The bridge to possible

Frustrate Attackers, Not Users: Zero Trust for the Multi-Environment IT

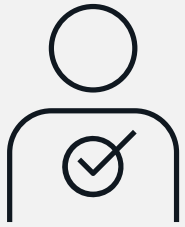
Cisco Live EMEA 2023 Innovation Talk

Lothar Renner, Managing Director, Cisco Security, EMEA
TK Keanini, CTO and VP of Architecture, Cisco Security
Luigi Vassallo, COO and CTO, Sara Assicurazioni

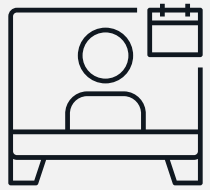
INTSEC-1670

The old security model no longer works

Businesses competing as ecosystems



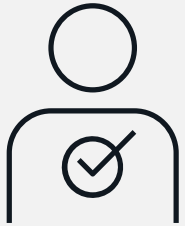
Everyone is an insider



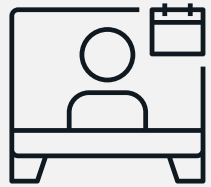
Hybrid work is here to stay

A modern approach is needed

Businesses competing as ecosystems



Everyone is an insider



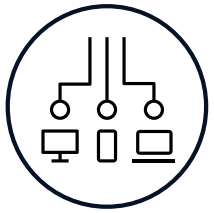
Hybrid work is here to stay

Zero Trust

Security Resilience

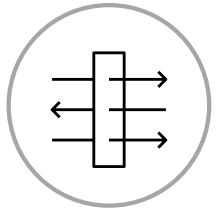
It’s segmentation

It’s ZTNA



It’s endpoint security

Zero Trust means different things to different people



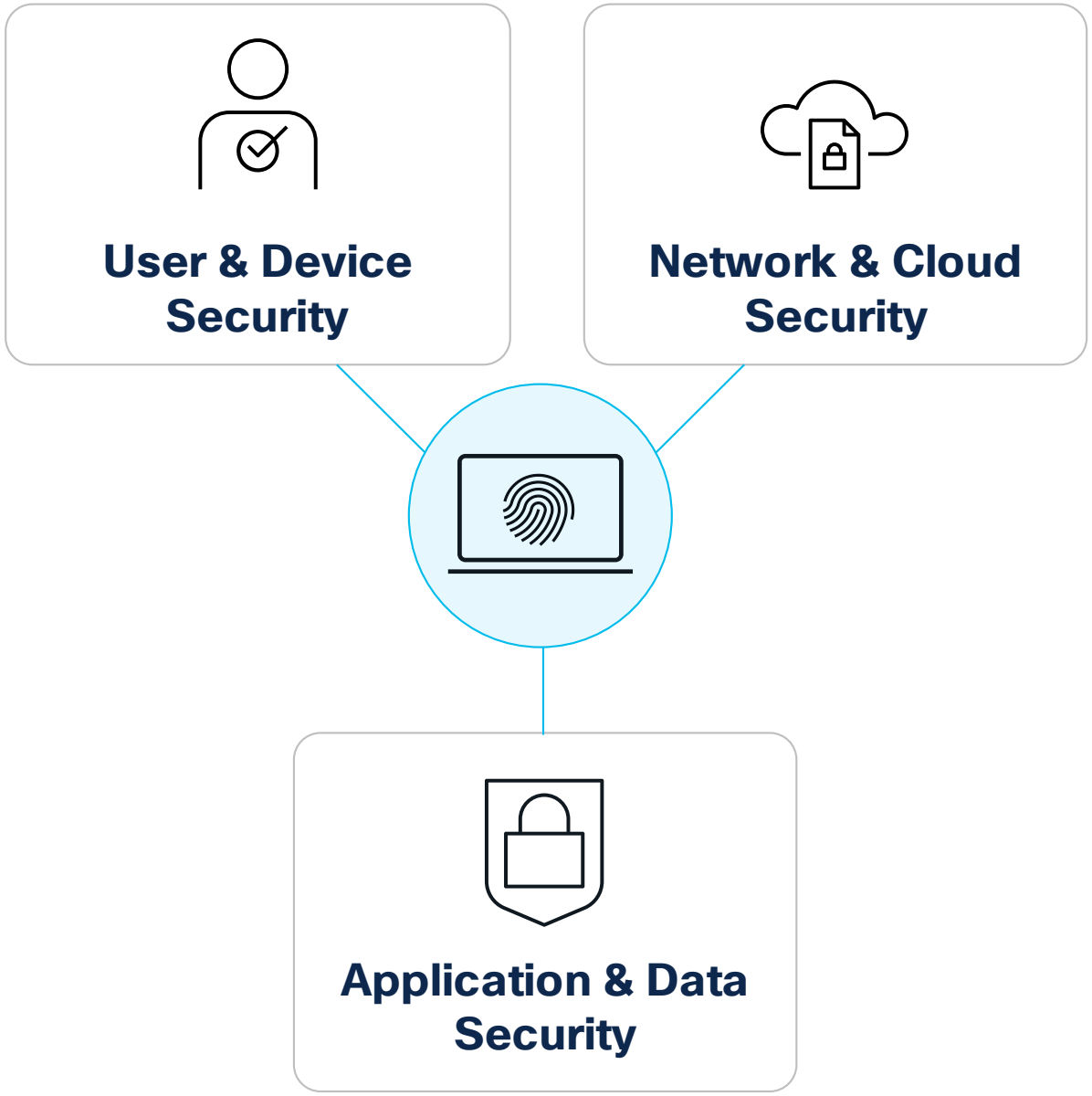
It’s firewall

It’s identity

Zero Trust Principles

1. Never assume trust
2. Always verify
3. Enforce least privilege

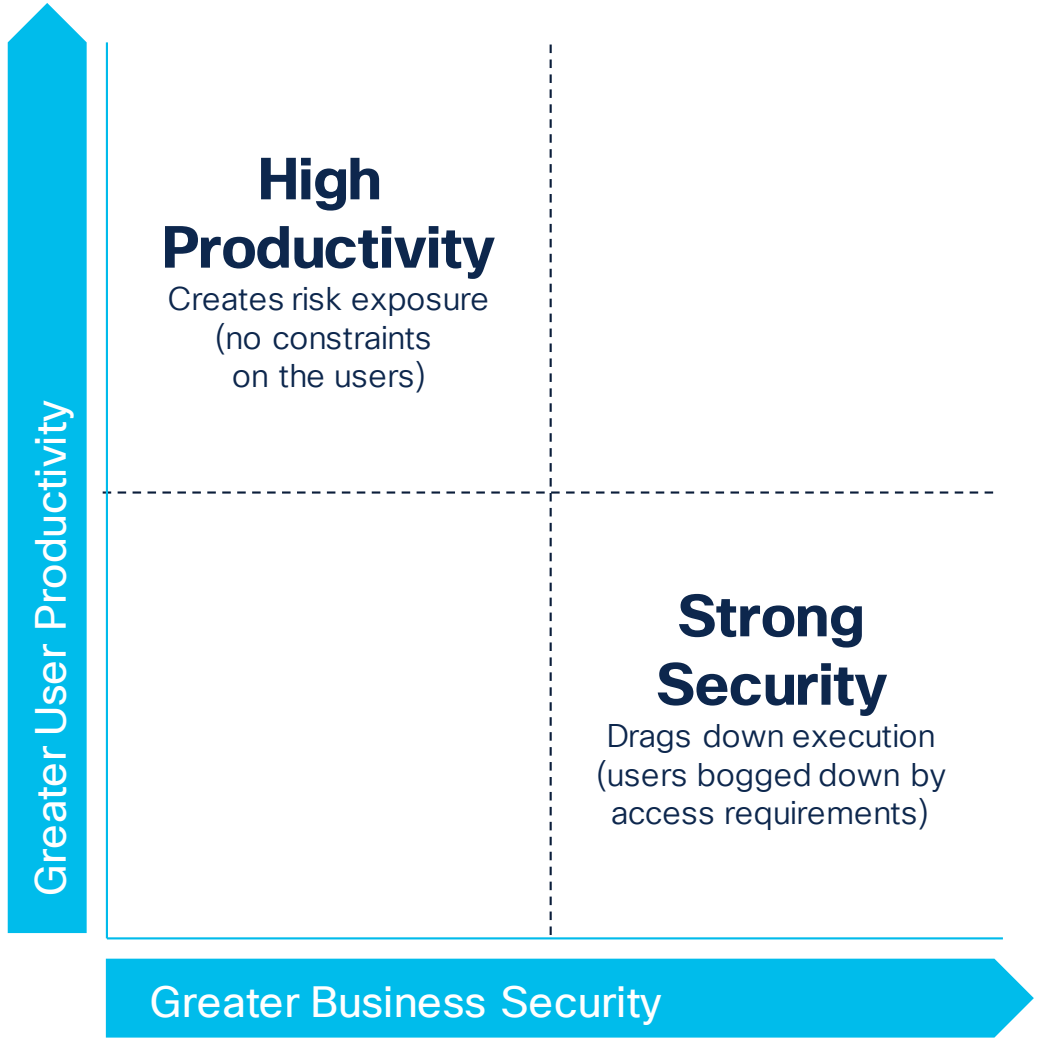
Cisco's recommended Zero Trust strategy



Embed Zero Trust across the fabric of multi-environment IT to protect the integrity of business by securing access in a way that frustrates attackers, not users.

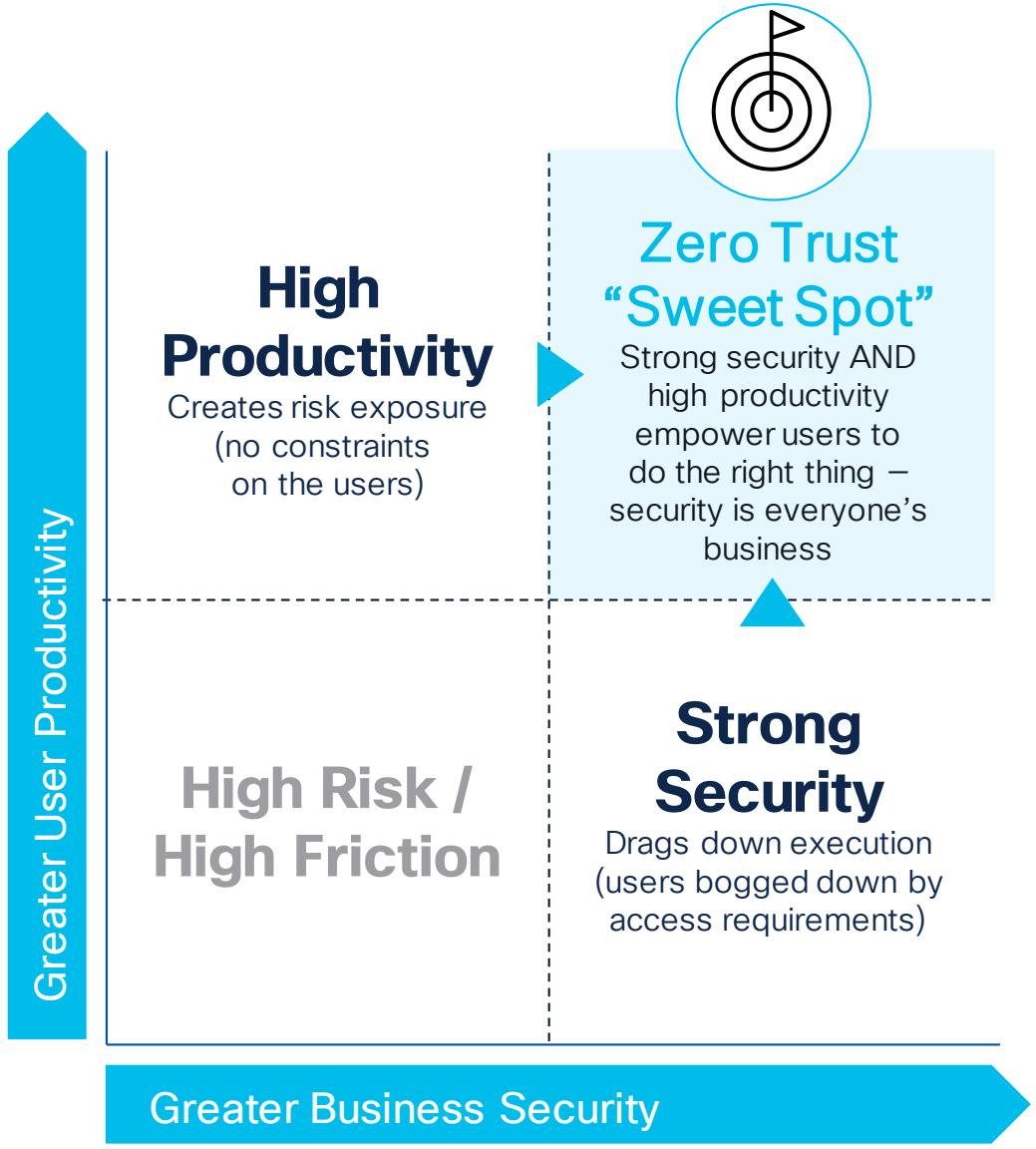
Today's trade-off is holding back Zero Trust

Security vs. productivity



Eliminate the trade-off

Frustrate attackers, not users



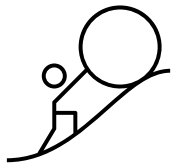
Customer perspective:

Luigi Vassallo

Chief Operating Officer and
Chief Technology Officer, Sara Assicurazioni

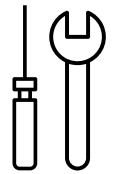
Sara Assicurazioni

A cloud-first insurance company



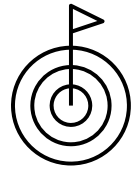
Challenges

- Disparate point-security solutions lack full visibility
- Multi cloud ecosystem demands holistic security approach
- Distributed user base connected to multiple environments via a diverse mix of devices



Solutions

- Cisco Secure Access by Duo
- Cisco Firepower
- Cisco Identity Services Engine
- Cisco Umbrella solution
- Cisco Secure Web Appliance
- Cisco Secure Endpoint
- Cisco Secure Email
- Cisco SecureX



Results

- Zero Trust adoption became more streamlined
- Full visibility into 2,000+ endpoints irrespective of user and device location
- Threat investigation and remediation efficiency improved by 20%
- Threat analysis effort reduced from eight days to only a few hours

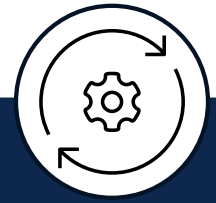
What it takes to get Zero Trust right

Zero Trust requirements

Establish Trust

Enforce Trust-Based Access

Continuously Verify Trust



Respond to Change in Trust

Cisco's Zero Trust capabilities

Establish Trust

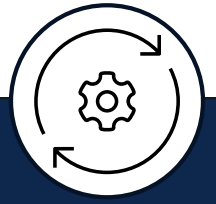
- User / device / service identity
- Posture + context
- Risk-based authentication

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

User & Device Security

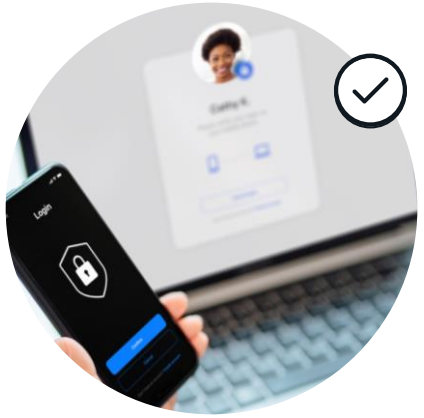
Network & Cloud Security

Application & Data Security

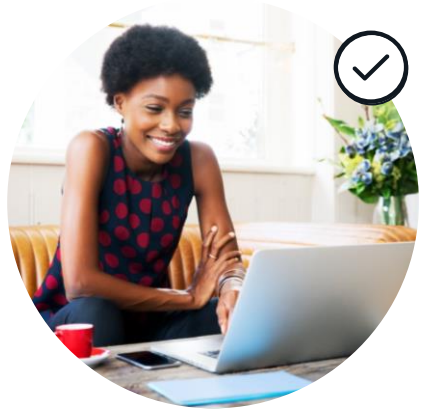
Product Innovations

How do we realize zero trust and frictionless user experience?

User starts authentication



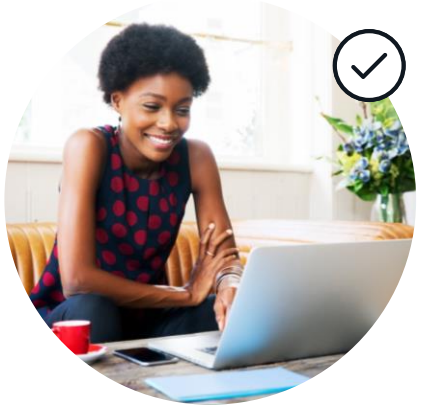
User gains the right access and session



User works securely from any device or location

By doing a tremendous amount of work in the background!

Risk-Based Authentication



RISK SIGNAL ANALYSIS

Device Trust

Location

Wi-Fi Fingerprint

Known Attack Patterns

No Re-Auth Required

Duo Push 2FA

Verified Duo Push

FIDO2 Authenticator

Block

CORPORATE RESOURCES

Risk-Based Authentication: Wi-Fi Fingerprint

Network 1

Network 2

Network 3

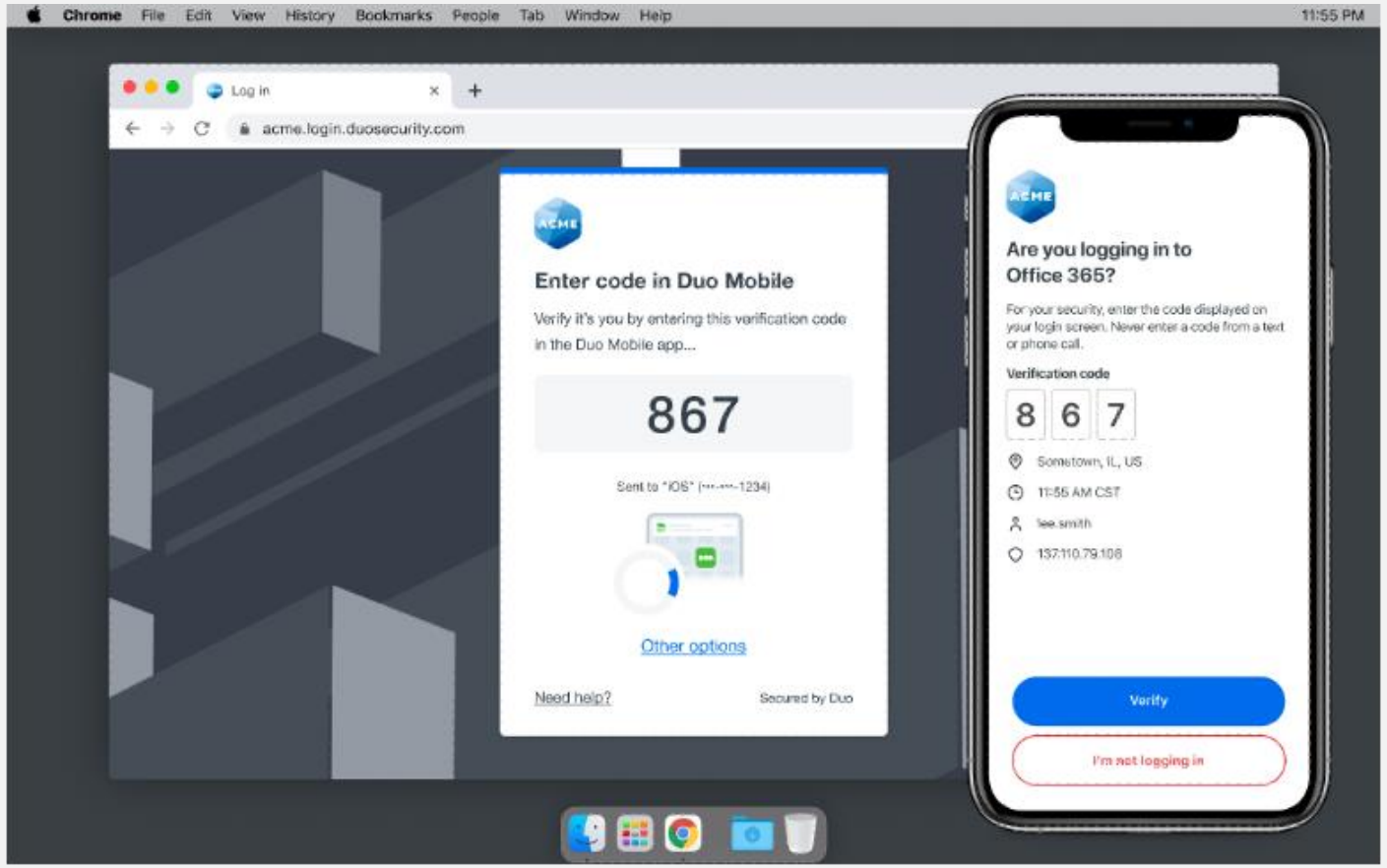
Anonymized Wi-Fi network data provides a **strong risk signal.**

Low Risk: Familiar network fingerprint

High Risk: Novel network fingerprint

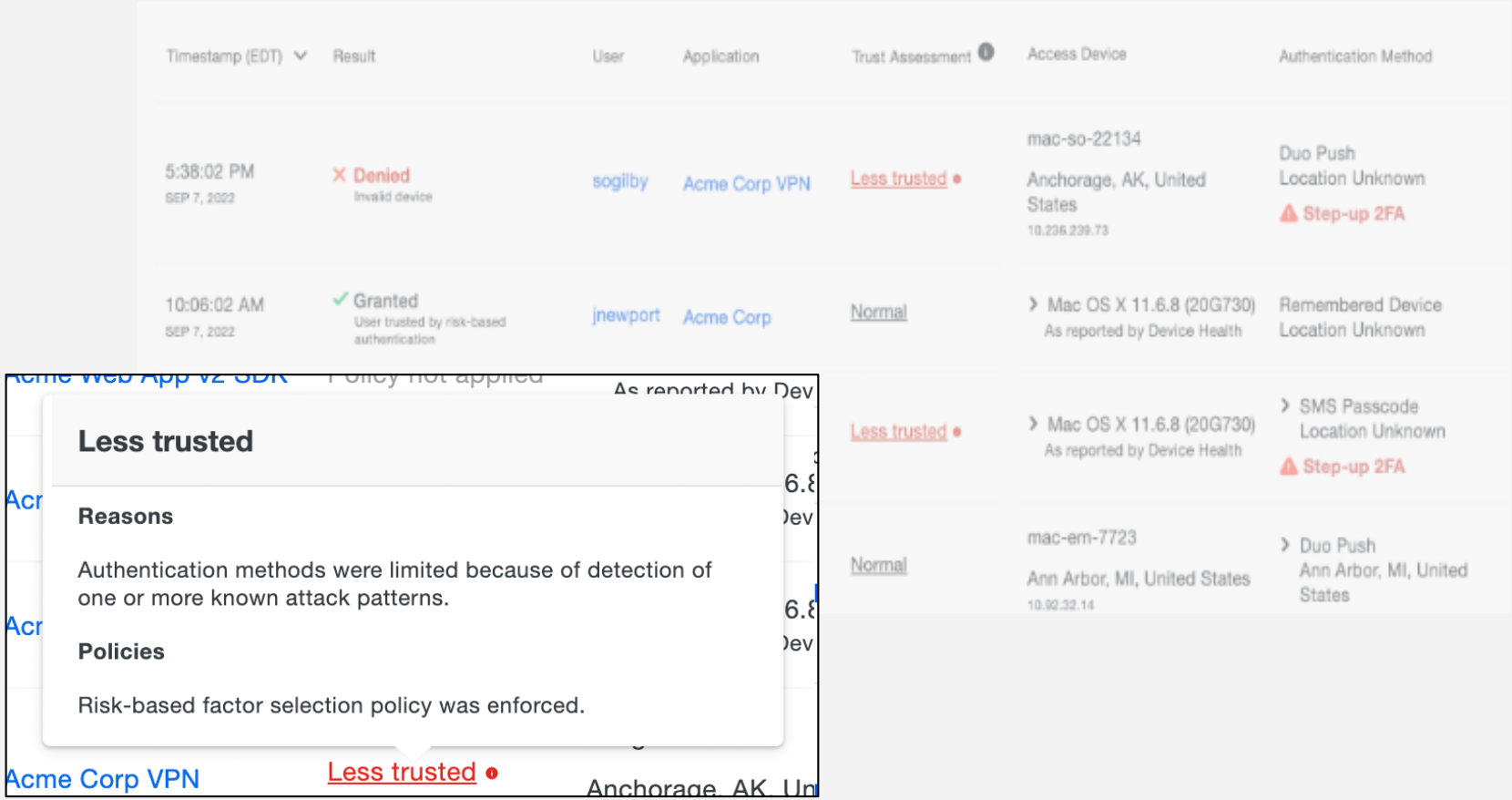
Risk-Based Authentication: Verified Duo Push

Self-remediate risky logins by invoking a **Verified Duo Push**.

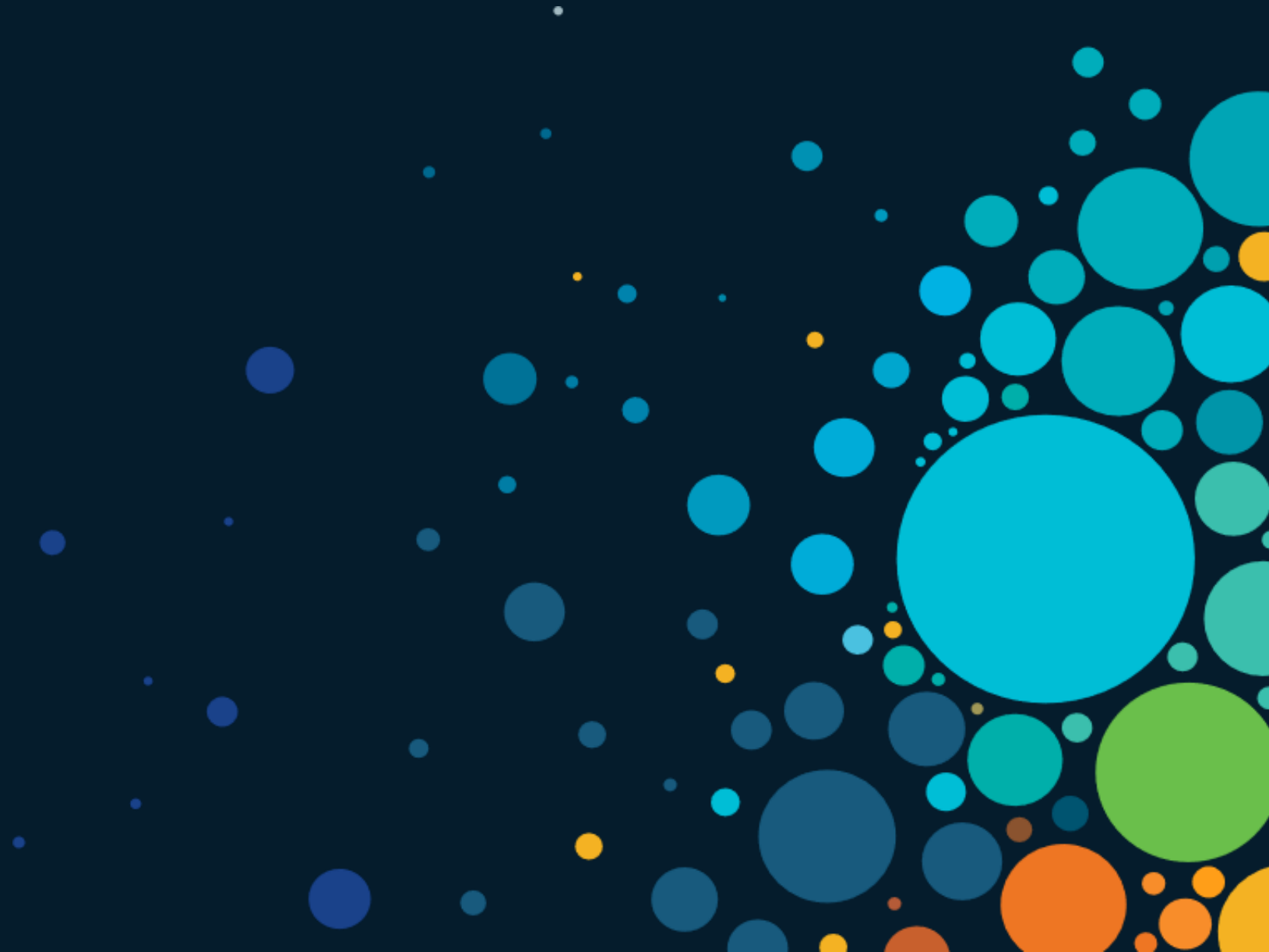


Risk-Based Authentication: Authentication Log

Risk assessment transparency through the Trust Assessment in the Authentication log

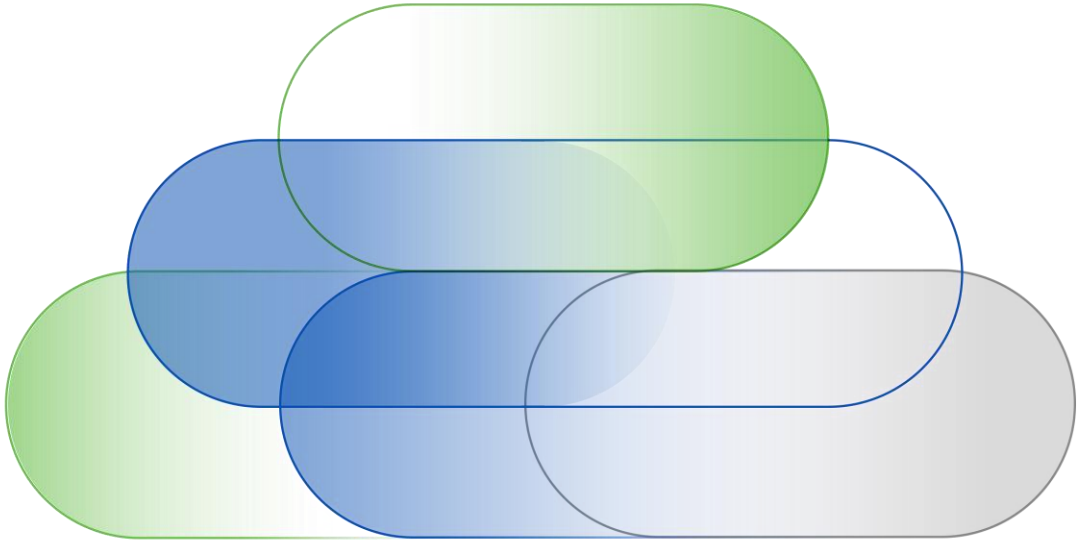


Demo



Cisco Security Cloud

Global, cloud-delivered, integrated platform that secures and connects organizations of any shape and size



Secrets of the Successful

Organizations having a mature zero trust implementation are twice as likely to report excelling across these areas:

- Gaining executive confidence
- Obtaining peer buy-in
- Creating a security culture

Source: Cisco's Guide to Zero Trust Maturity
(based on the survey results from 5000+ IT and security practitioners)

First Steps in the Journey

Define objectives

Desired zero trust outcomes

Perform gap analysis

Current zero trust challenges

Draft roadmap

Action plan for zero trust strategy

Continue the conversation

VISIT:

Want more?

1. Visit the “Zero Trust Security” booth at the Security Showcase and Café at WoS
2. Sign up for a Zero Trust Workshop at: https://cisco.com/go/zero-trust-workshops
3. Learn more at: https://cisco.com/go/zero-trust

Thank you

cisco Live!