CISCO
SECURE

The bridge to possible

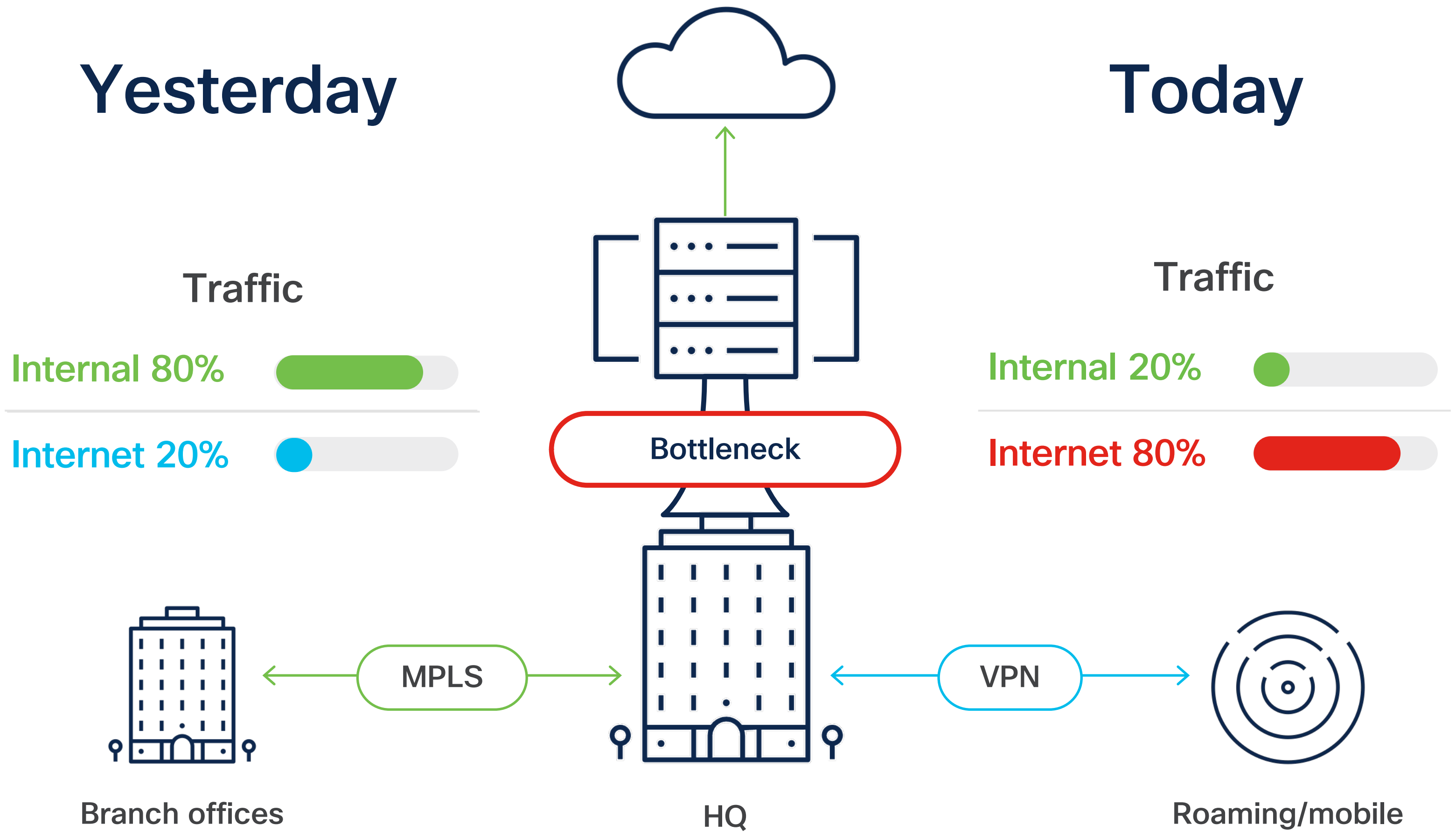
Stronger Security
Cisco Umbrella & Cisco Duo

Cloud-delivered security, simplified

Mark Jacobs, Cisco Systems Engineer

July 18th, 2023

How are you addressing common security problems?



Yesterday

Traffic

Internal 80%

Internet 20%

Today

Traffic

Internal 20%

Internet 80%

Bottleneck

MPLS

VPN

Branch offices

HQ

Roaming/mobile

Challenges

Connectivity needs change quickly

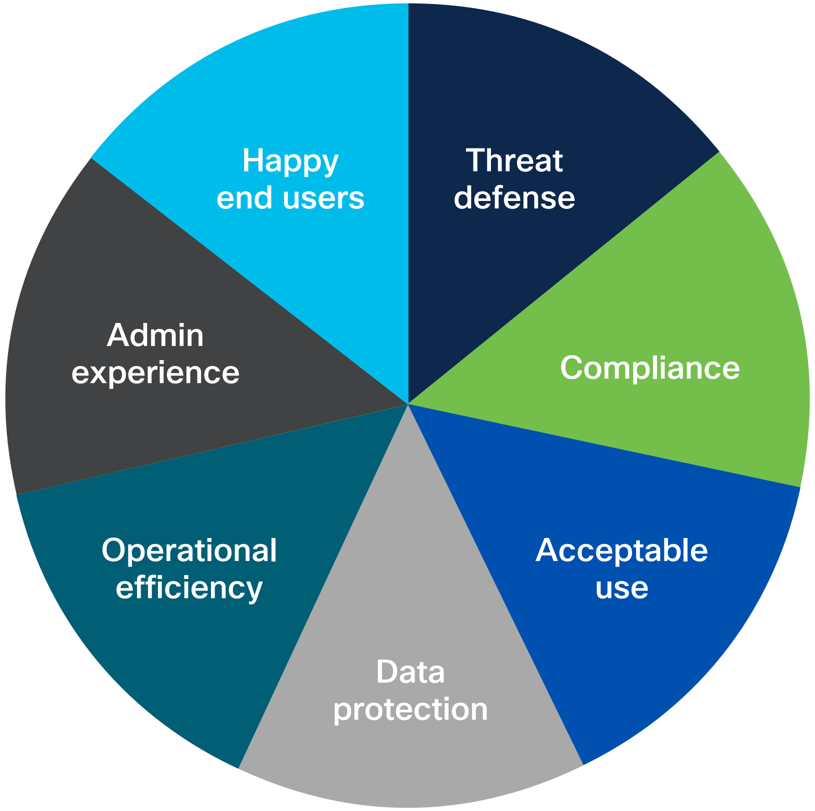
Data center can be a bottleneck

Complexity increases operational costs

App and network performance can drop

Common desired outcomes

- Protecting organization from threats
- Ensuring policy compliance
- Enforcing acceptable use policies
- Keeping sensitive data safe
- Achieving operational efficiency
- Delighting security administrators
- Maintaining end user satisfaction



Modernize with cloud-delivered security

Security Service Edge (SSE)-based architecture secures access to the internet and the usage of cloud services and private applications.

The market is evolving rapidly toward SSE.

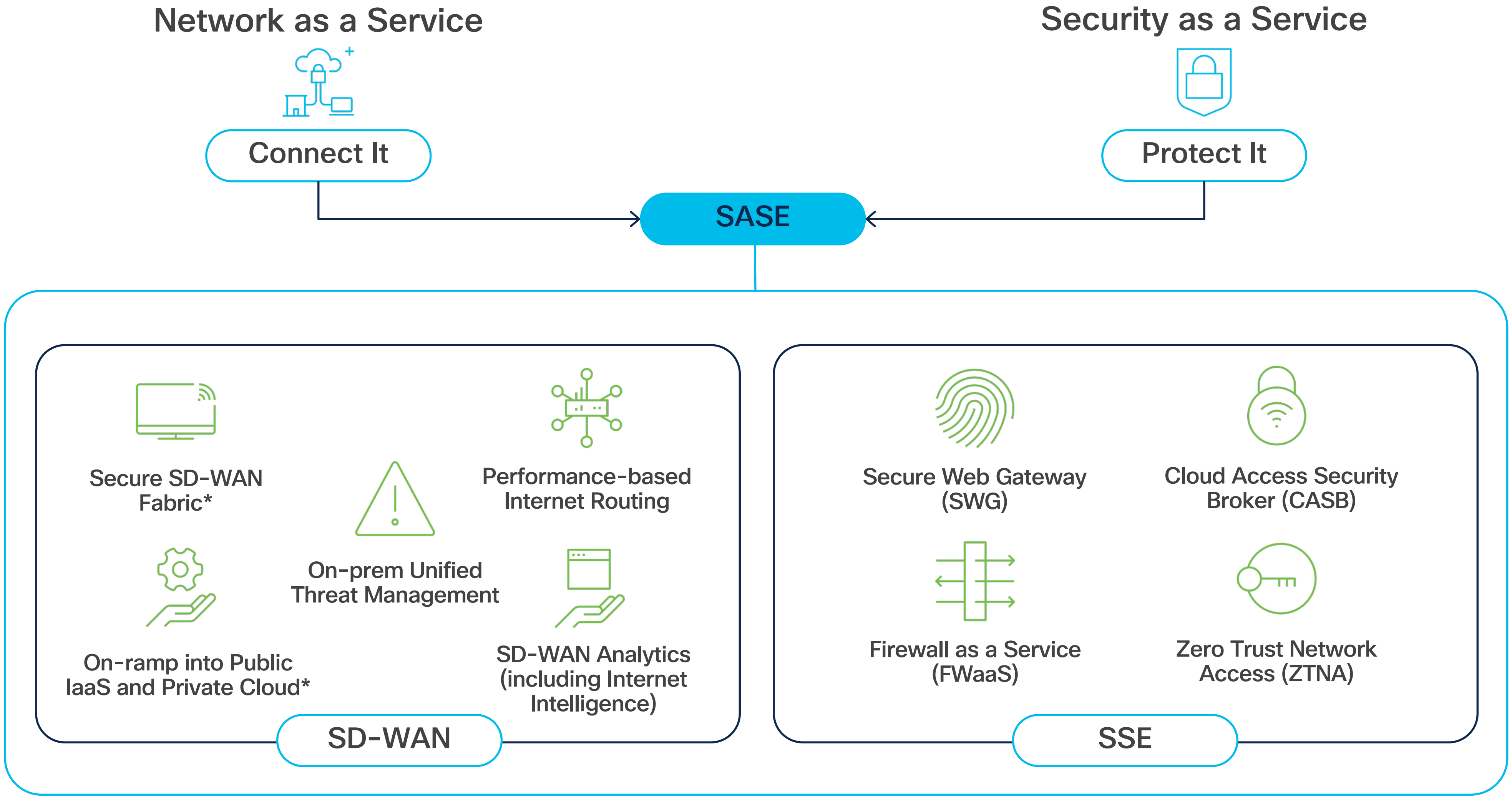
80%

of enterprises will have adopted a strategy to unify web, cloud services, and private application access using a SASE/SSE-based architecture by 2025.

Source: “Critical Capabilities for Security Service Edge,” Gartner, 16 February 2022

Secure Access Service Edge (SASE)

A modern, future-looking approach to secure connectivity



Network as a Service

Connect It

Security as a Service

Protect It

SASE

Secure SD-WAN Fabric*

On-prem Unified Threat Management

Performance-based Internet Routing

On-ramp into Public IaaS and Private Cloud*

SD-WAN Analytics (including Internet Intelligence)

SD-WAN

Secure Web Gateway (SWG)

Cloud Access Security Broker (CASB)

Firewall as a Service (FWaaS)

Zero Trust Network Access (ZTNA)

SSE

*with support for remote workers

Umbrella: Core for your SSE and SASE journey

Cisco Umbrella

DNS-layer security

Cloud-Delivered Firewall (FWaaS)

Cloud Access Security Broker (CASB)

- App Discovery and Control
- Cloud Malware Detection
- Data Loss Prevention (DLP)

Cisco Talos Threat Intelligence

Secure Web Gateway (SWG)

Remote Browser Isolation (RBI)

Cisco Talos drives Umbrella's threat intelligence

Trusted | Global | Unmatched

1.4+ million malware samples processed daily

625 billion web requests resolved daily

200+ new vulnerabilities discovered yearly

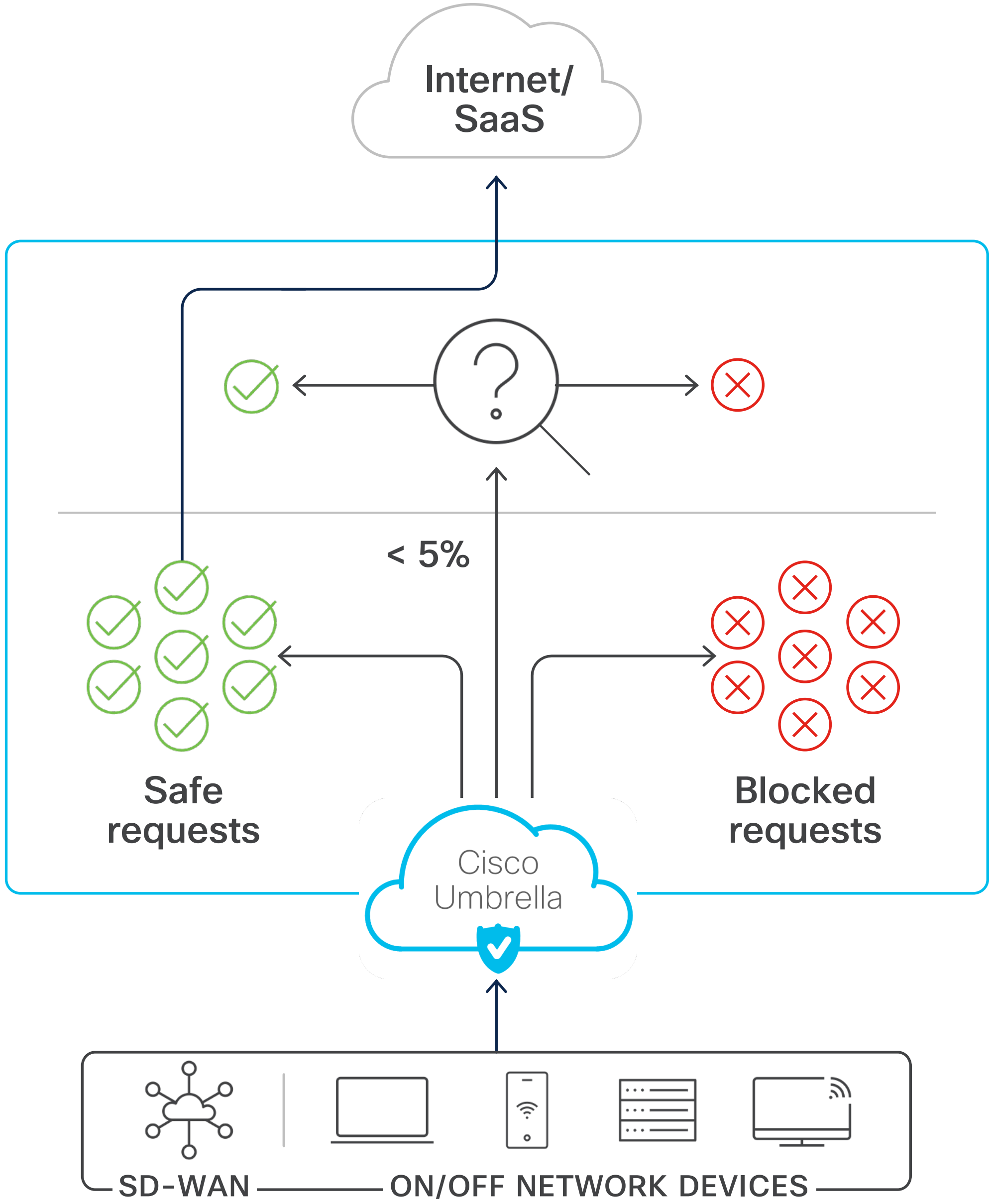
400+ full-time researchers + data scientists

We see more and automate more, so you can block more and respond faster to threats.

DNS-layer security

A differentiating first line of defense

- Deploy enterprise-wide in minutes
- Block malware, phishing, CNC callbacks–from anywhere
- Prevent or limit visits to nefarious web sites from guest Wi-Fi networks
- Stop threats at the earliest point to reduce triage of alerts
- Accelerate internet access; only proxy risky domains



Secure Web Gateway: Full web proxy

Deep inspection and control of web traffic

- Gain additional visibility via full URL logging and cloud app discovery
- Enforce acceptable use policy via granular app controls, content filtering, and URL block/allow lists
- Extend protection against malware via SSL decryption and file inspection
- Improve content security: Sandboxing + retrospective alerts on malware that's evaded initial detection
- View detailed reporting with full URL addresses, network identity, allow/block actions, external IP addresses

Cloud Access Security Broker (CASB)

Visibility, control, and protection

- Control SaaS app usage
  - Content, app, and tenant controls
  - Granular controls for uploads, posts, shares, and more
- Automate alerts about risky apps and activities
- Keep outbound web traffic secure with inline and out-of-band data loss prevention (DLP)
- Detect and remove malware from cloud file storage apps

Meeting compliance requirements with CASB

Discover compliance risks and violations in cloud app usage

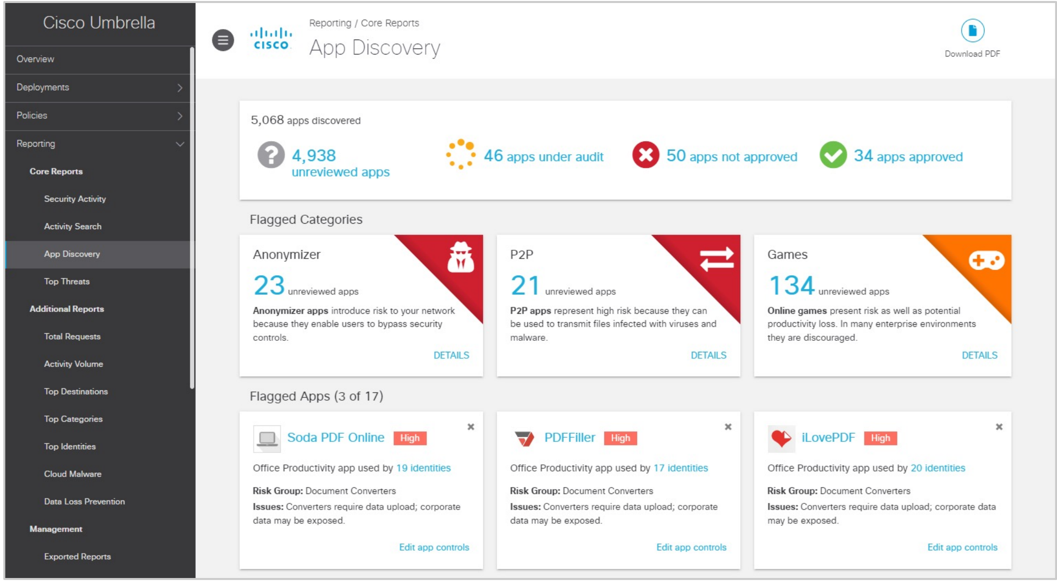
Enforce compliance via web proxy for data-in-motion

Maintain compliance requirements for data in or going to the cloud

Application Visibility and Control

Full view across managed and unmanaged cloud activity

- Minimize negative impact on productivity, expenses, security, and support issues
- Detect and monitor cloud apps in use across your environment



App Discovery

5,068 apps discovered

4,938 unreviewed apps

46 apps under audit

50 apps not approved

34 apps approved

Flagged Categories

Anonymizer

23 unreviewed apps

Anonymizer apps introduce risk to your network because they enable users to bypass security controls.

P2P

21 unreviewed apps

P2P apps represent high risk because they can be used to transmit files infected with viruses and malware.

Games

134 unreviewed apps

Online games present risk as well as potential productivity loss. In many enterprise environments they are discouraged.

Flagged Apps (3 of 17)

Soda PDF Online High

Office Productivity app used by 19 identities

Risk Group: Document Converters

Issues: Converters require data upload; corporate data may be exposed.

PDFFiller High

Office Productivity app used by 17 identities

Risk Group: Document Converters

Issues: Converters require data upload; corporate data may be exposed.

iLovePDF High

Office Productivity app used by 20 identities

Risk Group: Document Converters

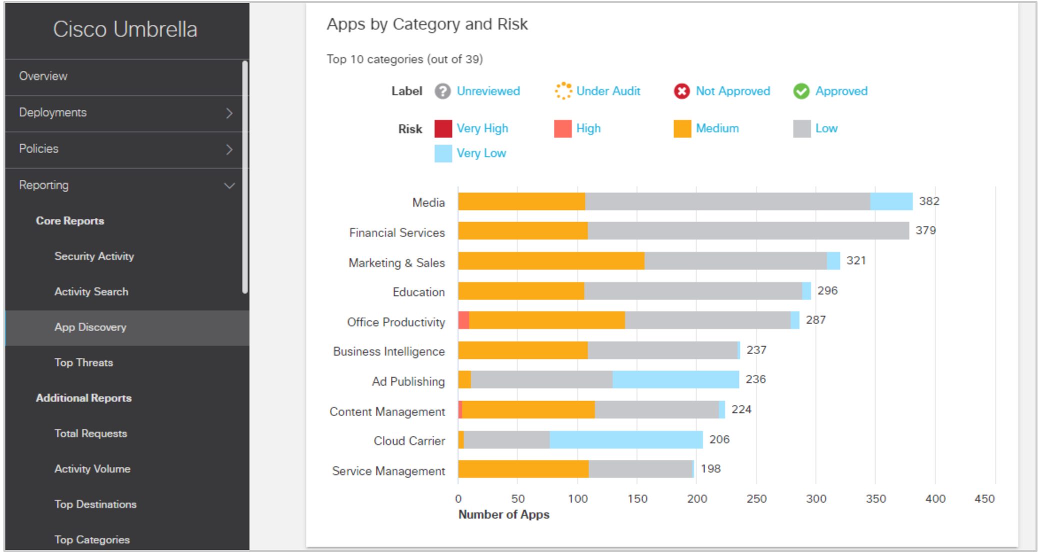
Issues: Converters require data upload; corporate data may be exposed.

Umbrella tracks 30K+ apps

Application Visibility and Control

Full view across managed and unmanaged cloud activity

- Minimize negative impact on productivity, expenses, security, and support issues
- Detect and monitor cloud apps in use across your environment
- Discover app names, vendors, categories, activity, risk rankings, and more
- Ensure access to essential cloud apps and block access to unapproved apps



https://umbrella.cisco.com/schedule-a-demo

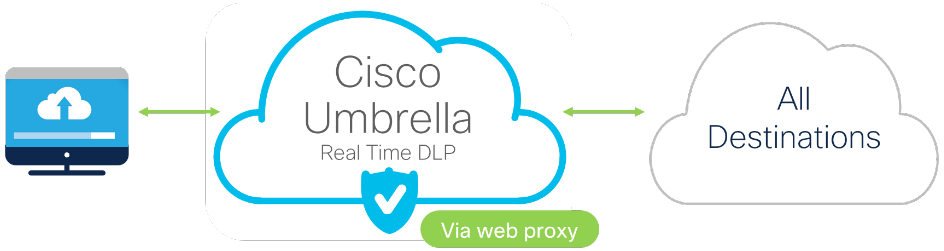
Animated

Multimode Cloud Data Loss Prevention (DLP)

Unified policies and reporting for a single console experience

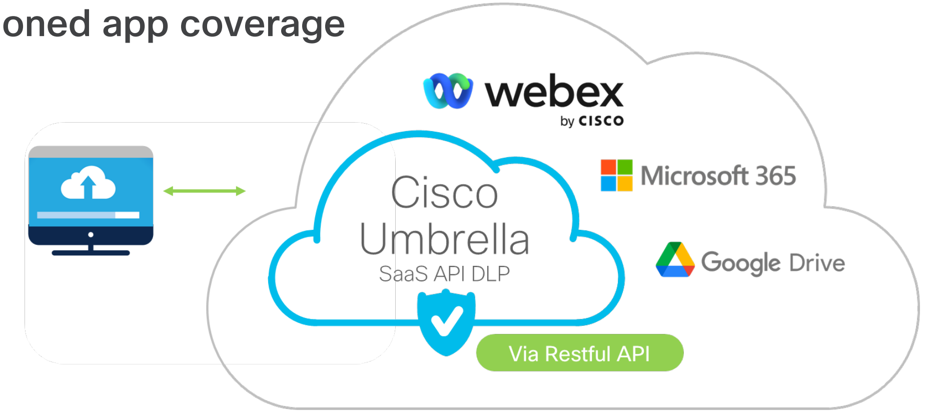
Real Time DLP

- Works via Umbrella Secure Web Gateway (SWG) proxy
- Scans web traffic inline for real-time enforcement
- All application coverage: sanctioned and unsanctioned



SaaS API DLP

- Works via cloud APIs for data at rest, without SWG proxy
- Scans web traffic out-of-band with near real-time enforcement
- Sanctioned app coverage

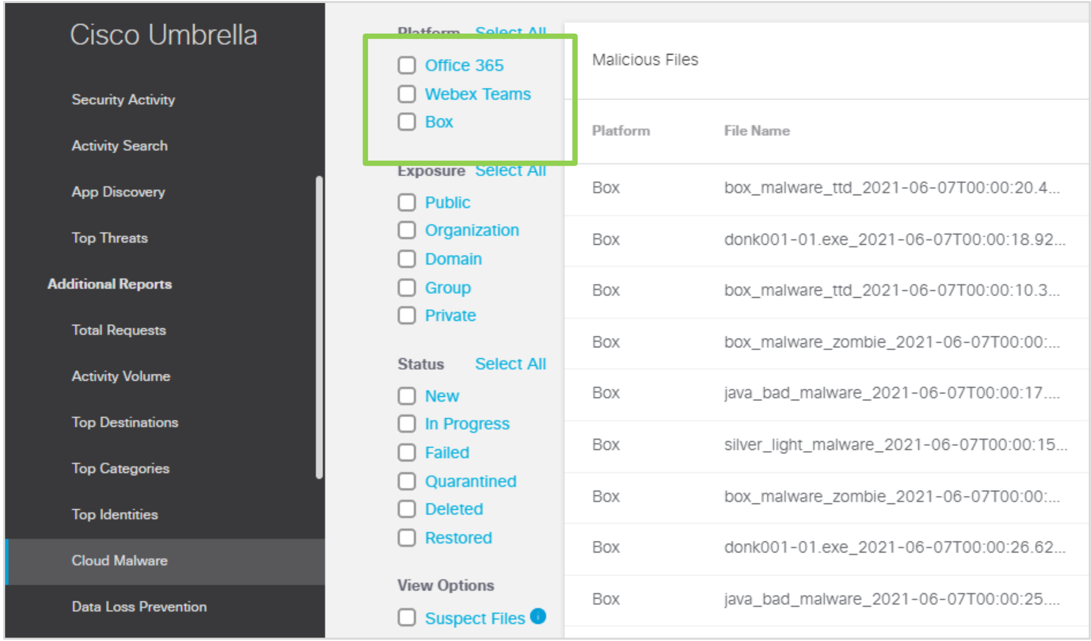


Same management interface

Cloud Malware Protection

Better intelligence drives better security

- Take advantage of comprehensive Cisco Talos threat intelligence
- Alert system admins to potentially malicious files in supported cloud apps



Platform Select All

□ Office 365
□ Webex Teams
□ Box

Exposure Select All

□ Public
□ Organization
□ Domain
□ Group
□ Private

Status Select All

□ New
□ In Progress
□ Failed
□ Quarantined
□ Deleted
□ Restored

View Options

□ Suspect Files

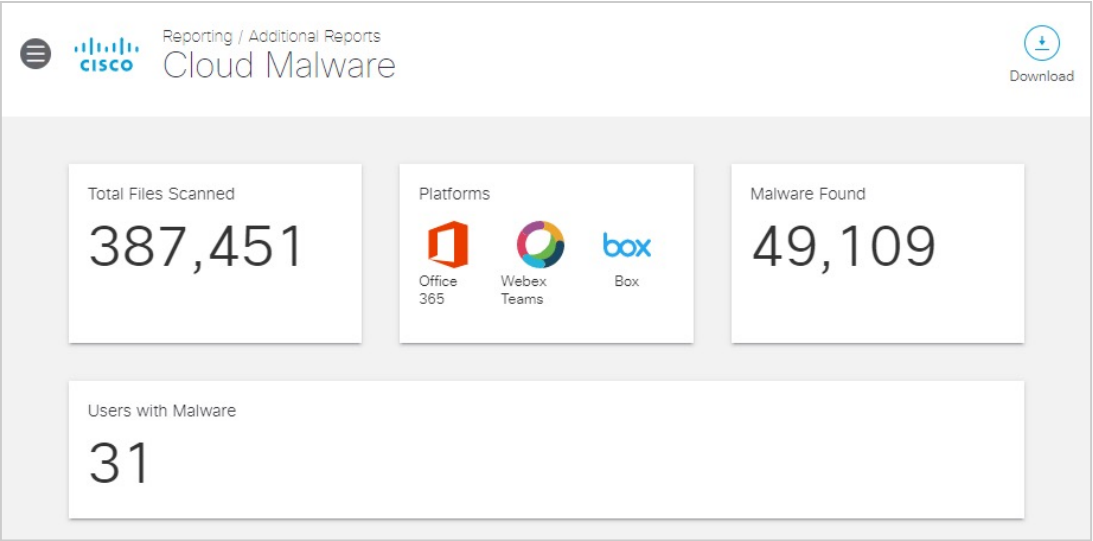
Malicious Files

Platform	File Name
Box	box_malware_ttd_2021-06-07T00:00:20.4...
Box	donk001-01.exe_2021-06-07T00:00:18.92...
Box	box_malware_ttd_2021-06-07T00:00:10.3...
Box	box_malware_zombie_2021-06-07T00:00:...
Box	java_bad_malware_2021-06-07T00:00:17....
Box	silver_light_malware_2021-06-07T00:00:15...
Box	box_malware_zombie_2021-06-07T00:00:...
Box	donk001-01.exe_2021-06-07T00:00:26.62...
Box	java_bad_malware_2021-06-07T00:00:25....

Cloud Malware Protection

Better intelligence drives better security

- Take advantage of comprehensive Cisco Talos threat intelligence
- Alert system admins to potentially malicious files in supported cloud apps
- Enable admins to quarantine or delete unsafe files before they reach endpoints
- Continually gather new threat data



Reporting / Additional Reports

Cloud Malware

Total Files Scanned 387,451

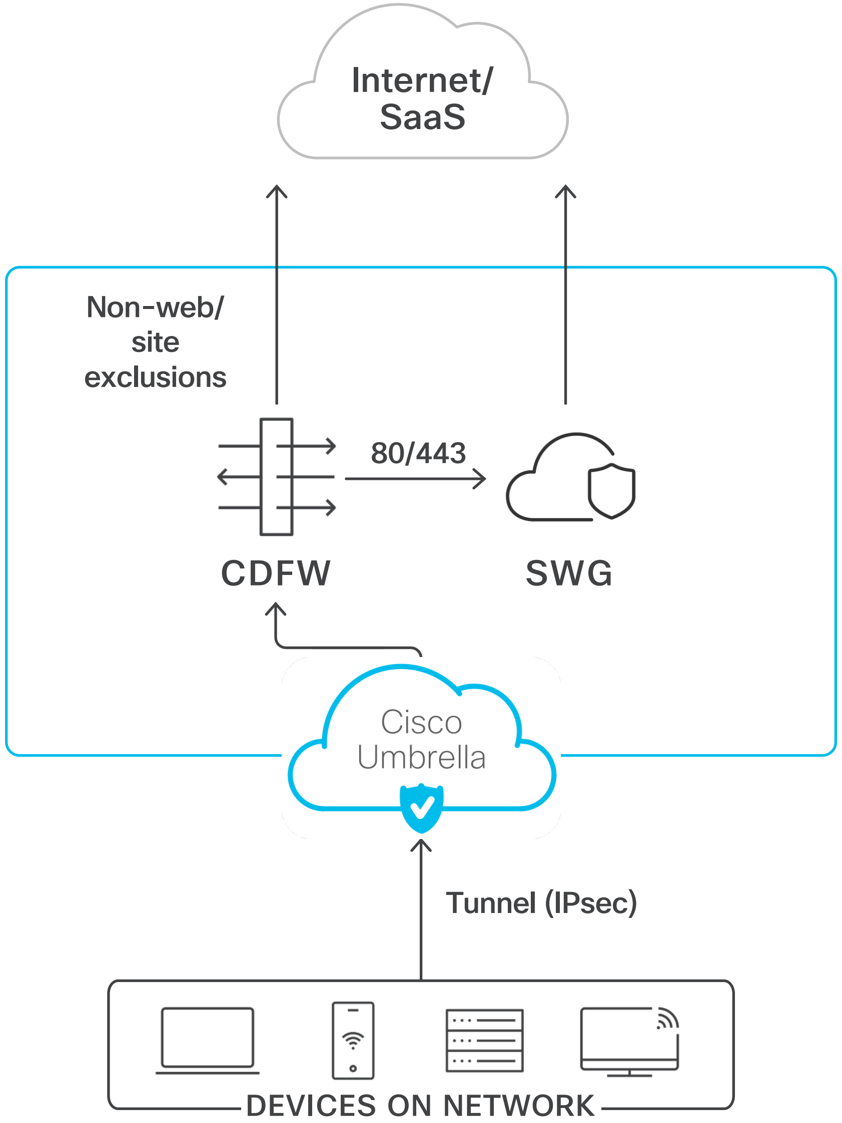
Malware Found 49,109

Users with Malware 31

Cloud-Delivered Firewall (CDFW)

Outbound traffic firewall for the cloud edge

- Block high risk, non-web applications
- Centrally manage IP, port, protocol and application rules (layer 3, 4, and 7)
- Deepen security with Snort 3 IPS
- Forward web traffic (ports 80/443) to secure web gateway
- IPsec tunnel termination



Remote Browser Isolation (RBI)

More protection from risky destinations

- Provide air gap between users, devices, and browser-based threats
- Deploy rapidly without changing existing Umbrella configuration
- Deliver secure web browsing with protection from zero-day threats
- Maintain employee productivity by ensuring safe access to risky destinations and protecting high-risk users

Umbrella wins 2022 PeerSpot awards

GOLD PeerAwards for:

- Secure Web Gateway (SWG)
- Cloud Access Security Broker (CASB)
- Secure Access Service Edge (SASE)

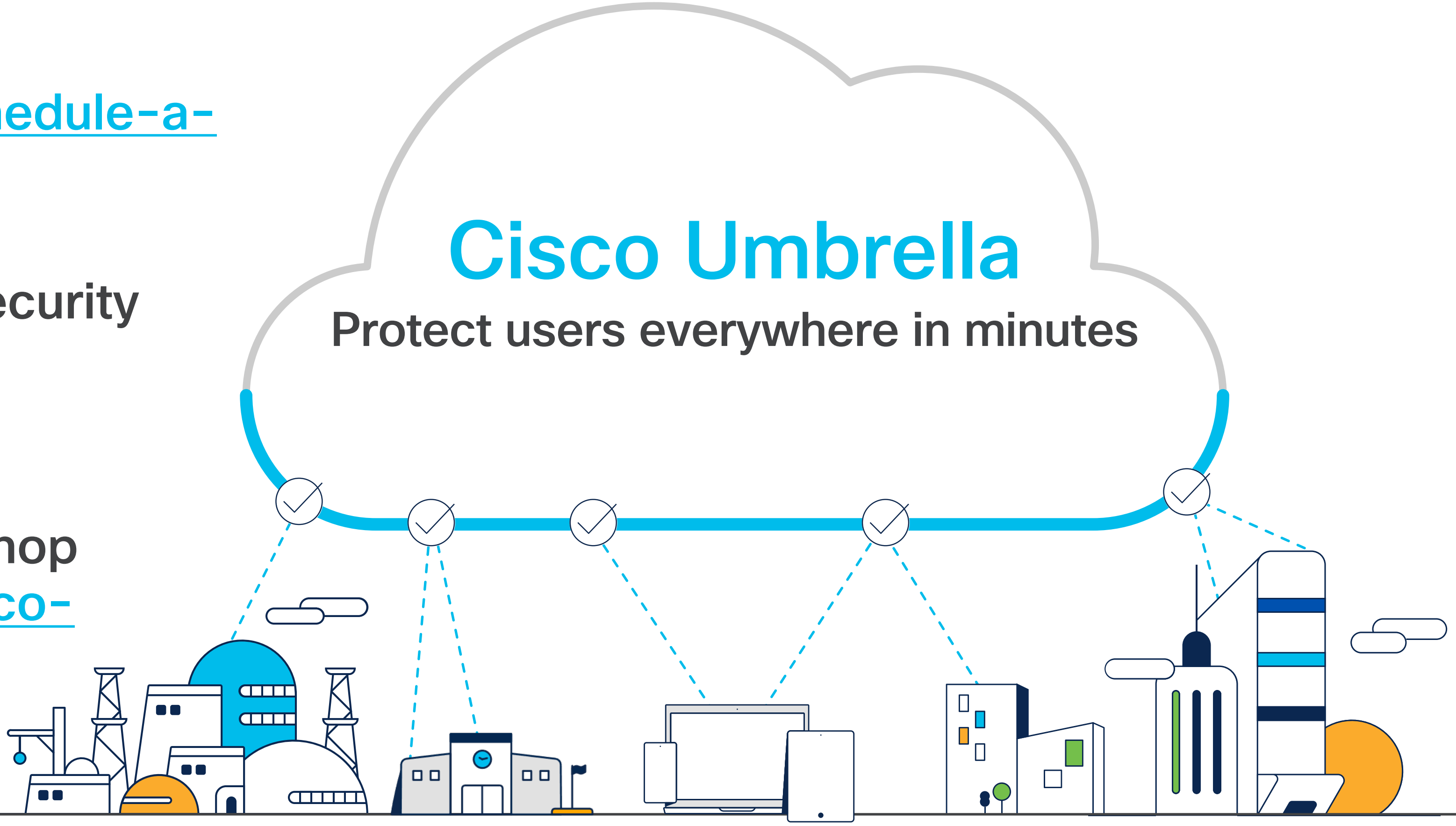
- PeerSpot is a buying intelligence platform where verified users evaluate B2B enterprise technology solutions
- PeerSpot Awards are an annual ranking of the top Enterprise IT products based on authentic user reviews

Next steps

- Schedule a demo
  https://umbrella.cisco.com/schedule-a-demo

- Sign up for a free DNS-layer security trial
  https://signup.umbrella.com/

- Join an Umbrella Studio workshop
  https://umbrella.cisco.com/cisco-umbrella-studio



Cisco Umbrella

Protect users everywhere in minutes

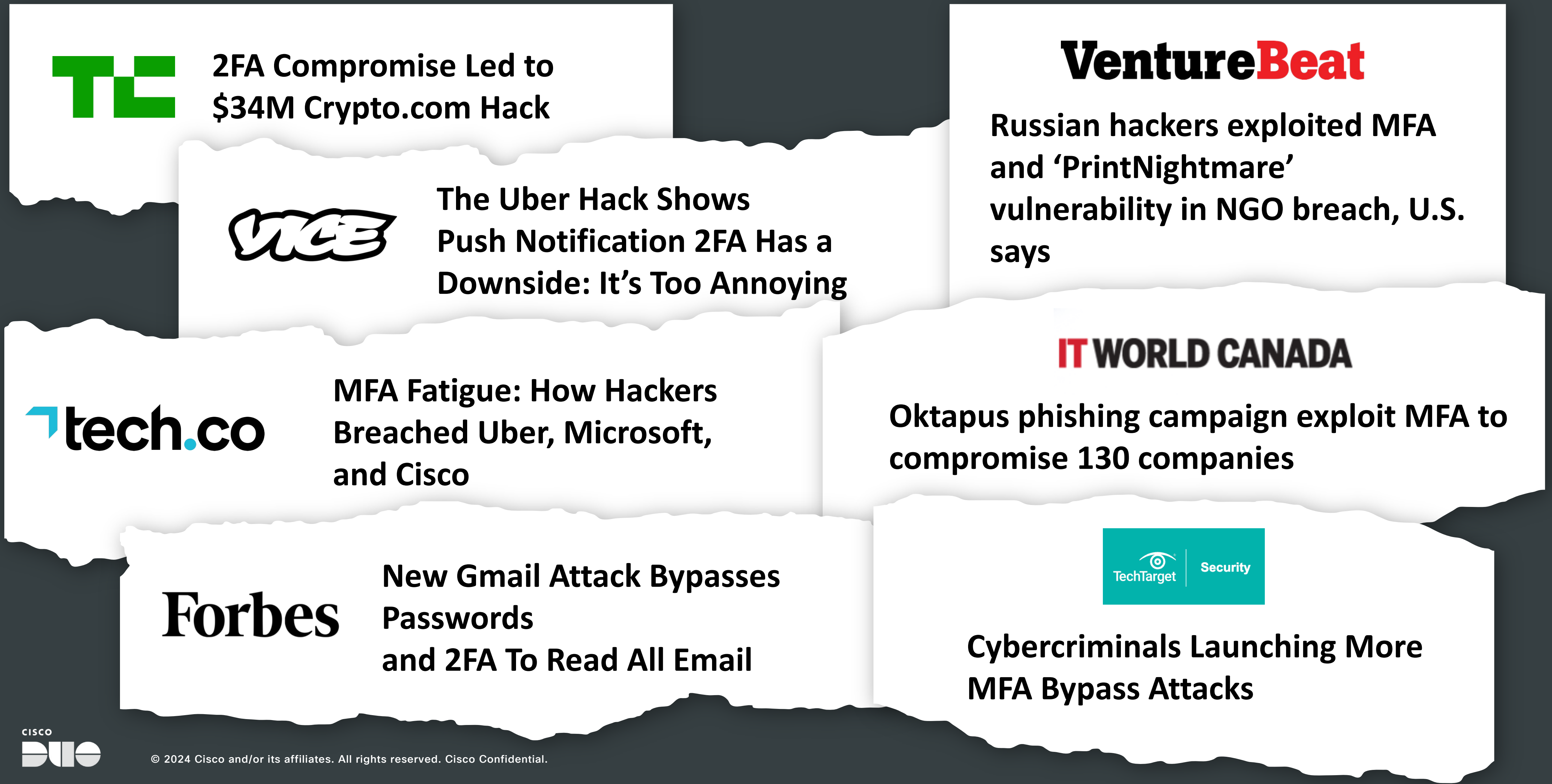
CISCO Duo

The bridge to possible

Stronger security with Duo

Protect against breaches while enabling high productivity

Recent attacks highlight risk in weaker MFA implementations



TC

2FA Compromise Led to $34M Crypto.com Hack

VICE

The Uber Hack Shows Push Notification 2FA Has a Downside: It's Too Annoying

VentureBeat

Russian hackers exploited MFA and 'PrintNightmare' vulnerability in NGO breach, U.S. says

tech.co

MFA Fatigue: How Hackers Breached Uber, Microsoft, and Cisco

IT WORLD CANADA

Oktapus phishing campaign exploit MFA to compromise 130 companies

Forbes

New Gmail Attack Bypasses Passwords
and 2FA To Read All Email

TechTarget Security

Cybercriminals Launching More MFA Bypass Attacks

Identity is the new perimeter

+

Attackers actively exploit identity gaps and weaknesses

+

80% of organizations are NOT prepared

2023 Cisco's Cybersecurity Readiness Index

The Perfect Storm

Redefining Access Management

Problem	Many passwords = bigger attack surface	Social engineering will be used against you	Devices not even touching your network
Solution	Reduce passwords	Enforce strong authentication	Verify devices
	Single Sign-On	Passwordless, Verified Push	Trusted Endpoints

Stronger Security

Security that frustrates attackers

- Implement phishing-resistant authentication
- Stop MFA fatigue attacks
- Only allow known and safe devices to access resources
- Detect attacks where visibility is nonexistent

Protect against breaches

FIDO2 Enforcement

Verified Duo Push

Trusted Endpoints

Risk-based authentication

Trust Monitor & Instant user triggered alerts

Adaptive and granular policies

- Leave no gaps in protection
- Automatically strengthen authentication requirements when risk rise
- Apply Zero Trust principles

Higher Productivity

Security that enables the business

- Only require user actions when necessary
- Accelerate identity related incidents detection and investigations
- Easy to use for Admins and Users

Boost user, IT and security productivity

Passwordless

Single Sign-on

Risk Based Authentication

Endpoint self-remediation

User self-service

Flexible authentication options

Simple Policies

Comprehensive authentication logs

VPN-less remote access

- Access resources swiftly and easily
- Reduce IT burden with user self-service

Unmatched Value

Security made easy

- ➢ Reduce IT costs and overhead
- ➢ Meet compliance & insurance requirements
- ➢ Seamlessly start Zero Trust journey

Smart & secure access management that pays for itself

User self-service

Policies
mapped to compliance requirements

Zero Trust for the Workforce

SaaS based

Infrastructure agnostic

Protect any application, any user, any device

- ➢ Fast speed to security
- ➢ Work with what you have
- ➢ Cover any use cases with a single solution

We saw an extremely high return on our investment with Duo. Not only was it easy to deploy and maintain, but it also enabled us to open our systems to our users more confidently without impacting the experience. That's the most important thing."

MATT HASCHAK

Bowling Green State University

We don't have an army of people – technology needs to be simple and straightforward to use. **... Our users are happy,** and Duo is one of those rare IT projects that doesn't drag on endlessly or ends up half-implemented."

IASEN OGNIANOV

Global Director of Cybersecurity
Diebold Nixdorf

We looked at various vendors, but Duo was an easy choice for us. It can help us to achieve our vision of zero-trust security. The deployment was effortless and smooth...**Duo has provided a perfect balance of security and end-user experience."**

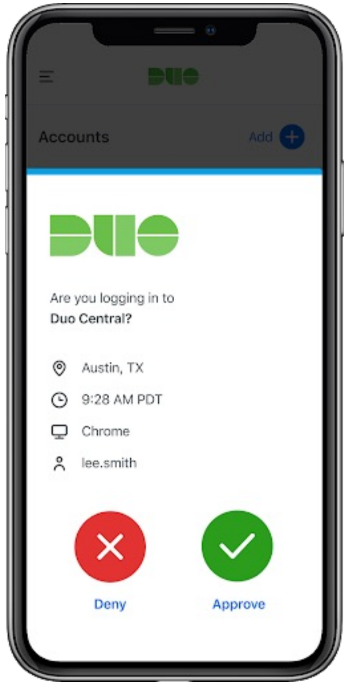
JEFF SMITH

Sr. Information Security Engineer
Sonic Automotive

Duo Capabilities

Authenticate Users

Verify users are who they say they are



Are you logging in to Duo Central?

Austin, TX
9:28 AM PDT
Chrome
lee.smith

Provide Strong Multi-Factor Authentication

Protects against unauthorized access using valid credentials

Implement Passwordless

Increase security and user productivity by logging in without a password

Quickly deploy and be protected

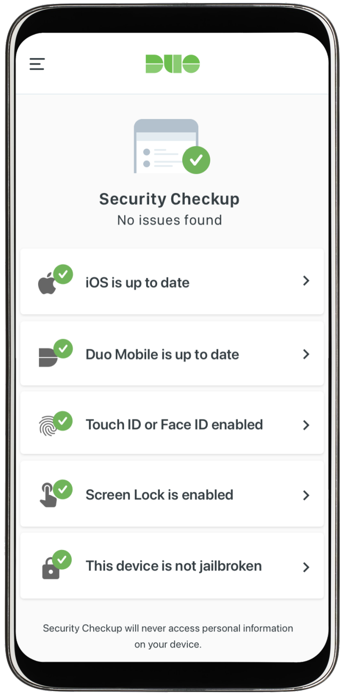
Cloud native and designed to be user friendly from the start, Duo allows any IT professional to implement at lightning speed

Prevent Push Phishing Attacks

Ensures users don’t fall victim to push phishing attacks

Verify Devices

Verify the trustworthiness devices before granting access



Security Checkup

No issues found

iOS is up to date

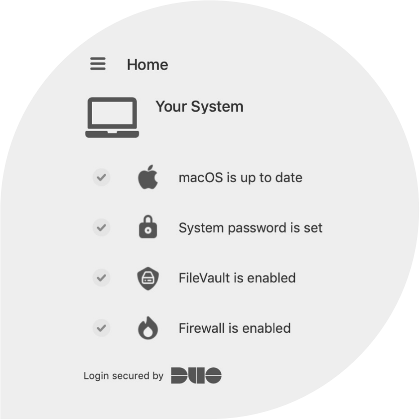
Duo Mobile is up to date

Touch ID or Face ID enabled

Screen Lock is enabled

This device is not jailbroken

Security Checkup will never access personal information on your device.



Home

Your System

✓ macOS is up to date

✓ System password is set

✓ FileVault is enabled

✓ Firewall is enabled

Login secured by DUO

Check Device Health

Assess Security Posture

Deny access to compromised or out of compliance devices

Guide Self-Remediation

Eliminate vulnerabilities and lower IT costs by empowering users to remediate their device

Verify Endpoint Trust

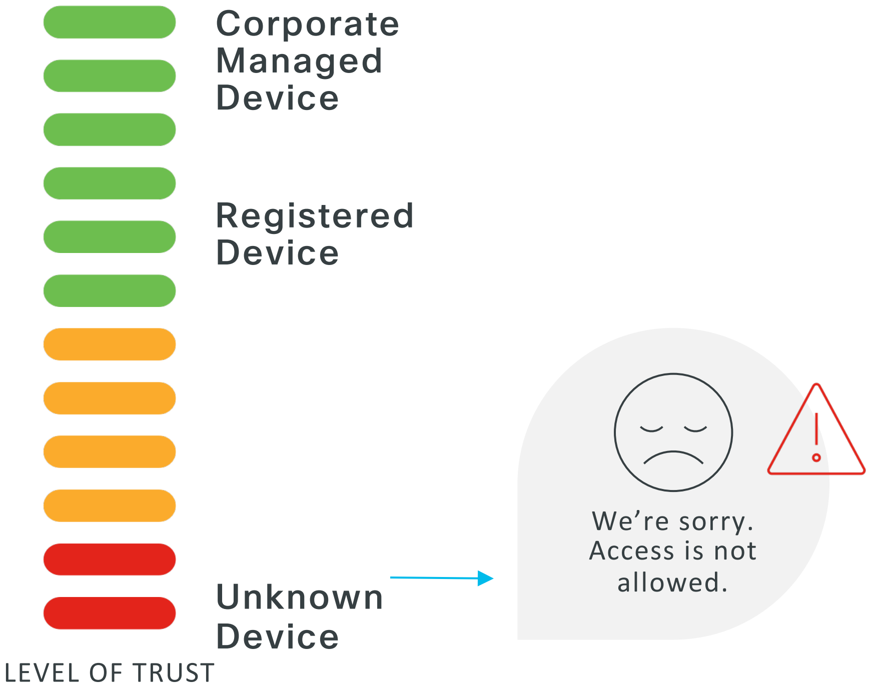
Block access from unmanaged and unknown devices

Provide Complete Visibility

Gain complete visibility
into all laptops and mobile devices accessing your resources

Trusted Endpoints

Block attackers by only allowing registered and managed devices to gain access to corporate resources



Block Attackers

Only allow registered or managed devices to gain access to corporate apps and resources

Cover BYOD

Safely allow BYOD and 3rd party devices without requiring Mobile Device Management software

Control Device Access

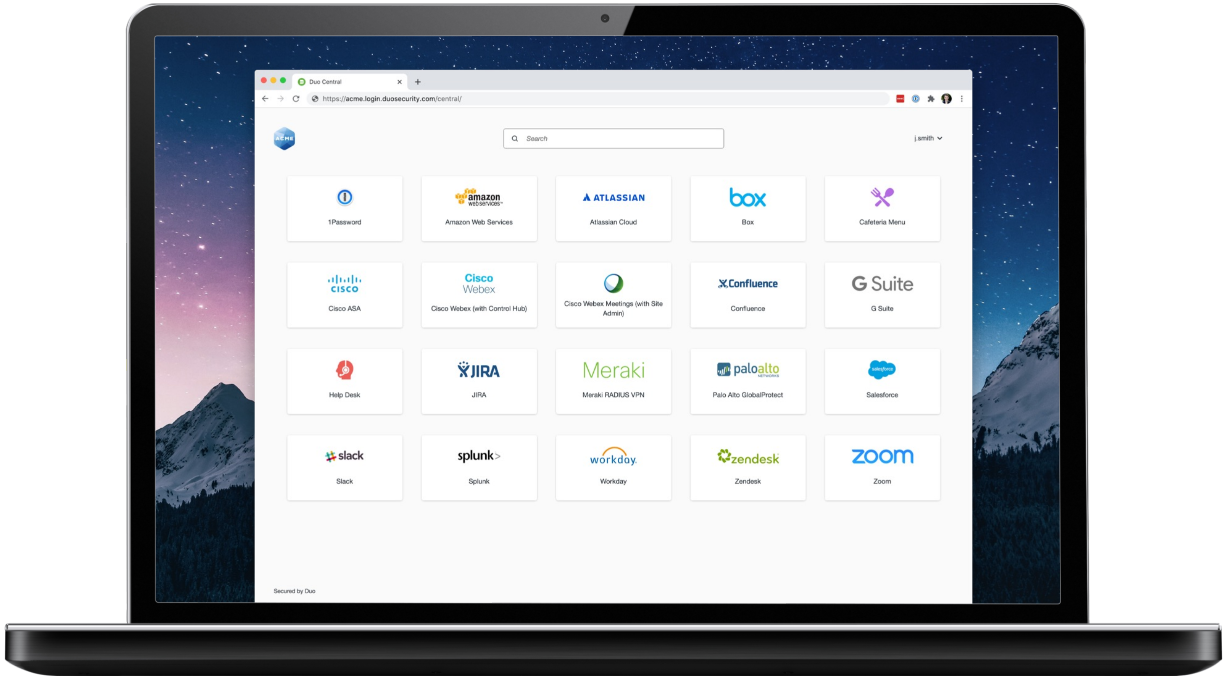
Give organizations control over which devices
can access corporate apps and resources

Mitigate Risk

When limited authenticator options are available

Enable Access

Simplify user experience while easily controlling who can access which corporate applications



Secure any corporate application

Covers the widest array and unlimited number of applications

Single Sign-on

Allow users to login only once to access multiple applications

Provide VPN-less Remote Access

Enable users to securely and easily
access on-premise resources

Why Duo

Cisco Zero Trust Deployment

170,000+ devices secured

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

100,000+ users onboarded

Only < 1% contacting helpdesk, $500,000 per year savings in helpdesk support costs

+

410,000+ fewer VPN auths/month

Users no longer need the VPN for access to over 100 applications (on-prem and SaaS), $3.4M in employee productivity savings per year

5-month deployment timeline

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

CISCO DUO

“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

Duo Partner Sales Plays

- Learn more

FTC Safeguards Rule Amendment

On December 9, 2022, the Federal Trade Commission (FTC) expanded the definition of a financial services company to include any company that processes and stores consumer financial data. As part of this Amendment, Multi Factor Authentication (MFA) and other security measures must be implemented by June 9, 2023.   Impacted companies: Auto Dealerships, Real Estate Brokers, Lending companies, etc.

Cyber Liability Insurance

Cyber Liability Insurance provides businesses with coverage that covers losses in the event of an attack.   These policies can help with ransomware, legal fees, public relations, and more. It's Duo's #1 win rate and covers nearly the entire Cisco Secure Portfolio, plus your value-added services to "wrap around" the offering.

Zero Trust Workshops

Host Zero Trust workshops where your customers can join security experts for a hands-on workshop to learn how they can successfully adopt a zero-trust security approach. Attendees will learn how to assess zero-trust readiness, gain hands on practice with Cisco Secure solutions to address core use cases and learn best practices for positioning Zero Trust.

What's Next - Cisco Security Partner Offers Overview

DISCOUNT

Security Step-up

Deploy three powerful lines of defense that are simple, secure, and empowering to your customers' business with Umbrella SIG, Duo and Email Threat Defense - in a single step.

Partner Benefit

Partners can earn up to 75% discount by leveraging this offer with Security Deal Registration and up to 70% discount with deal quoting.

Learn More

DISCOUNT

Connect and Protect Offers

Take advantage of hyper-competitive upfront pricing and rebates by selling Secure Firewall, AnyConnect, Umbrella DNS and Umbrella SIG to your customers.

Partner Benefit

Partners can earn up to 80% discount on Cisco Secure products, up to 25% incremental partner discounts for solutions support and adoption services and incremental 10% VIP rebates.

Learn More

DISCOUNT

“One Year on Us” Offer

Offer net new customers one year free when they purchase a minimum three-year subscription to one of our eligible security SaaS offerings.

Partner Benefit

Partners can get up to a 79% discount on eligible products by combining Security Deal Registration Discounts with the “One Year on Us “credit. Partners may use this additional margin at their discretion.

DISCOUNT

Fast Track Regional Discounting

Cisco Secure Firewall & (NEW!) SaaS products. Priced to Win. Increase Velocity & Scale

Partner Benefit

Immediate access to the right price with instant discounts.

Learn More

REBATE

Value Incentive Program (VIP)

Sell Cisco Firewall (NGFW & ASA) and other hardware to earn up to 7% rebate. Connect and Protect deals earn up to 17% rebate.

Learn More

Perform Plus

Earn and grow more through Perform Plus! Overall growth rebate + incremental 6% portfolio bonus on SaaS and Firewall by focusing on SMB customers.

Learn More

REWARD

Partner Seller Rewards

Double UP with Security aa In the Americas, Partner Sales/Account Manager (AM) & Systems/ Sales Engineer (SE) each can earn up to $3,000 per deal (maximum of 2 claims are eligible per deal) for selling specific Cisco Secure solutions.

Learn More

Shogun Rewards Partner SEs within the Partner Shogun Program are eligible for Shogun point payouts for completing specific inventive actions.

Learn More

The MFA Competition

The **Global Multifactor Authentication (MFA)** market is projected to reach 18.96 billion USD by 2025.[1]

Worldwide revenues for Unified Endpoint Management (UEM) are expected to grow to over 6 billion USD by year-end 2025.[2]

You’ll encounter competitors that fall into two tiers

Tier one competitors

okta

Microsoft

Tier two competitors

Legacy players

RSA

SECUREAUTH

gemalto

Niche players

Ping Identity

Centrify

imprivata

Microsoft as a technology partner

Duo is a key member of the **Microsoft Intelligent Security Association**.

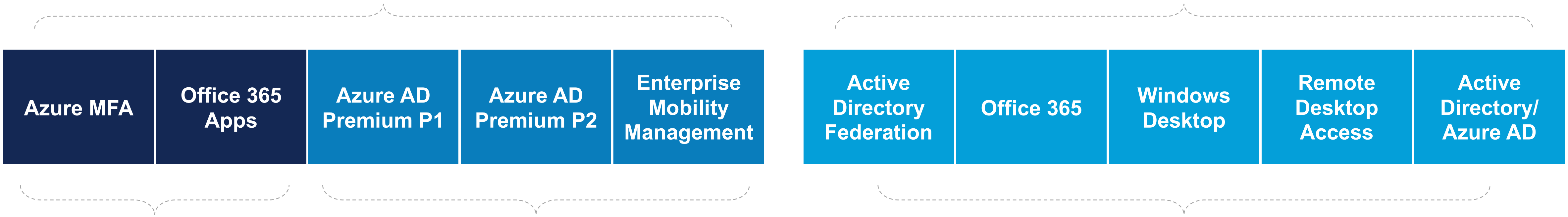
Duo also participates in **Microsoft's One Commercial Partner (OCP) Program**.

Microsoft is also an important partner in **Cisco's ecosystem**.

Microsoft overview

Microsoft's identity platform is comprised of:

Duo protects Microsoft's product suite:



Azure MFA

Office 365 Apps

Azure AD Premium P1

Azure AD Premium P2

Enterprise Mobility Management

Active Directory Federation

Office 365

Windows Desktop

Remote Desktop Access

Active Directory/ Azure AD

Where Duo goes head-to-head

Offers comprehensive, specialized alternative to Azure MFA

Where Duo integrates

- Provides a native authentication method in Azure AD Premium P1
- Supports other Microsoft solutions

Where Duo protects

Provides value for Microsoft customers by protecting key Microsoft services

Measuring strengths and weaknesses

Microsoft strengths

- Microsoft offers attractive "bundle" pricing
- Microsoft is a household name

Microsoft weaknesses

- Coverage of on-premises applications is limited
- Device visibility is not native to Microsoft MFA
- Microsoft MFA has a complex pricing model

Gaining the conversational advantage

- **Call out Duo's comprehensive regulatory compliance and risk mitigation characteristics**
- **Showcase Duo's device coverage**
- **Highlight Duo's unified app platform and admin panel**
- **Show Duo's broad app coverage by moving to a POV with non-Microsoft apps**
- **Identify a champion who can influence decision makers**
- **Leverage partnerships and Duo's ability to support Microsoft environments**

We Would Love Your Feedback!

- **What topics would you like to see covered in the future?**
- **Where have you faced challenges selling Duo and Umbrella?**
- **Where have you found success selling Duo and Umbrella? Any recurring use cases?**

Please respond in chat or email me at evolve@scansource.com Thanks!

Thank you!
Q&A

cisco SECURE