Shift in IT Landscape
Users, devices & apps are everywhere

Remote Users, Contractors & Third-Parties

Personal & Mobile Devices

IoT Devices

Evolving Perimeter

Cloud Applications

Hybrid Infrastructure

Cloud Infrastructure

2
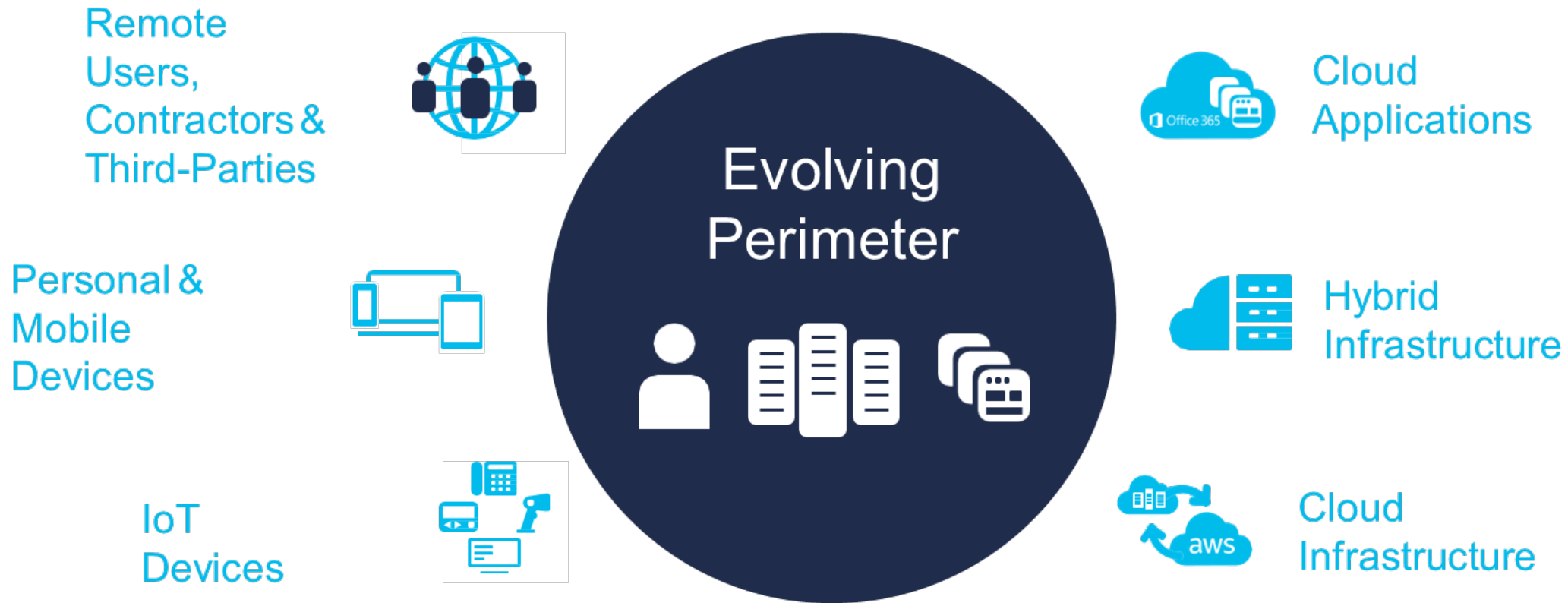
Business Challenges
Increased access, attack surface & gaps in visibility

How do we know users are who they say they are?

Are their devices secure & up to date?

What's on the network? How does it connect?

What data's in the cloud? Who/what accesses it?

How can we view & secure all connections?

What exists in the cloud? How does it connect?

Threats Today, As a Result
A new approach to security is needed – zero trust – to address identity, app & network threats

Targeting Identity
81% of breaches involved compromised credentials

Targeting Devices
300% increase in IoT malware variants

Targeting Apps
54% of web app vulnerabilities have a public exploit available

What's Different in a Zero-Trust Approach

The Traditional Approach

Trust is based on the network location that an access request is coming from.

→

Enables attackers to move laterally within a network to get to the crown jewels.

Doesn't extend security to the new perimeter.

The Zero Trust Approach: Never implicitly trust, always verify

Trust is established for every access request, regardless of where the request is coming from.

→

Secures access across your applications and network. Ensures only right users & devices have access.

Extends trust to support a modern enterprise with BYOD, cloud apps, hybrid environments & more.

What it takes to get Zero Trust right

Establish Trust

Enforce Trust-Based Access

Continuously Verify Trust

Respond to Change in Trust

How to deliver Trust

Verify users' identities

WITH

Multi-factor
authentication (MFA)

Gain device visibility
& establish trust

WITH

Endpoint health &
management status
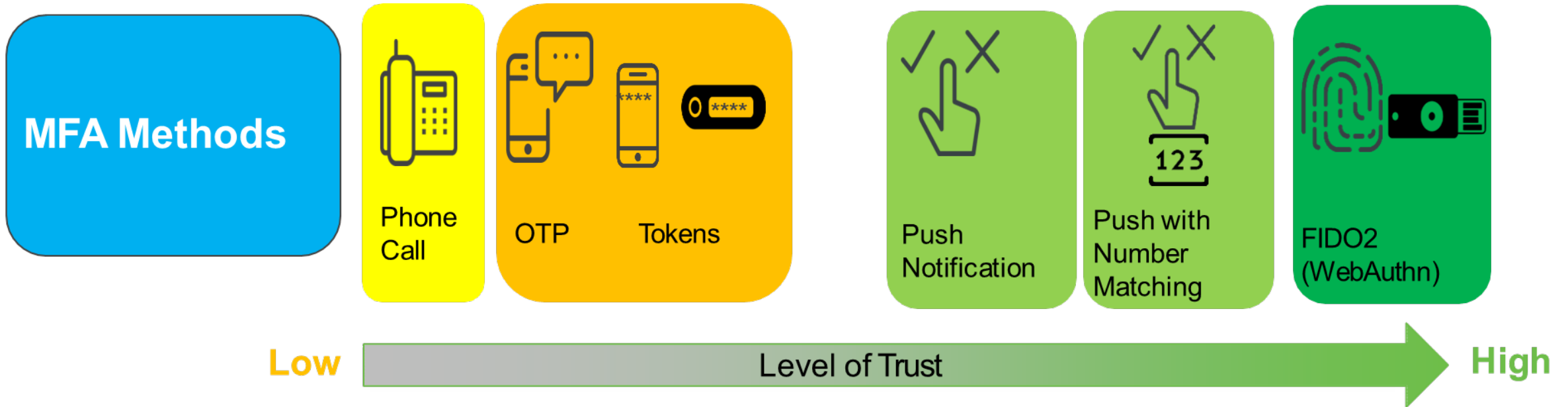
Enforce policies for
every access attempt

WITH

Adaptive & role-based
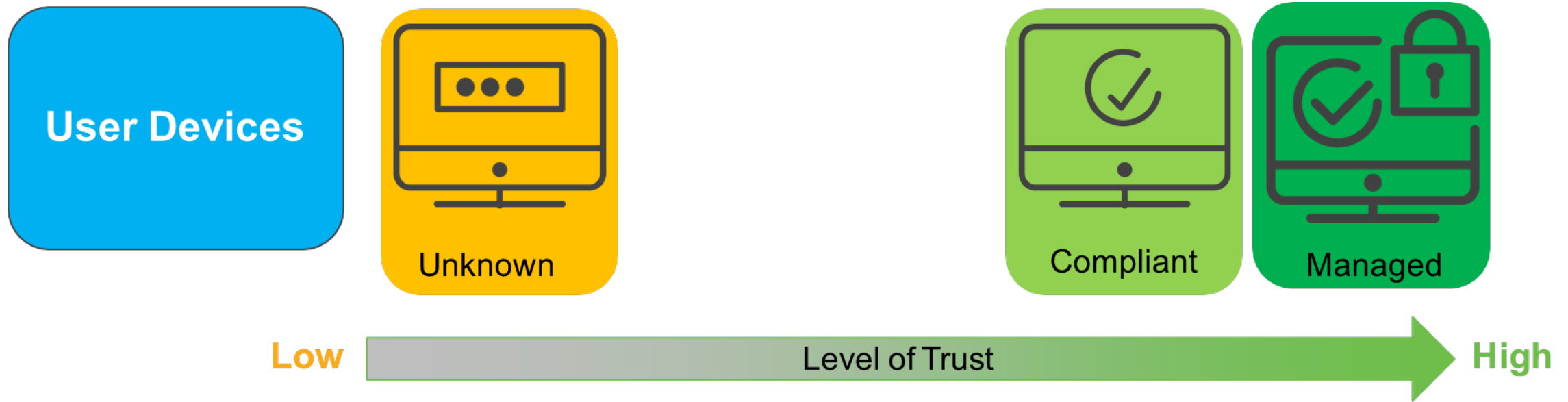access controls

Stronger MFA Methods means Stronger Trust
Choose Strong MFA methods
for User Authentication & Device Enrollment

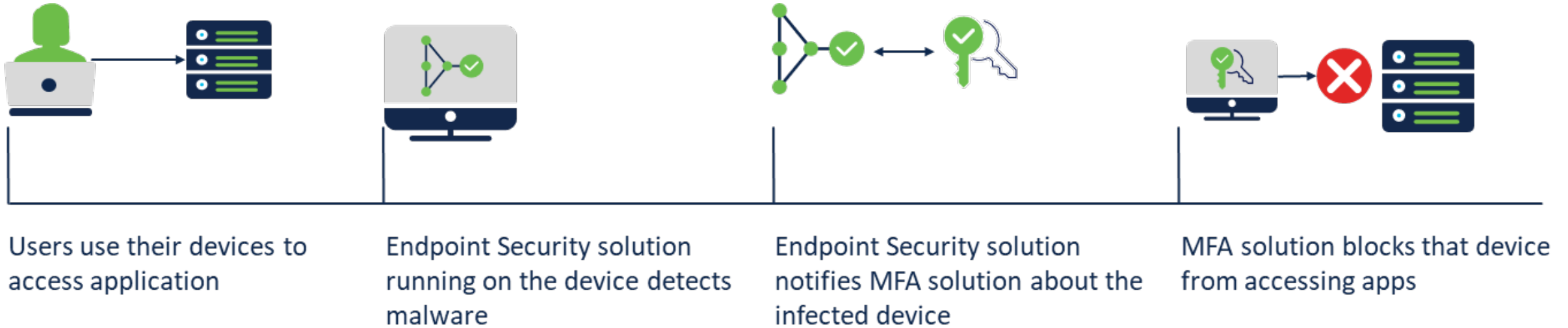# Strengthen Device Trust by increasing level of Management
Prevent Attackers
from using their device to access your applications

User Devices

Unknown

Compliant

Managed

Low ───────── Level of Trust ───────── **High**

Assess Security Posture Endpoint Use Case

Keeping compromised devices from accessing resources

Users use their devices to access application

Endpoint Security solution running on the device detects malware

Endpoint Security solution notifies MFA solution about the infected device

MFA solution blocks that device from accessing apps

Cisco's Zero Trust capabilities

Establish Trust

- User / device / service identity
- Posture + context
- Risk-based authentication

Enforce Trust-Based Access

- Micro-segmentation
- Unified access control
- Least privilege + explicit trust

Continuously Verify Trust

- Re-assessment of trust
- Indicators of compromise
- Shared signals
- Behavior monitoring — threat and non-threat activity
- Vulnerability management

Respond to Change in Trust

- Prioritized incident response
- Orchestrated remediation
- Integrated + open workflows
- Visibility and observability

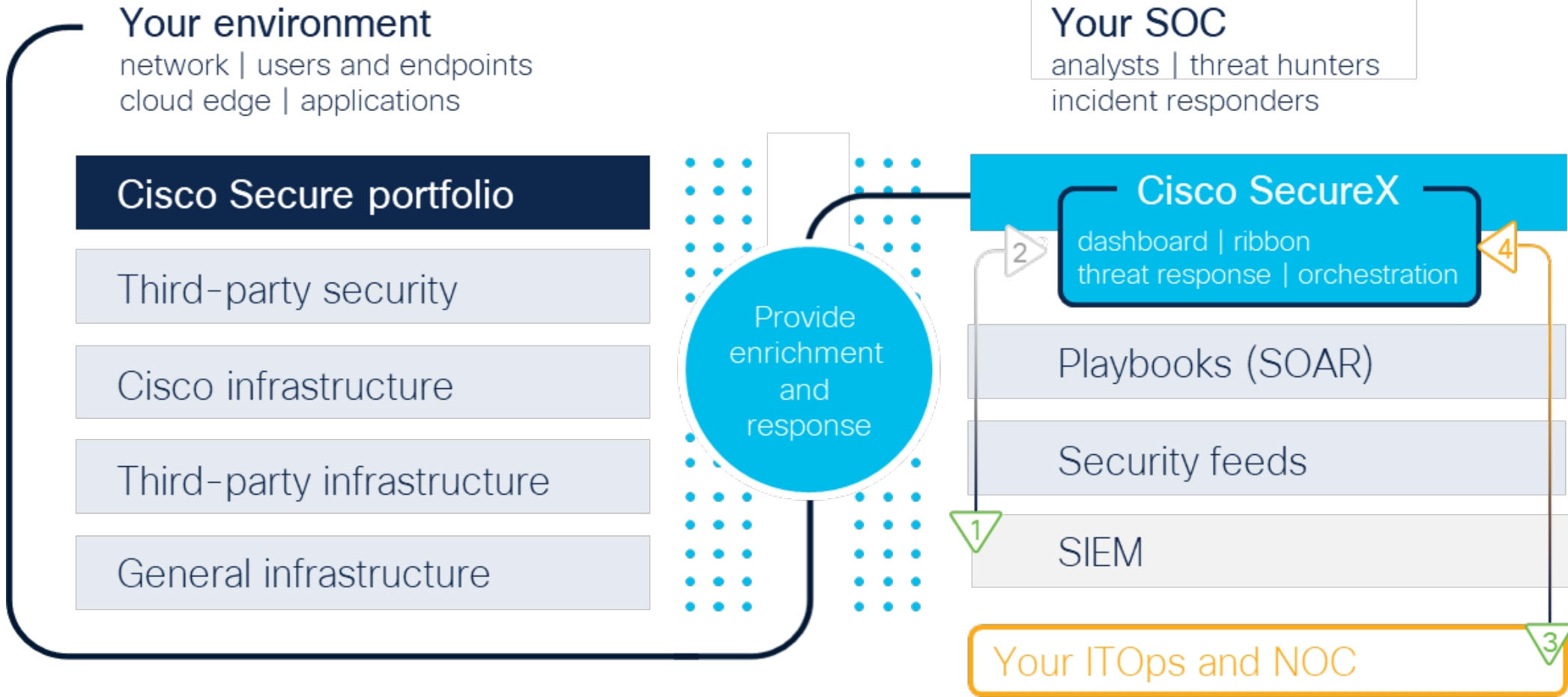**User & Device Security**

Network & Cloud Security

Application & Data Security

SecureX Trust Monitor Dashboard Tile
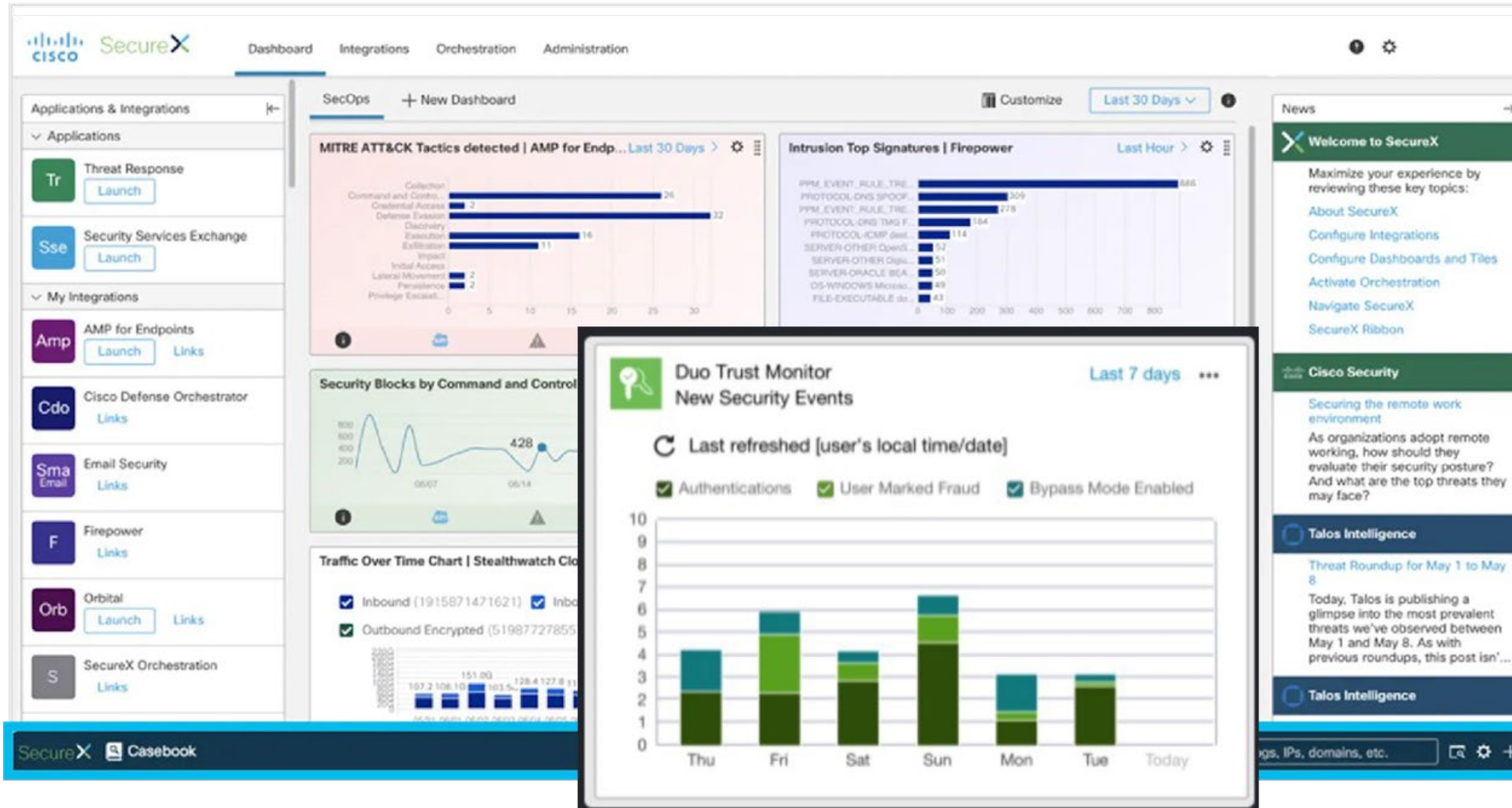
SecureX seamlessly **integrates** into your SOC

Space Hellas Cybersecurity Services

- 24x7 monitoring of the infrastructure (via SoC)
  - Certified Security Experts
  - Threat Intelligence
  - Automated Response
  - Vulnerability Management
- Hands on attack mitigation
- Incident Response
- Penetration Tests
- Vulnerability Assessment as a Service
- Digital Forensics / Malware Analysis

Why Space for Partner

- 35+ years in the market
- Cisco Gold Integrator partner
- Financially healthy ('longevity')
- Customer loyalty
- Integrated Security (holistic approach)
- Experience, know-how

CISCO
Partner
Gold Integrator