Duo and AMP

Establish Endpoint Trust

Challenges of Protecting Endpoints

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 the network 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 trust established in devices?

Establishing Trust in Endpoints

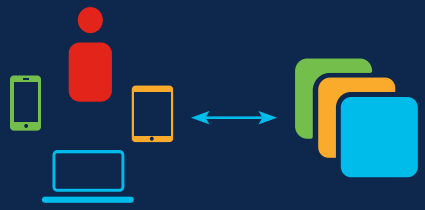
To establish trust in user devices, device-based policies should be in place to prevent any risky or unknown devices from access by validating the device is healthy and meets security policies. Validating devices and ensuring they are trustworthy are key components of the Cisco Zero Trust security approach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

Duo Security verifies user identities and establishes device trust before granting access to applications.

AMP for Endpoints prevents breaches and blocks malware at the point of entry, then rapidly detects, contains, and remediates advanced threats at the endpoint

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

Get started with a free trial of Duo.

Prevent - Detect - Respond

With Duo and AMP, organizations have the tools in place to effectively establish trust in users' devices connecting to protected applications. The ability to prevent, detect and respond are key elements when considering device trust in a zero-trust security approach for the workforce.

Prevent

Duo Security

Evaluates risk conditions, the health of the device and security status on every access attempt.

AMP for Endpoints

Strengthens defenses using the best global threat intelligence, and automatically blocks known fileless and file-based malware.

Detect

Duo Security

Blocks access from endpoints that don't meet defined risk conditions

AMP for Endpoints

Detects stealthy threats by continuously monitoring file activity, while allowing you to run advanced search on the endpoint.

Respond

Duo Security

Prompts users to take appropriate action to remediate when access has been denied.

AMP for Endpoints

Rapidly contain the attack by isolating an infected endpoint and accelerating remediation cycles.

Learn More

Learn more about Cisco Zero Trust Security
https://www.cisco.com/c/en/us/products/security/zero-trust.html