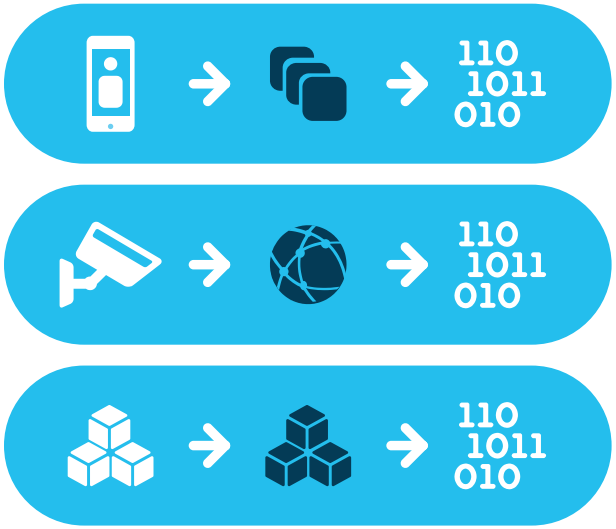
Cisco Trusted Access

A practical Zero Trust approach to security

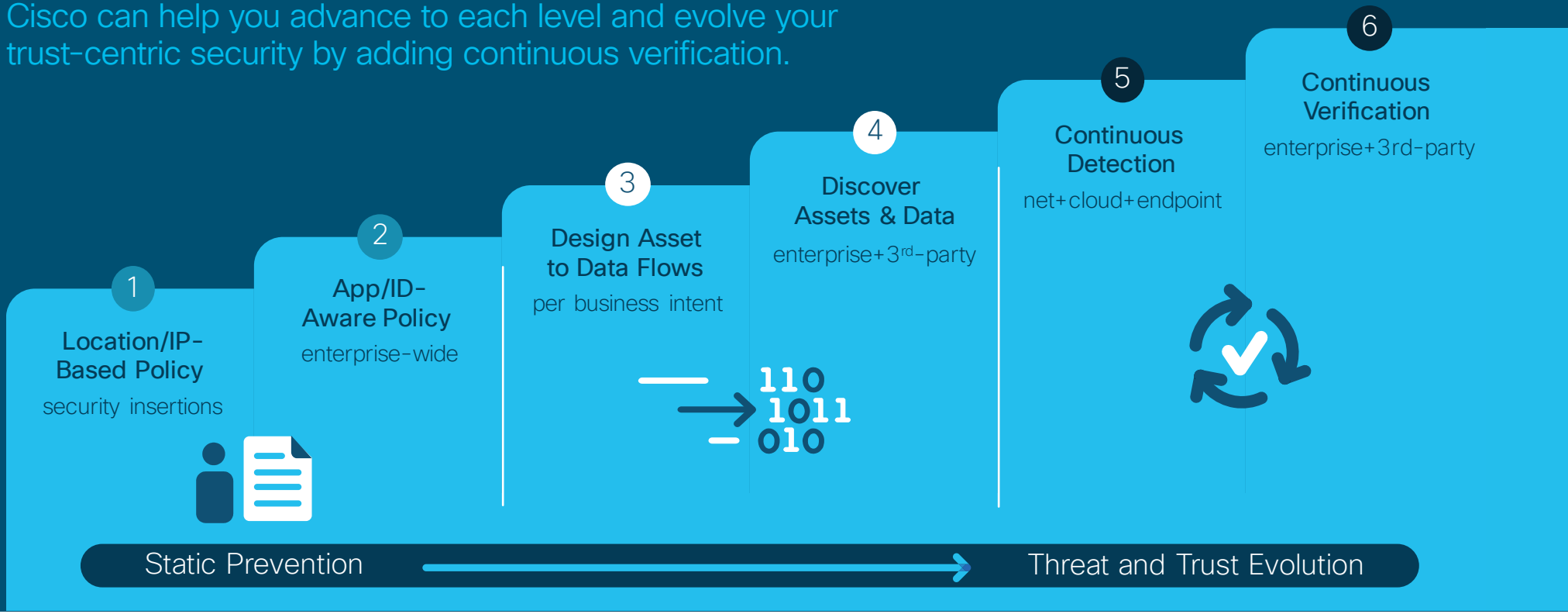


With your workforce on the go, workloads in many clouds, and devices outside your control—knowing who and what to trust is the big IT security challenge. And now everyone is telling you to adopt Zero Trust for your network. But what does that mean? What about apps beyond the network? Do we begin with multi-factor authentication or micro-segmentation?

Cisco Trusted Access makes is easier and safer to grant and restrict access by establishing trust and software-defined access based on dynamic context; not just static credentials or network topologies.

What's your security maturity level?

Cisco can help you advance to each level and evolve your trust-centric security by adding continuous verification.



Infrastructure enforcement

Right now, you have firewalls (1) and may even bake security into the LAN and WAN (2). You have port and IP policies that allow normal or deny abnormal activity (1). And these policies have evolved to be application and identity aware (2).

Yet, everything you're doing is still based on single points in time. This creates gaps.

Risk management

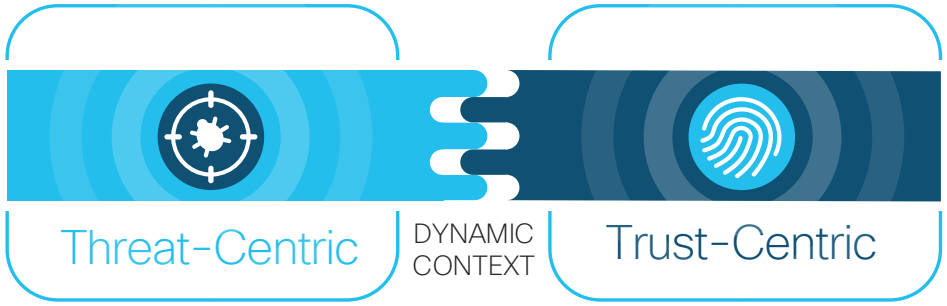
How do you know that you're providing the right data access based on a level of trust as things change over time (3)?

As orgs become more agile, data is accessed from anywhere and often by third-parties due to M&A, supply chains, and contractors. Can you discover all users, devices and workloads requesting access to learn where breach risk is highest (4)?

Dynamic context

If passwords are stolen from authorized users or vulnerabilities are exploited on authorized devices or workloads, could you stop an unauthorized app, network or data center access?

Just as Cisco has evolved threat-centric security by adding continuous detection (5), we're evolving trust-centric security by adding continuous verification with Cisco Trusted Access (6).



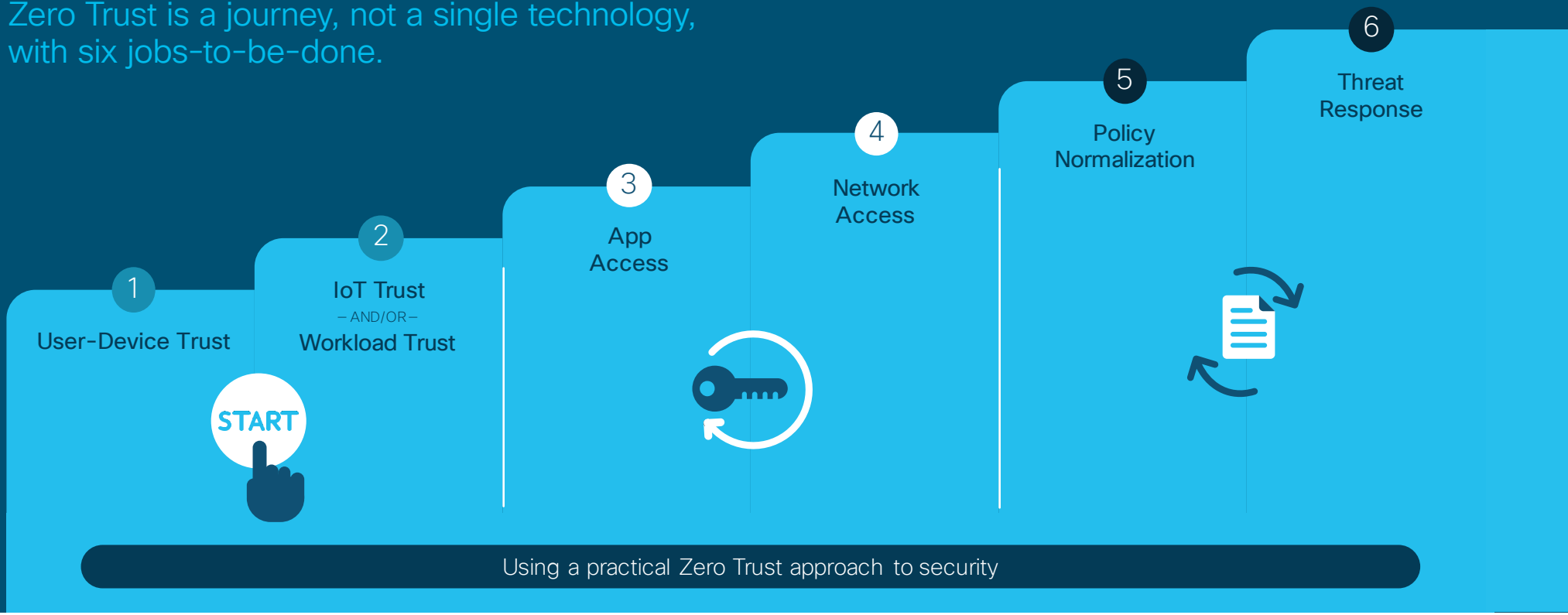
Complementary security approaches

It is a basic level of security maturity to prevent attacks via an intelligence-based policy – then detect, investigate, and remediate.

It is a good security practice to verify before granting access via an identity-based policy – for any user, any device, any app, in any location.

Cisco will map out your journey

Zero Trust is a journey, not a single technology, with six jobs-to-be-done.



Establish trust levels

For user-device trust, add Cisco's multi-factor authentication for any user with agent(less) assessments for any device (1).

For IoT trust, use Cisco's wired(less) network sensors, active probes, and partner exchange to classify headless devices. Or for workload trust, add Cisco's host sensors for containers, virtual machines (VMs), or bare metal to baseline East-West traffic (2).

Establish software-defined access

Use Cisco's cloud and remote access security with single sign-on to restrict access for any user and device, managed or not, to specific public or private apps within sofware-defined access based on trust, roles and risk (3).

Use Cisco's network and app fabric or enterprise firewalls to enforce software-defined perimeters and micro-segmentation policies based on intent rather than network topology (4).

Automate adaptive policies

Use Cisco's integrated portfolio, partner exchange, product APIs and implementation services for end-to-end policy normalization (5).

Use Cisco's continuous detection of network traffic, endpoint behavior, cloud usage, and app behavior to baseline what normal access requests look like and integrate responses to abnormal activity (6).

Trusted user-device access

Verify user identity and assess device hygiene before granting access to your cloud and on-premises apps. Add strong, easy-to-use two-factor authentication. Gain visibility into corporate-issued and personal devices with either agentless or agent-based assessments. Enforce adaptive policies based on authorized user-device combinations and app risk for secure access.

Learn about Duo Security

Trusted IoT access

Verify compliant device profiles before granting software-defined access to your network. Discover and classify connected devices by leveraging your wireless and wired network sensors and active probes as well as IoT platform partner feeds. Enforce adaptive policies based on authorized devices and tagged East-West traffic to secure and segment network access.

Learn about Cisco Software-Defined Access

Trusted workload access

Baseline East-West traffic and verify app behaviors before granting access to your hybrid data center and multi-cloud infrastructure. Use host and network sensors to inventory processes, detect vulnerabilities, and generate a normal activity whitelist based on unsupervised machine learning. Enforce whitelist policies for micro segmentation based on workload risk.

Learn about Cisco Tetration

Rebuild trust wherever there's an access decision

Cisco makes it easier and safer to adopt Zero Trust in weeks, not years.

Reduced exposure to unauthorized access

Continuous verification stops untrusted or compromised users, devices or workloads from accessing apps and network

Happier users foster a security culture

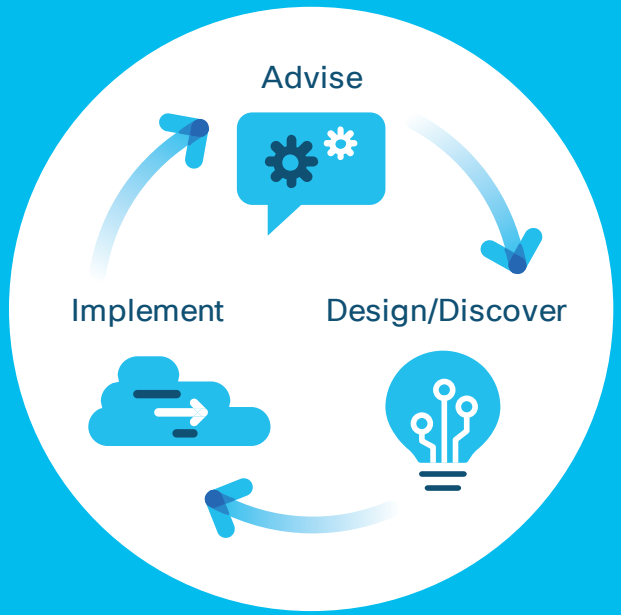
Shift automation to Cisco and some remediation to end-users to reduce friction for lean IT teams

Fast compliance right where it's needed

Authorized software-defined access and micro-segmentation for regulated data within specific apps or the network

Leverage Cisco's expertise

Cisco Trusted Access solves more use cases than anyone else. Accelerate prioritizing your top use cases or compliance requirements using our services and integrated portfolio. Our experts can map your journey to any trust-centric approach including Forrester ZTX, Gartner CARTA, Google BeyondCorp, CIS 20, NIST 800-171, or ISO 27000.



Learn about Cisco Services

Learn about ZTX, BeyondCorp, and CARTA