Accelerate Your Journey to Zero Trust

Arun Joshi
CIO for ASEAN, CGEM (AMER)

Jeff Yeo
Regional Technical Solutions Architect,
ASEAN and Greater China

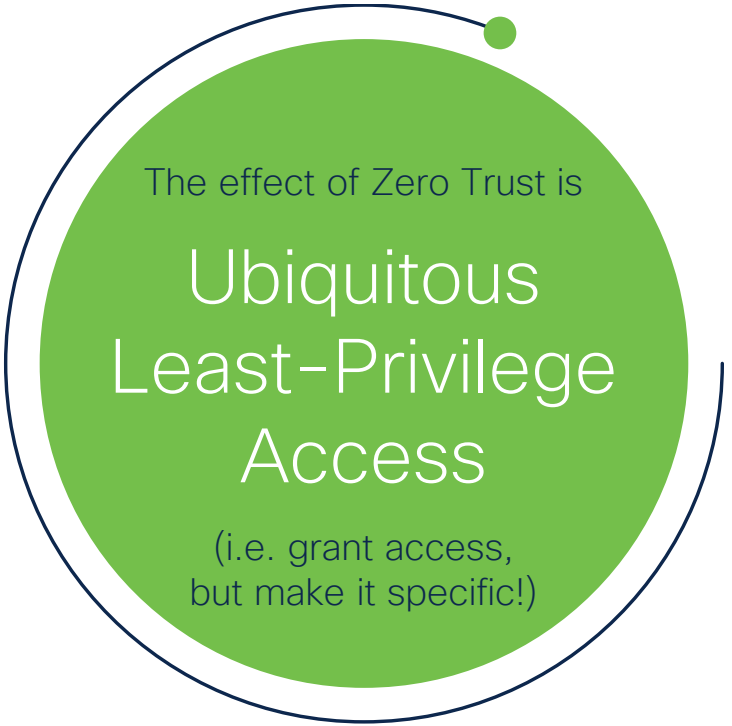
Agenda

- What is Zero Trust?
- Cisco IT Zero Trust Strategy
- Architecture
- Challenges
- Key Takeaways & Lessons Learned

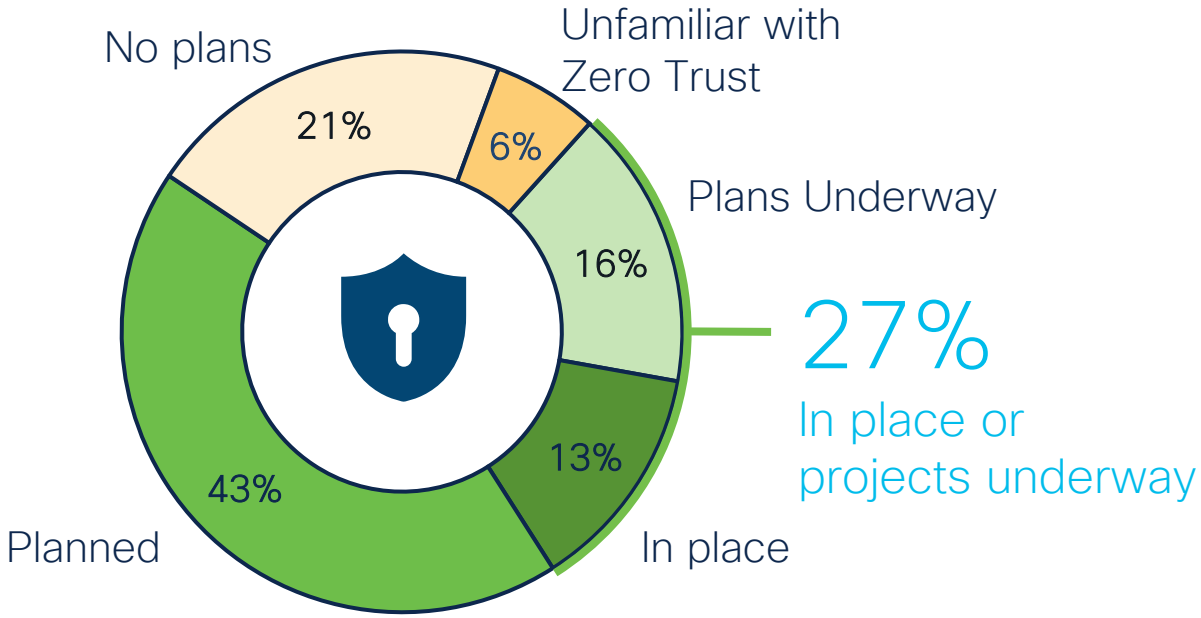
What Is Zero Trust?

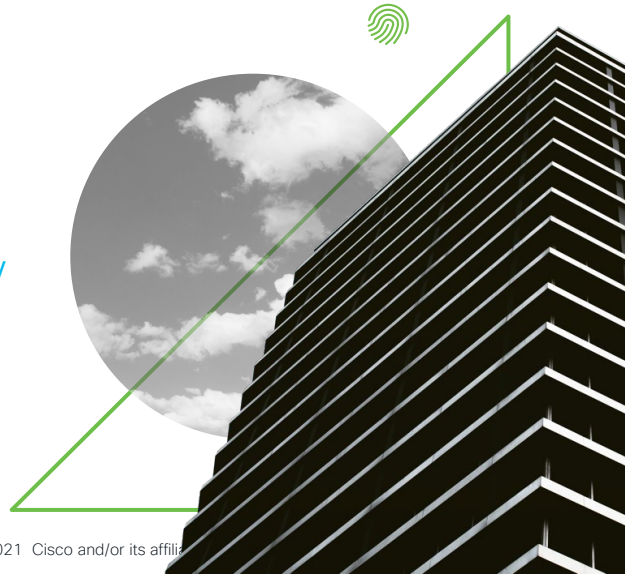
Five Fundamental Assertions of Zero Trust

- The network is always assumed to be hostile
- External and internal threats always exist on the network
- Network locality is not sufficient for deciding trust in a network
- Every device, user, and network flow is authenticated and authorized
- Policies must be dynamic and calculated from as many sources of data as possible



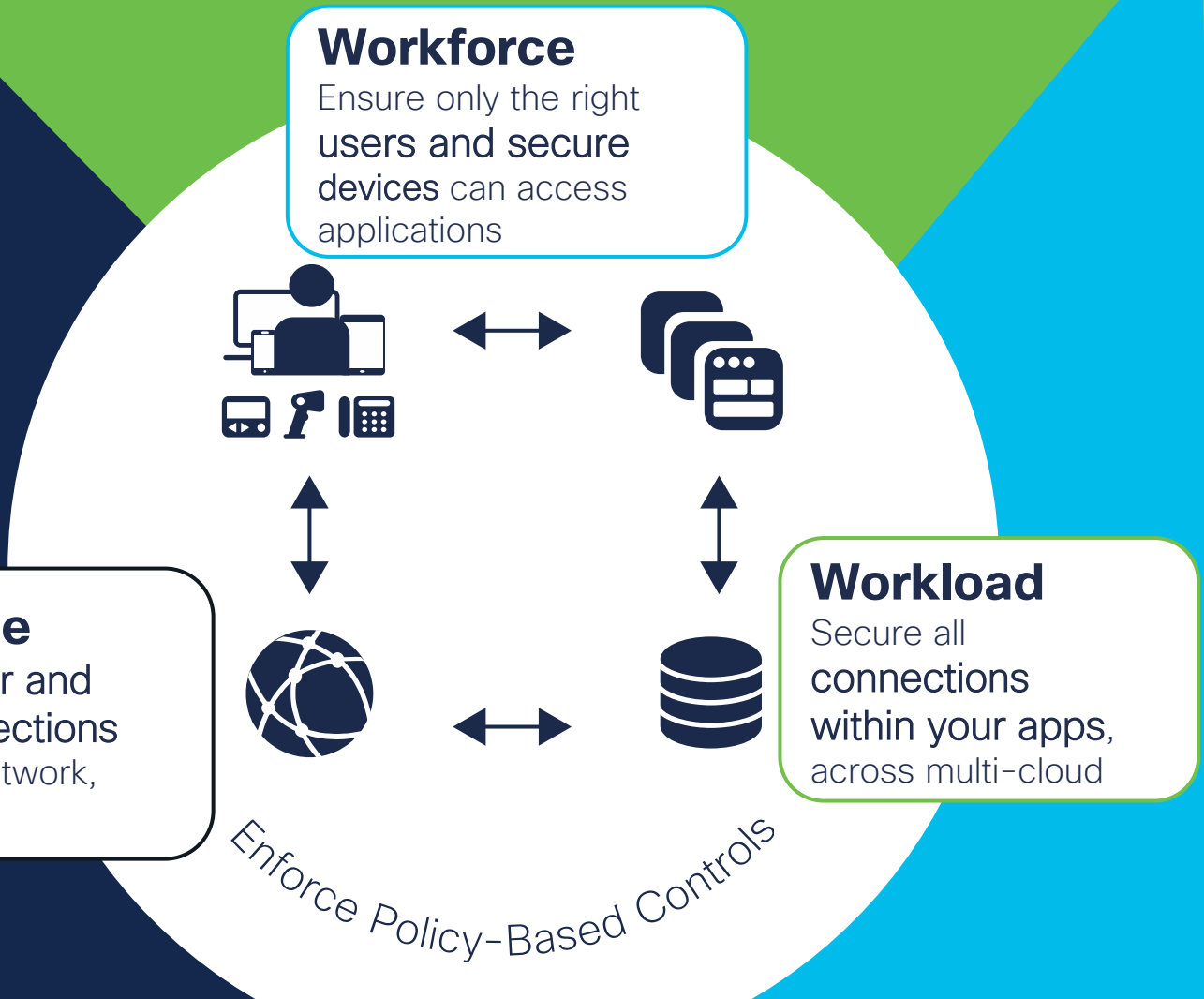
73% of Organizations Plan to Implement Zero Trust





Cisco Zero Trust

A zero-trust approach to secure access across your applications and environment, from any user, device and location



Incremental Implementation

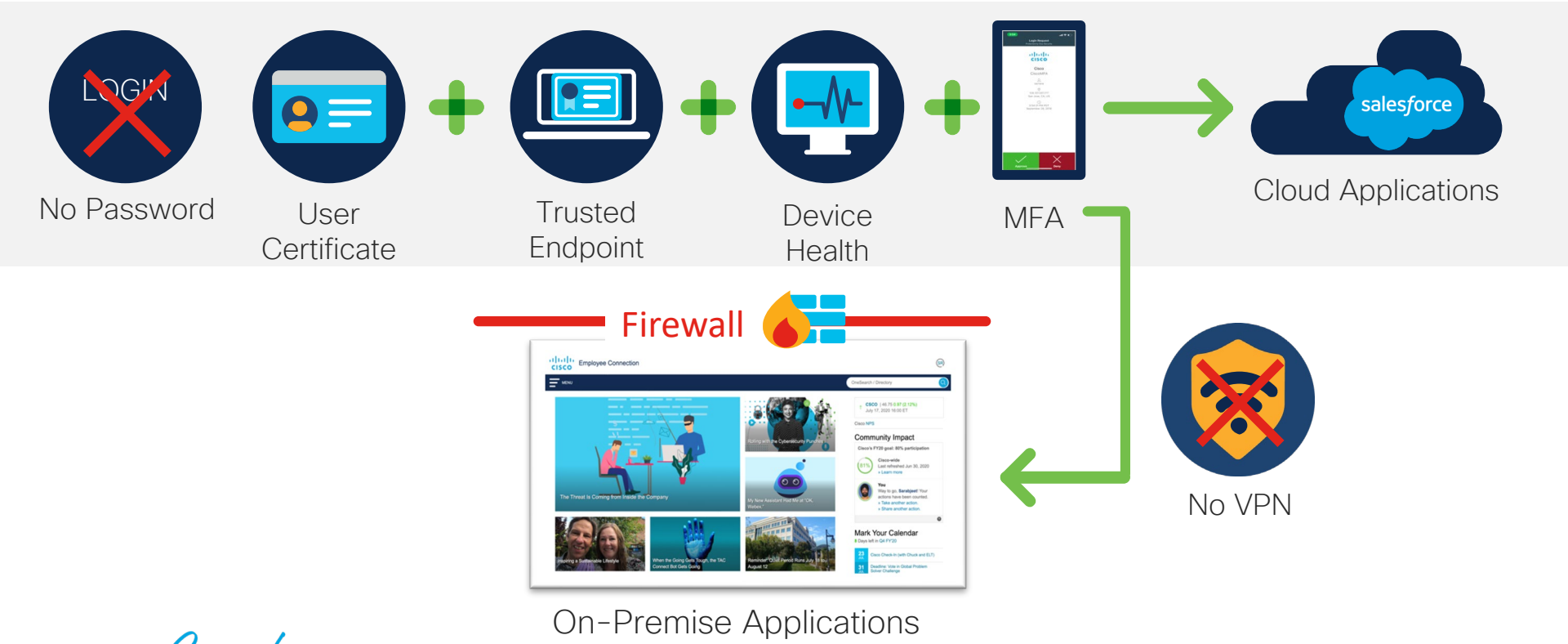
> “Implementing a ZTA is a journey rather than a wholesale replacement of infrastructure or processes.”

NIST SP 800-207, “Zero Trust Architecture”
https://csrc.nist.gov/publications/detail/sp/800-207/final

Cisco on Cisco Approach to Zero Trust

CISCO Connect ASEAN

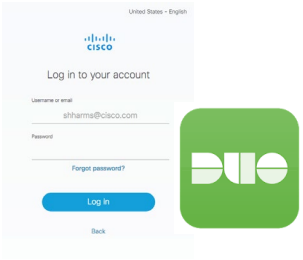
Zero Trust:
Borderless Access with Improved Authentication

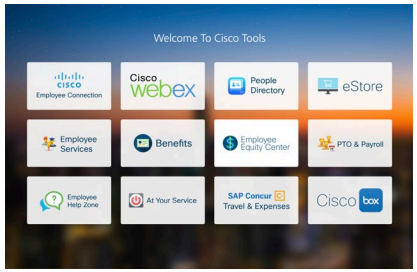


Duo MFA adoption in Cisco:

Cisco on Cisco

Single Sign On with Duo





Borderless Access to O365

Office 365

VPN with Duo

Multiple *options for the users.*

Duo Push

SMS code

Voice call

Mac TouchID

+

Tokens
Touch to Authenticate

+

Digipass

Based on availability
Limited browser support

Limited
Exception only

Challenges

Applications	• Infosec requirements • Application dependencies
Infrastructure	• Timeline to deploy highly available infrastructure
Endpoint	• Complexity in deploying a variety of endpoint configurations • Achieve a seamless user experience
Overall	• Aggressive timelines

Security outcomes & benefits

Cisco's security outcomes

- 100,000+ users and 120,000 devices secured
- <1% of users contacted help desk
- 2.6 million health checks per month
- 48,000 devices per month remediated
- 260,000 auths/month through DNG (VPN-less)

With Zero Trust, Cisco can

- Require that only managed devices can access certain applications with Trusted Endpoints
- Know if a login attempt is unusual, abnormal and possibly fraudulent with Trust Monitor
- Make sure users' computers are safe and let users know how to update them with Duo Device Health app
- Block risky logins from unknown or unsafe devices, geographies or networks with adaptive access policies that are customizable per application
- Provide users one location to access all of their applications with the Duo Central feature or Duo's SSO
- Securely allow borderless application access without a VPN using Duo Network Gateway

Key takeaways and lessons learned

Executive Buy-in/Sponsorship

- 'Air Cover' enables team to be bold and move quickly

Introducing Zero Trust principles to organization

- Share benefits to employees/leadership
- Start small, gain experience, expand (ex. start with a pilot and solicit feedback, monitor mode first before full enforcement)

Lean team structure for the cross functional team

- Ensure you have empowered individuals who can make decisions on behalf of their organization

Active communications

- Ensure you have the ability to respond publicly to public input/critique (ex. via internal employee forums, chat rooms, etc)
- Leveraging a weekly newsletter directed to stakeholders creates momentum and sense of urgency

Zero Trust Service Journey

Define future state, Identify priorities, Develop actionable roadmap

- Defined organizational Zero Trust capabilities
- Current and recommended target Zero Trust state
- Considers more than just technology
- Highlights the value of moving to that future state
- Multi-year, actionable roadmap is provided, identifying key milestone projects that bring alignment to Zero Trust
- Recommendations for year 1 are easier to achieve, boost security and deliver quick wins

Zero Trust Strategy Service

Architect, design and implement Zero Trust capabilities

- Carry out initiatives and work packages as defined in your Zero Trust roadmap
- Move through maturity phases by gaining visibility into user and device activity, network, applications; their posture and communication flows.
- Define and enforce granular, adaptive (micro)segmentation policies.
- Design and implement efficient and effective SOC services

Segmentation Advisory Service
SOC Advisory Service
Design and Implementation Services

Optimize and Improve, Manage risk

- Continuously improve your Zero Trust capabilities through automation and integration
- Identify potential new threat vectors; perform risk reviews against changing context
- Increase your preparedness to respond to Security Incidents.
- Improve staff skills and abilities to effectively detect and manage security incidents.

Business Critical Services
Threat Hunting Service, Secure Range
Incident Response Services