The bridge to possible

Resilienz in Netzwerken

07.06.2023

Christoph Koch
CTO/Specialists Lead

Agenda

Setting
the scene

How
do we help?

Resilience
at Cisco

Setting the scene

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

resilience

“the capacity to withstand or to recover quickly from difficulties”

How do we help?

Connect

Secure

Automate

CISCO

Help customers **connect, secure** and **automate** to accelerate their digital agility

©2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Customer Focus, Connected Portfolio

Cross-Architectures

Connect

Technology that is connected provides business resiliency and flexibility

Automate

Platforms with closed-loop visibility, insight and action provide business agility

Secure

Trustworthy integrated solutions with built-in security to keep your users, applications and data secure

©2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Closed Loop Visibility, Insight and Action

Monitoring & Analytics enable AIOps

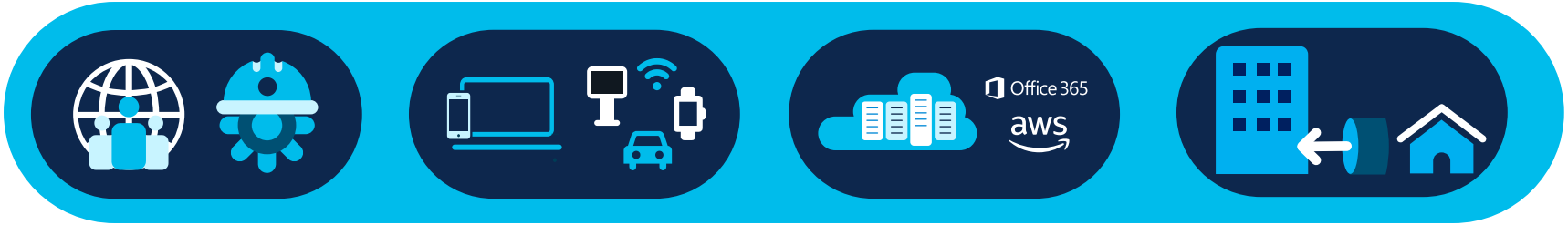
Application

Data Center

Network

©2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

What customers are asking for...



Any User
- Employee
- Contractor
- Partner

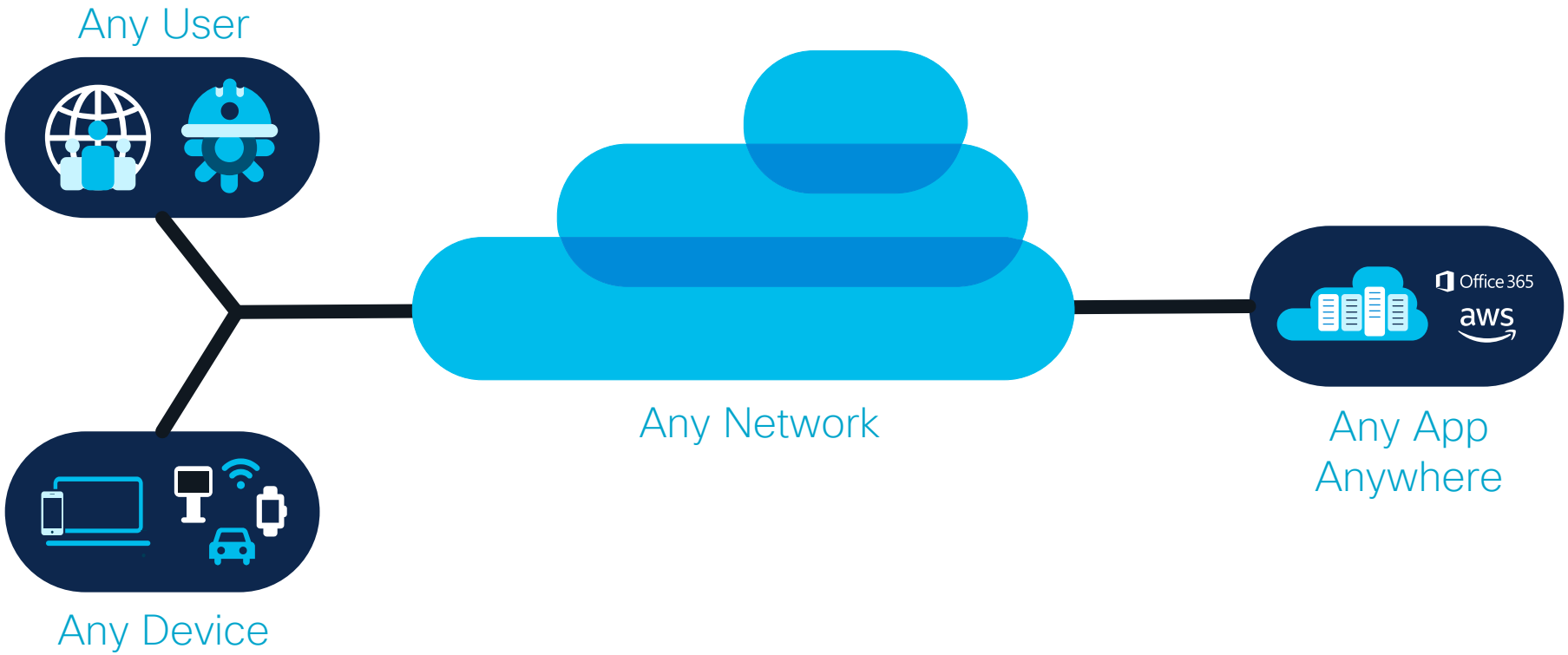
Any Device
- Corporate-Issued
- Bring-Your-Own
- IoT

Any App
- Data Center
- Multi-Cloud
- SaaS

In Any Location
- On-Premises
- On-VPN
- Off-Network

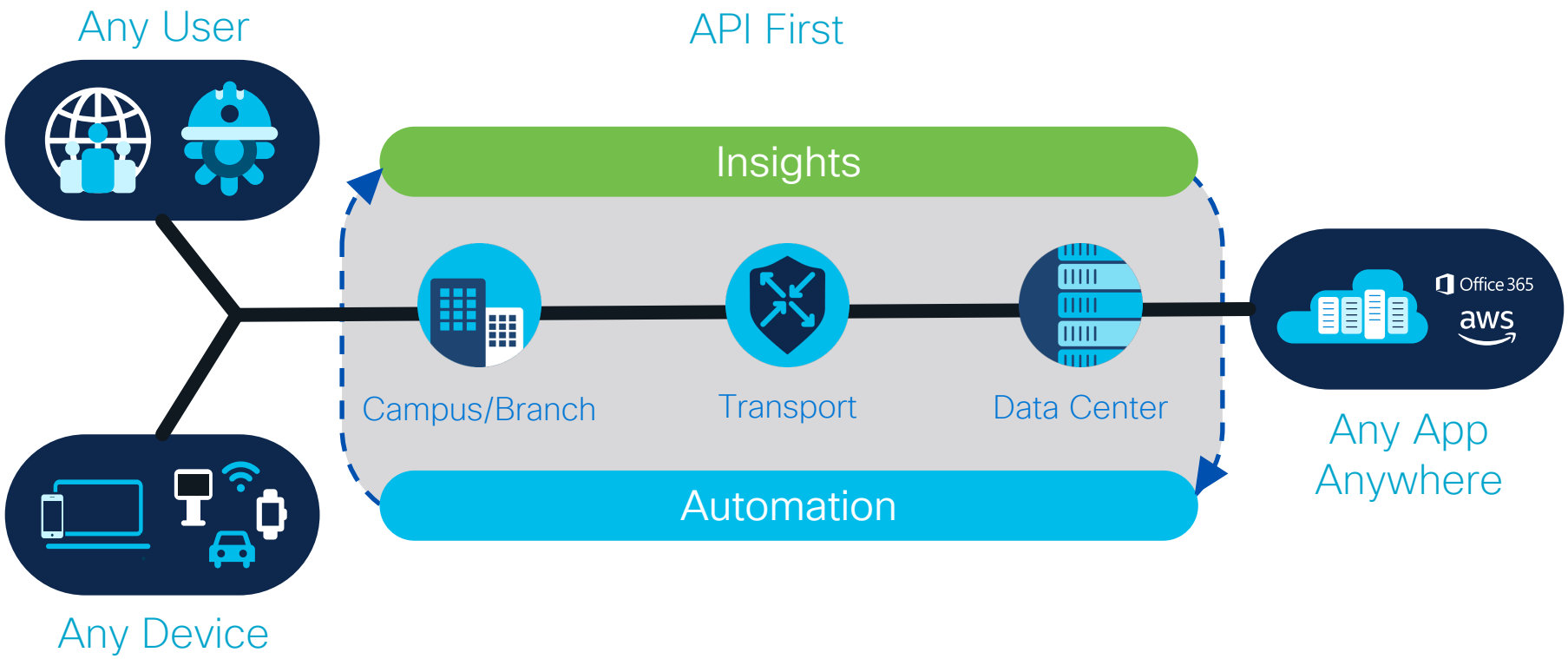
©2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cisco Strategy



©2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Intent-Based Multidomain Architecture

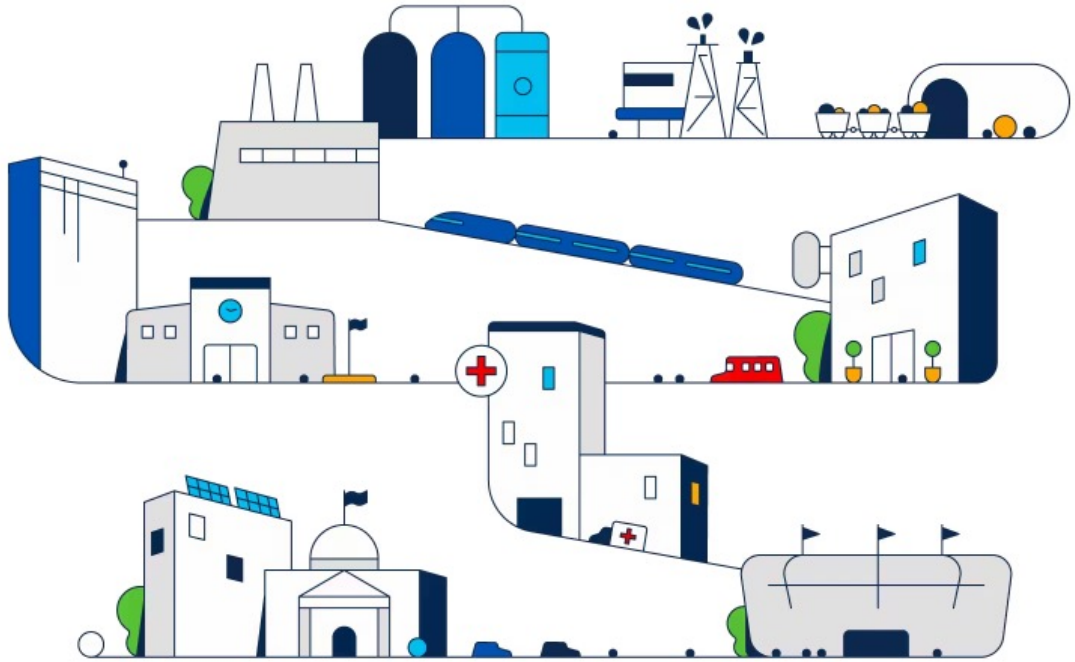


©2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cisco portfolio explorer

Explore the use cases and architectures that are making a difference in your industry.

Education	Financial Services
Government	Healthcare
Manufacturing	Mining
Oil and Gas	Retail
Smart Buildings	Sports, Media, and Entertainment
Transportation	Utilities



https://www.cisco.com/c/m/en_us/solutions/industries/portfolio-explorer.html

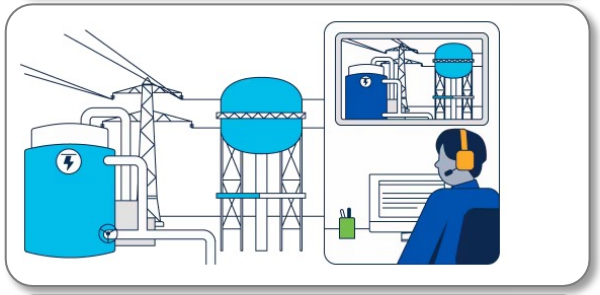
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

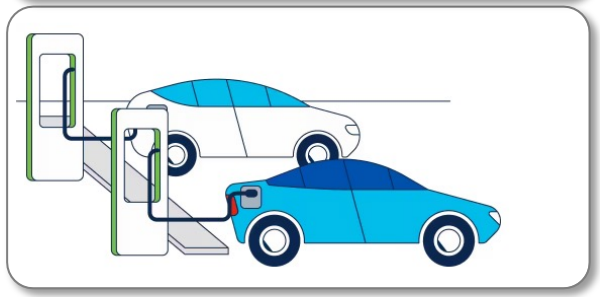
Cisco portfolio for utilities: What can we help you solve today?

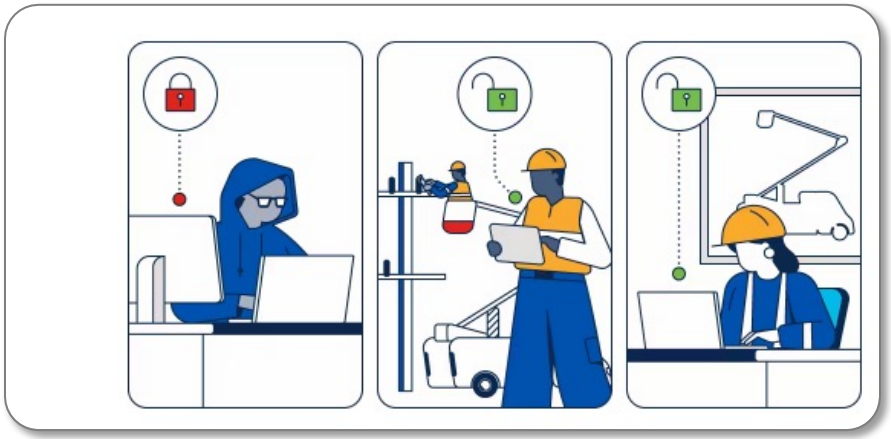
Utilities

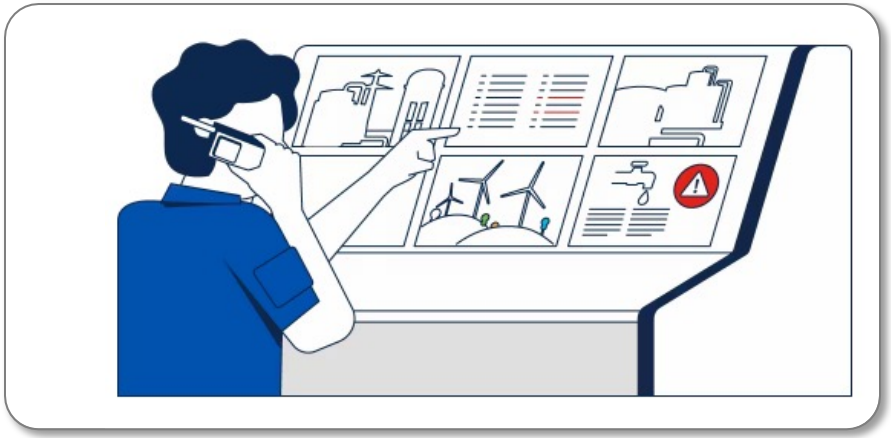
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Use Cases

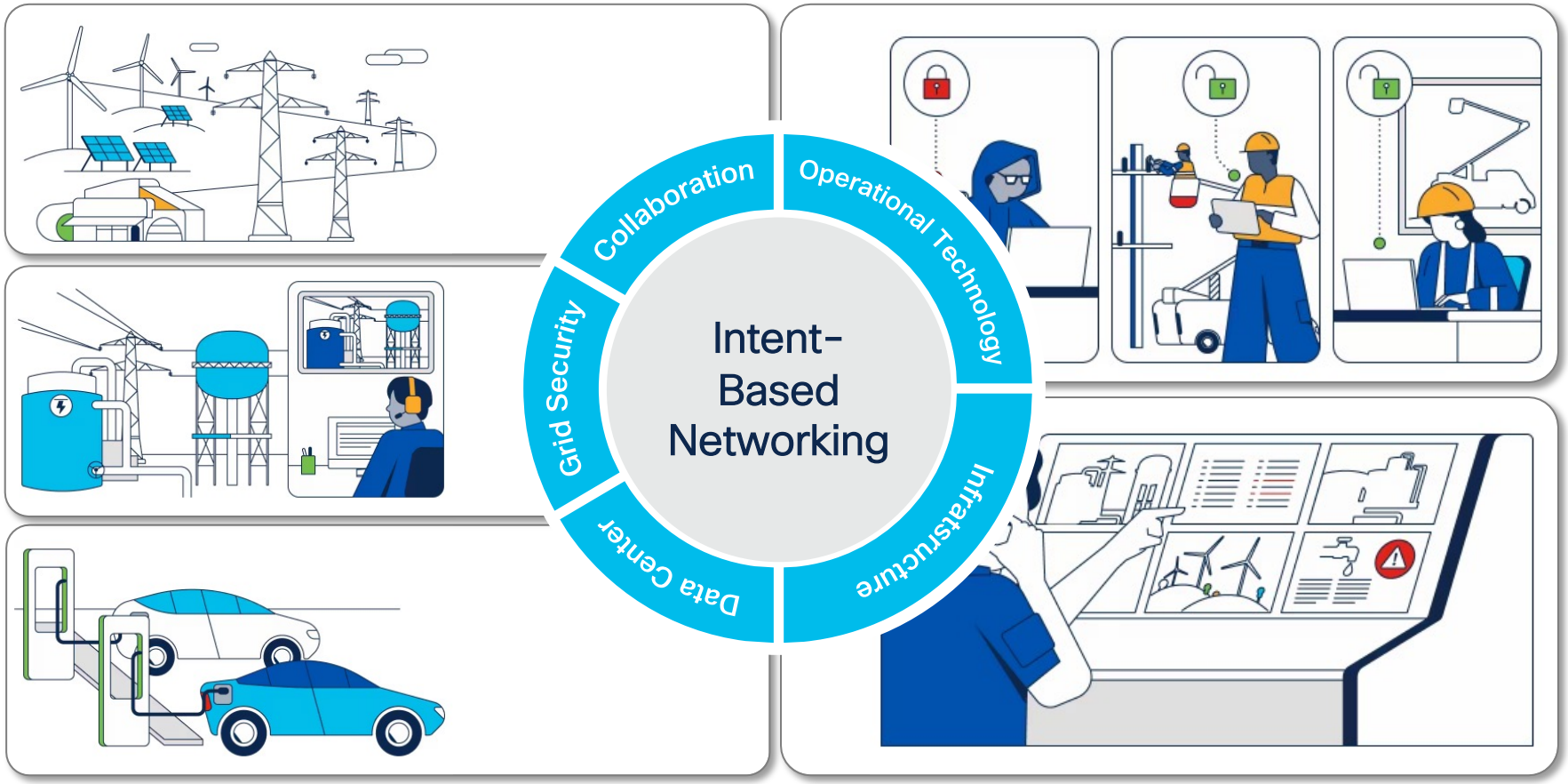




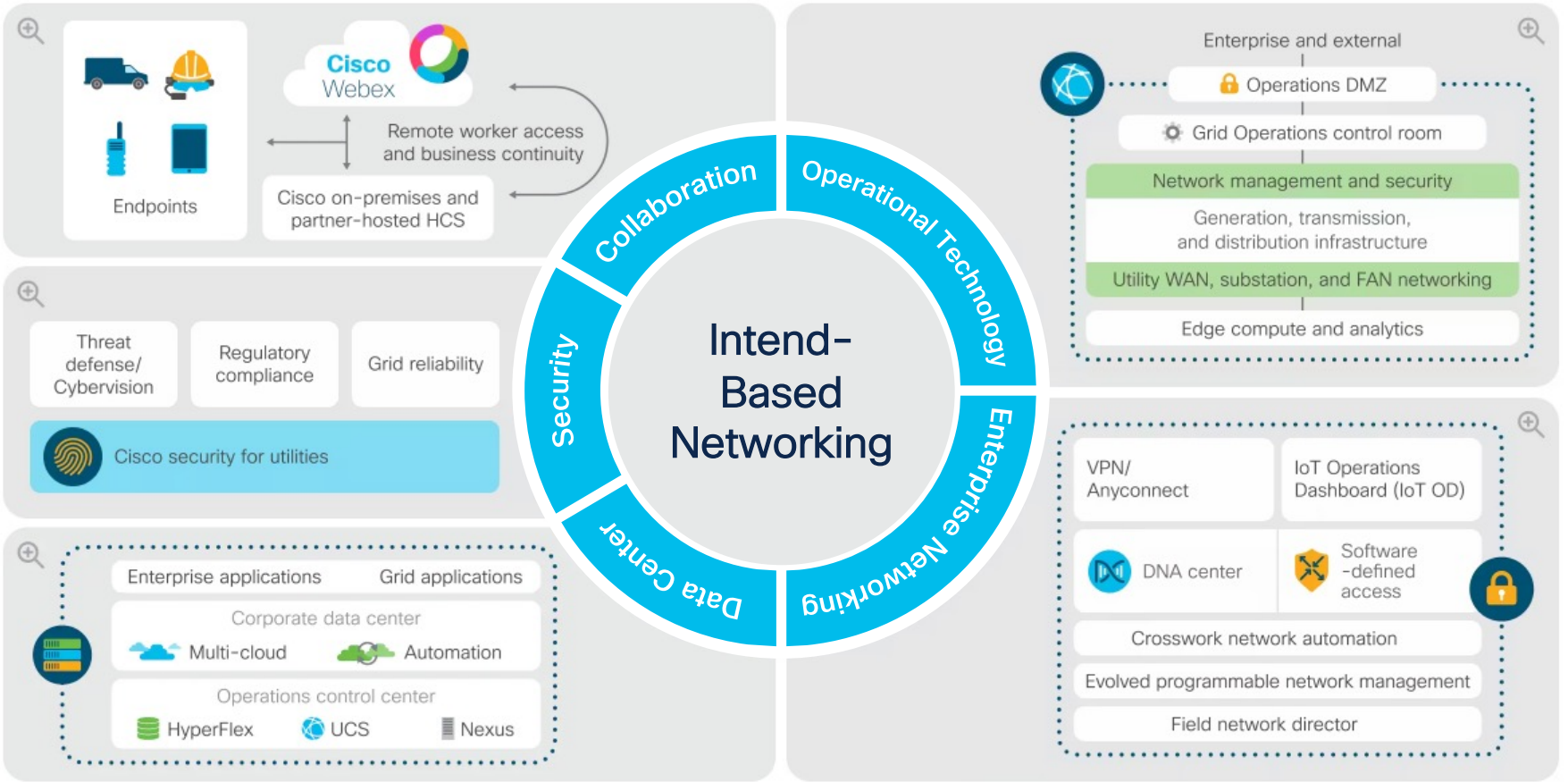




© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Overview – Cisco Solution Groups

Collaboration

Security

Cloud

Enterprise Networking

Data Center

IoT

Service Provider

©2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Overview – Cisco Solution Groups

Collaboration

Security

Cloud

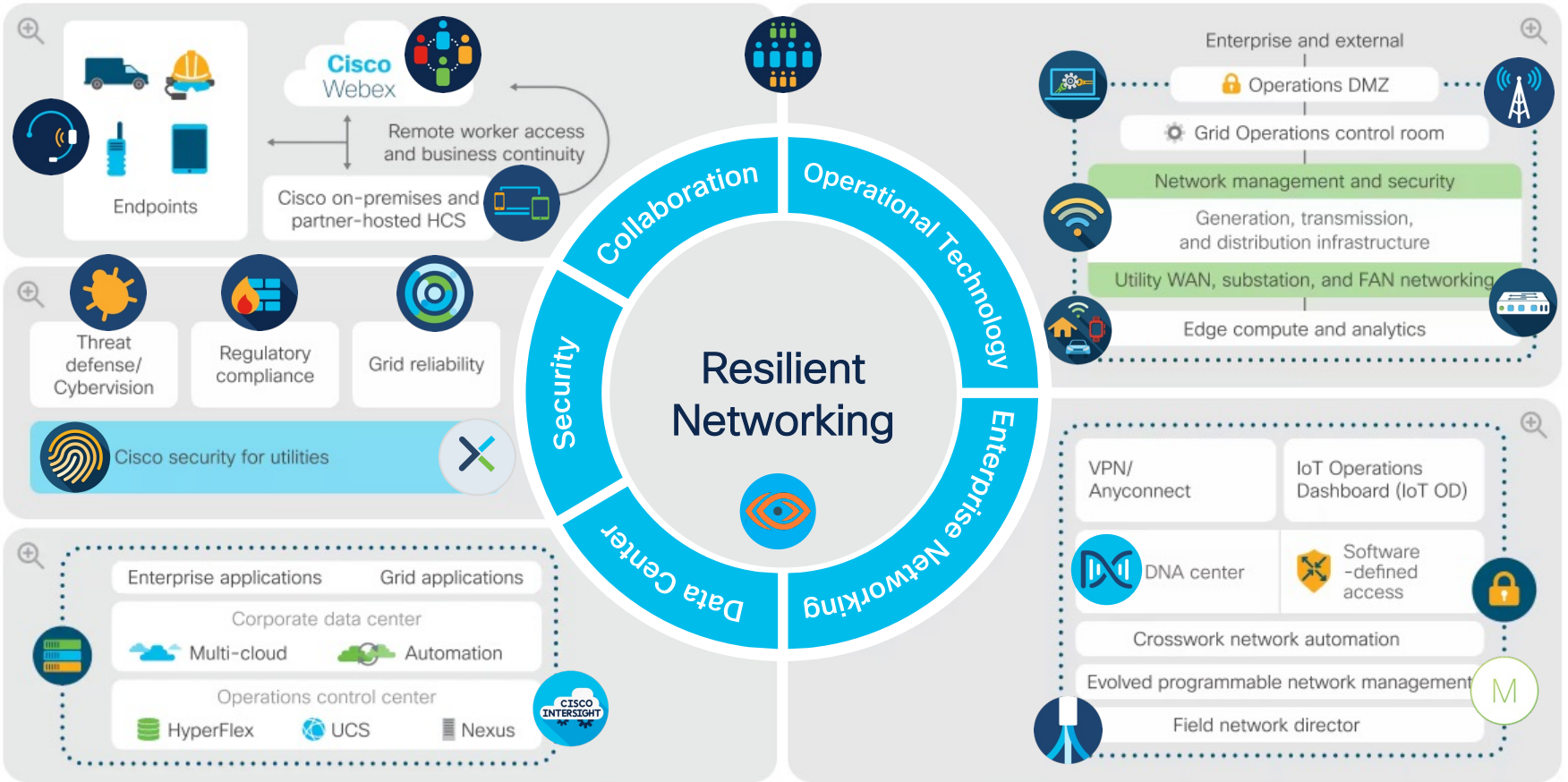
Enterprise Networking

Data Center

IoT

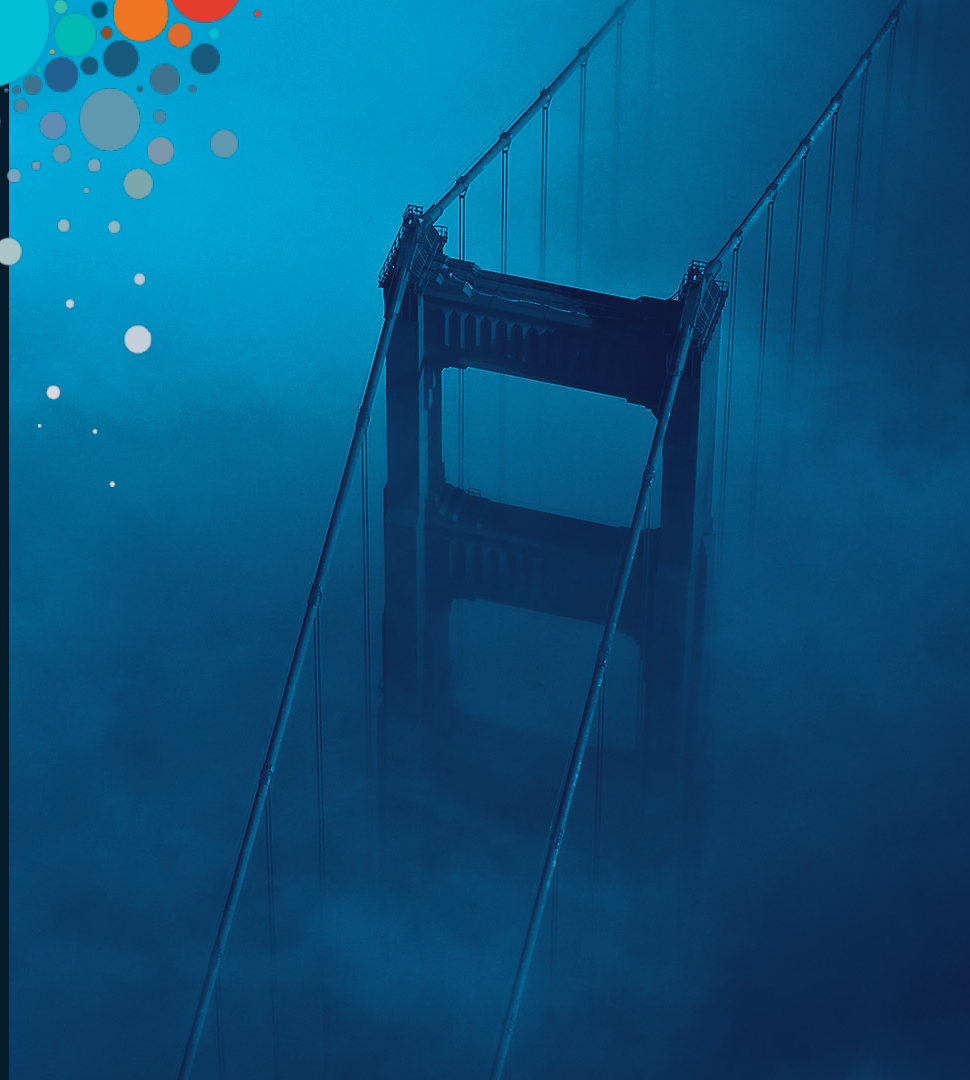
Service Provider

©2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Resilience at Cisco



In a moment. When a connection is made.

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

And in today's world,
it's a million connections...
behind every moment...
behind every opportunity.

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

EXPERIENCES

RELY ON

Connections

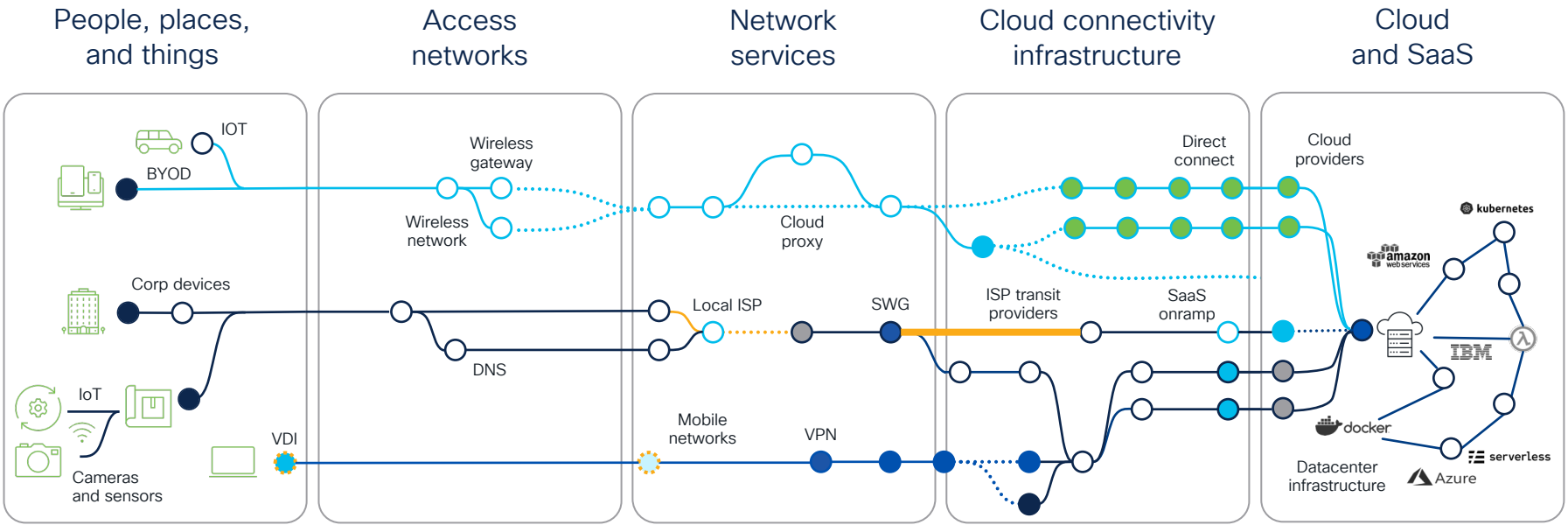
Dynamic
Sustainable
Resilient
Secure
Personal
Safe
Mobile
Personal

Highly variable
Diverse
Flexible
Sovereign
Empathetic
Inclusive
Simpler

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

These connections...

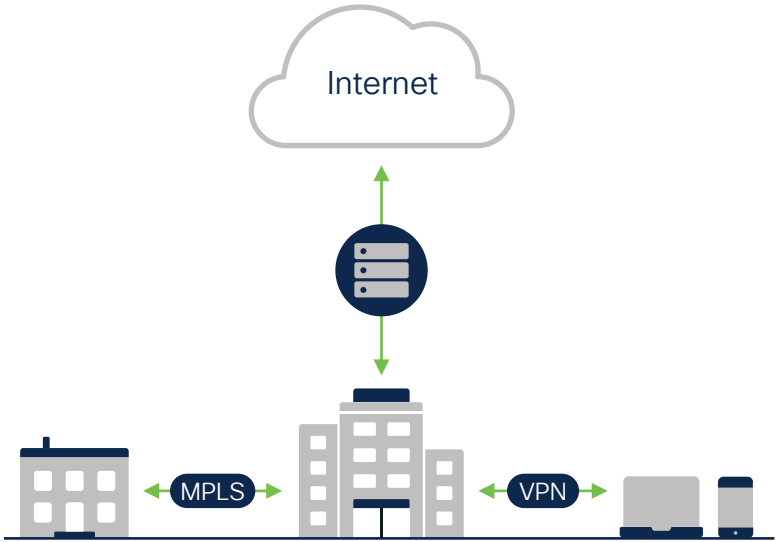
are **more complex** than they appear on the surface



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

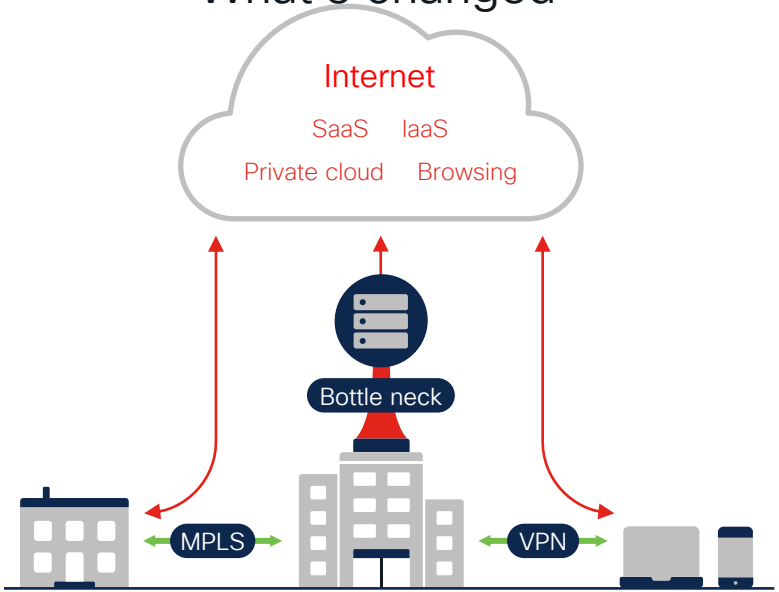
Shift in network traffic and destinations

Before



Apps: Hosted in data center
Users: Connected to corporate network to work
Network: Centralized
Security: On-premises security stack

What's changed



Apps: More hosted in the cloud
Users: More work done off-network
Network: De-centralized
Security: Gaps in protection

Getting Zero Trust right is essential for Cyber Resilience

The ability to protect the integrity of every aspect of the organization's mission to withstand unpredictable threats or changes...

...and emerge stronger.

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Zero Trust means different things to different people

It’s segmentation

It’s ZTNA

It’s endpoint security

It’s firewall

It’s identity

©2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cisco's journey

We've made our $50B global company a test-bed for Zero Trust

"It's not often that you can say you are improving security while also improving the user experience, but that's what we have achieved with this rollout."

– **Josephina Fernandez**
Director, Security Architecture & Research, Cisco

170,000+ devices secured

5.76 million health checks/month
86,000 devices/month remediated

100,000+ users onboarded

Only < 1% contacting helpdesk

410,000+ fewer VPN auths/month

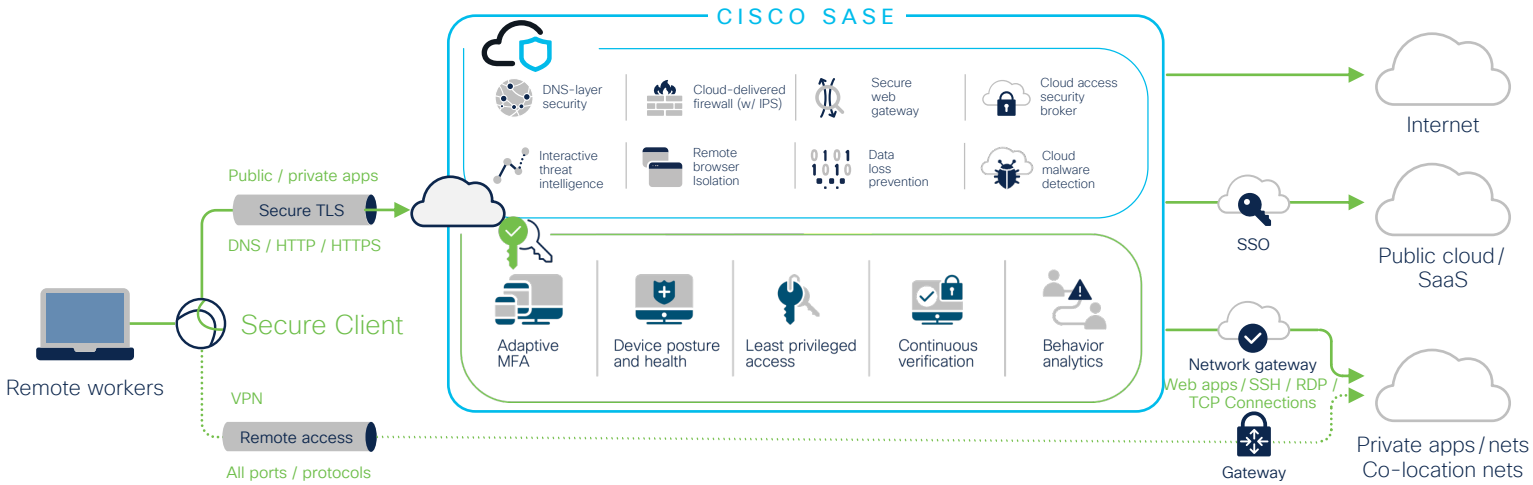
Users no longer need the VPN for access to more than 100 applications (on-premises and SaaS)

5-month deployment timeline

From defining requirements in July to enterprise-wide rollout of 98 countries in December

Zero Trust at Cisco

Advanced application experience with comprehensive security



Cisco's journey

Compelling ROI with the zero-trust model

$3.4M

Annual savings in employee productivity[1]

$500K

Annual savings in IT helpdesk support costs[2]

86K

Potential compromises averted per month[3]

Source: Cisco IT based on the implementation of a zero-trust framework

1. As a result of 410,000 fewer VPN authentications per year
2. With <1% users contacting IT help desk vs 7% for typical security technology rollouts
3. 86,000 vulnerable devices self-remediated/month based on 5.76M device health checks/month

©2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Network Resilience

Credentials
Choose complex passwords and community strings. Avoid default credentials. Use multi-factor authentication.

Monitoring
Secure monitoring and configuration traffic with encryption (SNMPv3, HTTPS, SSH).

Restrict Access
Restrict access and monitor credential systems (TACACS+, jump hosts).

System Lifecycle
Do not operate or deploy end-of-life or end-of-support hardware and software.

Patch Management
Keep software and infrastructure systems up to date.

Change Management
Proactively monitor the environment for unexpected changes and improve change management procedures.

Infrastructure Logs
Review syslog and AAA logs regularly for abnormal activities.

Authorization
Utilize AAA (Authentication, Authorization, & Accounting) best practices to prevent unauthorized configuration changes.

Management Plane
Protect the management plane with infrastructure ACLs (iACLs).

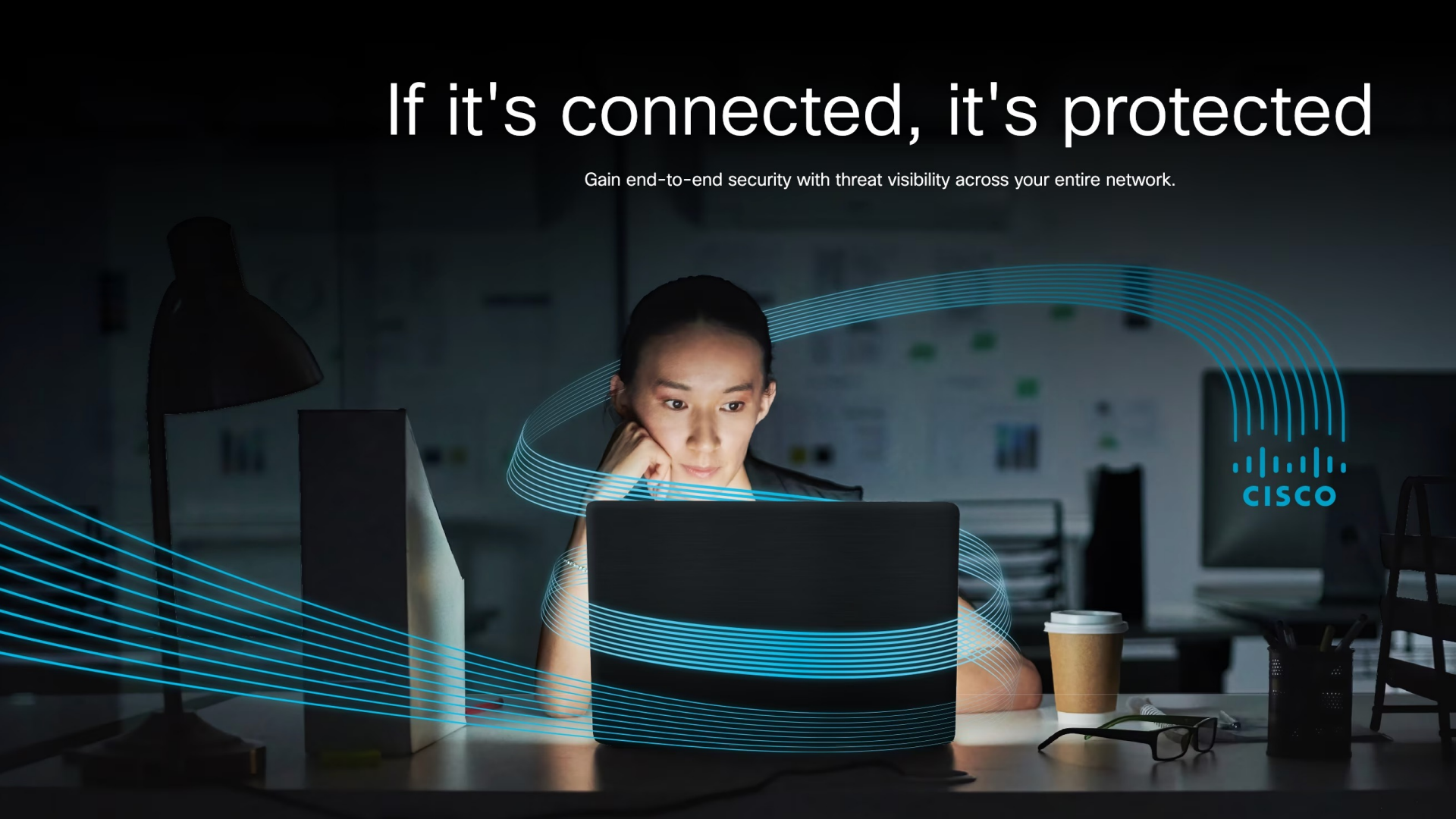
Seek Assistance
Seek assistance from Cisco TAC or PSIRT for security incidents involving Cisco products.

https://www.cisco.com/c/en/us/about/trust-center/network-resilience.html

©2023 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

If it's connected, it's protected

Gain end-to-end security with threat visibility across your entire network.



Our Solutions

Reimagine Applications

Empower Teams

Secure Enterprise

Transform Infrastructure

Continuity

Insights

Security

Connectivity

Operate

Secure

Scalable

Simple

Sustainability

Sovereign

PLATFORMS

Webex

App Dynamics

Thousand Eyes

DNA Center

Meraki

vManage

SecureX

Intersight

Nexus Dashboard

CX Cloud

Buying Programs

PRODUCTS

Our Solutions

Reimagine Applications

Empower Teams

Secure Enterprise

Transform Infrastructure

C I S C O

Secure

Scalable

Simple

Sustainability

Sovereign

PLATFORMS

Webex

App Dynamics

Thousand Eyes

DNA Center

Meraki

vManage

SecureX

Intersight

Nexus Dashboard

CX Cloud

Buying Programs

PRODUCTS

Thank you!