Duo Security and Cisco Secure Endpoint

Establish Endpoint Trust

With an estimated 70% of breaches starting on endpoints – laptops, workstations, servers and mobile devices – organizations need visibility into the devices connecting to applications both on-premises and in the cloud. Transparency into every endpoint reveals what may be introducing risk, but transparency alone doesn't establish that the device can be trusted.

Organizations need the ability to establish trust in the devices connecting to resources containing sensitive information. But how is device trust established?

Establishing Trust in Endpoints

To establish trust in user devices, device-based policies should be in place to prevent any risky or unknown endpoints from access by validating the device is healthy and meets security policies. Validating both managed and unmanaged (personal or third-party contractor) devices and ensuring they are trustworthy are key components of the Cisco Zero Trust security approach for the workforce.

Benefits

- **Duo Security** continuously verifies user identities and establishes device trust before granting access to applications
- **Cisco Secure Endpoint** prevents breaches and blocks malware at the point of entry, then rapidly detects, contains and remediates advanced threats at the endpoint
- **Duo Security and Cisco Secure Endpoint work together** to detect malware and automatically respond to threats by blocking risky endpoints with access policies

Zero Trust for the Workforce

Cisco Zero Trust for the Workforce enables Security/IT teams to:

- Verify users and establish device trust with multi-factor authentication (MFA)
- Enforce access policies for every application with adaptive and role-based access controls
- Continuously monitor and respond to risky devices with endpoint health and management status

Get started with a free Duo trial.

Together, Duo Security and Cisco Secure Endpoint provide organizations with the tools needed to establish trust in users' devices before granting access to protected applications. The ability to prevent, detect and respond is a key element when considering device trust in a zero trust security approach for the workforce.

	Prevent	Detect	Respond
Duo Security	Evaluates risk conditions, the health of the device and security status on every access attempt.	Blocks access from endpoints that don't meet defined risk conditions.	Prompts users to take appropriate action to remediate when access has been denied.
Cisco Secure Endpoint	Strengthens defenses using the best global threat intelligence and automatically blocks known fileless and file-based malware.	Detects stealthy threats by continuously monitoring file activity, while allowing you to run advanced search on the endpoint.	Rapidly contains the attack by isolating an infected endpoint and accelerating remediation cycles.

Learn more about Cisco Zero Trust Security:

https://www.cisco.com/site/us/en/solutions/security/zero-trust/index.html