



# Reimagining Small Business in a Cloud Connected World

Subtitle goes here

Aseem Javed  
ASEAN Small Business Architecture Leader



*“Companies are adapting quickly to the new work from home reality and many will adopt a **hybrid model** to support both on- and off-site work environments.”*

Chuck Robbins – Cisco Systems CEO

# Pandemic accelerated key technology trends for Small Business

“What used to take a decade now took 8 weeks<sup>1</sup>”

Ecommerce grew to 27% of retail in March/April from 6% - >16% in past 10 years



Videoconferencing platforms saw growth of up to 30X



Cloud Services grew 30-50% during pandemic months

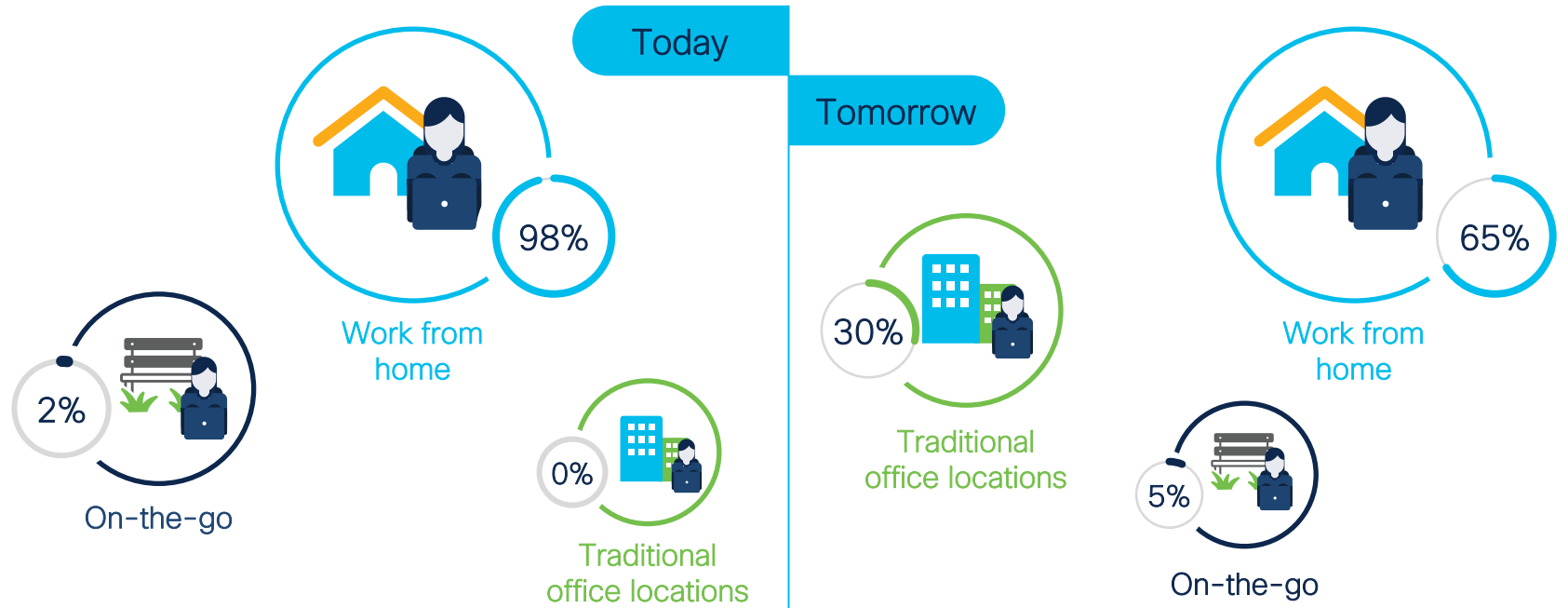


Cybersecurity top of mind – cyberattacks spiking 600% with work from home



# Cisco Designed enables work flexibility without compromise

Yesterday many SMBs were relying on free-ware  
Today businesses owners must look beyond temporary solutions



# Why Cisco Designed?

Simple



End-to-end simplicity  
Easy to try, buy  
and use

Secure



Protecting small business  
with easy-to-use  
enterprise-grade security

Flexible



Tailored solutions for all  
small business needs

Curated for small business



## Connect

Meraki  
Cisco Business Portfolio  
Catalyst 1K  
Routing  
Wi-Fi 6



## Compute

Hyperflex Edge  
UCS  
Intersight



## Collaborate

Webex  
Hand/Headsets  
Video Endpoints



## Secure

Duo  
Umbrella  
AnyConnect  
ASA/Firepower  
AMP

*Products and Services Designed and Curated for Small Businesses*

# Technology Trends for SMBs

## SASE for SMBs

Secure Access Service Edge (SASE) is a cloud-delivered service that aggregates Cisco's Network and Security functions to address the needs of today's hybrid workforce.

# SASE for SMBs

A cyclist in a blue jacket and helmet is riding away on a paved road that curves through a landscape of rolling hills and a winding river. The sky is a mix of blue and orange, suggesting a sunset or sunrise. The overall scene is peaceful and scenic.

## Pandemic accelerated cloud adoption for SMBs

- Cloud services proved valuable for organizations that needed to adapt to the pandemic on short notice
- 30-50% increase in cloud adoption

## Users are dispersed

- Remote Work is here to stay
- 98% of Small Businesses with employees working from home

## Applications are everywhere

- 60% of organizations expect majority of apps to now be hosted in cloud
- Faster deployment, lower costs, subscription-based model with low upfront investment





## SASE for SMBs

You don't have to be a technology expert or have big IT budget to get started with SASE

Even if you don't have a large (or any) IT team, you can do it. But you need tools that:

Work well together

1

2

Simple to maintain

Improve Productivity

3

4

Omni-Present Security

# Cisco's three Cs for SASE

## Connect



Deliver secure, seamless connections to applications anywhere (SD-WAN)

## Control



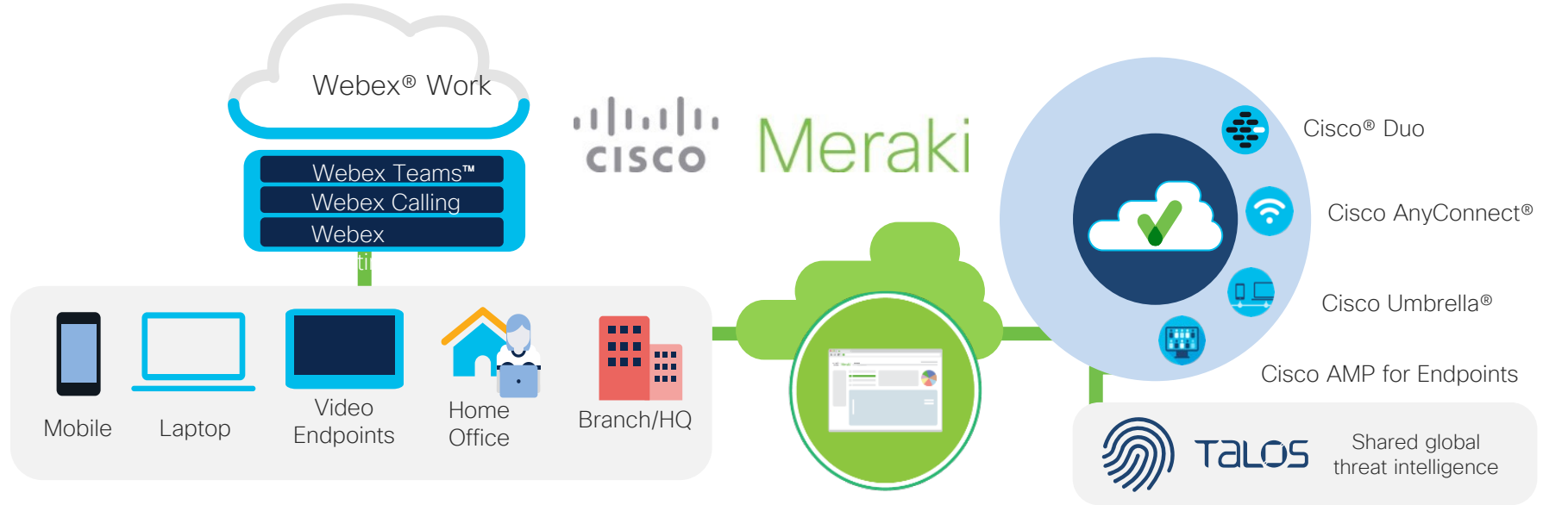
Establish zero trust access and leading threat protection (CASB, FWaaS, ZTNA)

## Converge



Integrate cloud-delivered networking and security

# SMB's Architecture Blueprint



Simple, smart collaboration  
from anywhere

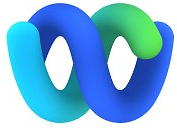
Secure cloud-managed  
networking

100% cloud-delivered; no on-  
site IT required

# Collaborate Easily and Securely

CISCO *Connect* ASEAN

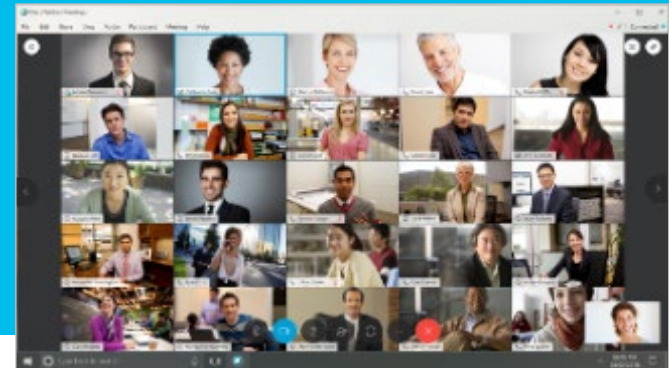




# Cisco Webex® Meetings

## The #1 Web conferencing platform in the world

- Easy to use
- Strong security and privacy
- Video-first experience
- Anyone can join from any device
- Easily share content
- Record meetings
- Integrates with your apps



*“Privacy is a fundamental human right, and we need security and transparency to protect it.”*



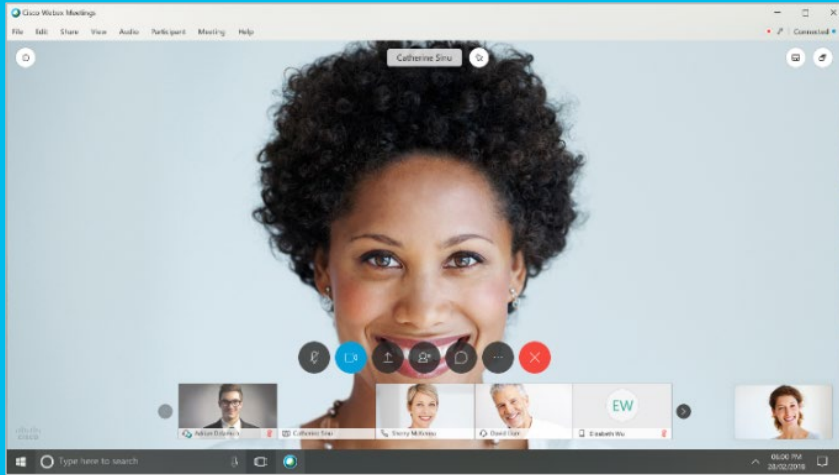
Chuck Robbins  
Chairman and CEO, Cisco  
February 7, 2019

## Three Security Principles:

Privacy, Security and Transparency

1. Committed to the **privacy** of your data
2. Secure **by design** and **by default**
3. **Transparent** about security

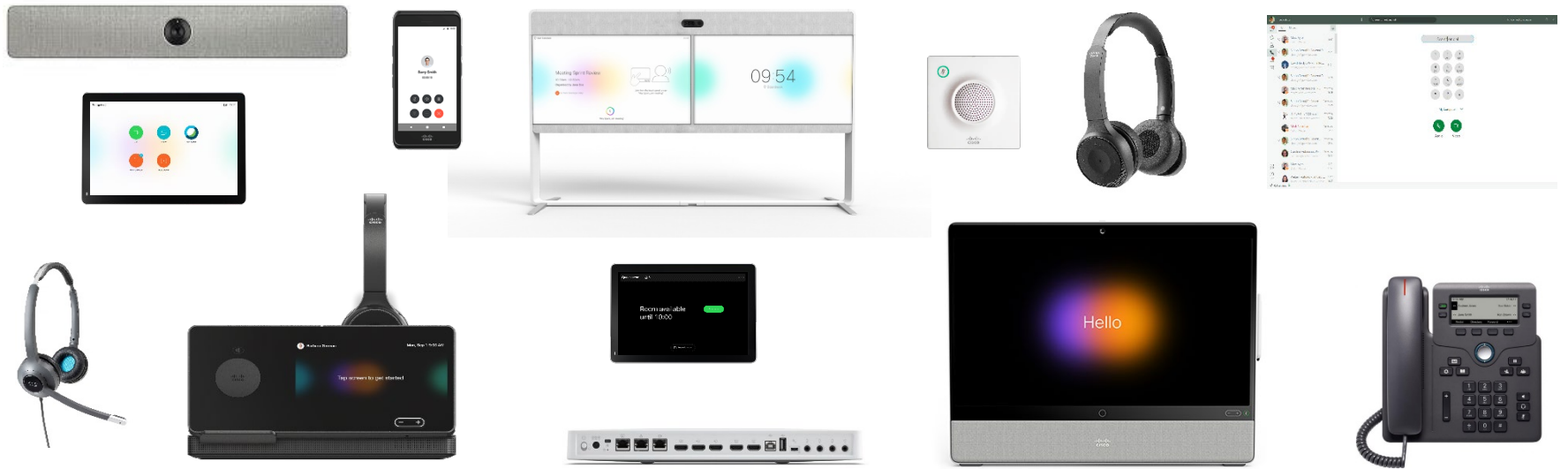
# Make Sure Your Videoconferences Are Secure



Video conferencing makes communication easy, but it needs to be:

- **Secure** with built-in encryption to protect the privacy of both the data in use and in transit
- **Easy to use** with one-click sign-on, high-quality video, and simple screen sharing
- **Flexible** so you can participate from browsers, mobile, or video room devices—even third-party devices
















# Time to bring all of this together...





# Match Devices to Worker Type & Style

## Workstyles

		 Collaborators	 Communicators	 Concentrators
Worker Type	 Fully Remote			
	 Hybrid			
	 Office Resident			

# Comprehensive Portfolio: Video Endpoints make the experience more immersive

## Collaboration Room Video



Webex Room 55



Webex Room 55D



Webex Room 70S G2



Webex Room 70D G2



Webex Room Panorama



Webex Board 55S



Webex Board 70S



Webex Board 85S

## Co-Creation

## In-Room Sharing



Webex Share



Cisco IP Phone 8845 and 8865



Webex DX80



Webex Desk Pro

## Collaboration Desktop Video



Webex Room Kit Mini  
Webex Room USB



Webex Room Kit



Webex Room Kit Plus



Webex Room Kit Pro

## Collaboration Room Kits

## Headsets



Cisco Headset 500 Series



Cisco Headset 700 Series

## Desktop Voice



Cisco IP Phone 6800, 7800, and 8800 Series

## Wireless Voice



Cisco IP Phone 6825 DECT

## Conference Audio



Cisco IP Conference Phones 7832, 8832

# Don't Skimp on Security



# Top of mind for CXO's

58%

security is  
the  
biggest  
challenge

95%

Say  
cybersecurity  
is important

7.7M

average  
cost of a  
Cyber  
Incident

You can't afford to overlook security when setting up hybrid workspaces. Look for security solutions that:

- Provide secure network access no matter what device people are using
- Protect your sensitive data by verifying the identity of users, devices, and applications
- Defend against threats with cloud-delivered security
- Detect and block cyberattacks

# Keep Your Workplace Safe

**4,000**

Daily attacks

**43%**

Target small business

**62%**

Reported breaches

<https://enterprise.verizon.com/resources/reports/dbir/>

You can't afford to overlook security when setting up remote workspaces. Look for security solutions that:

- Provide secure network access no matter what device people are using
- Protect your sensitive data by verifying the identity of users, devices, and applications
- Defend against threats with cloud-delivered security
- Detect and block cyberattacks

# Threats Today, As a Result

A new approach to security is needed – zero trust – to address identity, app & network threats.

## Workforce



### Targeting Identity

81% of breaches involved compromised credentials

## Workloads



### Targeting Apps

54% of web app vulnerabilities have a public exploit available

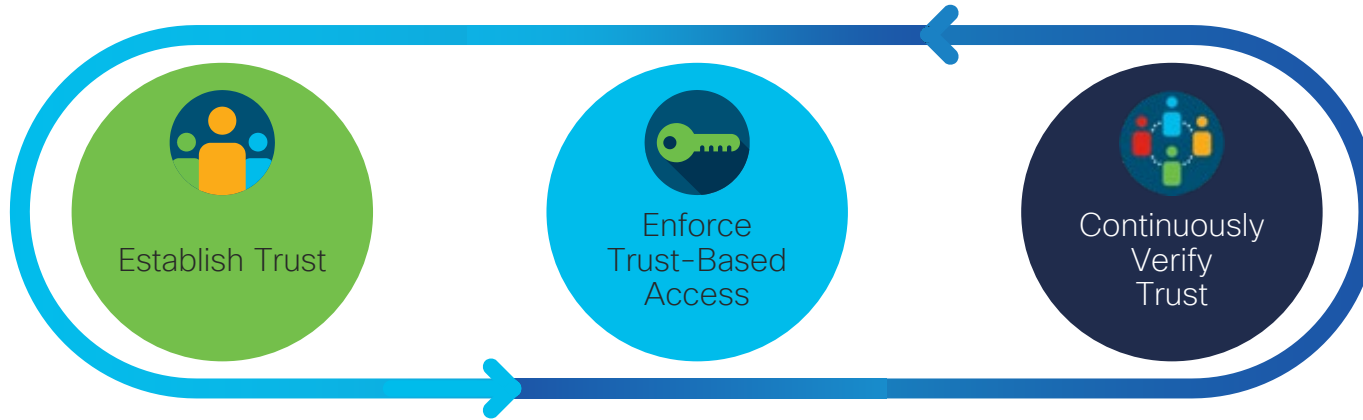
## Workplace



### Targeting Devices

300% increase in IoT malware variants

# Cisco's Implementation of Zero Trust



## We establish trust by verifying:

- ✓ User & device identity
- ✓ Device posture & vulnerabilities
- ✓ Any workloads
- ✓ App/service trust
- ✓ Any indicators of compromise

## We enforce least privilege access to:

- ✓ Applications
- ✓ Network resources
- ✓ Workload communications
- ✓ All workload users/admins

## We continuously verify:

- ✓ Original tenets used to establish trust are still true
- ✓ Traffic is not threat traffic
- ✓ Any risky, anomalous and malicious behavior
- ✓ If compromised, then the trust level is changed

# Secure Authentication

Instantly integrates with all apps

Users self-enroll in minutes

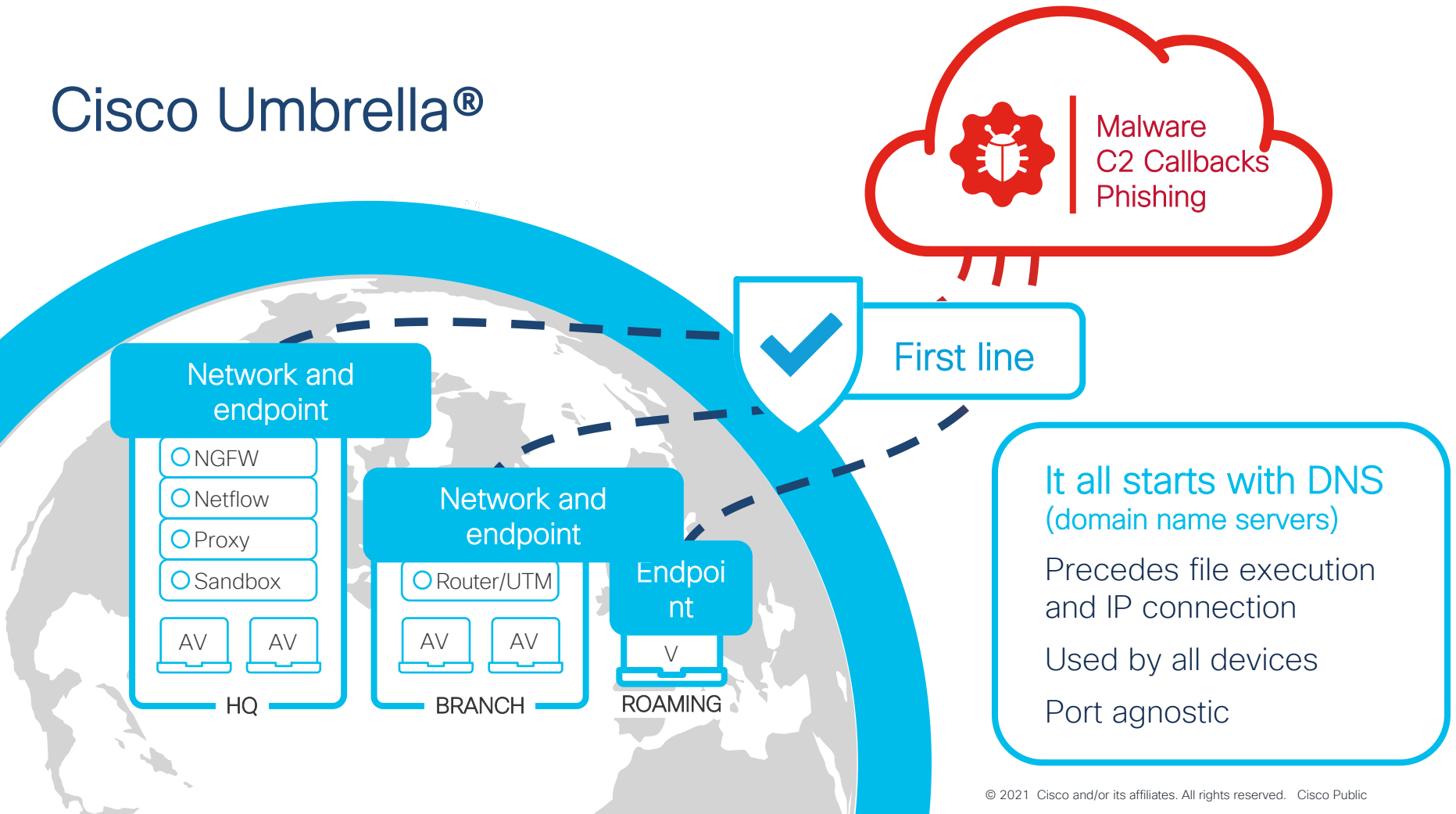
Users authenticate in seconds  
with no codes to enter

Cisco® Duo





# Cisco Umbrella®



# Other noteworthy security solutions for SMB's



[Stealthwatch](#) can detect connections to SMB shares, correlating this activity to alert administrators.



[AMP's](#) continuous monitoring and retrospective security capabilities are ideally suited to keep you safe against attacks such as WannaCry and Nyetya.



Network Security appliances like [NGFW](#), [NGIPS](#), and [Meraki MX](#) can detect malicious activity associated with SMB attacks.



[Threat Grid](#) helps identify malicious file behavior and automatically informs all Cisco Security products.

# Key Takeaways

# Questions to Ask Yourself



Is my current WFH service secure?

How are you communicating with your teams and customers?

Are you able to provision and monitor your network – zero touch provisioning?

Are you prepared by for long term hybrid work?

Are you ready to reopen your offices safely?



Thank you

