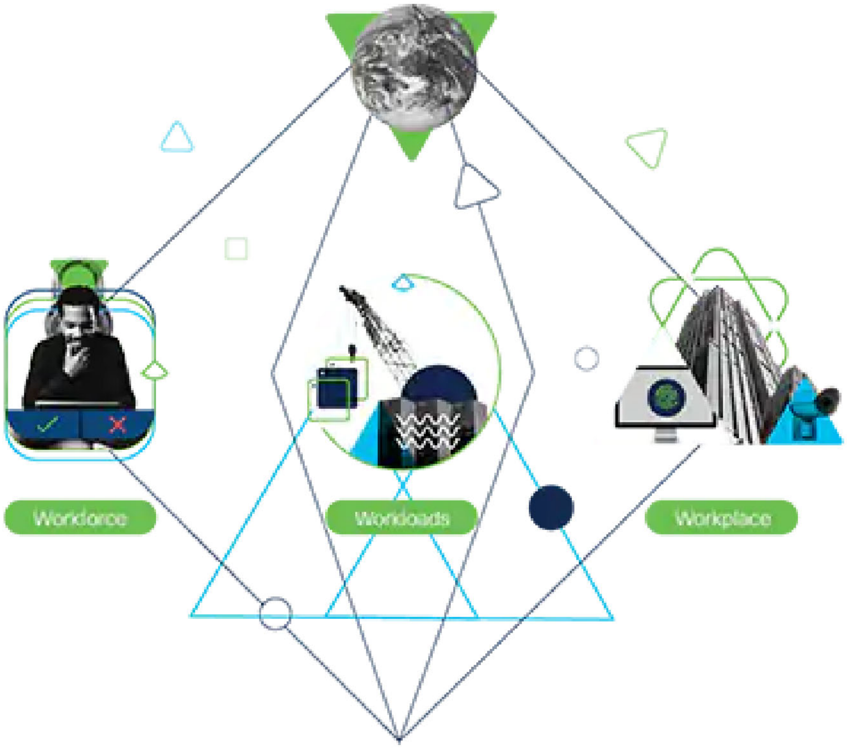
Cisco Zero Trust Security



Establish trust at point of access

Cisco Zero Trust offers a comprehensive solution to secure all access across your applications and environment, from any user, device, and location. This complete zero trust security model allows you to mitigate, detect, and respond to risks across your environment. See how you can make your environment Cisco Secure today.

Watch overview (2:30)

Attend a workshop

The 2021 Duo Trusted Access Report

Using data from millions of authentications, Duo examines how organizations are enabling work from anywhere, on any device, by implementing controls to ensure secure access to applications.

Get the Report

Zero trust explained

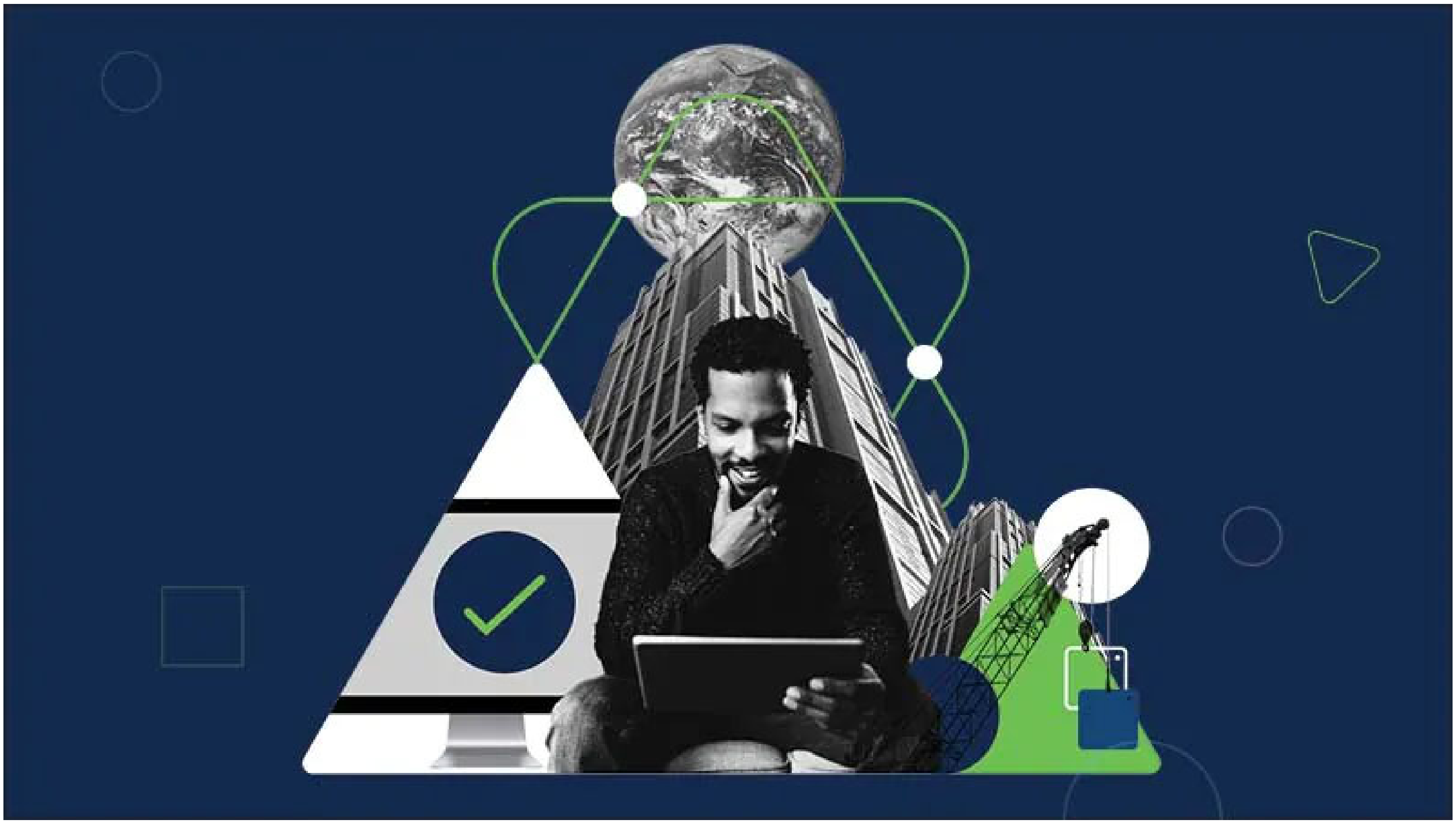
What is zero trust?

Zero trust is a strategic approach to security that centers on the concept of eliminating trust from an organization's network architecture. Trust is neither binary nor permanent. We can no longer assume that internal entities are trustworthy, that they can be directly managed to reduce security risk, or that checking them one time is enough. The zero-trust model of security prompts you to question your assumptions of trust at every access attempt.

How is a zero-trust approach different?

Traditional security approaches assume that anything inside the corporate network can be trusted. The reality is that this assumption no longer holds true, thanks to mobility, BYOD (bring your own device), IoT, cloud adoption, increased collaboration, and a focus on business resiliency. A zero-trust model considers all resources to be external and continuously verifies trust before granting only the required access.

m



Cisco rides the wave as a leader in zero trust

"Cisco pushes the zero trust envelope the right way." Learn why Forrester has identified Cisco as a market leader in its Zero Trust eXtended Ecosystem Platform Providers, Q3 2020 report.

Read the report

Read the blog

Why adopt a zero-trust security approach?

With the zero-trust model, you gain better visibility across your users, devices, containers, networks, and applications because you are verifying their security states with every access request. You can reduce your organization's attack surface by segmenting resources and only granting the absolute minimum access needed.

Adopting this model provides you with a balance between security and usability. Security teams can make it harder for attackers to collect what they need (user credentials, network access, and the ability to move laterally), and users can get a consistent and more productive security experience--regardless of where they are located, what endpoints they are using, or whether their applications are on-premises or in the cloud.

The most successful zero-trust solutions should seamlessly integrate with your infrastructure without entirely replacing existing investments. Cisco Zero Trust provides a comprehensive approach to securing all access across your applications and environment, from any user, device, and location, by:

Establishing trust

We establish trust by verifying:

- User and device identity
- Device posture and vulnerabilities
- Any workloads
- Application and service trust
- Any indicators of compromise

Enforcing trust-based access

We enforce least privilege access to:

- Applications
- Network resources
- Workload communications
- All workload users and administrators

Verifying trust continuously

We continuously verify:

- That original tenets used to establish trust are still true
- That traffic is not threat traffic
- Any risky, anomalous, and malicious behavior
- That the trust level is changed, if compromised

Zero-trust pillars

Security is not one-size-fits-all. When approaching zero-trust design, it is easier to break it down into three pillars: workforce, workload, and workplace. These align with the model proposed by Forrester to simplify adoption. There are nuances to address in each area, while all work toward the same goal.

Zero trust for the workforce

This pillar focuses on making sure users and devices can be trusted as they access systems, regardless of location.

Zero trust for the workplace

This pillar focuses on secure access to the network and for any and all devices (including IoT) that connect to enterprise networks.

A comprehensive zero-trust security approach

The platform approach of Cisco Zero Trust provides a balance between security and usability. Security teams can make it harder for attackers to collect user credentials and network access and to move laterally, and users can get a consistent and more productive security experience--regardless of where they are located, what endpoints they are using, or whether their applications are on-premises or in the cloud. Its comprehensive approach to securing all access protects the workforce, workloads, and workplace.

Read zero-trust white paper

Securing the federal workforce

Zero trust has become a dominant security model for the changes brought about by mobility, consumerization of IT, and cloud applications. Our guide can help your organization implement the principles of zero trust at a sustainable pace.

Download the white paper

Cisco Zero Trust

With Cisco Zero Trust you can:

- Consistently enforce policy-based controls
- Gain visibility into users, devices, components, and more across your entire environment
- Get detailed logs, reports, and alerts that can help you better detect and respond to threats
- Provide more secure access, protect against gaps in visibility, and reduce your attack surface with Cisco Zero Trust
- Automate threat containment based on any changes in the "trust level"

Cisco Zero Trust for the workforce

Cisco Zero Trust provides solutions that establish trust in users and devices through authentication and continuous monitoring of each access attempt, with custom security policies that protect every application. It allows you to:

- **Protect against credential compromise**

Verify your users' identities with multi-factor authentication.

- **Gain visibility into access activities**

Get visibility into access activity across all locations, devices, and users. Control cloud application access and prevent malicious connections.

- **Enforce access policies for every application**

Set policies based on your organization's risk tolerance level and requirements.

tacks and malware.

- Block access from compromised devices

Protect endpoints, network, and email and get visibility into network and endpoint threats while blocking and removing malware.

Get started today

Cisco Zero Trust for workloads

Cisco Zero Trust secures connections for all APIs, microservices, and containers that access your applications, whether in the cloud, data center, or other virtualized environment. Cisco Zero Trust, deployed on-premises or in the cloud, secures your app stack, and micro-segmentation helps you contain threats and protect against lateral movement.

- Visibility into applications

Have control over every connection from users and devices to both your applications and your network, across a multicloud environment.

- Application segmentation

Minimize lateral movement for on-premises and multicloud environments.

- Monitor application performance

Identify root causes of threats with deep diagnostic capabilities.

- Enforce policies and controls

Enforce application-specific user and device access policies to meet your organization's security requirements for access. Flag anomalies using behavioral analysis to reduce your attack surface.

h flow maps.

Get started now

Cisco Zero Trust for the workplace

Cisco Zero Trust enables users to securely connect to your network from any device, anywhere while restricting access from non-compliant devices. Our automated network-segmentation capabilities let you set micro-perimeters for users, devices, and application traffic without requiring network redesign.

- Secure network access

Get complete visibility by identifying, classifying, and assembling the necessary context on users and endpoints, including IoT.

- Network segmentation

Build granular segmentation directly into the network, eliminating the need for complicated infrastructure configurations.

- Encrypted traffic analytics

Identify malware in encrypted traffic using network analytics.

- Dynamic visibility

Build visibility-based network segmentation and policy control into your security architecture.

- Automated threat containment

Implement adaptive threat containment to ensure the organization's security posture evolves as threats do.

as in the network, based on encrypted traffic analytics.

Extended protection and trust

Zero-trust security for any enterprise

To support the successful implementation of a zero-trust security approach, Cisco Zero Trust provides a comprehensive portfolio of Cisco Secure solutions and the Zero Trust Strategy Service. It integrates with an ecosystem of other products to provide complete zero-trust security for any enterprise environment.

Accelerate your journey to zero trust with Cisco SecureX

Simplify your security by connecting the Cisco Secure portfolio and your infrastructure with SecureX, our cloud-native, built-in platform experience.

Explore SecureX

Watch demo (4:36)

Cisco's own journey to zero trust

“Security is constantly changing. As we move forward, Duo is going to be a critical enabler to allow us to have zero trust.”

Steve Martino, CISO, Cisco

View case study

Featured zero-trust resources

Zero-trust approach to enterprise security

Learn the fundamentals of zero trust, including its three pillars, risks, options for implementing, and proposed maturity models.

Zero-trust evaluation guide for the workforce

fying your users and their devices as they are accessing

What is zero trust, and how does Cisco define it? (2:30)

Learn more about securing your workforce, workloads, and workplace by watching this explainer video.

Resources

Workforce: Zero-trust evaluation guide for the workforce

Demo: Duo Secure Access

Workplace: Forrester ZTX networks guide

Demo: Secure network

Workloads: Platform for workload protection data sheet

Demo: Secure workload

Begin your zero-trust journey with Secure Choice

Let your Cisco Zero-Trust journey with Secure Access by Duo and Identity Services Engine (ISE) begin by buying through Secure Choice, one easy-to-manage agreement.

Explore Secure Choice >

For partners

Are you a Cisco partner? Log in to see additional resources.

Looking for a solution from a Cisco partner? Connect with our security technical alliance partners.

Secure

Twitter Facebook Instagram LinkedIn YouTube Blogs Communities

Quick Links −

About Cisco

Contact Us

Careers

Meet our Partners

Resources and Legal −

Feedback

Help

Terms & Conditions

Privacy Statement

Cookies

Trademarks

Sitemap