

Protecting your People Wherever Work Happens

Powered by Cisco Systems

Managed by Coeus Consulting



COEUS

Managed IT • Cybersecurity • Cloud • Compliance

Cybercriminals are targeting SMBs more than ever

Attackers are no longer skipping over smaller businesses. In fact, they're increasingly targeting them. The N-able team observed a surge in detected threat instances—from approximately 48,749 in June 2024 to over 13.3 million by June 2025—a 273x increase

What is Tycoon 2FA?

Tycoon 2FA is a Phishing-as-a-Service (PhaaS) provider that allows threat actors to easily and affordably conduct BEC attacks. The service provides everything an attacker needs to impersonate a Microsoft 365 or Google Workspace login page, among other target services, and steal credentials from unwitting victims



COEUS

Managed IT • Cybersecurity • Cloud • Compliance

Agenda

11:30 AM - 12:00 noon PM
Introduction and Networking

John Gormally

Introduction to the Cisco Systems and Coeus Consulting team. A brief overview of the changing world of authentication and borderless security.

Demo: Seamless Authentication

12:00 PM - 12:30 PM
The Invisible Shield Presented by Cisco Systems

Chris Balestrieri

When your team works from anywhere, your network needs to be everywhere. Cisco is redefining SMB connectivity by combining **password less authentication** with **AI-driven visibility**. We align these tools into one seamless strategy, ensuring your 'borderless' network is as secure as it is flexible.

12:30 PM - 1:00 PM
Managed services for the Borderless Network

John Gormally

Coeus Consulting bridges the management-IT gap, transforming complex Cisco architectures into a seamless, 24/7 managed shield. From licensing and deployment to proactive monitoring at 2:00 AM, we handle the complexity, so your security is always optimized, and your team is always protected



COEUS

Managed IT • Cybersecurity • Cloud • Compliance

Current Authentication Tools Remain Relevant

These foundational tools remain essential for blocking unauthorized access and ensuring baseline compliance:

- Password Managers: Enforce strong, unique credentials across your team.
- One-Time Passwords (OTP): Provide a secondary layer of dynamic verification.
- Certificates: Offer phishing-resistant, device-level security.
- Multi-Factor Authentication (MFA): Serve as your critical first line of defense.
- Microsoft Authenticator
- Cisco Duo free version

Future-Proofing Your Enterprise: Advanced Security, Unmatched Capability

Transitioning toward the future begins with a comprehensive audit of your current framework to identify hidden risks and operational inefficiencies. This evaluation will determine if your security posture requires a progression to next-generation, **AI-driven authentication** for real-time, adaptive protection.



COEUS

Managed IT • Cybersecurity • Cloud • Compliance

Understanding the Shift

While free tools provide basic "locks," premium licenses provide a "security system" that thinks and reacts.

The Survival Stat: According to the National Cyber Security Alliance, 60% of small businesses that suffer a cyberattack go out of business within six months.

As you audit your current authentication strategy, it is helpful to visualize how security is evolving from a single "checkpoint" to a continuous process.

1. Risk Analysis: Identify where static passwords or SMS-based MFA might be vulnerable to modern phishing or "MFA fatigue" attacks.

2. Operational Efficiency: Measure the time your IT team spends on password resets versus the potential for automated, autonomous verification.

3. Scalability: Evaluate if your current tools can handle increasingly complex remote-work environments and deepfake threats.



COEUS

Managed IT • Cybersecurity • Cloud • Compliance

The changing world of authentication and borderless security

The Rise of Passwordless Defaults

To address the vulnerabilities of traditional passwords, enterprises have transitioned to **passwordless authentication**. This transition relies on two primary technologies:

- **Passkeys:** Cryptographic keys that eliminate the need for memorized credentials.
- **Liveness Biometrics:** Advanced biological scans designed to verify a physical presence in real time. This is used to counter the threat of AI-generated deepfakes that attempt to mimic human features.

Autonomous and Continuous Verification

Security is no longer a "one-time" event occurring only at login. Modern networks now employ **autonomous verification**, which utilizes **continuous authentication** through AI agents. These agents analyze persistent behavioral signals, including:

- Unique typing rhythms and patterns.
- Geographic location data.
- Real-time device health and integrity.



COEUS

Managed IT • Cybersecurity • Cloud • Compliance

The Invisible Shield Managed by Coeus Consulting & Powered by Cisco Systems

When your team works from anywhere, your network needs to be everywhere. Discover how Cisco is redefining SMB security with intelligent, borderless protection.



THE NEW REALITY

When Your Team Works From Anywhere, Your Network Needs to Be Everywhere



Remote Work Explosion

Over 50% of today's workforce operates remotely, with 85% bypassing traditional VPNs entirely

Rising Cyber Threats

SMBs face unprecedented security challenges as cloud apps proliferate and shadow IT expands rapidly

Seamless Security

Cisco redefines connectivity by securing every user, device, and location in one unified strategy

⚠ CRITICAL CHALLENGE

The Challenge: Securing a Borderless Network

Obsolete Perimeter Security

Traditional network boundaries have vanished in today's cloud-first, mobile-driven world. The castle-and-moat approach no longer protects modern enterprises.

Credential Compromise Crisis

Compromised credentials are responsible for 80% of data breaches. Phishing attacks remain the number one threat vector targeting unsuspecting users.

Expanding Attack Surface

Shadow IT applications and unmanaged devices multiply daily, dramatically increasing organizational risk exposure and creating blind spots in security posture.

Cisco Duo: Passwordless, Zero Trust Authentication



Continuous Verification

Verifies user identity and device health continuously before granting access to any resource



Phishing-Resistant Methods

Supports modern authentication: passkeys, security keys, and Duo Push for frictionless security



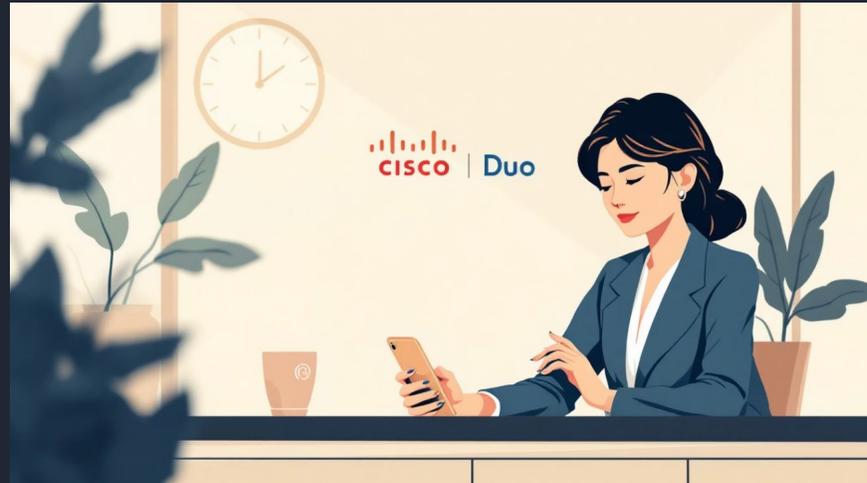
Flexible Policy Engine

Enables adaptive policies with step-up authentication and risk-based access controls



Reduced Attack Surface

Enforces least privilege access and multi-factor authentication across all applications



Cisco Umbrella: AI-Driven Cloud Security Everywhere



DNS-Layer Security

Blocks malware, ransomware, and phishing attempts before connections are even established



Cloud-Delivered Protection

Integrated firewall, secure web gateway, CASB, and data loss prevention in one platform



Complete Visibility

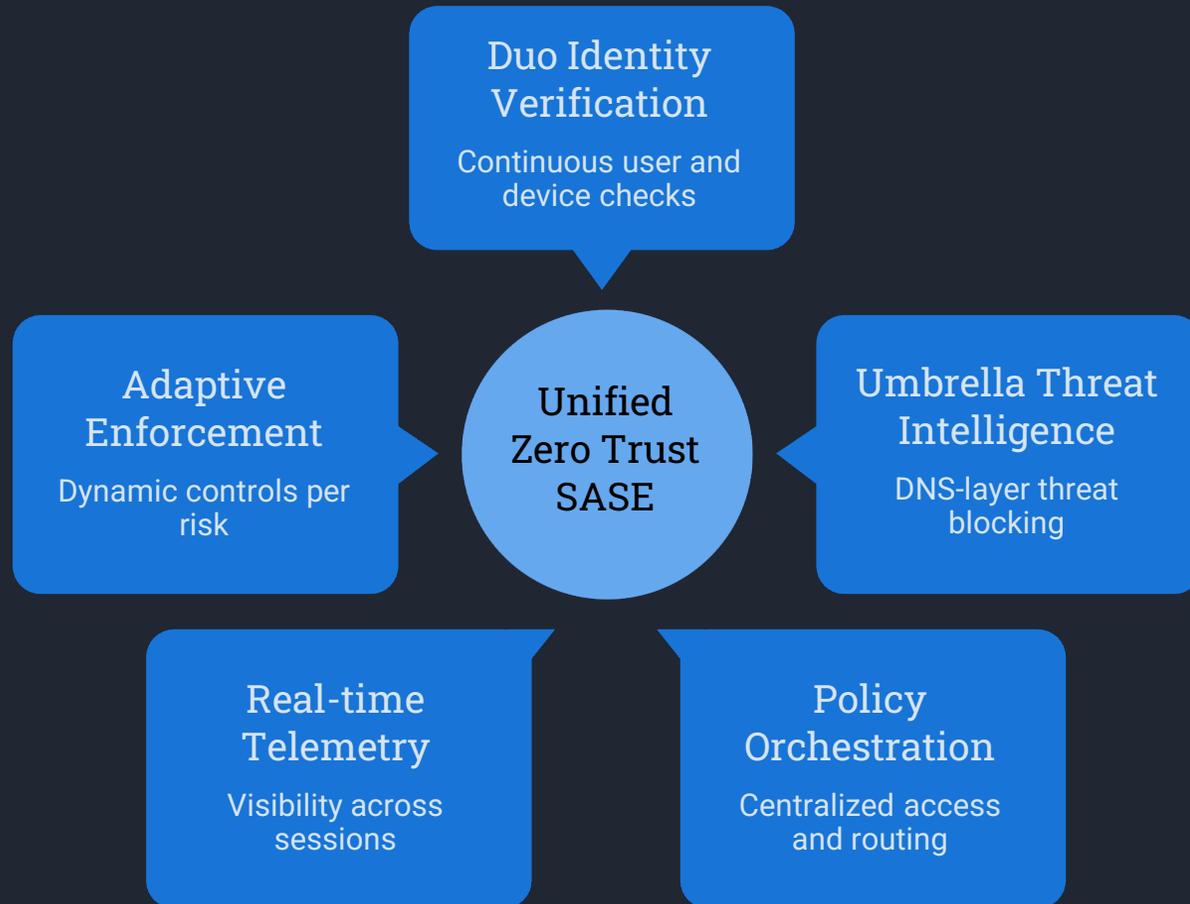
Comprehensive insights into internet activity across all users and devices globally



Universal Coverage

Protects roaming users and IoT devices with zero latency or added complexity

Better Together: Unified Zero Trust & SASE Security



Powerful Integration Benefits

- Duo and Umbrella work together to deliver continuous trust verification combined with real-time threat blocking
- Enterprise customers like Hitachi report dramatically enhanced global protection and simplified security management
- Organizations with mature Zero Trust implementations experience 30% higher security resilience according to Cisco's Security Outcomes Report

Cisco's Secure Access Service Edge (SASE) architecture converges networking and security in the cloud, delivering seamless protection at scale.

Real-World Impact: SMBs Securing Remote Workforces

"Simple, easy-to-use Duo and Umbrella significantly improved our security posture"

— Hynds Group IT Manager

Insurance Compliance

Duo MFA satisfies cyber liability insurance requirements by securing user identities with proven multi-factor authentication

Anywhere Protection

Umbrella's DNS-layer security ensures safe internet access anywhere, anytime, on any device or network

Rapid Deployment

Enterprise-wide protection deployed in minutes, with seamless scalability designed for SMB growth trajectories

Seamless User Experience Meets Robust Security



01

Unified Access

Duo Single Sign-On eliminates password fatigue by providing unified access to all cloud applications from one secure portal

02

Passwordless Security

Modern authentication methods enhance security dramatically without compromising user convenience or productivity

03

Fast Performance

Umbrella's cloud-native platform delivers lightning-fast, reliable protection with minimal user disruption or latency

04

Adaptive Protection

Intelligent policies automatically adapt to user context, device posture, and real-time network risk dynamically

✦ FUTURE-READY

The Future of SMB Security: AI-Powered, Cloud-Delivered, Borderless



AI-Driven Detection

Duo's advanced risk detection and adaptive authentication continuously evolve with the changing threat landscape



Next-Gen Defense

Umbrella's upcoming Secure Access adds SaaS API DLP and advanced cloud malware scanning capabilities



Seamless Transition

Cisco Elevate Program guides SMBs smoothly to comprehensive Security Service Edge (SSE) architecture



Invisible Shield

Together, Duo and Umbrella create an invisible shield empowering secure, flexible work anywhere

Your Invisible Shield Starts Now

Comprehensive Protection

Secure every user, device, and location with the integrated power of Cisco Duo and Umbrella

Zero Trust & SASE

Embrace modern security architecture to protect your borderless SMB network infrastructure

Work Anywhere

Experience seamless security that works everywhere your team does, without compromise

Partner with Coeus & Cisco

Build a resilient, future-ready security posture with Coeus as your trusted partner

Managed services for the Borderless Network

Coeus Consulting's managed services are essential for securing the modern SMB borderless network. We bridge the gap between Cisco's advanced hardware and your operational security by providing:

- **Seamless Deployment:** Expertly integrating Cisco's passwordless authentication to eliminate credential-based vulnerabilities.
- **AI Oversight:** Implementing total visibility into AI prompts to prevent sensitive data leaks.
- **Continuous Protection:** Managed monitoring of decentralized, edge-free environments.



COEUS

Managed IT • Cybersecurity • Cloud • Compliance

Coeus Consulting: Seamless Deployment

Strengthen your security with **seamless Cisco passwordless deployment**, eliminating credential vulnerabilities. Our expert integration optimizes performance while ensuring robust protection across your entire digital enterprise:

- **Credential Elimination:** Removes passwords to stop phishing attacks.
- **Expert Integration:** Rapid, low-friction deployment into existing infrastructures.
- **Enhanced Security:** Proven protection against credential-based breaches.



COEUS

Managed IT • Cybersecurity • Cloud • Compliance

Enabling AI Oversight (Cisco Secure Coming Soon)

Prevent Data Exfiltration: Gain 100% visibility into every AI interaction to ensure employees aren't inadvertently sharing trade secrets, client data, or internal intellectual property with public LLMs.

Real-Time Leak Intervention: Use Cisco AI's automated oversight to detect and block sensitive information—like social security numbers or API keys—before the prompt ever leaves your secure environment.

Compliance & Audit Readiness: Maintain a comprehensive forensic trail of AI usage to help your SMB meet rigorous cyber-insurance requirements and industry regulations that free, unmonitored tools cannot satisfy.



COEUS

Managed IT • Cybersecurity • Cloud • Compliance

Coeus Consulting: Purpose-Built Solutions for Every Client

While Cisco builds the tools, **Coeus Consulting** provides the oversight necessary to operationalize them. This managed approach includes:

- **Continuous Compliance Monitoring:** Ensuring your AI usage aligns with strict regulatory standards like HIPAA, CMMC, and GDPR.
- **Proactive Threat Detection:** Utilizing 24/7 Security Operations Center (SOC) expertise to identify and stop sophisticated cyberattacks before they impact your business.
- **AI Security and Operational Efficiency:** Identifying and removing friction in your IT environment so that AI acts as an accelerator for growth rather than a source of complexity.



COEUS

Managed IT • Cybersecurity • Cloud • Compliance

Call to Action

Maximize security with Cisco AI oversight and passwordless deployment, managed by Coeus Consulting experts

Thank you for attending today's event!

Please take a moment to fill out the surveys!



COEUS

Managed IT • Cybersecurity • Cloud • Compliance