data. Gain visibility into the devices and applications in use, including controls in place to verify trust. Go beyond on-premises applications to include securing cloud applications.

Critical capabilities:

- Duo’s Cloud-Based SSO
- Passwordless
- Duo Network Gateway

Phase 4

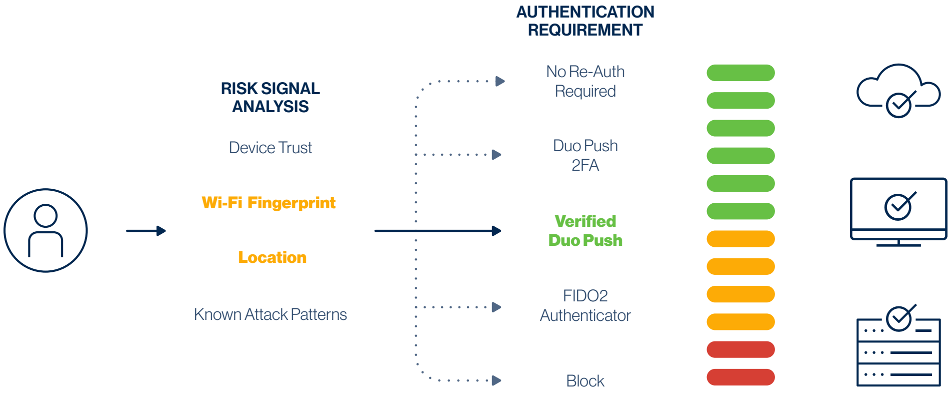
Enforce contextual access policies with adaptive and risk-based authentication. Increase device visibility, and adapt access dynamically based on risk signals in real-time. Step up access based on increased risk and ease up access requirements based on lowered risk. Respect the user's privacy and productivity by anonymizing location data and eliminating unnecessary decisions.

Key activities:

Start with a baseline level of trust for all users and devices regardless of what they're accessing, and then add more to reach the level of risk management needed for access to the most sensitive tiers. Use context to enforce policy compliance dynamically.

Critical capabilities:

- Device Insight
- Adaptive Access Policies
- Risk-Based Authentication
- Duo Trust Monitor



Features like Verified Duo Push continuously verify trust before granting access

Phase 5

Verify trust continuously with session trust analysis. By leveraging open protocols to communicate signals and react to changes in risk, session trust analysis brings visibility and control to a traditionally opaque surface: risk remediation during the established session.

Key activities:

Identify critical access applications and users, as well as vulnerable attack surfaces. Tighten security policies to mitigate modern attacks. Train users on strong, phishing-resistant authentication factors. Act to continuously validate people and devices.

Critical capabilities:

- Continuous Trusted Access

Summary

Changing the security lifestyle of an organization takes dedicated work, but once the controls fit more closely to where they belong – the users, their devices, and the applications – you'll be addressing the gaps in today's traditional security paradigm and moving beyond it.

To learn more about how to adopt zero trust in your organization, register for a free Zero Trust Workshop today. Ready to get started with Duo? Sign up for a free trial now.