Cisco Zero Trust

A comprehensive approach to secure access for your workforce, workloads, and workplace.

Shift in IT landscape

Users, devices and apps are everywhere

Cisco® Zero Trust is a comprehensive approach to securing all access across your networks, applications, and environment. It helps secure access from users, end-user devices, APIs, the Internet of Things (IoT), microservices, containers, and more.

Modern enterprise challenges

There's been a shift in the IT landscape—users, devices, and the cloud has moved control and visibility outside of the traditional network. As a result, there's increased points of access, a larger attack surface, and more gaps in visibility.

Traditional security approach	Zero-trust approach
Trust: Based on network location that an access request is coming from	**Trust:** Established for every access request, regardless of where the request is coming from
As a result: ▪ Attackers can move laterally to get to an organization's crown jewels ▪ It doesn't extend security to the new perimeter	**As a result:** ▪ Secures access across your applications and network ▪ Ensures only the right users and devices have access ▪ Extends trust to support Bring Your Own Device (BYOD), cloud apps, hybrid environments, and more

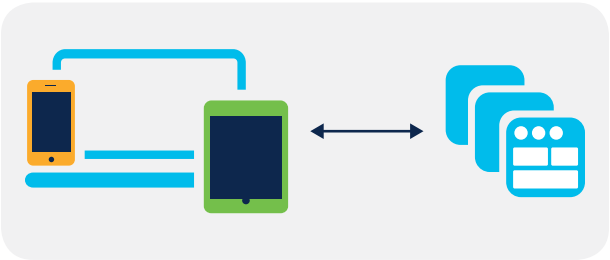
Cisco Zero Trust

Secure access across your applications and environment, from any user, device, and location.

Cisco Zero Trust allows you to:

- 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.



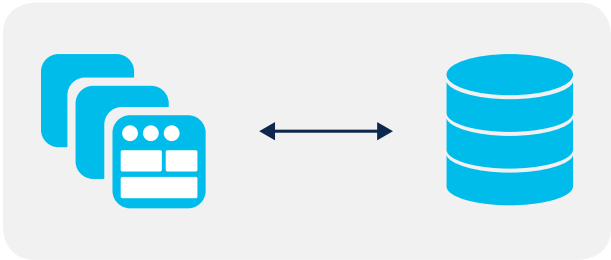
Zero Trust for the workforce

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

Duo Security:

- Verifies users' identities with MultiFactor Authentication (MFA)
- Allows you to gain device visibility and establish trust with endpoint health and management status
- Enables you to enforce access policies for every app with adaptive and role-based access controls

Learn about Duo Security



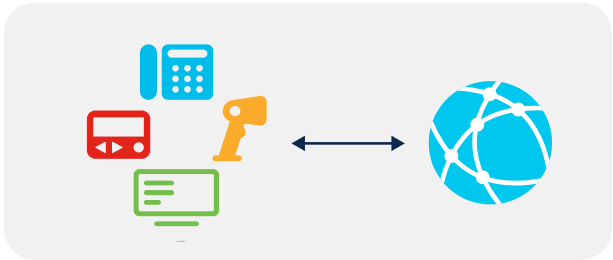
Zero Trust for workloads

Secure all connections within your apps, across multicloud.

Cisco Tetration:

- Gives you visibility into what's running and what's critical by identifying workloads and enforcing policies
- Allows you to contain breaches and minimize lateral movement with application microsegmentation
- Alerts you or blocks communication in case of a policy violation by continuously monitoring and responding to indicators of compromise

Learn about Tetration



Zero Trust for the workplace

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

Software-Defined (SD) Access:

- Grants the right level of network access to users and devices with network authentication and authorization
- Classifies and segments users, devices, and applications on your network with network segmentation
- Contains infected endpoints and revokes network access by continuously monitoring and responding to threats

Learn about SD-Access

Extended protection

Duo, Tetration, and SD-Access are the three primary products for workforce, workload, and workplace security. Cisco Zero Trust also integrates with a larger ecosystem of other products to provide complete zero-trust security for any enterprise.

Extend trust

Cisco Advanced Malware Protection (AMP)

Protect your endpoints, network, and email with AMP. Get deep visibility into network and endpoint threats, and block and remove malware.

Cisco Umbrella™

Get visibility to protect Internet access across all devices on your network, all office locations, and roaming users.

Next-Generation Firewalls

With deep network and security visibility, you can detect and stop threats fast before they reach your workforce, workloads, and workplace.

AnyConnect®

Provide secure access to the workforce and workplace, as well as more insight into user and endpoint behavior across your entire enterprise.

Email Security

Defend against data loss and encrypt sensitive information with Cisco Email Security to protect against phishing, business email compromise, and ransomware.

Meraki® Systems Manager

Unified device management and control of mobile and desktop devices, allowing for seamless onboarding and automated application of security policies.

ACI

Application-Centric Infrastructure (ACI) allows for consistent, policy-based automation for connectivity and segmentation across on-premises and cloud.

Detect and respond

Cisco Stealthwatch®

Find out who is on your network and what they are doing using network infrastructure telemetry. Detect threats and respond to them quickly with a scalable solution.

Cisco Threat Response

Automate integrations across Cisco security products to accelerate detection, investigation, and remediation.

Extend to any integration

Our technical partnerships make it easy to integrate security with your existing platforms.

Any endpoint management platform	Any infrastructure platform	Any third party
Protect any endpoint management platform and integrate with Microsoft, Symantec, VMware, MobileIron, Jamf, and more.	Integrate with any infrastructure platform, such as Google, Kubernetes, Microsoft Azure, Amazon Web Services (AWS), VMware, and more.	Work with third parties like identity providers and Security Information and Event Management (SIEM) systems such as Exabeam, Okta, Splunk, IBM, Google, Dell, Ping Identity, Oracle, and others.

Learn more about Cisco partners > Duo partners > Duo integrations

C22-742591-00 08/19