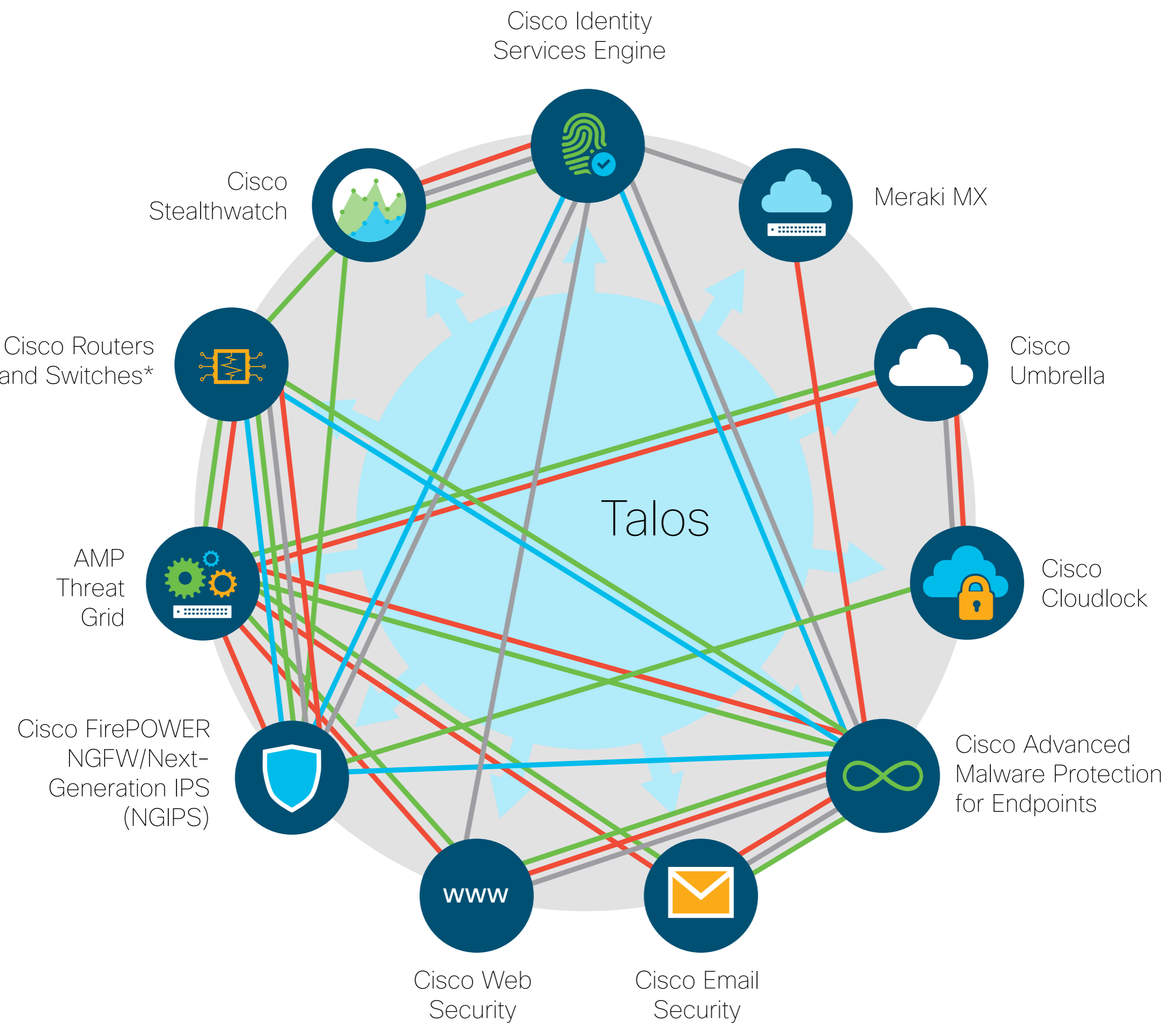
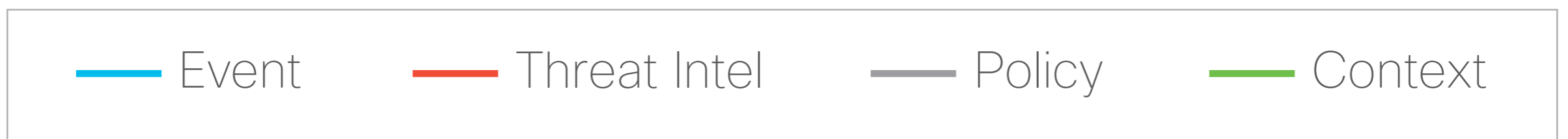


# Cisco Security

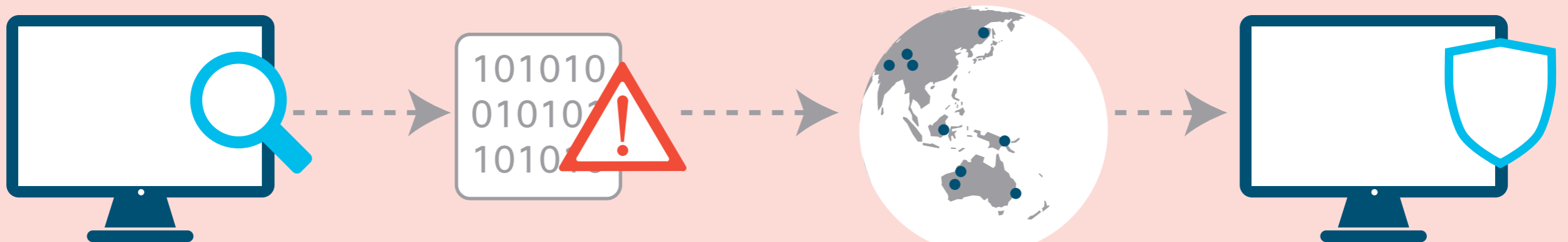
Cisco Security products communicate because they are open, automating and simplifying processes, making security more effective.



\*Cisco Integration/Aggregation Services Routers (ISR/ASR) and Catalyst Switches

## Threat Intel

Speed time to detection by sharing **threat intelligence**.



Advanced Malware Protection (AMP) for Endpoints identifies a malicious file for a Cisco customer in London.

Talos is updated with information about that file.

Talos shares that information with AMP for Email customer in India.

AMP for Email blocks the file even though it hasn't seen it before.

## Policy

Respond faster by automatically changing **policy**.



Cisco Stealthwatch identifies a user as compromised.

Cisco Stealthwatch notifies the Cisco Identity Services Engine (ISE), which changes the user's profile to "compromised."

Through an integration with ISE, the Cisco Web Security Appliance (WSA) automatically changes the user's policy.

## Context

Prevent threats from spreading by sharing **context**.



Through an integration with ISE, next-generation firewall (NGFW) and WSA policy can control context such as user, device, and location.

## Events

Quickly identify a threat by sharing **events**.



Cisco Cognitive Threat Analytics (CTA) identifies a breach.

CTA shares the alert with AMP for Endpoints.

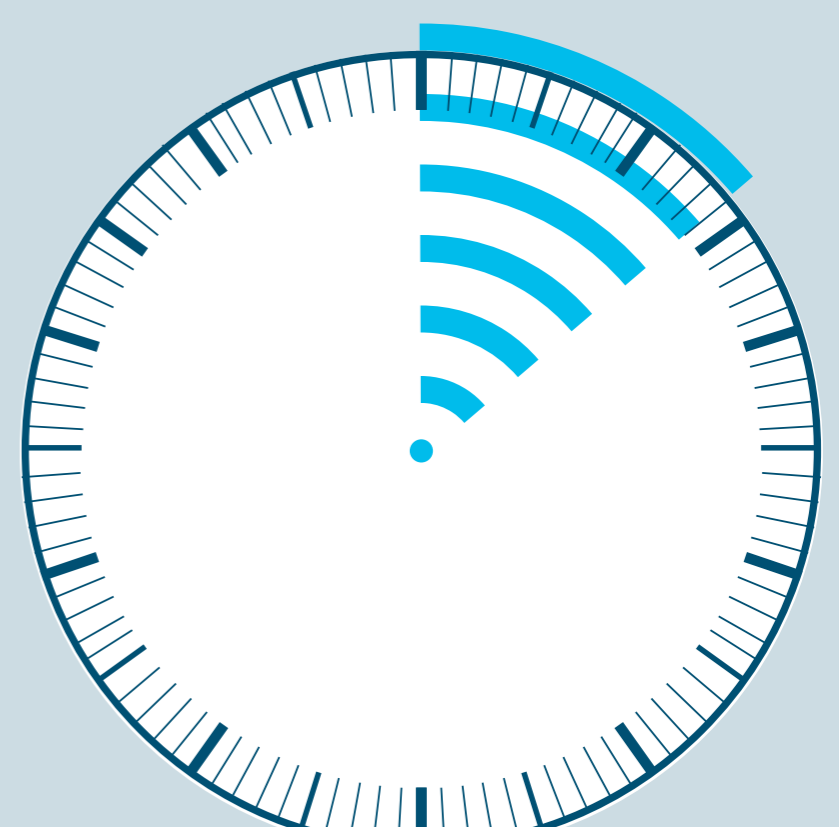
The alert and user details are visible in the AMP dashboard.

Remove a malicious file responsible for the breach on all infected devices with one click.

## Effective

Cisco's total time to detection is **14 hours**, versus the industry average of **100-200 days**.

Cisco 2017 Annual Cybersecurity Report



Visit [cisco.com/go/security](http://cisco.com/go/security) to learn more >