

Cybersecurity in a Remote Work Era



Agenda

- 1 Introductions
- 2 IT and Security Landscape
- 3 Cisco Duo
- 4 Meraki
- 5 Evron Wrap-Up
- 6 Q&A Session

Presenters



Amit (Sunny) Sahni

Executive Vice President &
CTO at Evron



Trevor Darr

Business Development
Manager at Duo Security



Peter Fasano

Virtual Sales Specialist
at Cisco Meraki

Evron's 4 Solution Pillars to Drive Business Success



Business anywhere



Safeguard your business



Grow efficiently



Connect with customers





By Pia Araneta • Global News

Posted June 11, 2021 8:00 am • Updated June 12, 2021 12:07 pm

Should you be worried about the biggest password leak in history?



Money expert Kelley Keehn breaks down the largest password hack, rise of online scams and Canadians' growing consumer debt — Jun 9, 2021

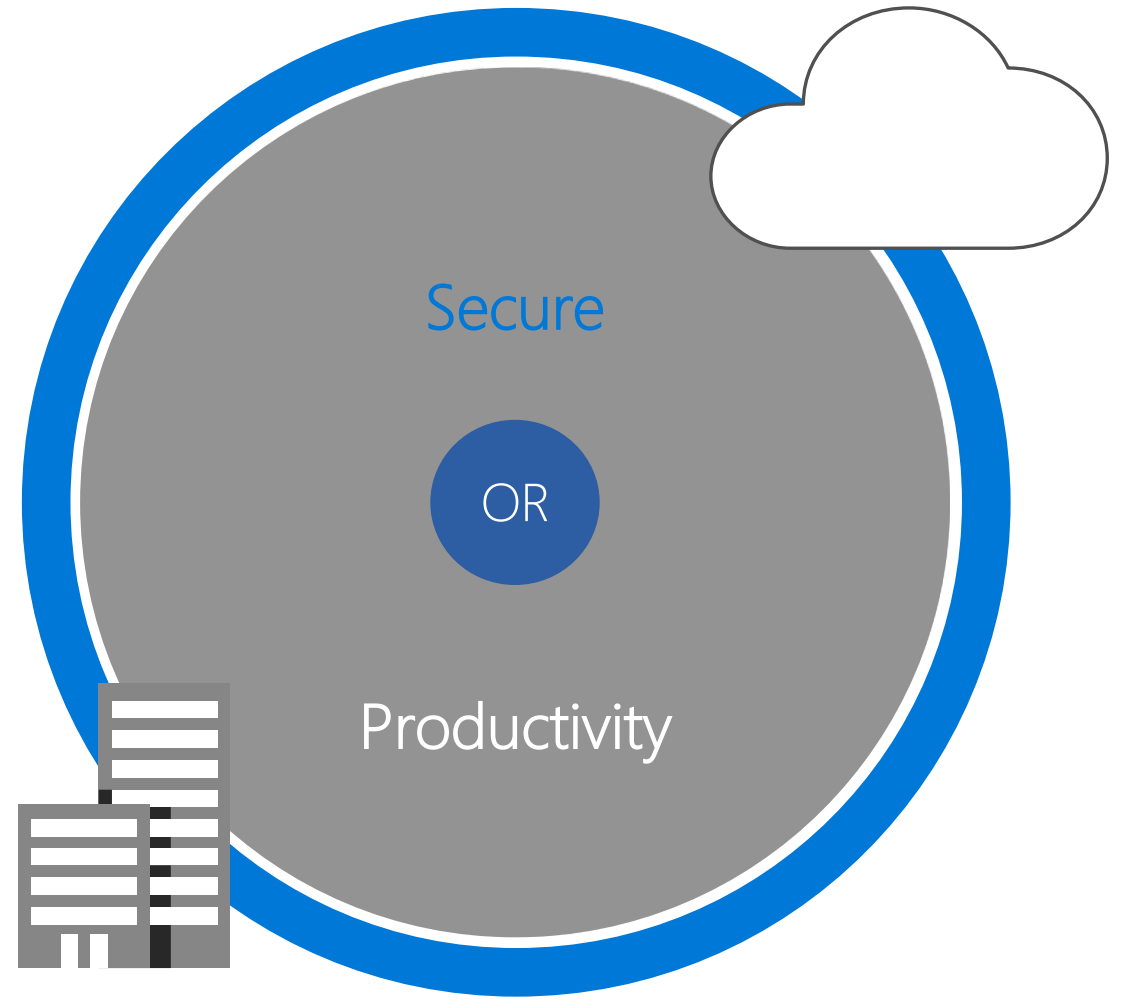
“A compilation of 8.4 billion words, phrases and previous password leaks was shared on a hacker forum... RockYou2021.”



YOUR
IT ENVIRONMENT



How do we enable productivity without compromising security?



It's a delicate balance

Duo Security

Trevor Darr, Duo BDM
trdarr@cisco.com



Agenda

Duo Overview

Features and Benefits

Questions to Ask

Editions and Pricing

Resources

What is Multi Factor Authentication?



Answer:

Something you know



Something you have



Security Risks Persist with Traditional MFA

Poorly deployed, cannot support
all applications;
exposing security gaps

No help for device vulnerabilities

81%

of breaches leverage
either stolen or weak
passwords

72%

of breaches due to
device
vulnerabilities





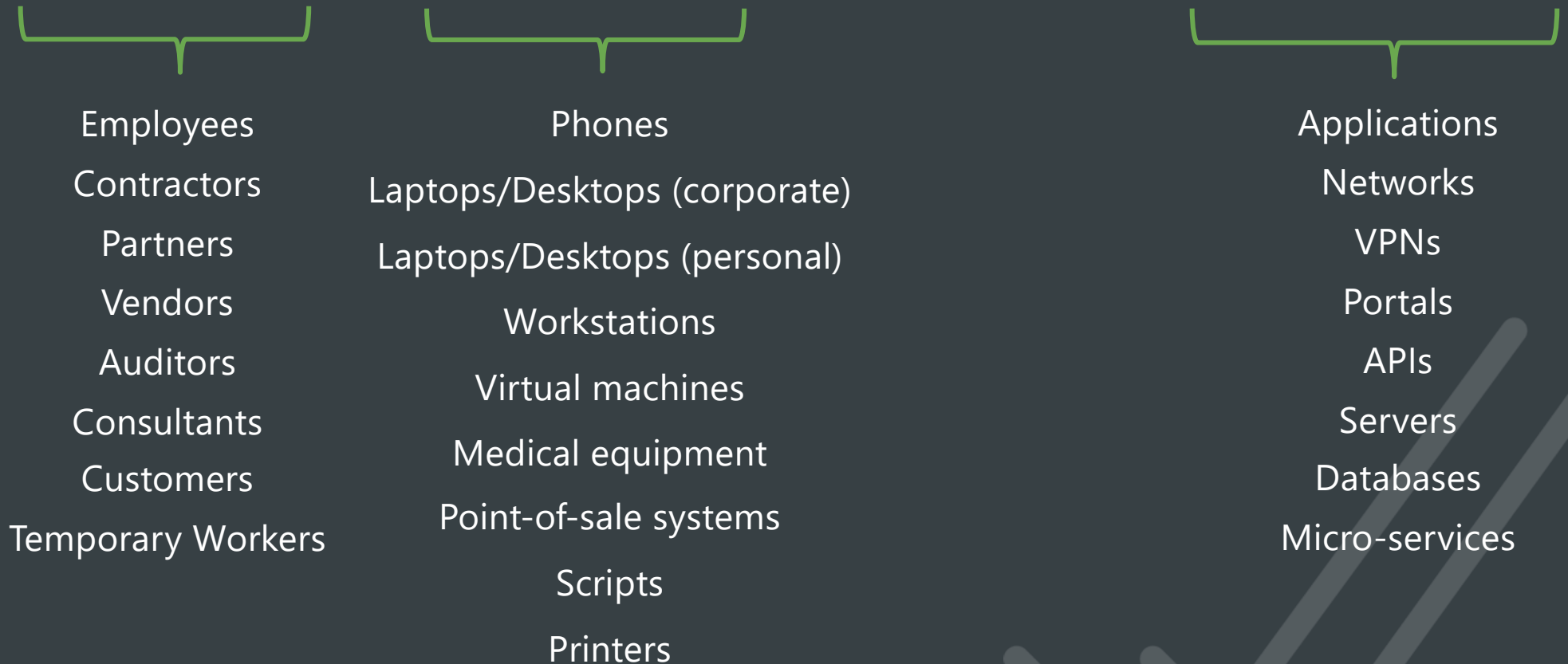
Duo Overview

Duo Security Provides:

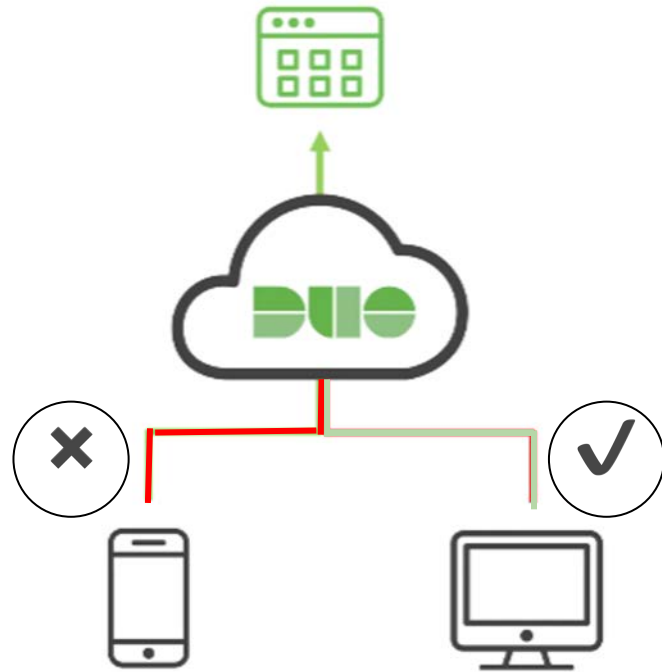
Secure access for
all users connecting to
any application from
any device



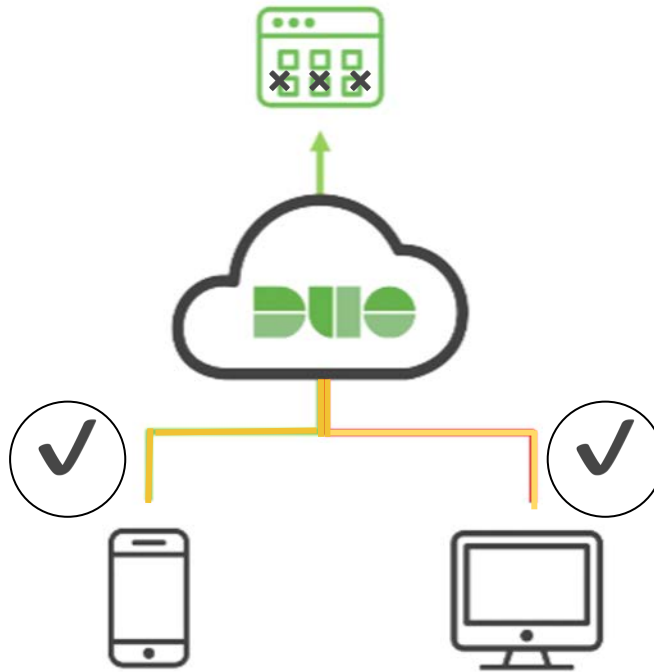
Secure how someone or something is accessing work assets.



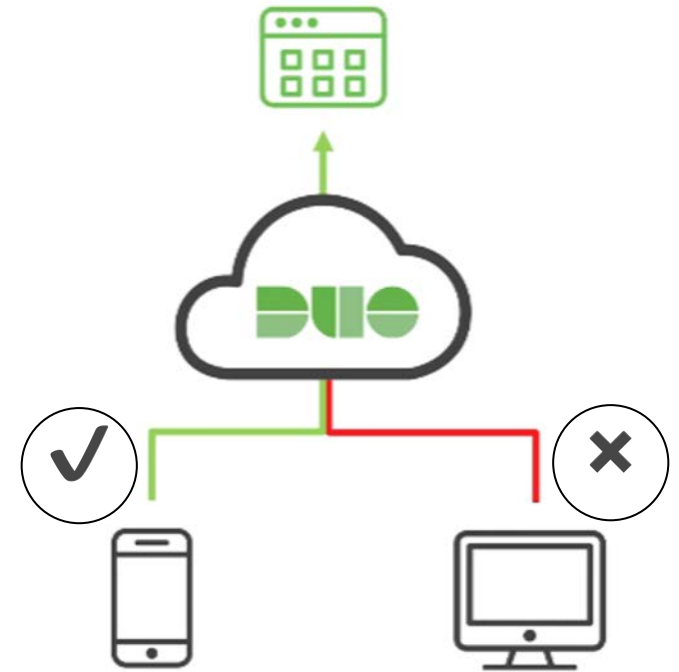
If you can't *Directly Manage* All Devices, Still *Verify* with Access Policies



No Personal
Phone if Out of
Date

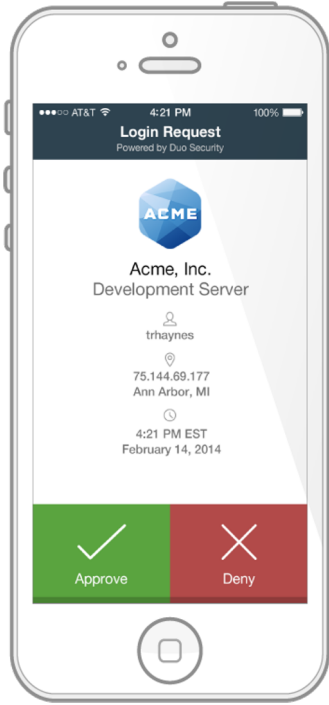


Vendor,
Auditor, or
Consultant
Phone &



No Personal
Laptop

Easiest and Most Secure MFA



- One tap authentication, no codes to enter
- Several authentication options for end-users
- No shared secrets; Out-of-band authentication

Authentication methods for your end-users



Push



Soft Token



SMS



Phone Call



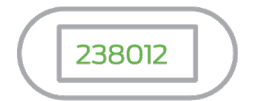
U2F



Wearables



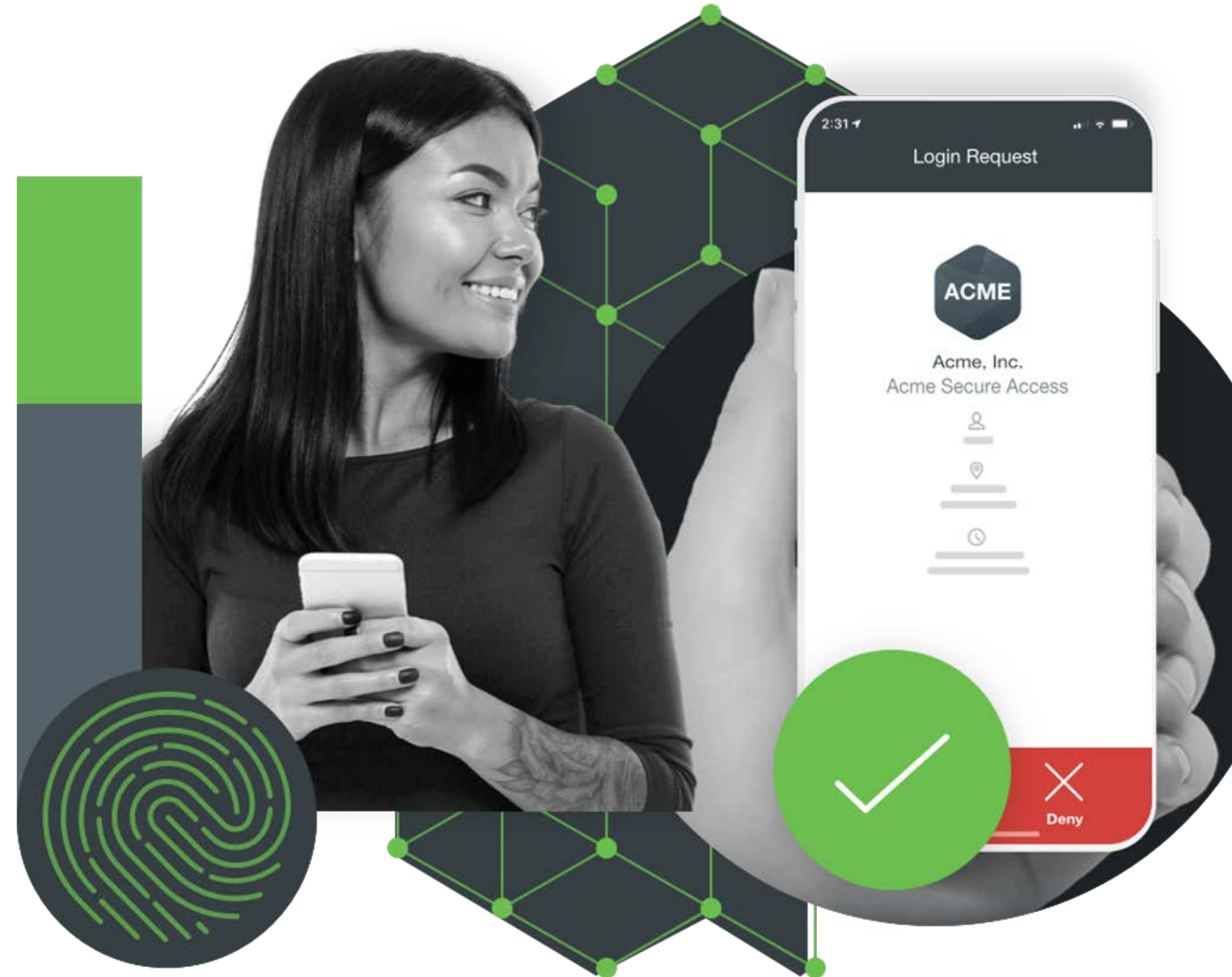
Biometrics



HW Tokens

Duo is the World's Easiest and Most Secure MFA

- One-tap Authentication (No Codes)
- Absurdly Quick to Deploy
- Simply User Enrollment
- Agnostic Partnerships
- Named Integrations & generic protocols
- Consistent User Experience
- Easy to Manage
- Customizable Policy Control
- Unlimited Applications & Policies
- High NPS Score

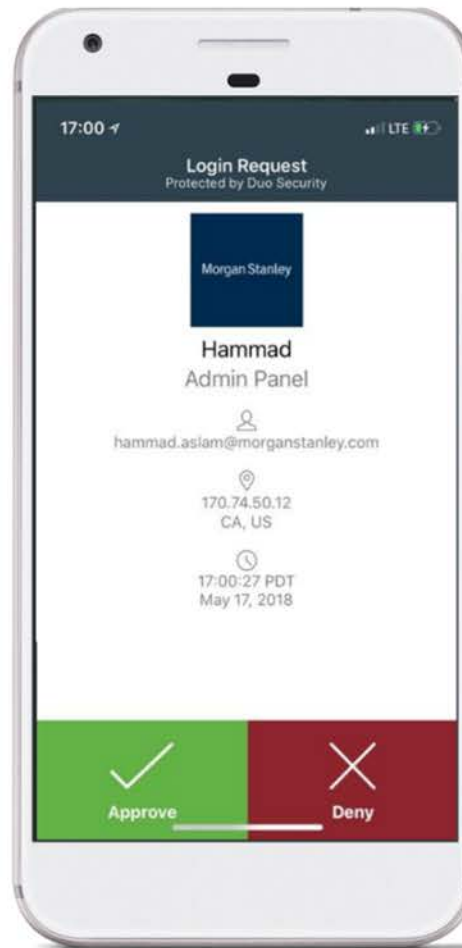


Easy to Use & Deploy

Easy to Onboard and Deploy



Automated and Extensible



Reduce Security Burden of IT



"The industry needs to change the way it looks at security. We need to make the process simpler, smarter and more secure. Period."

– Jon Oberheide, CTO & Co-Founder

**Loved by users
AND security staff**



Top 3 Reasons Customers Choose Duo

Easy

- Deploy in hours
- Least friction for end users
- No change in login workflows
- Out-of-the-box integrations
- Several ease-of-use innovations
- High design values in the product

More Secure

- Truly isolated solution
- Truly out-of-band (OOB)
- No shared secrets
- Automated product updates
- Security standards (NIST, SOC2)
- Fraud alerts from end users

Lower TCO

- No servers to deploy and maintain
- Up to 85% lower help desk calls
- No upgrade/patching costs
- No maintenance cost
- Unlimited integrations with apps
- Truly isolated solution

Here's What We Do ...And How We Do It



① Verify the
**Identity of
Users**

—
MFA



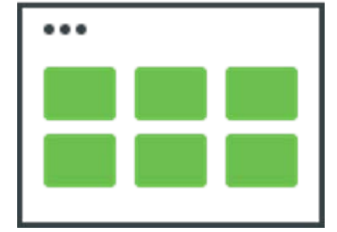
② Verify the
**Health of their
Devices**

—
Device
Checks



③ Control which **Users**
and Devices gain
access

—
Access Control
Policies

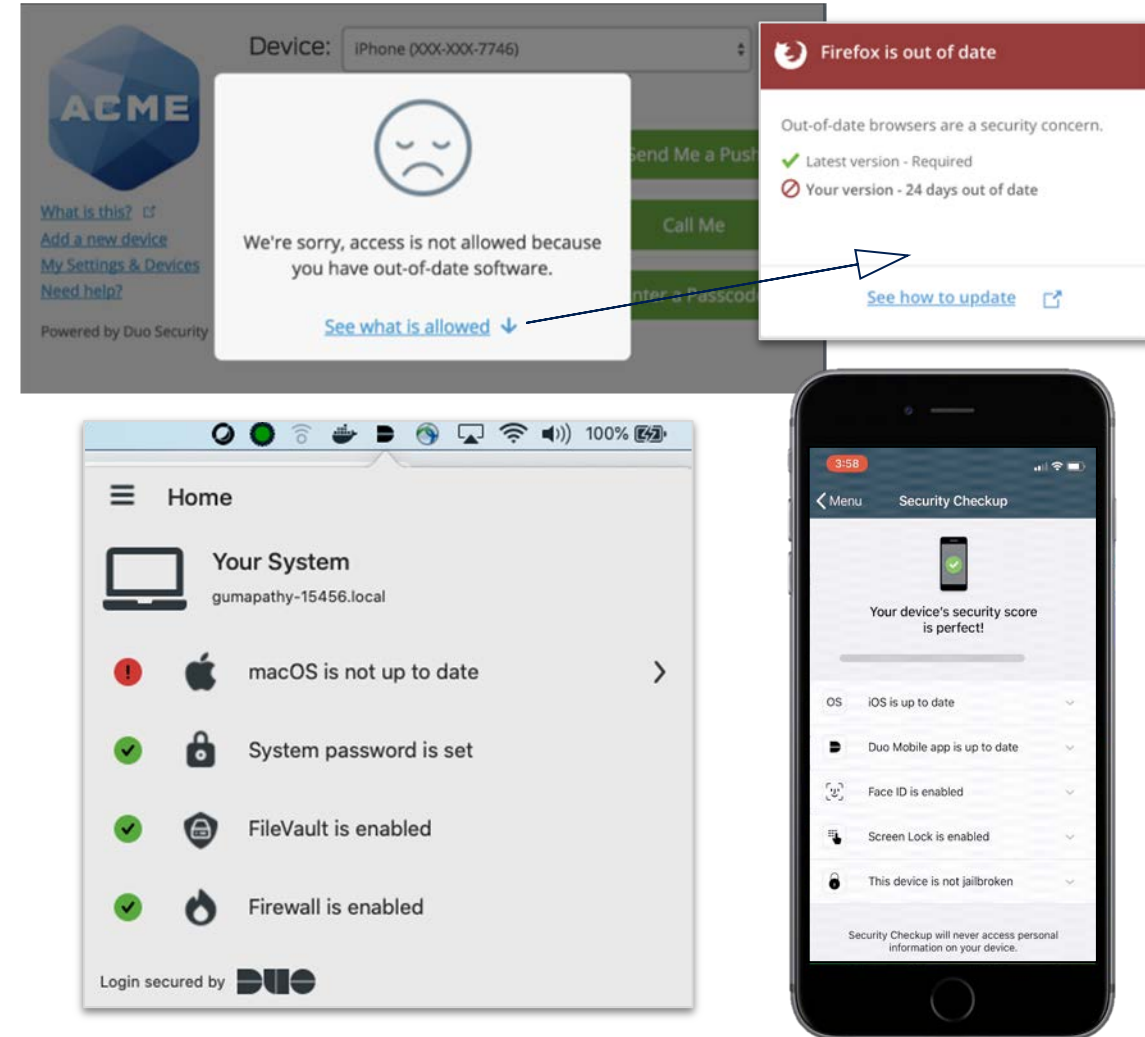


④ Protect **all the**
Applications they
use, **all the time**

—
Zero Trust &
SSO

② Verify the Health of their Devices - Device Checks

- Verify Device Health at every authentication attempt
- Check hygiene of all devices (main vs. second-factor device, BYOD vs. corporate, etc.)
- No “agent” required to deploy Duo, but we can integrate with your existing tools (e.g. MDM)



③ Control which Users and Devices gain access - Access Policies

- Apply layered policies to everyone, one user or application, or groups (e.g. department or office location)
- Blocking and/or Remediation prompts can be configured to your needs
- Ensure consistency across all users & devices at access, and monitor device health continuously via tools like AMP

The image shows a 'Global Policy' configuration page with a list of security settings. A modal window is open, displaying an alert titled 'Unrealistic Geovelocity'. The alert states: 'The velocity between the two authentications is not plausible. ~7389 miles in ~19 minutes'. It compares two authentication events: 'Previous Authentication' in 'Bohemia, NY' and 'This Authentication' in 'Shanghai, SH'. Below this, it shows IP ranges and carriers for both locations.

Policy Name	Status	Description
New User Policy	Enabled	Allow unenrolled users to pass through without two-factor authentication.
Authentication Policy		Require two-factor authentication or enrollment when applicable, unless there is a superseding policy configured.
User Location	Enabled	No action: Canada, United States. All other countries: Deny access.
Trusted Endpoints		Allow all endpoints.
Device Health Application		Don't require users to have the app.
Remembered Devices	Enabled	Users may choose to remember their device for 4 hours for all web applications.
Operating Systems	Enabled	Show restrictions
Browsers	Enabled	Notify users when their browser version is out of date. Block users when their browser version is more than 2 weeks out of date. Only allow devices accessing applications using Chrome Mobile, Chrome, or Firefox.
Plugins	Enabled	Block devices
Authorized Networks		No network
Anonymous Networks	Enabled	Deny access
Authentication Methods	Enabled	Only allow
Duo Mobile App	Enabled	Require up
Tampered Devices	Enabled	Don't allow
Screen Lock	Enabled	Don't allow
Full-Disk Encryption	Enabled	Don't allow
Mobile Device Biometrics	Enabled	Require ad

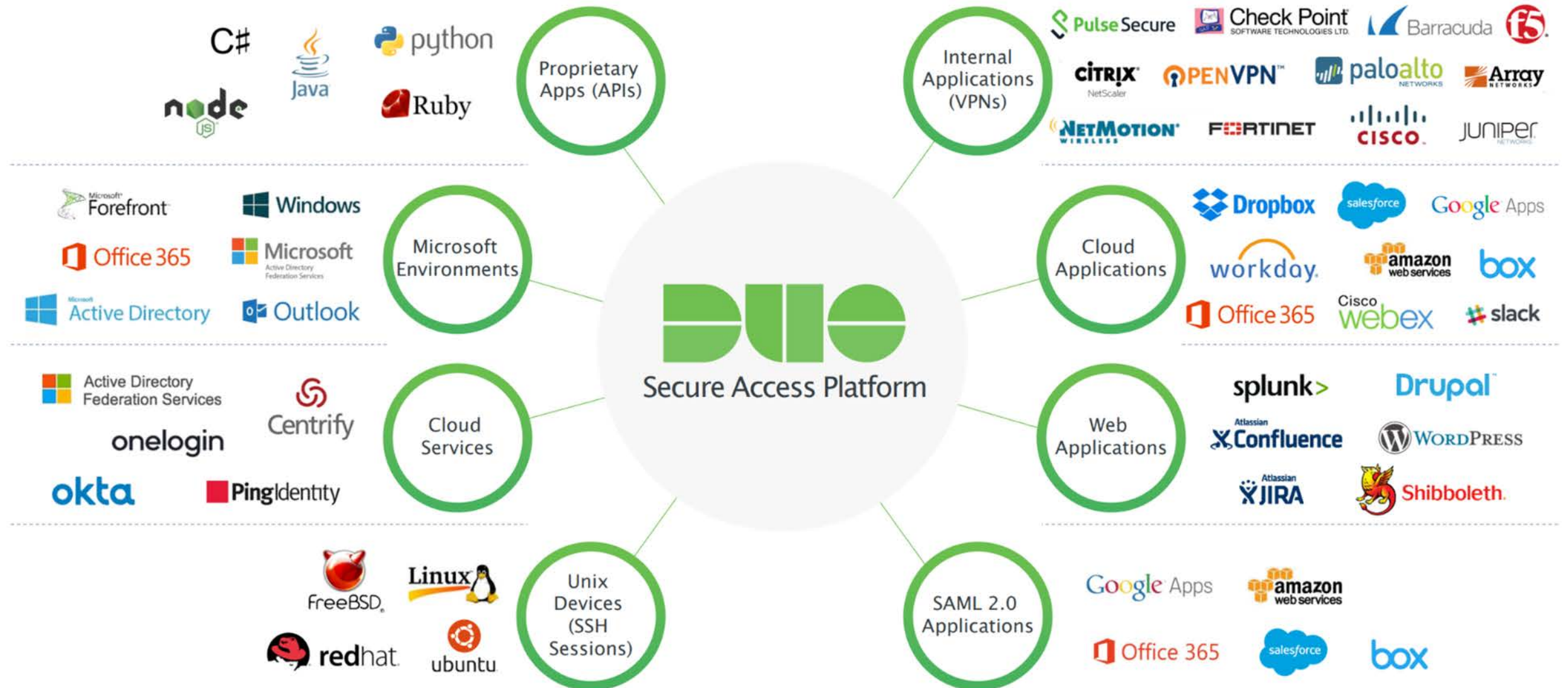
Unrealistic Geovelocity

The velocity between the two authentications is not plausible.

~7389 miles in ~19 minutes

Previous Authentication	→	This Authentication
Bohemia, NY		Shanghai, SH
IP Range and Carrier		IP Range and Carrier
198.206.46.0/23, national oceanic and atmospheric administration		17.88.224.0/19, apple inc.

④ Protect all the Applications they use, all the time - ZT & SSO



Duo MFA



- Protect application access with flexible two-factor authentication
- High-level summary of device hygiene
- Automate the management of your Duo solution through Admin API's
- Single Sign-On offering to provide seamless and secure access across on-prem and cloud applications
- Protect any application - cloud or on-premise



Duo Security is
now part of Cisco.



Duo Access



- Complete **visibility** into devices accessing applications
- Evaluate both **mobile and laptop security hygiene** at the point of access
- Enforce **access policy** on who can access which applications under what conditions
- Encourage users to **update their devices** by enforcing access based on device hygiene
- **Security analytics** feature Trust Monitor that highlights anomalous and risky logins



Duo Security is
now part of Cisco.



Duo Beyond



- Detect if a device is **managed** or **unmanaged**
- Detect if a device has the proper **antivirus** or **EDR** software installed
- Evaluate if endpoint has been compromised before allowing access
- Enforce policies to allow only healthy, managed devices to access sensitive applications
- Enable **secure, granular remote access** to on-premise web applications and infrastructure



Duo Security is
now part of Cisco.



Duo MFA

Duo Access

Duo Beyond

MFA	✓	✓	✓
SSO Cloud Apps	✓	✓	✓
Adaptive Authentication		✓	✓
Device Visibility		✓	✓
Device Remediation		✓	✓
Trusted Endpoints			✓
VPN-less Remote Access			✓

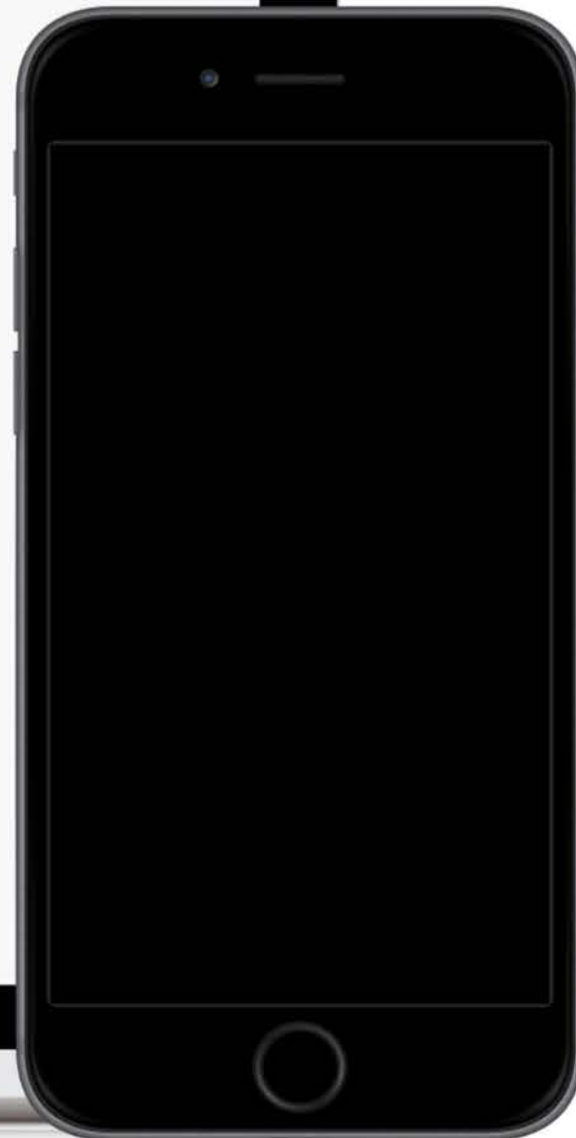


Email:

chris@acmecorp.com

Password:

 sign in





[What is this?](#)

[Add a new device](#)

[My Settings & Devices](#)

[Need help?](#)

Powered by Duo Security

Device:

Choose an authentication method



Duo Push RECOMMENDED

Send Me a Push



Call Me

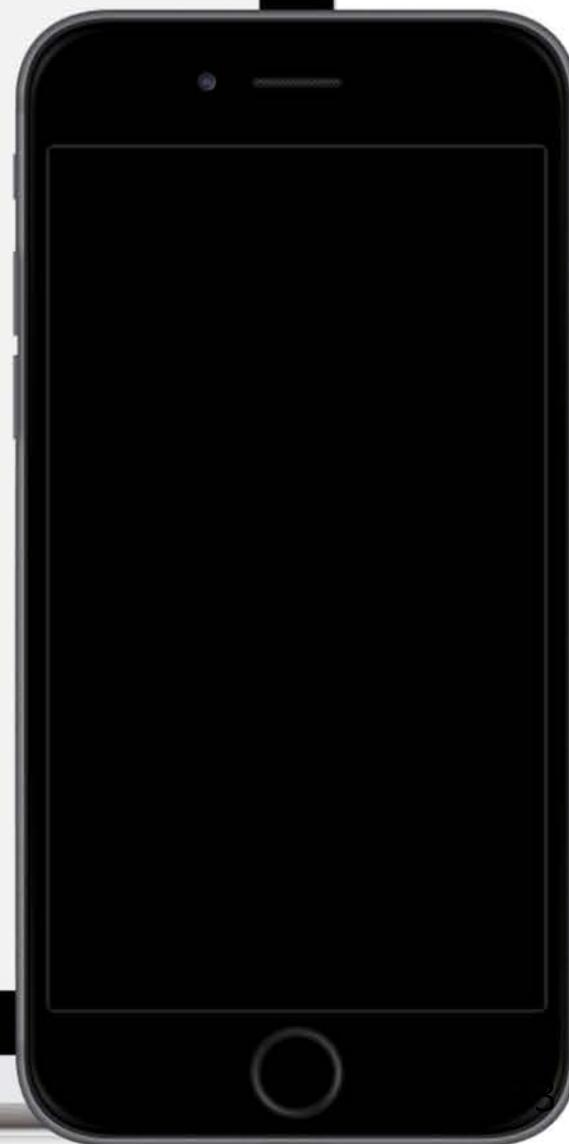
Call Me



Passcode

Enter a Passcode

☐ Remember me for 1 day





[What is this?](#)
[Add a new device](#)
[My Settings & Devices](#)
[Need help?](#)

Powered by Duo Security

Device: iPhone (XXX-XXX-7746)

Choose an authentication method

☒ Duo Push RECOMMENDED

Send Me a Push

☐ Call Me

Call Me

☐ Passcode

Enter a Passcode

☐ Remember me for 1 day

Pushed a login request to your device...

Cancel



2:50

Monday, August 8



Duo Mobile now
Login request: Outlook Web App
slide to view

> slide to unlock





[What is this?](#)
[Add a new device](#)
[My Settings & Devices](#)
[Need help?](#)

Powered by Duo Security

Device: iPhone (XXX-XXX-7746)

Choose an authentication method

☒ Duo Push RECOMMENDED

Send Me a Push

☐ Call Me

Call Me

☐ Passcode

Enter a Passcode

☐ Remember me for 1 day

Pushed a login request to your device...

Cancel

2:47 PM

Login Request
Protected by Duo Security



Duo Demo
Outlook Web App

chris@acmecorp.com

21.63.00.177
Ann Arbor, MI, US

2:47:04 PM EDT
August 8, 2016

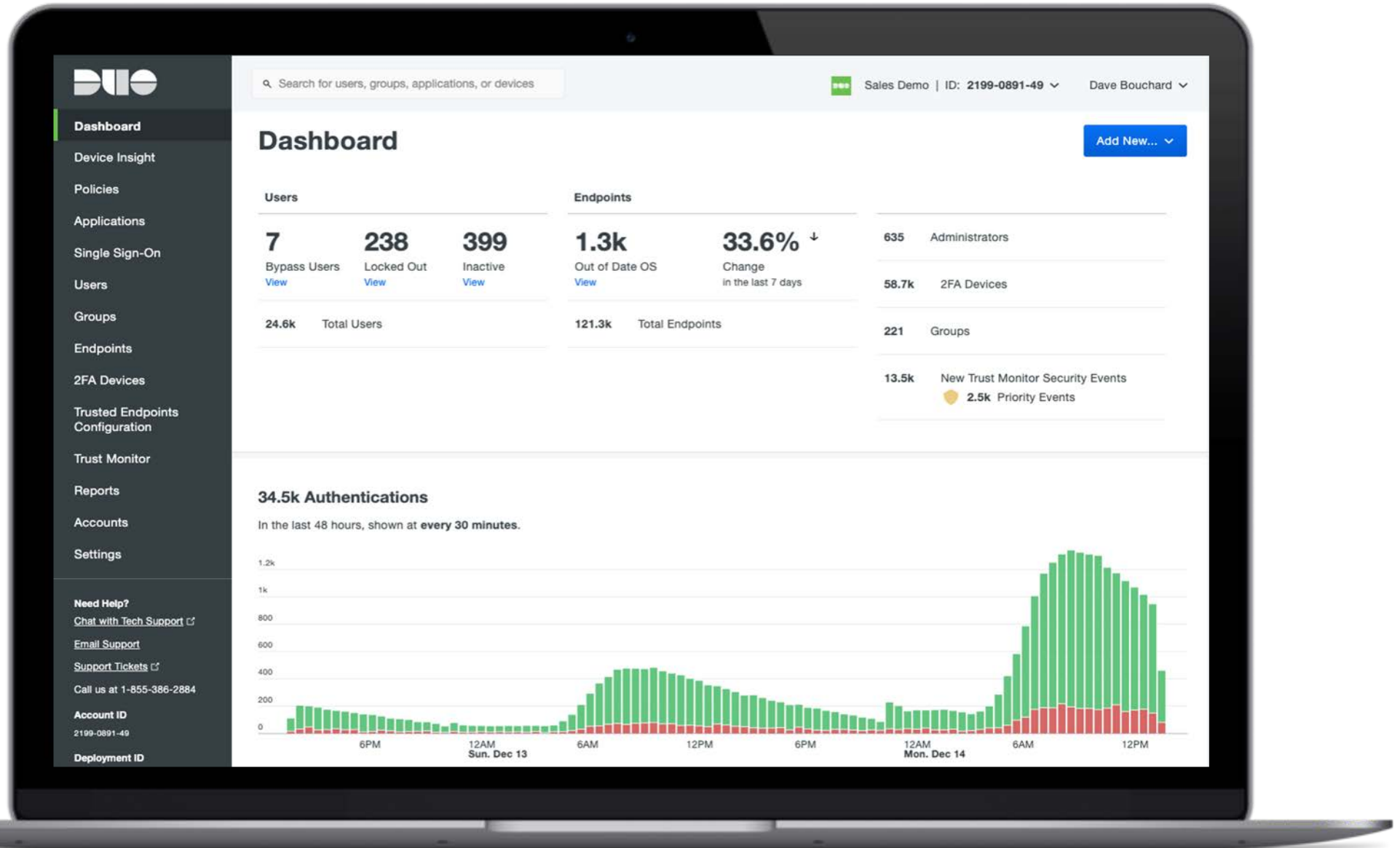
✓
Approve

✗
Deny

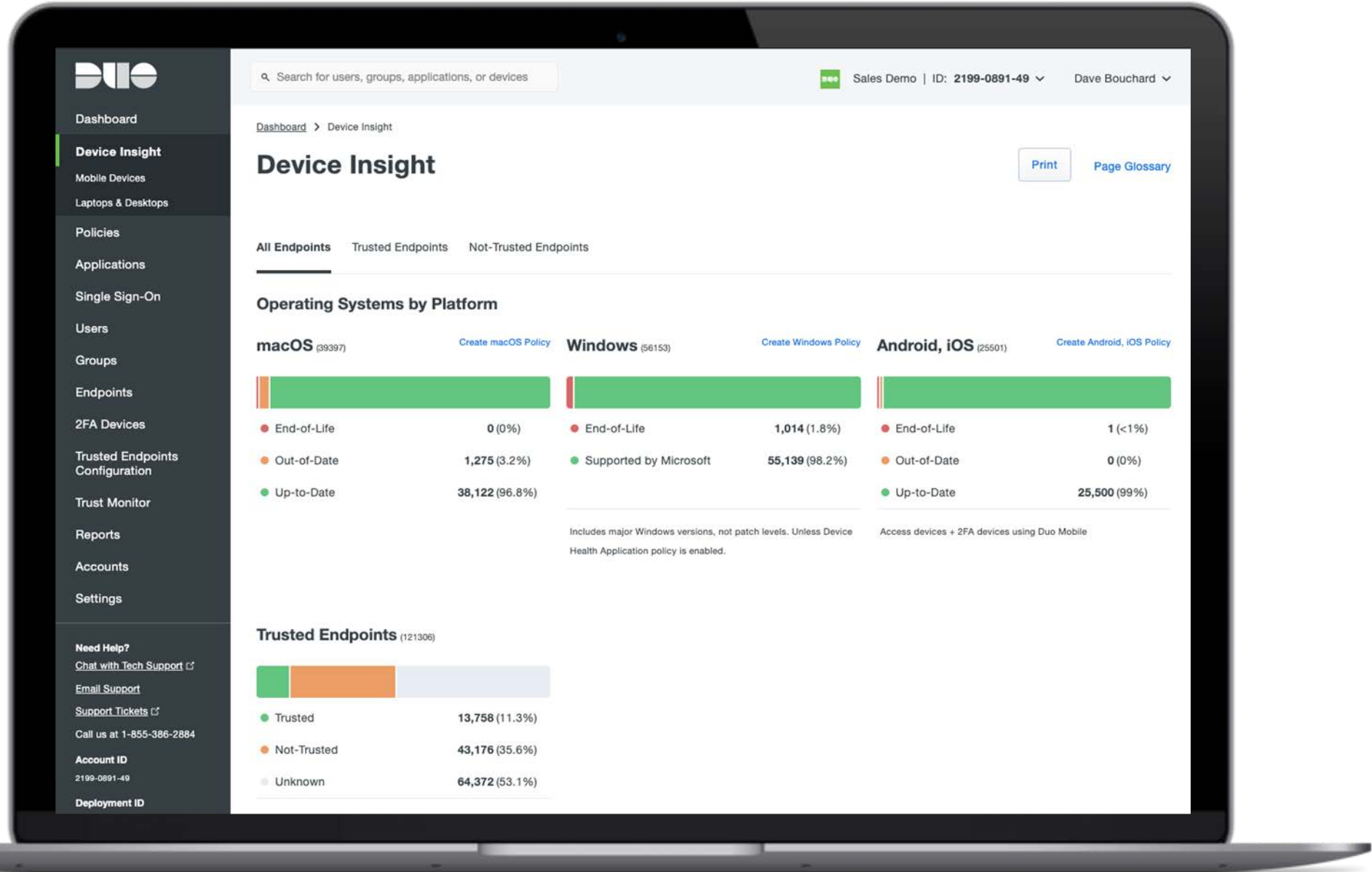


Admin Experience

One Dashboard for Everything



Insights Across Both Managed + Unmanaged Devices



Granular Detail Across All Users

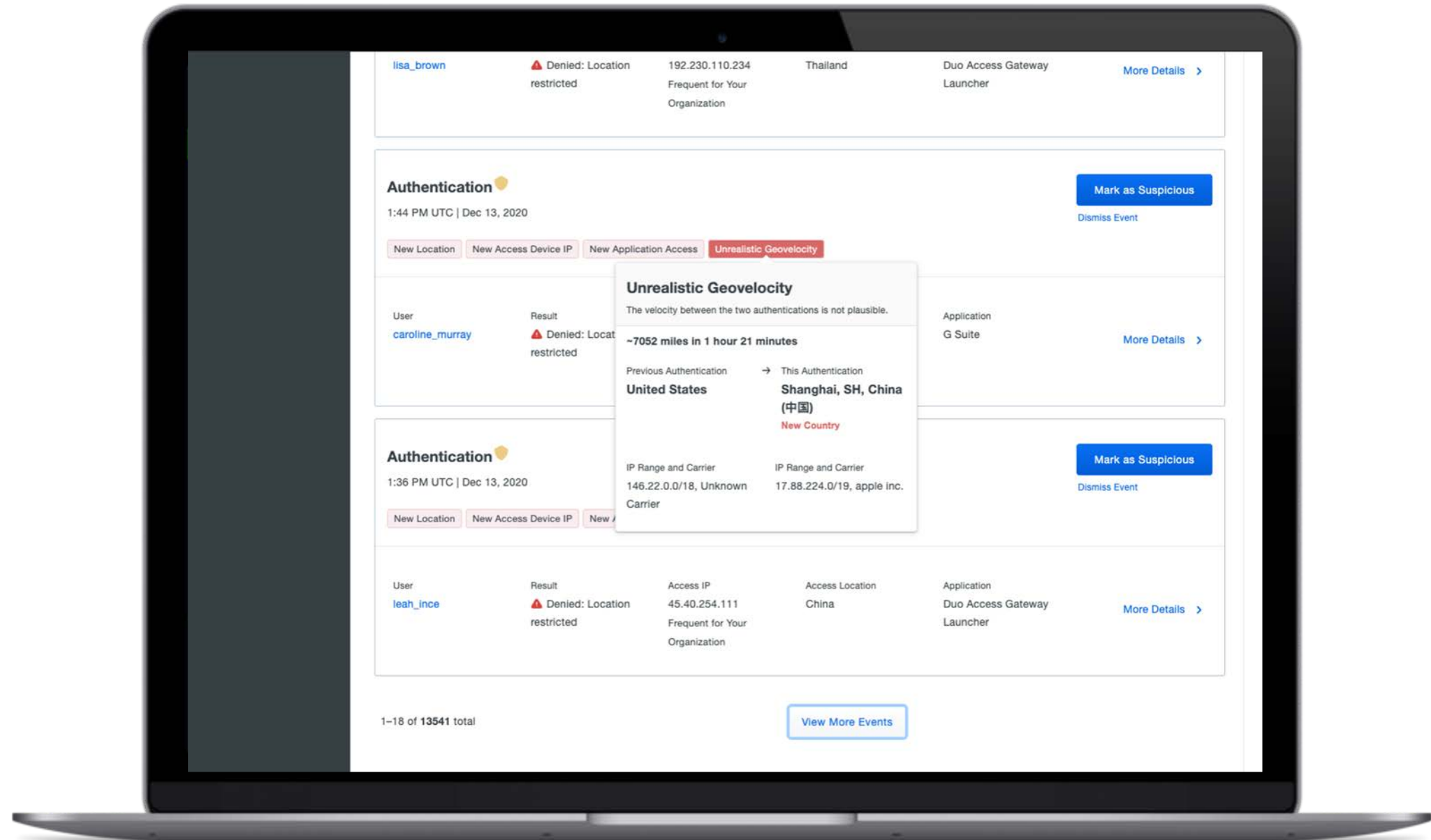
The screenshot displays the Duo Mobile management console. On the left is a dark sidebar with navigation links: Dashboard, Device Insight, Policies, Applications, Single Sign-On, Users, Groups, Endpoints, 2FA Devices (highlighted), Hardware Tokens, WebAuthn & U2F, Trusted Endpoints Configuration, Trust Monitor, Reports, Accounts, Settings, Need Help?, Chat with Tech Support, Email Support, Support Tickets, Call us at 1-855-386-2884, and Account ID.

The main content area is titled 'Phones' and includes a search bar at the top. Below the title are filters for Android and iOS versions, tampered status, screen lock, disk encryption, and biometrics. A table lists individual devices with columns for Device, Platform, Model, Duo Mobile, Security Warnings, and Users.

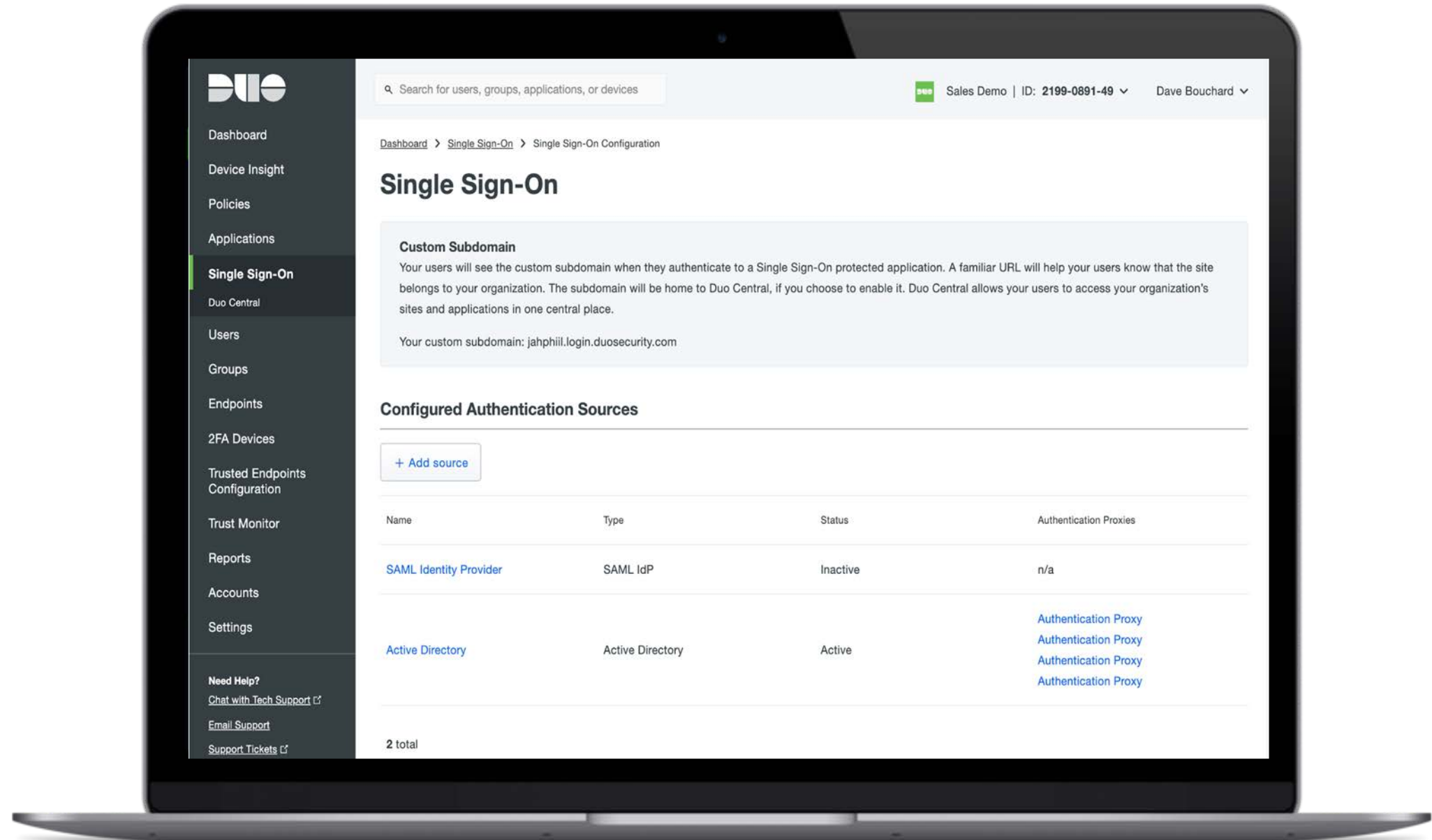
Device	Platform	Model	Duo Mobile	Security Warnings	Users
Generic Smartphone	Generic Smartphone	Unknown		✓ No warnings	joshua_abraham
Apple iPad Air	iOS 12.4.8	Apple iPad Air	3.38.0.21	✗ Passcode Lock Not Enabled	animal
Generic Smartphone	Generic Smartphone	Unknown		✓ No warnings	abigail_allan
Generic Smartphone	Generic Smartphone	Unknown		✓ No warnings	abigail_burgess
Old iPod Touch	iOS	Unknown		✓ No warnings	abigail_avery
Apple iPhone13,4	iOS 14.2.1	Apple iPhone13,4	3.44.0.20	✓ No warnings	admin, dave, testuser2223
Generic Smartphone	Generic Smartphone	Unknown		✓ No warnings	abigail_black
Generic Smartphone	Generic Smartphone	Unknown		✓ No warnings	sean_anderson



Duo Trust Monitor, ML-based Anomaly Detection



Duo Single Sign-On, a cloud-hosted SAML identity provider



Additional Common Use Cases

Cisco AnyConnect VPN - lowest hanging fruit!

O365 - Best solution for securing MSFT O365 (Duo is a native integration)

Protecting SaaS solutions - Salesforce, Workday, Box, etc.

Securing VPN Connections - Cisco AnyConnect, PAN, Pulse Secure, etc.

Privileged Access to Infrastructure - Firewalls, Servers, etc.

Looking for easy multi-factor authentication

Audits & compliance



Key Driver: Meet Compliance Requirements

Every security best practices guide and regulation asks for MFA and device visibility

Meet MFA requirements outlined in PCI-DSS 3.2 Section 8.3



Helps meet NIST 800-63 and 800-171 access security requirements



Meet DEA's EPCS requirements when approving e-prescriptions



Aligned with GDPR data protection laws in Europe



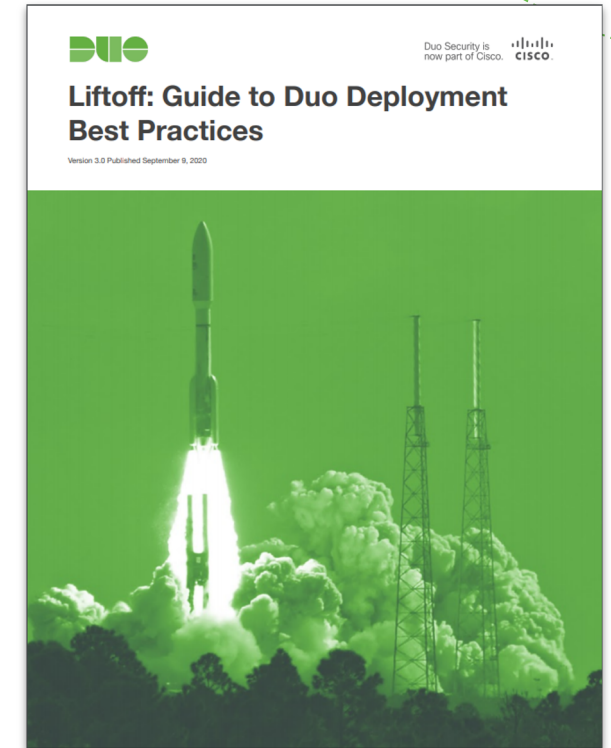
Meet FFIEC requirements for financial applications




Get visibility into personal devices used to access PHI



- Duo's documentation is free and public, with best practice documents and step-by-step guides (screenshots & video) for our integrations
- Our Standard Support staff is here for you
- Premium Support is also available
 - Main Support page
 - For Admins
 - Easy end-user demos
 - End-user guide



A woman with dark hair in a ponytail, wearing a light-colored long-sleeved shirt and a white apron, is standing in a shop or cafe. She is holding a tablet computer and looking at it. In the background, there are shelves with various items, including jars and bottles. To the right, there are several potted plants, including a hanging plant with large green leaves and a plant with small white flowers. The overall atmosphere is warm and professional.

Simpler and more resilient networking

Cisco Meraki for Small & Midsize Business

Topics

SMB trends
& needs

Building on the
foundation of the
Meraki Platform

**Business
resiliency**
solutions

Resources

Lean IT teams are
overwhelmed by **limited**
time, budgets, and
resources





Most IT networking
solutions today
are not simple

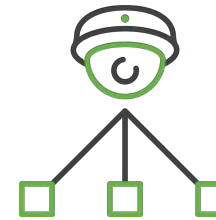
To adapt and thrive, **resilient** businesses need **simple, secure, and intelligent** IT tools for:



SECURE EDGE



FUTURE OF WORK



SMART SPACES

And they need to access & manage their network **from one place**



Connecting **passionate people** to their mission
by **simplifying** the digital workplace.

Thrive with the Meraki Platform

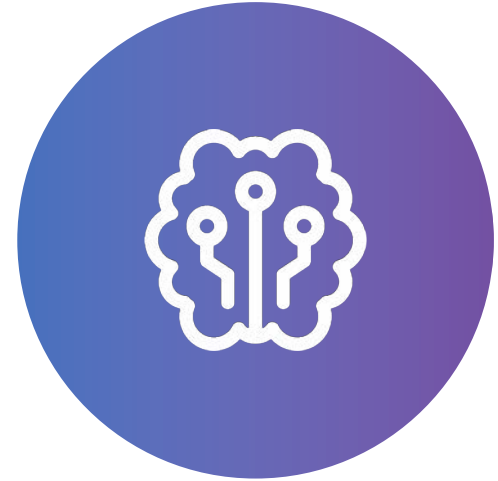
The World's Best Cloud Platform



Simple



Secure



Intelligent

The Meraki Platform

A Complete Cloud-Managed IT Portfolio from a Single Pane of Glass



MR

Wireless Access Points



MS

Ethernet
Switches



MX

Security & SD-WAN
Appliances



MG

Cellular
Gateways



MI

Insight
[Application & WAN]



SM

Endpoint
Management



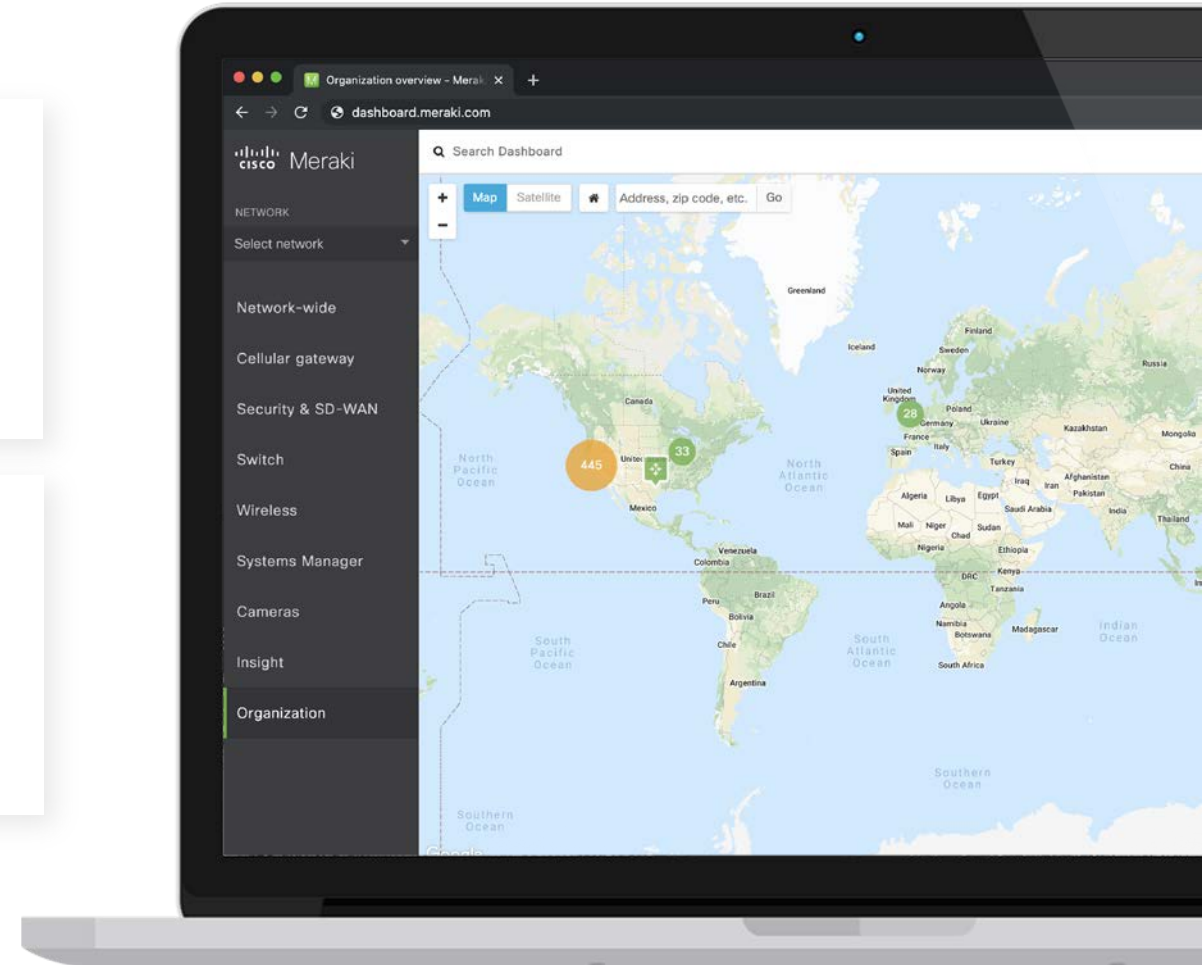
MV

Smart
Cameras



MT

Smart Sensors

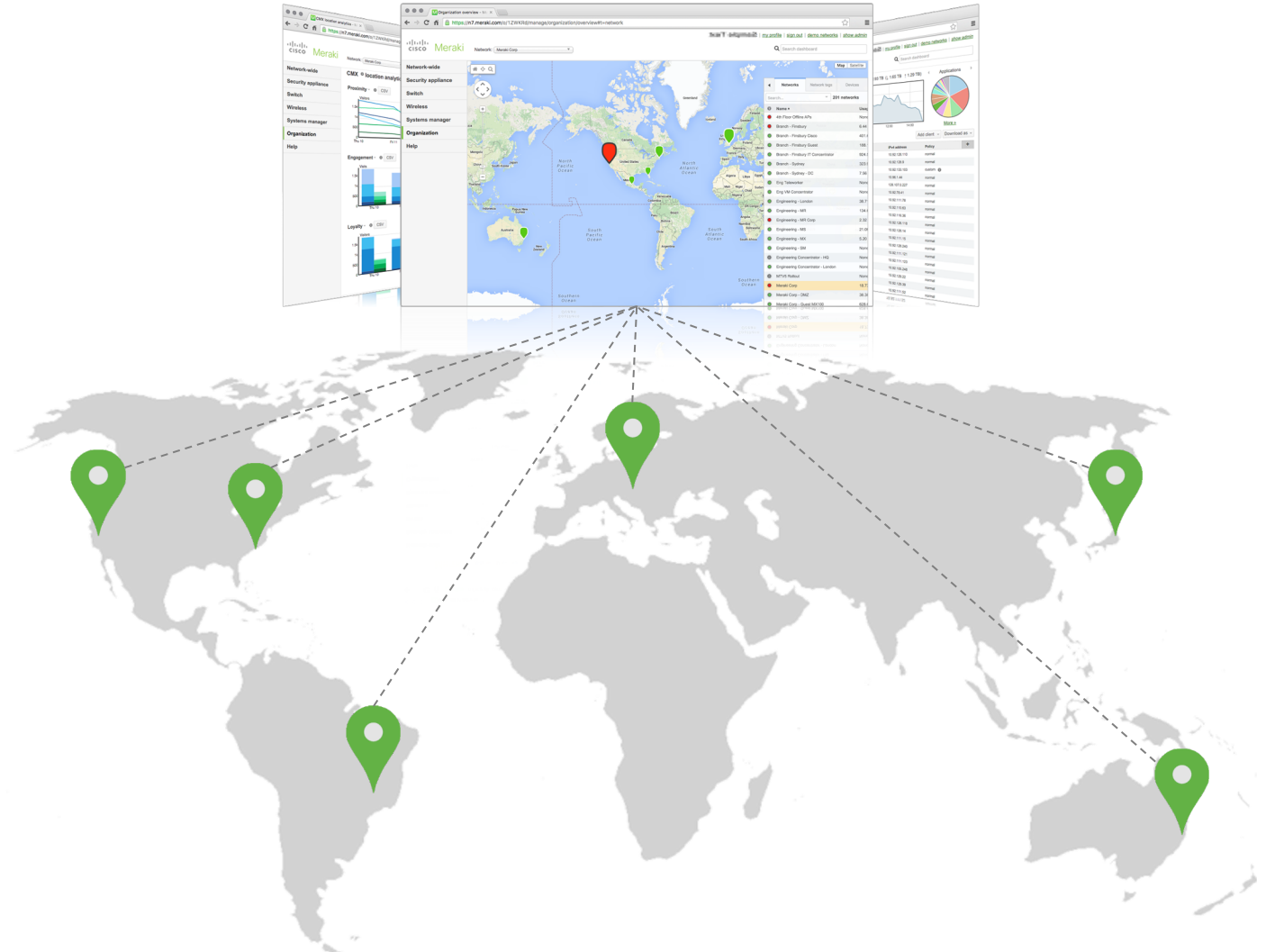


With the Meraki full stack you can...

Deploy and grow networks at branch locations or large campuses **easily and rapidly**

Manage and monitor those networks with robust analytics from a **single pane of glass**

Reduce administrative overhead with **simple all-inclusive licensing** models and tools



Powerful cloud
infrastructure
under the hood

Utterly **simple**,
so you can **do more**
with less.



Benefits of a cloud-managed solution



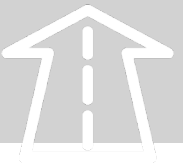
SECURITY



RELIABILITY

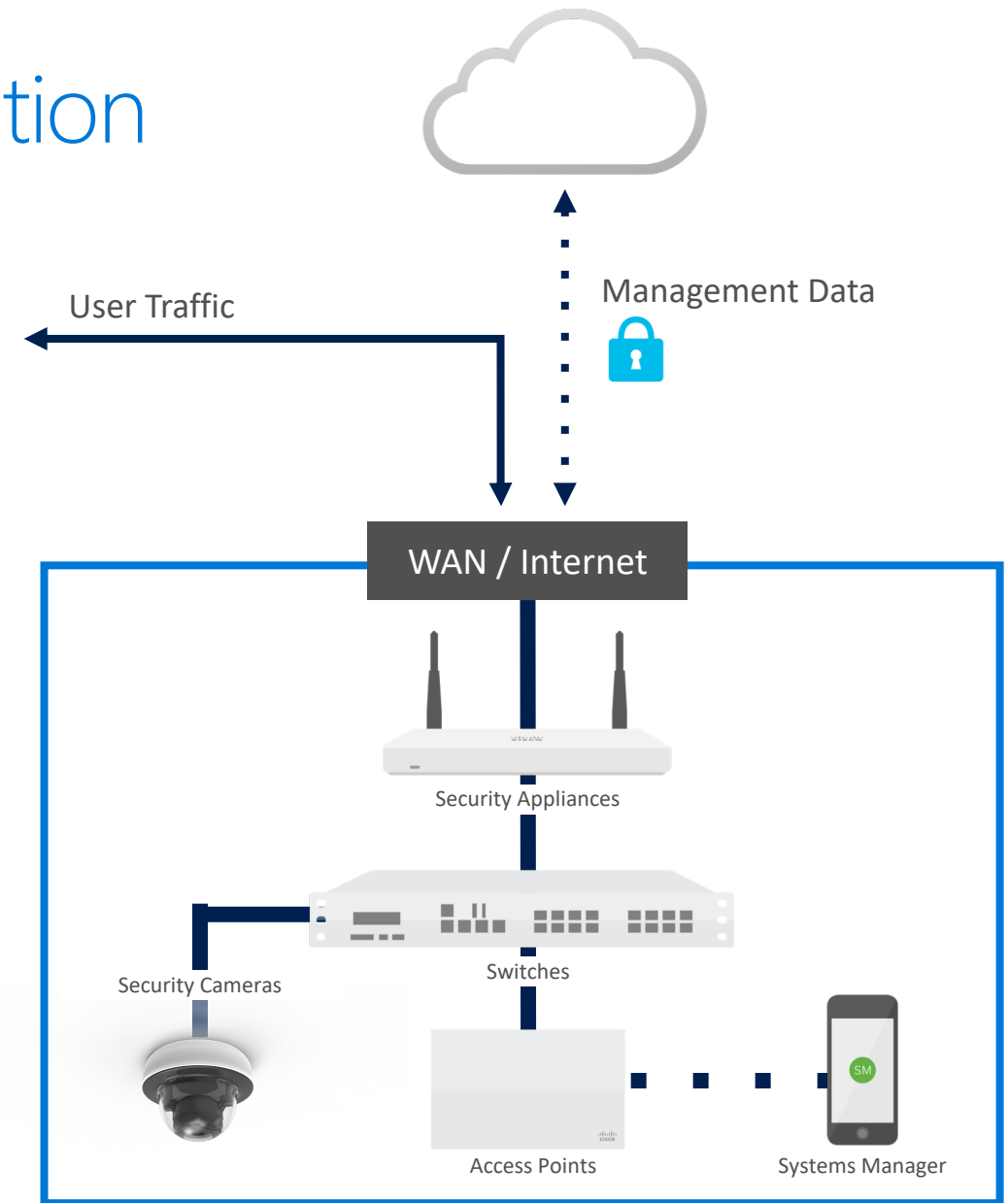


SCALABILITY



FUTURE-PROOFING

Reliability and security information at meraki.cisco.com/trust
GDPR information at meraki.cisco.com/gdpr



DESIGNED FOR

Ease of new

EASY

Plug & play

Save time and costs from utterly **simple** use and troubleshooting, even with limited IT experience

OPERATE

Leaner

Do more with less; **save costs** by continually growing and innovating

EASY TO

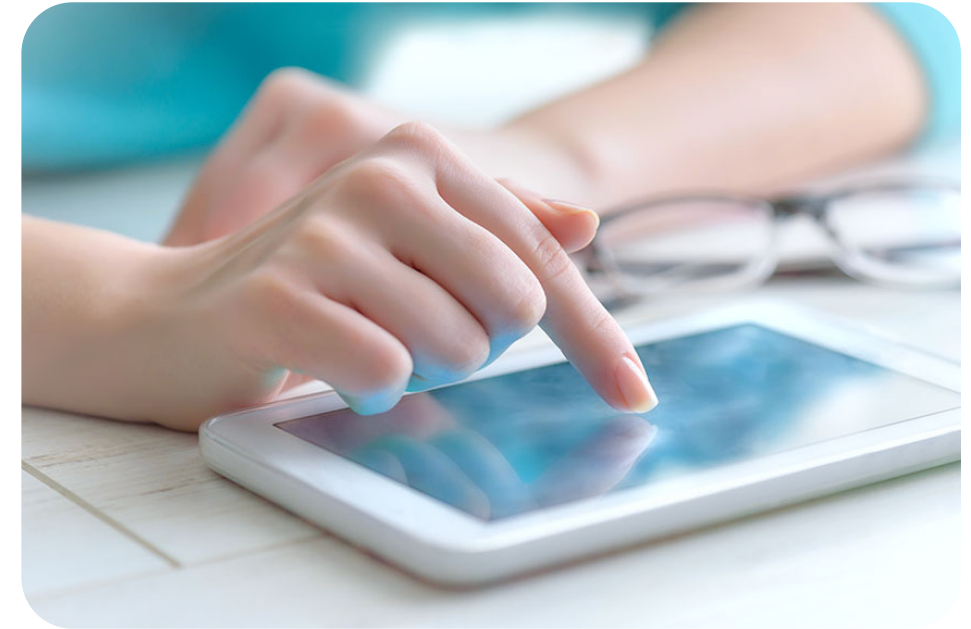
Scale

Have more accessibility to technologies that empower **faster growth** & innovation

SERVE MORE

Customers

Serve more customers in the most demanding environments via **deep insights & analytics**



Out-of-the-box management and open APIs
for deep analytics and intelligence

BUILT FOR

Ease of change

SINGLE **Interface**

Save time through **easy configuration** and monitoring from a single interface

TIGHT **Integration**

Scale via tight integration with the broadest range of networks, applications, and connected devices

RADICALLY **Faster**

Save money & resources from **radically faster deployment, management, & troubleshooting**

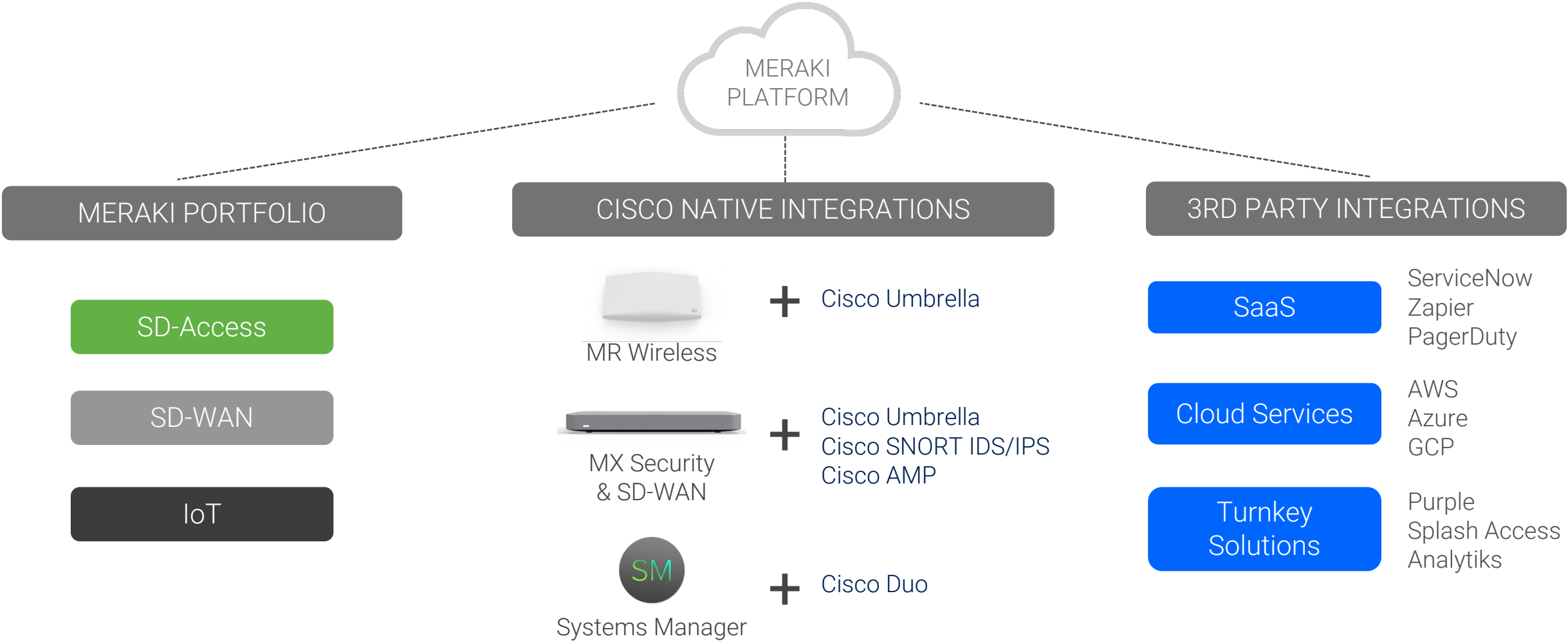
OPERATION **Simplification**

Automate lean IT teams with **real-world insights** to improve experiences faster



Broad integration across Meraki, Cisco, and 3rd party systems

Seamless integrations powered by the Meraki platform



Key solutions

Business resiliency with Meraki



Secure Edge

Consolidate your technology to protect your network, users, and devices



Future of Work

Create secure environments and seamless productivity wherever work happens



Smart Spaces

Enable physical security & remotely monitor processes



✓ Secure edge

SASE (Secure Access Services Edge) is a consolidated architectural solution that provides effective & homogenous levels of **security** and **experience** for users on any device.

SASE converges **networking** (SD-WAN, SD-Branch) and **network security** (secure web gateway, firewall, CASB, etc.) towards an **as-a-service** cloud edge model..

KEY PRODUCTS:

- MX & SD-WAN + Cisco Umbrella for **threat protection**
- Z3 teleworker devices for **seamless remote work**
- MR Wireless + Cisco Umbrella for **DNS-layer protection**

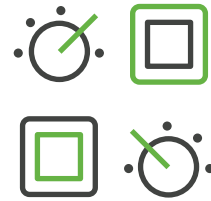


***For all verticals (distributed or offices):** Retail, Healthcare, Financial Services, Manufacturing, Professional Services, Hospitality, etc.*

How Meraki delivers SASE



CONNECT



CONTROL



CONVERGE

CONNECT

High quality of experience with SD-WAN

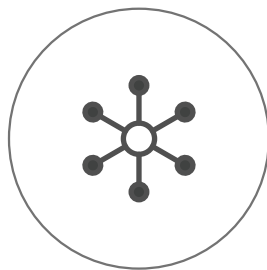


Advanced Analytics with ML

Platform-wide visibility

Auto VPN telemetry

Web App, WAN, VoIP Health



SD-WAN Connectivity

Site-to-site Auto VPN

Public IaaS clouds

Controlled & performance-based
path selection



Integrated Agile Security

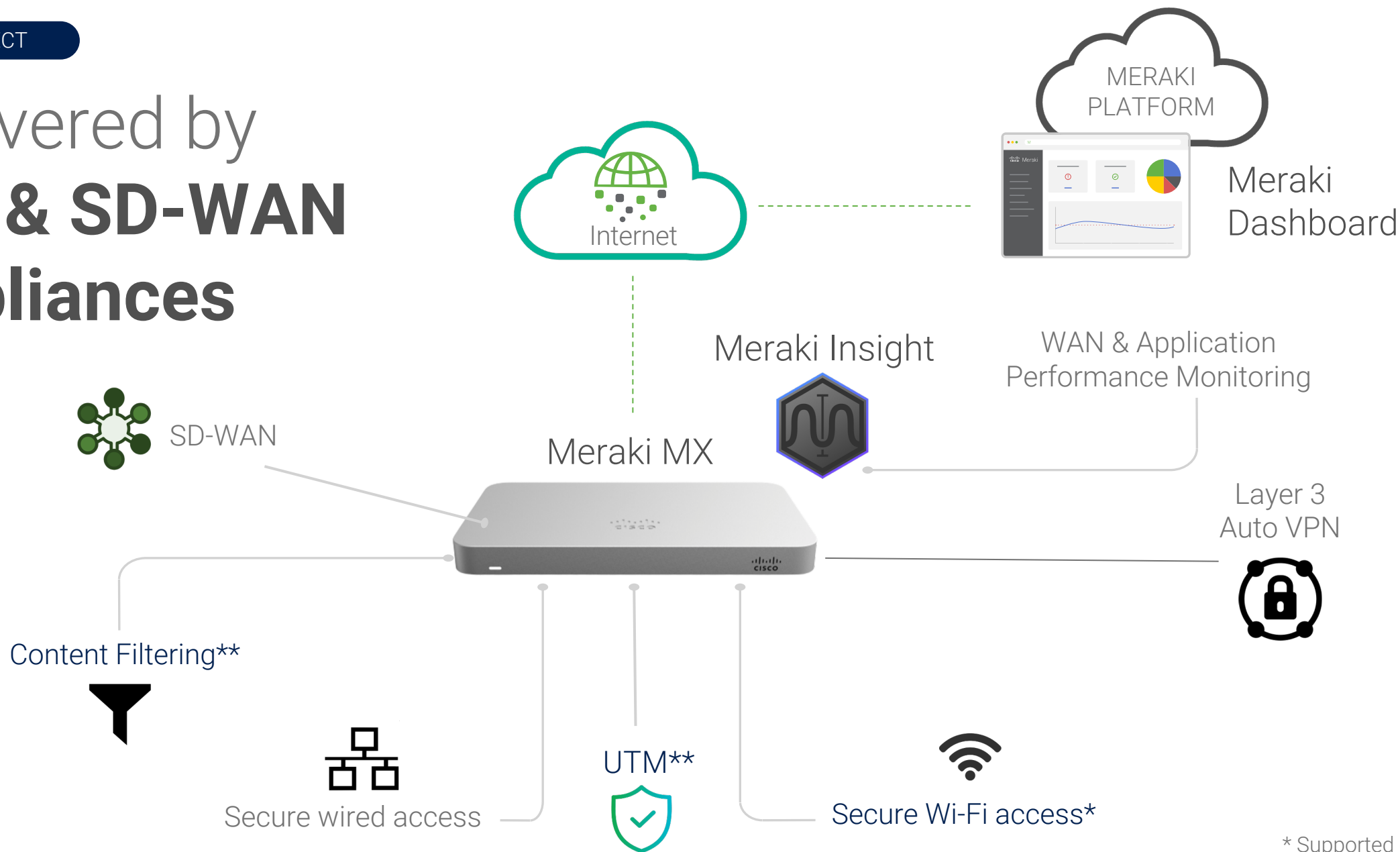
Informed by Cisco Talos

Cisco Umbrella cloud security

On-prem unified threat
management

CONNECT

Delivered by **MX & SD-WAN** Appliances



* Supported on MX64W

** Requires Advanced Security License

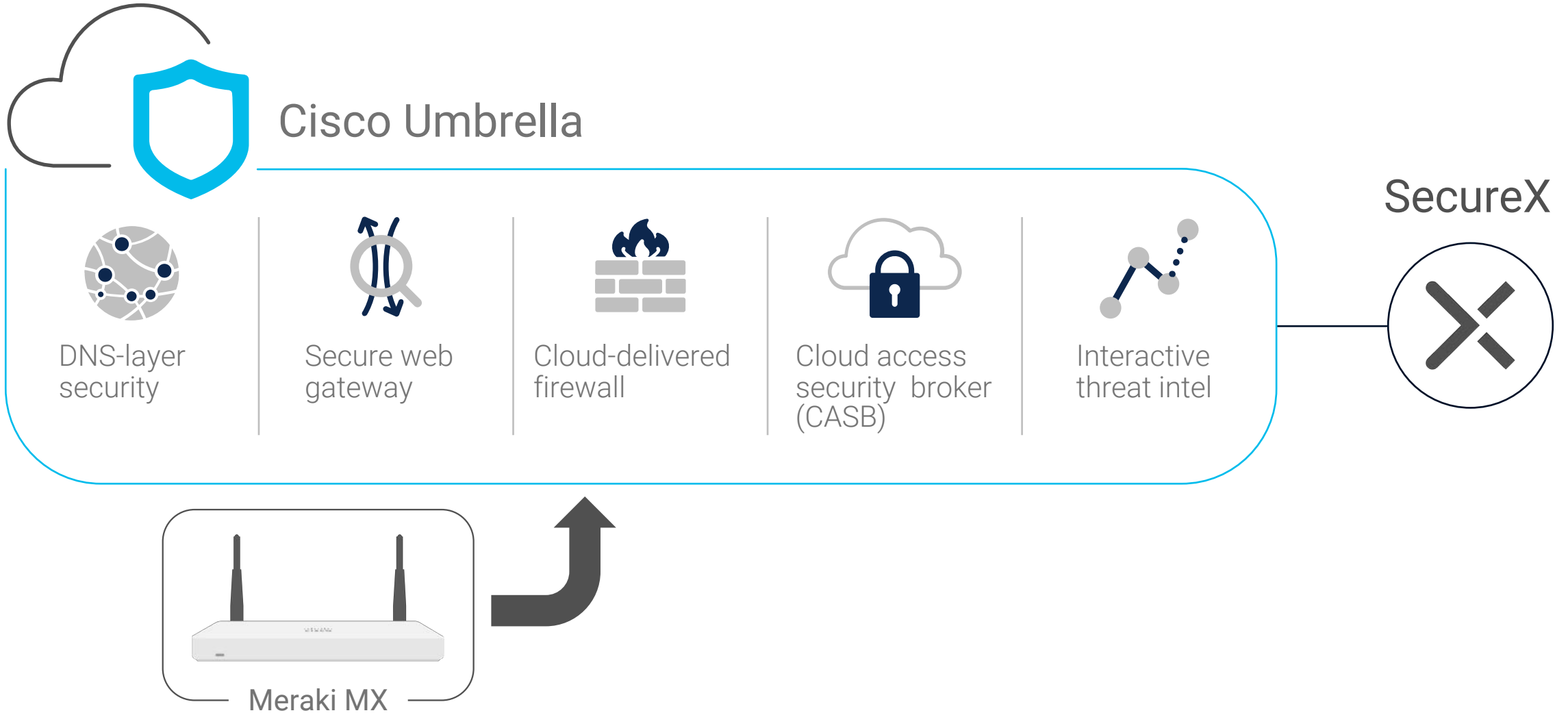
CONTROL

Best-in-class integrated security



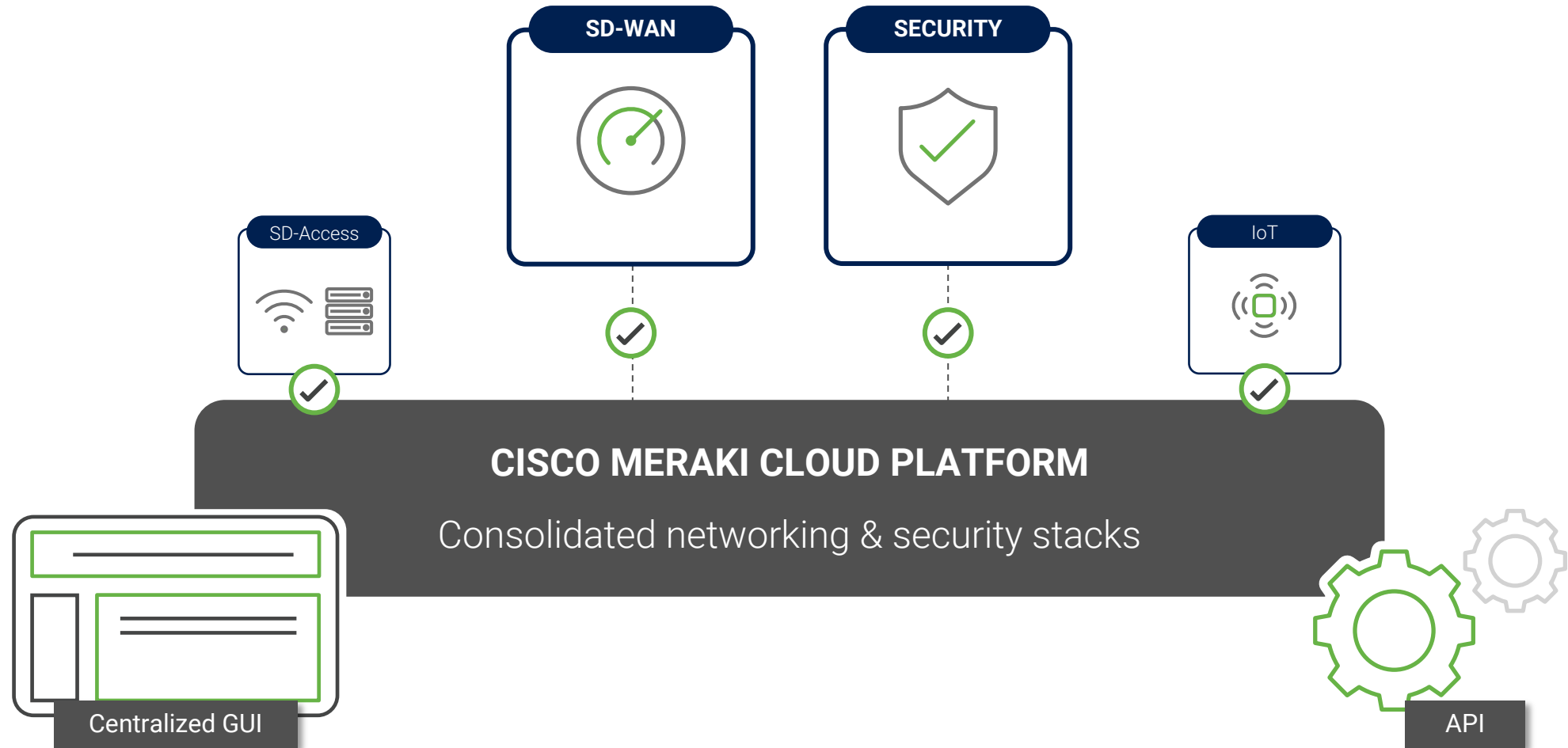
Cisco Talos blocks **20B** threats daily

Best-of-breed security capabilities



CONVERGE

A platform designed to easily embrace SASE



✓ Future of work

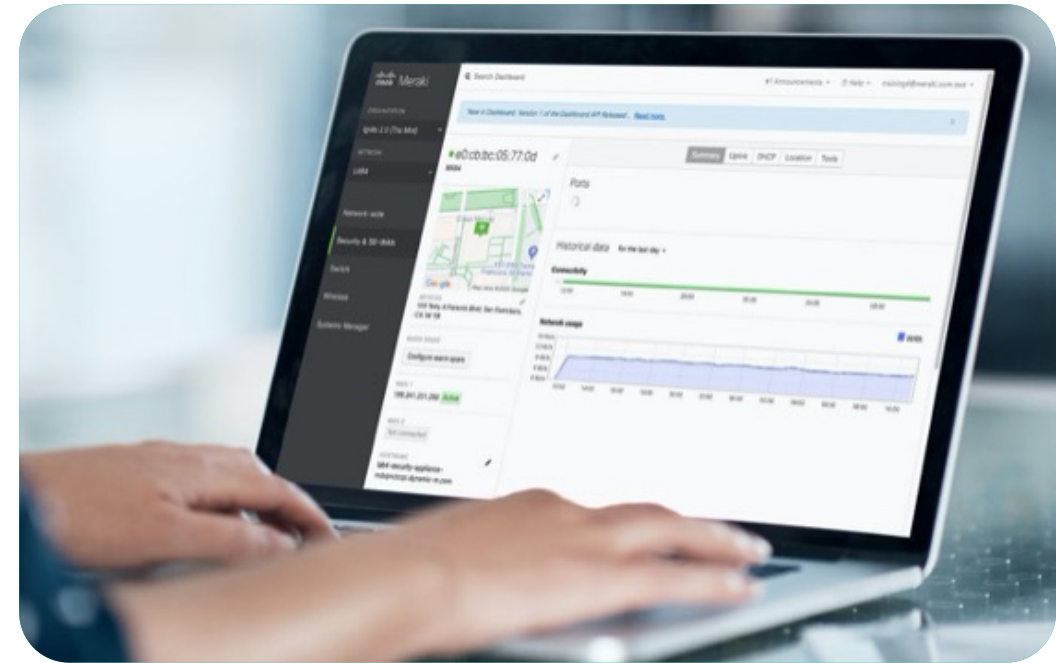
Increase **productivity, security, and connectivity** for remote, hybrid and/or in-office workers.

REMOTE OFFICE PRODUCTS:

- Z3 Teleworker Gateway, Meraki Insight, Systems Manager + Duo

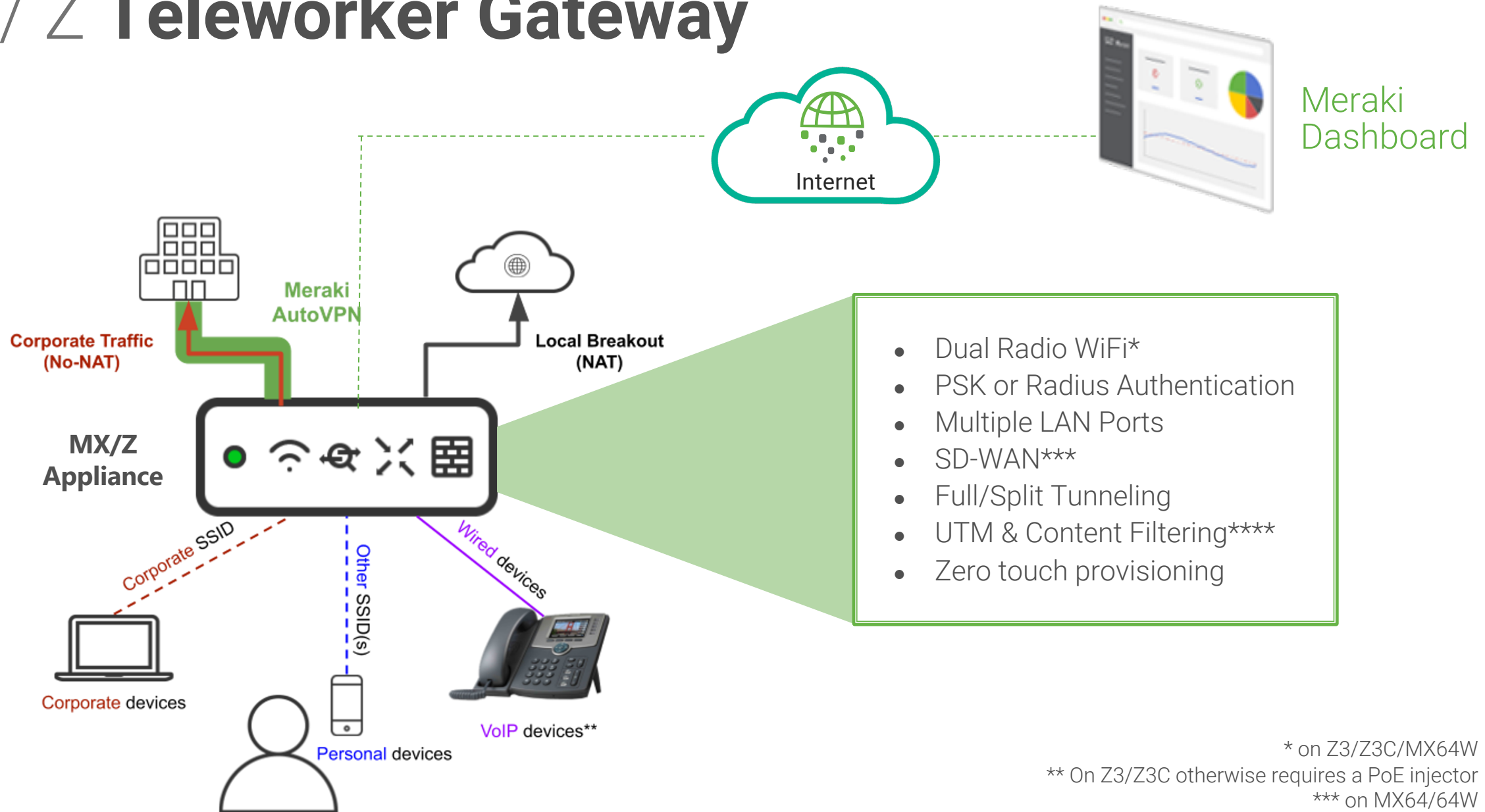
HYBRID OR PHYSICAL OFFICE PRODUCTS:

- MX & SD-WAN or Z devices + Cisco Umbrella **threat protection**
- Meraki Insight for **deep application insights** used by remote workers and reduced troubleshooting time
- Systems Manager + Duo for **secure BYOD** environments
- MR Wireless for **high performance Wi-Fi 6** connectivity
- MS Switches & MG Cellular Gateway for **extended connectivity**



Key Verticals (offices or distributed):
Retail, Healthcare, Financial Services, Professional Services, Education

MX / Z Teleworker Gateway



* on Z3/Z3C/MX64W

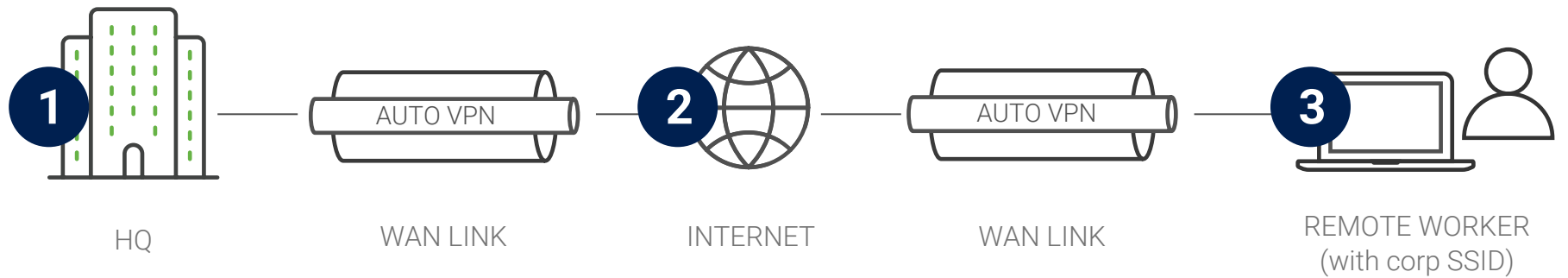
** On Z3/Z3C otherwise requires a PoE injector

*** on MX64/64W

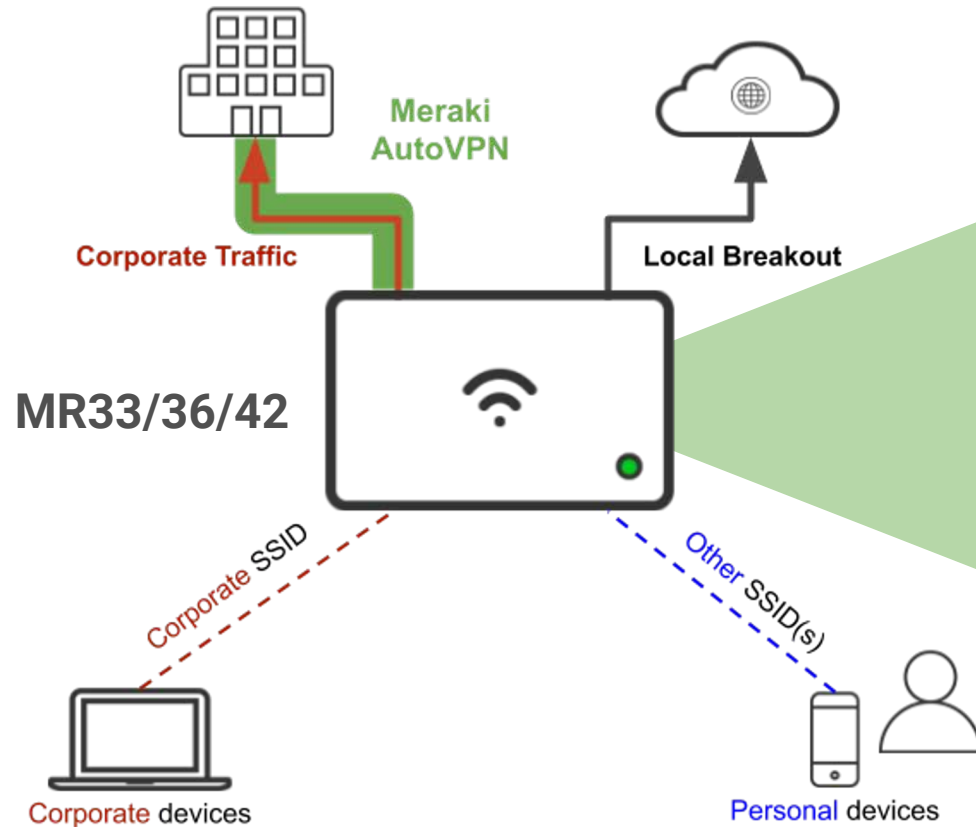
**** Requires MX with Advanced Security license

MX Appliance – **Auto VPN**

- Secure connectivity **in 3 clicks**
- **Automatically configured** VPN parameters
- **Redundancy** built-in



MR Wireless – Teleworker Solution



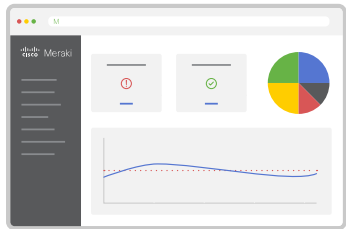
- 802.11ac wave 2 and Wi-Fi 6*
- PSK or Radius Authentication
- GigE uplink
- Full/Split tunneling
- Layer 7 Firewall
- DC or PoE**
- Content Filtering***
- Zero touch provisioning

* on MR36

** Requires an adaptor or PoE injector

*** Requires Advanced license

Systems Manager - **BYOD**



Meraki
Dashboard



Systems
Manager

- Easy enrollment via email or SMS or via mobile browser
- Monitor devices regardless of their location or connection type
- Hassle free VPN & Wi-Fi provisioning
- Manage hardware and software inventory
- Protect devices, enforce encryption and remote wipe

✓ Smart spaces

Enable **safe operations** for teams, and monitor indoor & outdoor activity and IT assets remotely.

MV smart cameras & Meraki APIs bring **increased visibility** into operations, and **advanced analytics** to easily track usage patterns and detect objects.

MT sensors monitor IT assets & facilities for greater visibility, **employee safety**, and **cost savings**.

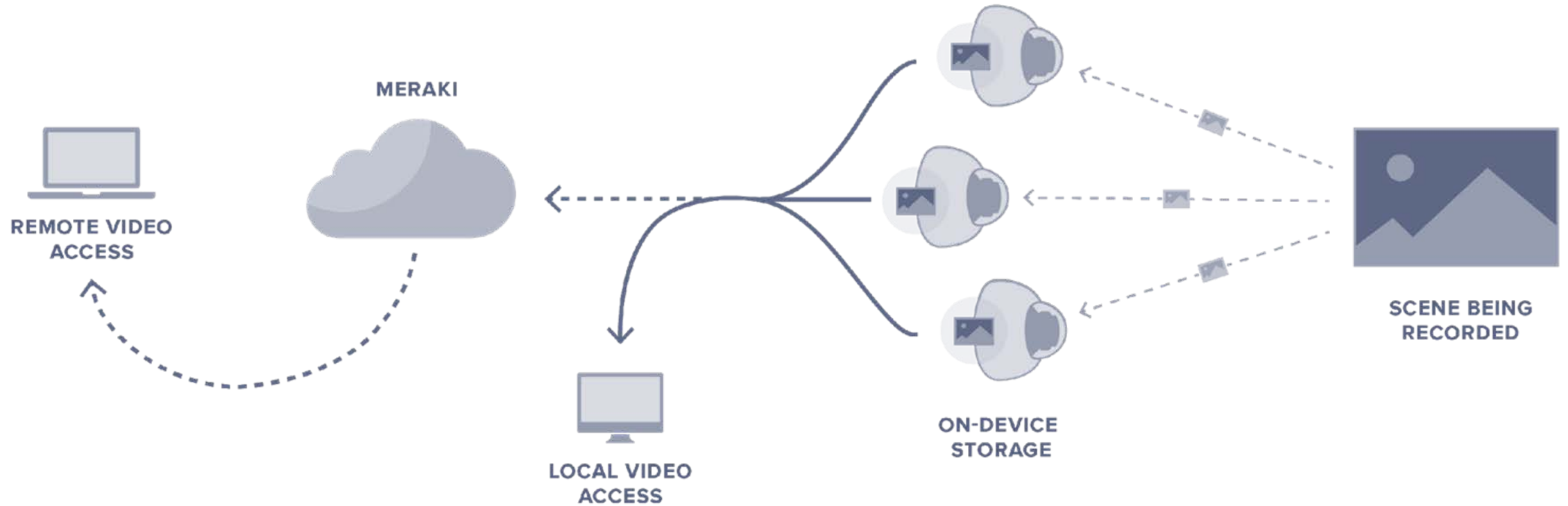
KEY PRODUCTS

- MV smart cameras
- MT sensors
- Meraki APIs & Meraki Marketplace



Key Verticals (offices or distributed): Retail, Healthcare, Financial Services, Professional Services, Hospitality

MV Smart Cameras



BANDWIDTH CONSCIOUS

Less than 50kpbs upstream bandwidth per camera when not watching video

INTELLIGENT STREAMING

View locally, or view remotely via cloud proxy streaming, from the Meraki dashboard

HYBRID VIDEO PROCESSING

Video is analyzed on camera, motion indexed in the cloud

MT Sensors



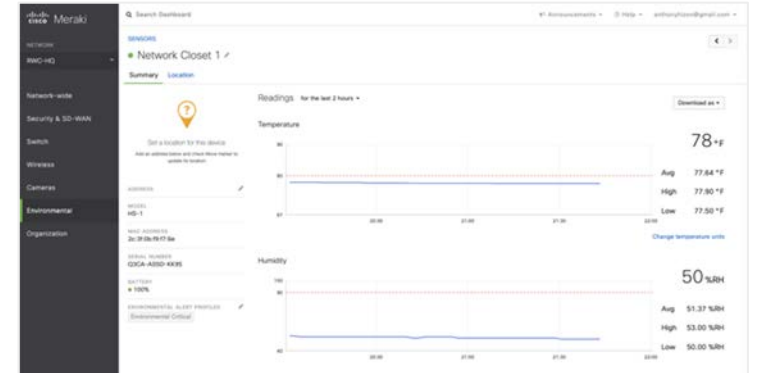
MT

BLUETOOTH



MR / MV
(Gateway)

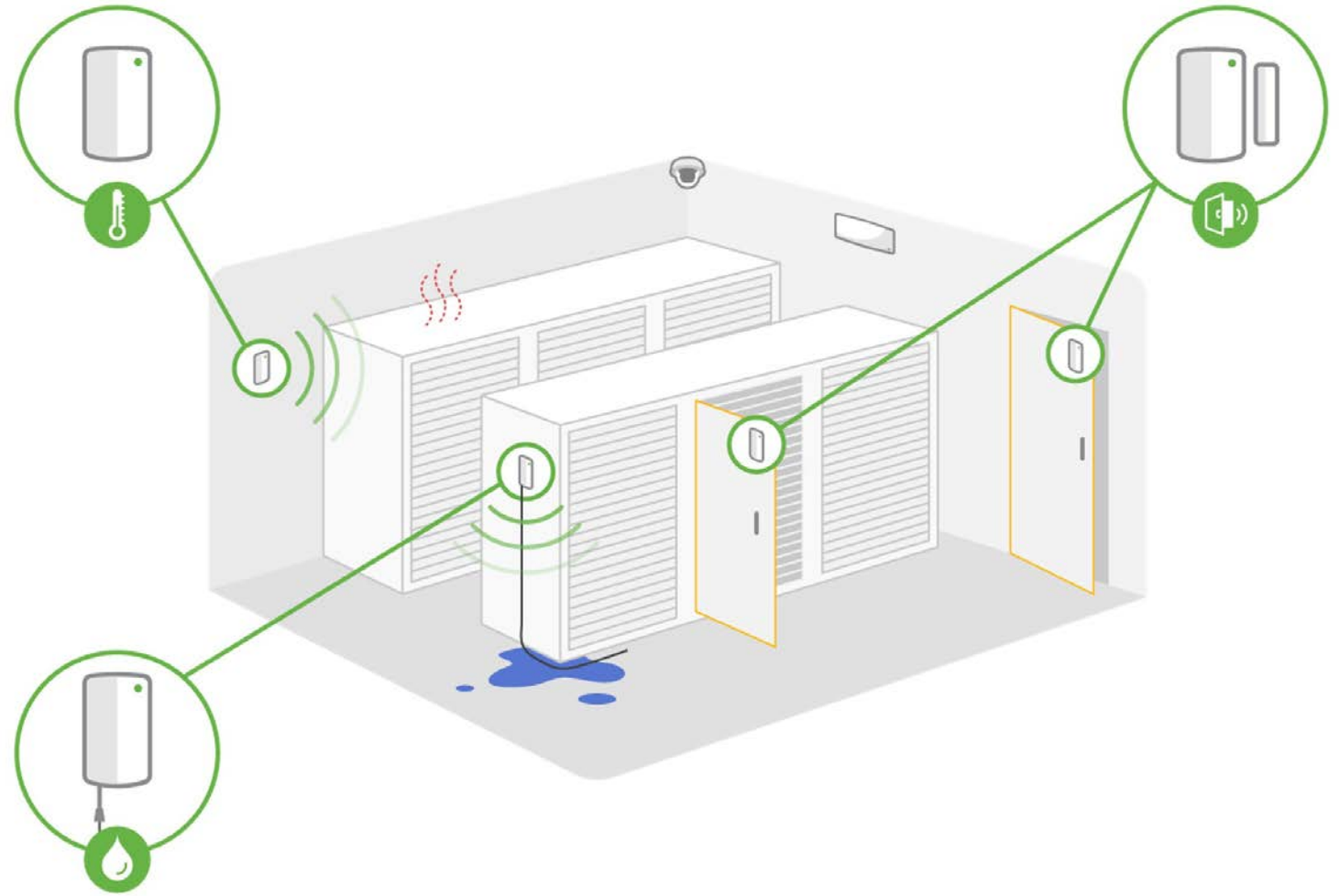
CLOUD



MERAKI
DASHBOARD

MT Sensors

Protecting Business-Critical
Infrastructure




Resources


Meraki Community

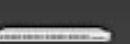
- ✓ Developer & APIs board
- ✓ Learning resources
- ✓ DevNet Certs
- ✓ Developer Q&A
- ✓ Product & feature requests


community.meraki.com


Join the conversation. Select a product to get started:


 Wireless LAN


 Security / SD-WAN


 Switching







 Mobile Device Management




 Meraki Insight



 Smart Cameras

 Wireless WAN

 Sensors

Other topics:  Full-Stack  Dashboard & Administration  Developers & APIs  Off the Stack  Português  Español

Learn more about Meraki:  Projects Gallery  Meraki Unboxed Podcast  Feature Announcements

For partners:  MSP Forum  パートナーコミュニティ

Learn about our training offerings in the [Meraki Learning Hub](#)

Latest Topics

SUBJECT	AUTHOR	LATEST POST
MS-355 Layer 3 pros/cons	ToryDav	20m ago

New here?

Thank you for joining the Meraki Community! If you haven't already, please [introduce yourself](#) so we can all learn who's here.

Next steps

Get a [free trial](#)
of any Meraki
products

Start an
[instant demo](#)
of the Cisco Meraki
platform

[Watch on-demand
webinars](#)
and demos of key
solutions

Q&A Session

To request a demo or to learn more about IT security, Cisco Duo, or Meraki, please contact us at:

info@evron.com

www.evron.com/contact-us



Tweet Your Questions
[@evroncomputers](https://twitter.com/evroncomputers)

Thank you!

Contact Us: info@evron.com | www.evron.com



Don't Forget to Follow Us!

