

The background is a vibrant, abstract graphic. On the left, there are overlapping, wavy shapes in shades of red, orange, and yellow, resembling a stylized cloud or a series of overlapping circles. On the right, a bright white light source emits a series of colorful rays in shades of blue, green, and yellow, creating a sunburst effect. The overall color palette is a rainbow spectrum.

cisco *Live!*

Let's go

#CiscoLiveAPJC



The bridge to possible

Zero Trust Network Access (ZTNA) Demystified

What It Is, Why You Need It and the Cisco
Technologies That Make Frictionless Security Possible

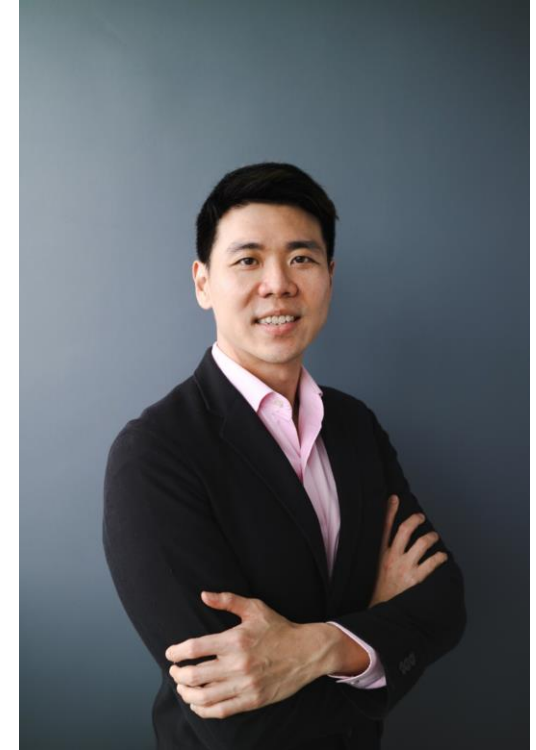
Jeff Yeo, Leader Solutions Engineering (SSE Incubation)
BRKSEC-2079

CISCO *Live!*

#CiscoLiveAPJC

About Your Speaker

- Security Leader for Incubation Technologies including Zero Trust and SSE
- 15 years in industry including Aruba(HPE), Citrix, BT Global Services, Singapore Gov
- Tech blogger, speaker and foodie



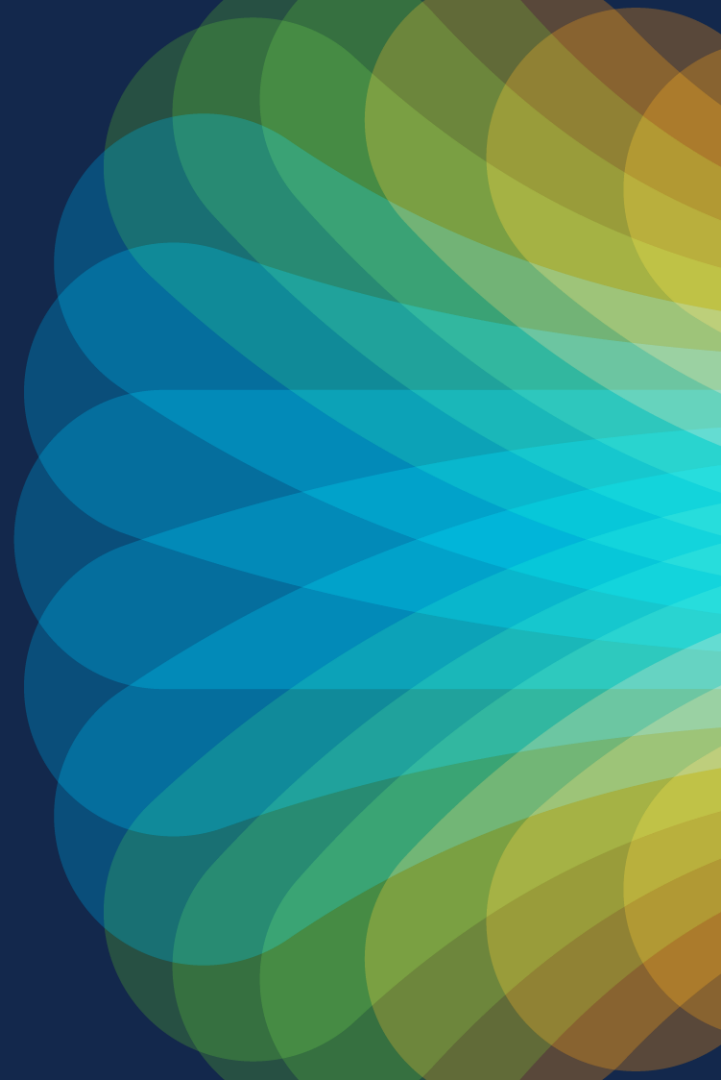
Certified Cloud
Security Professional



Agenda

- The What & Why of ZTNA
- Cisco Secure Firewall
- Cisco Secure Firewall + Duo
- Duo Network Gateway (DNG)
- Cisco Secure Access

The What & Why of ZTNA



Why Zero Trust?



Dissolving perimeter



Attackers actively exploiting
gaps and weaknesses



80% of organizations are
NOT prepared

2023 Cisco's Cybersecurity Readiness Index

ZTNA

Zero Trust Network Access

ZT
Zero Trust
Principals



NA
Network Access

Three Factors To Select ZTNA Offerings



1. Strategy

- Aligned to SSE
- Independent of SSE



2. Use Case

- Internal-workforce remote access
- Extended-workforce remote access and BYOD
- Privileged remote access
- On-premises access



3. Key Capabilities

- Platform
- Connectivity
- Visibility and control
- Risk scoring

Source: Gartner
795038_C

Evolution of ZTNA



Evolution of ZTNA: Organisation Adoption



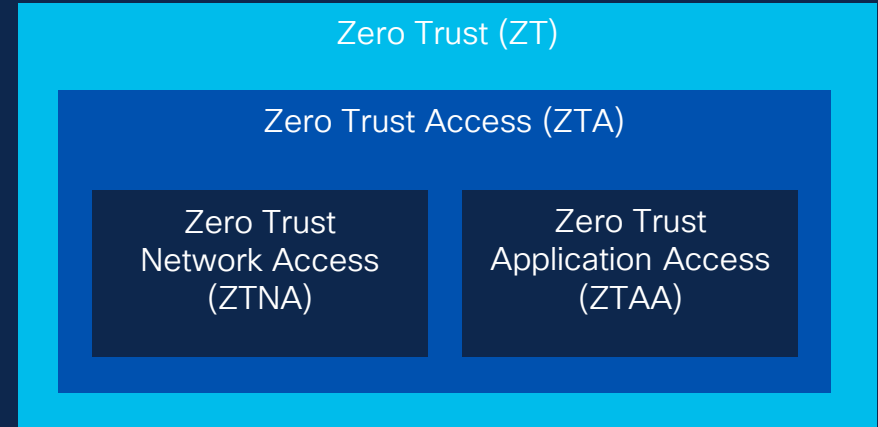
ZT vs. ZTA vs. ZTNA vs. ZTAA

- Zero Trust

- A comprehensive security framework that prioritises least privilege, strict access controls, and continuous monitoring to mitigate risks and protect resources.

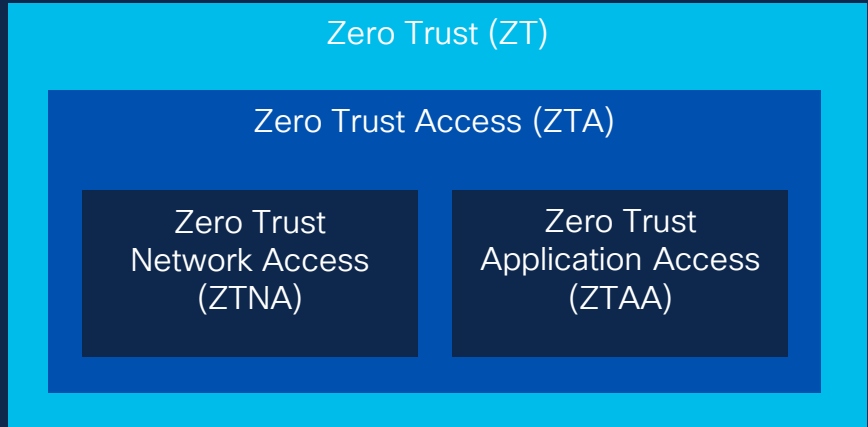
- Zero Trust **Access**

- A specific aspect of Zero Trust that **focuses on managing and enforcing access** to resources



ZT vs. ZTA vs. ZTNA vs. ZTAA

- Zero Trust **Network** Access (ZTNA)
 - A subset of Zero Trust Access that focuses on secure **access to networks**.
- Zero Trust **Application** Access (ZTAA)
 - A subset of Zero Trust Access that focuses on secure **access to individual applications**.



ZTNA vs. ZTAA

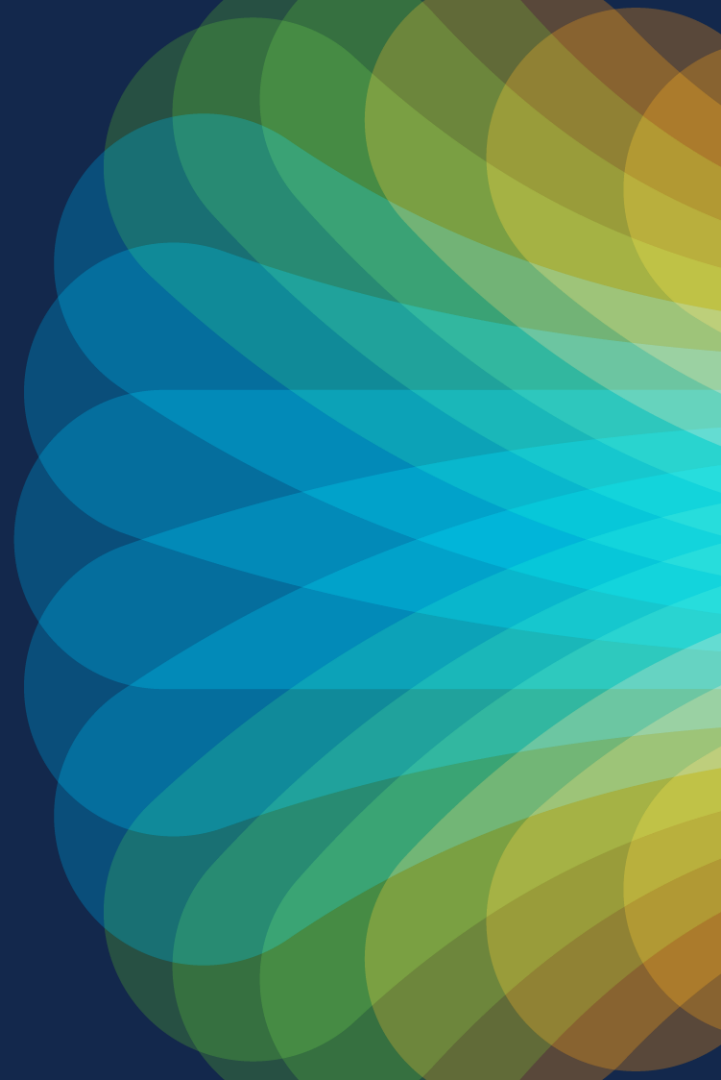
	Zero Trust Network Access (ZTNA)	Zero Trust Application Access (ZTAA)
Allow Access To:	Corporate Network (10.0.0.0/8 or *.example.com)	Production Jira App (jira.example.com)
When:	User Identity (Lee authenticated via MFA)	
	Device Posture (Fully patched device)	
	Location (United States)	
	Continuous Monitoring (TLS decrypt and IPS inspection)	

The primary difference between ZTNA and ZTAA is the granularity of access in the policy

Types of Zero Trust Access

	Clientless Zero Trust Access	Client-Based Zero Trust Access
General Description	A lightweight method of securely accessing resources.	A more feature rich method of securely accessing resource.
Application Support	Supports web applications (HTTP/HTTPS) without any software and other select protocols (SMB/RDP/SSH/etc.) via a portal or small helper application.	Broad application support via client software on the user's device.
Partner/BYOD Use	Preferred method	Yes, if desired/needed
Employee Use	Yes, if desired	Preferred method

Cisco Secure Firewall Zero Trust Access (ZTA)



Secure Firewall Zero Trust Access (ZTA)



Background

- For organizations wanting to adopt a Zero Trust posture, they were required to have additional software installed (like AnyConnect) on client devices. Where the client application acted as a proxy and handled authentication and access. That is until 7.4.



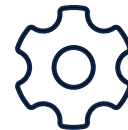
What's New

- Clientless Zero Trust Application Security functionality to the FTD
- SAML based authentication of users with support for Duo, Azure AD, Okta, & other Identity Providers
- No additional network equipment needed. Simply upgrade to FTD v7.4.



Benefits

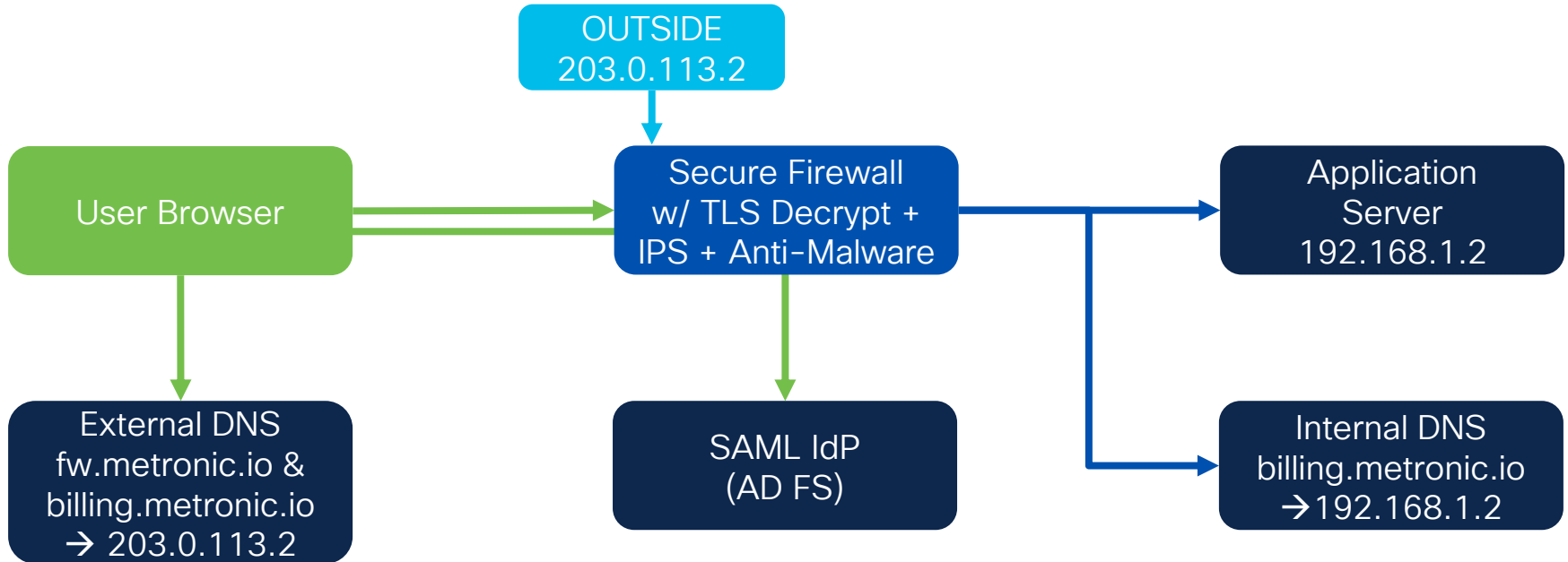
- Enables users to access applications without requiring additional software on personal devices.



Requirements

- Secure Firewall 7.4
- Snort 3
- FMC On Prem + FMC REST API or cdFMC
- Not supported on ASA
- Only Routed mode supported
- Not supported on individual mode cluster

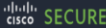
Demo Setup: Secure Firewall ZTA w/ AD FS



Config: Secure Firewall ZTA w/ AD FS

 Firewall Management Center
Policies / Access Control / Zero Trust Application

OverviewAnalysisPoliciesDevicesObjectsIntegration

Deploy 🔍 ⚙️ ? admin ▾ 

↩️ Return to Zero Trust Application

No Warnings Discard Save

ZTNA-ADFS ✎

Targeted: 0 devices

Groups: 0 Applications: 3

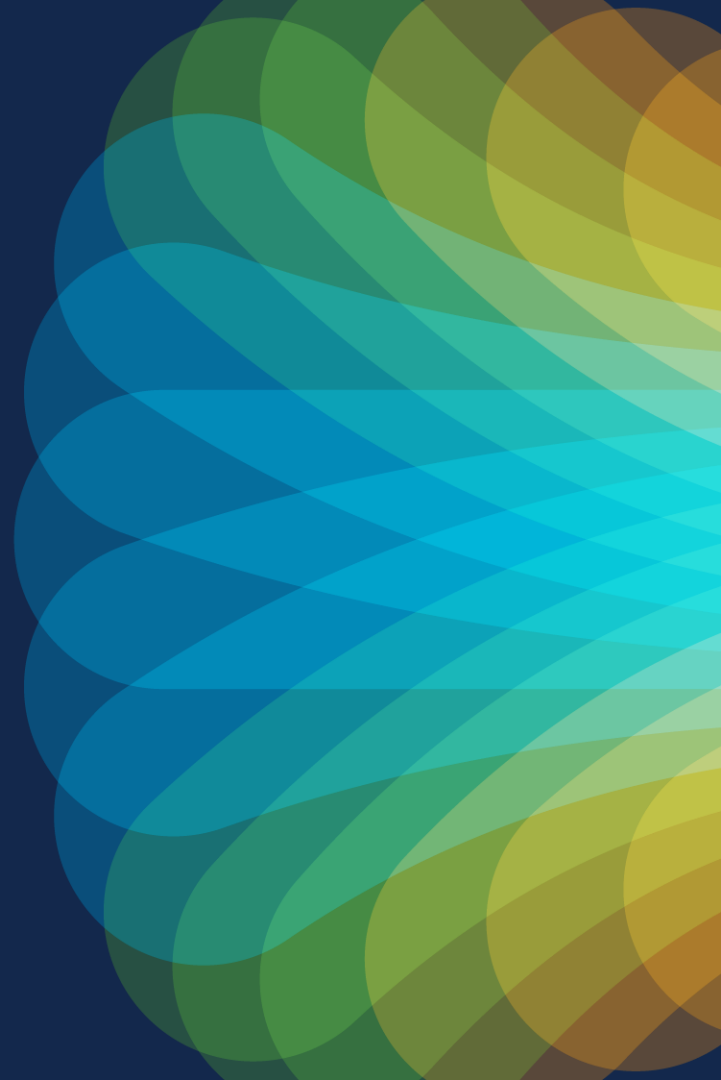
ApplicationsSettings

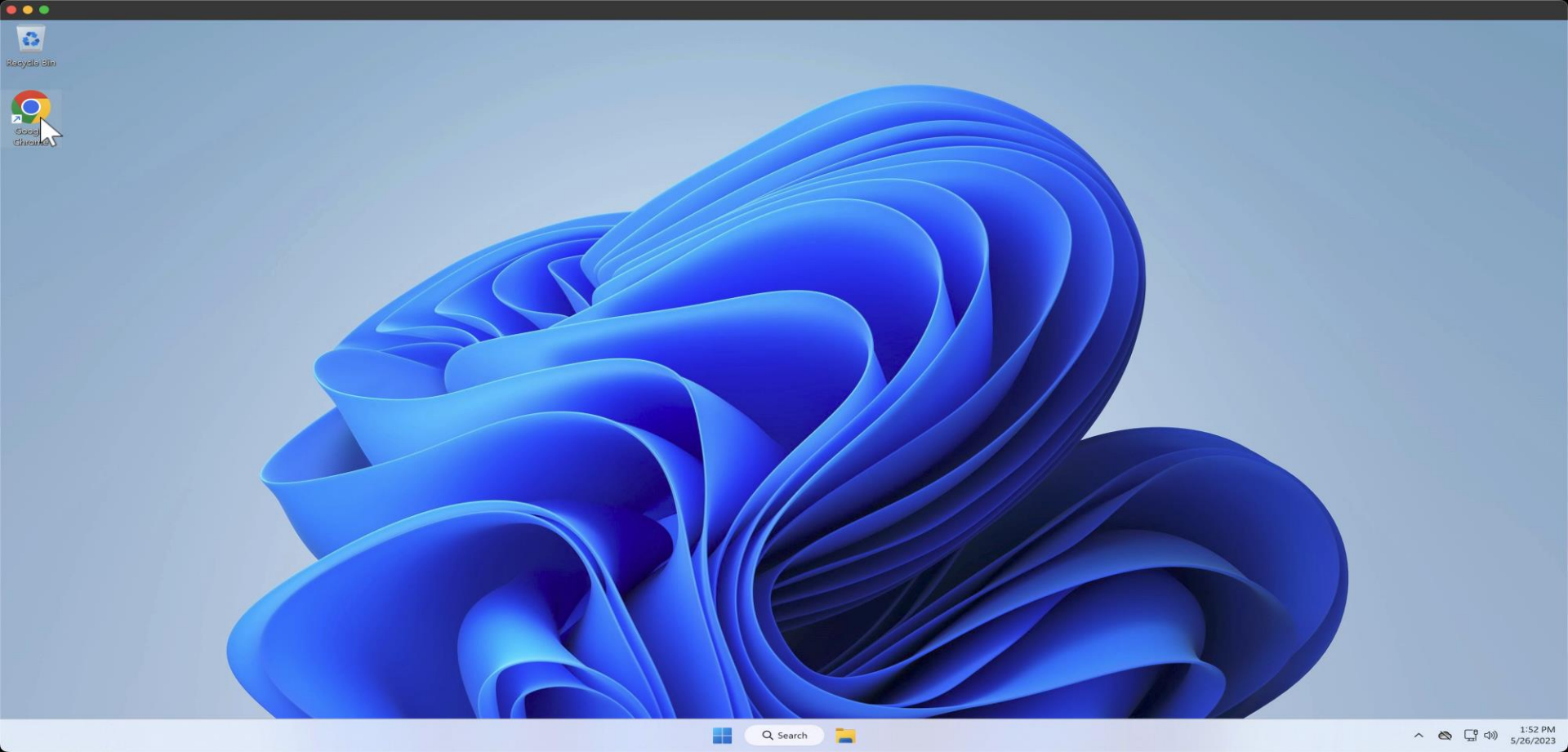
Bulk Actions ▾ 🔍 Filter by Name, IdP SAML missing, Enabled/Disabled

Add Application GroupAdd Application

Name	External URL	Application URL	SAML Entity ID	Security Zones	Intrusion Policy	Malware and File Policy	Enabled	
▼ Ungrouped (3 Applications)								
☐ Billing	https://billing.metronic.io	https://billing.metronic.io	http://fs.metronic.io/adfs/...	OUTSIDE (Inherited)	Balanced Security and Connectivity (Inherited)	Block Malware (Inherited)	True	✎ 🗑
☐ Dashboard	https://dashboard.metronic.io	https://dashboard.metronic.io	http://fs.metronic.io/adfs/...	OUTSIDE (Inherited)	Balanced Security and Connectivity (Inherited)	Block Malware (Inherited)	True	✎ 🗑
☐ SEO	https://seo.metronic.io	https://seo.metronic.io	http://fs.metronic.io/adfs/...	OUTSIDE (Inherited)	Balanced Security and Connectivity (Inherited)	Block Malware (Inherited)	True	✎ 🗑

User Demo: Cisco Secure Firewall ZTA + AD FS

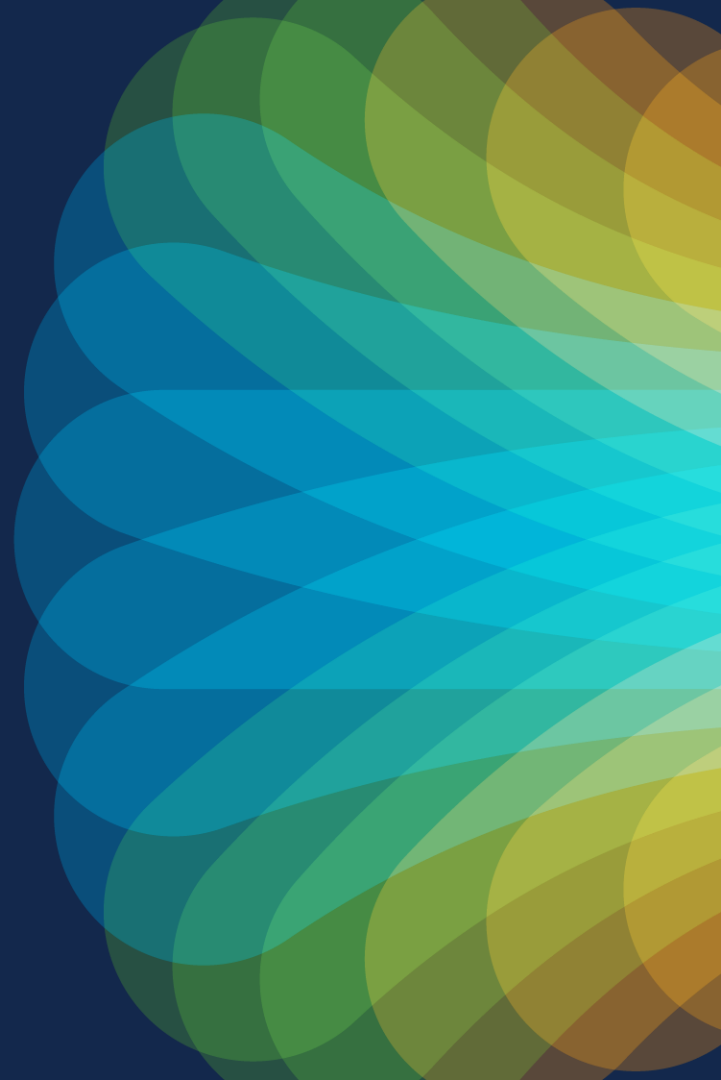






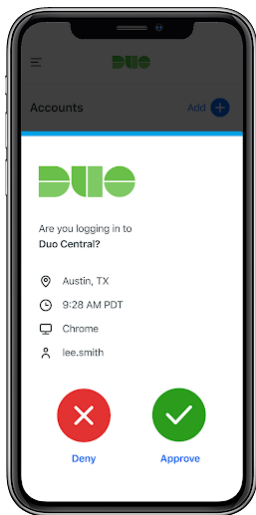
I'm Lee. I use
the same
password
everywhere.

Cisco Secure Firewall ZTA + Duo



Authenticate Users

Verify users are who they say they are



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

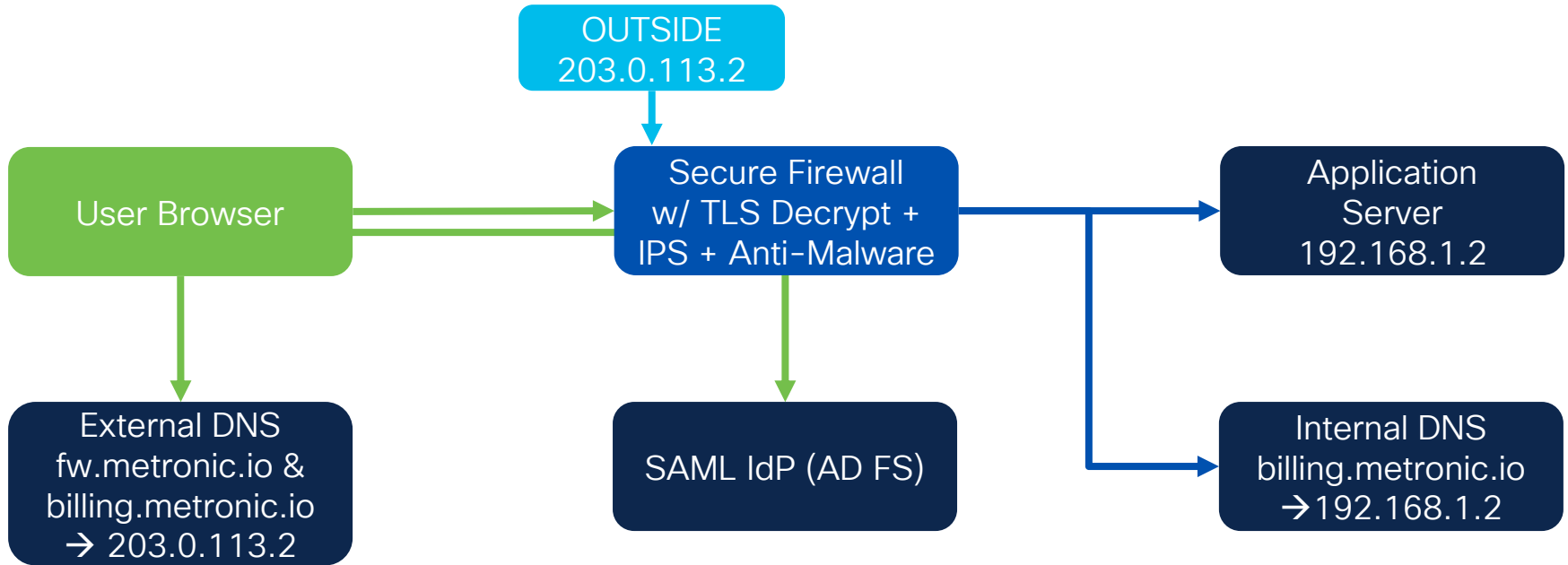
Cloud native and designed to be user friendly from the start, Duo allows any IT professional to implement at lightning speed



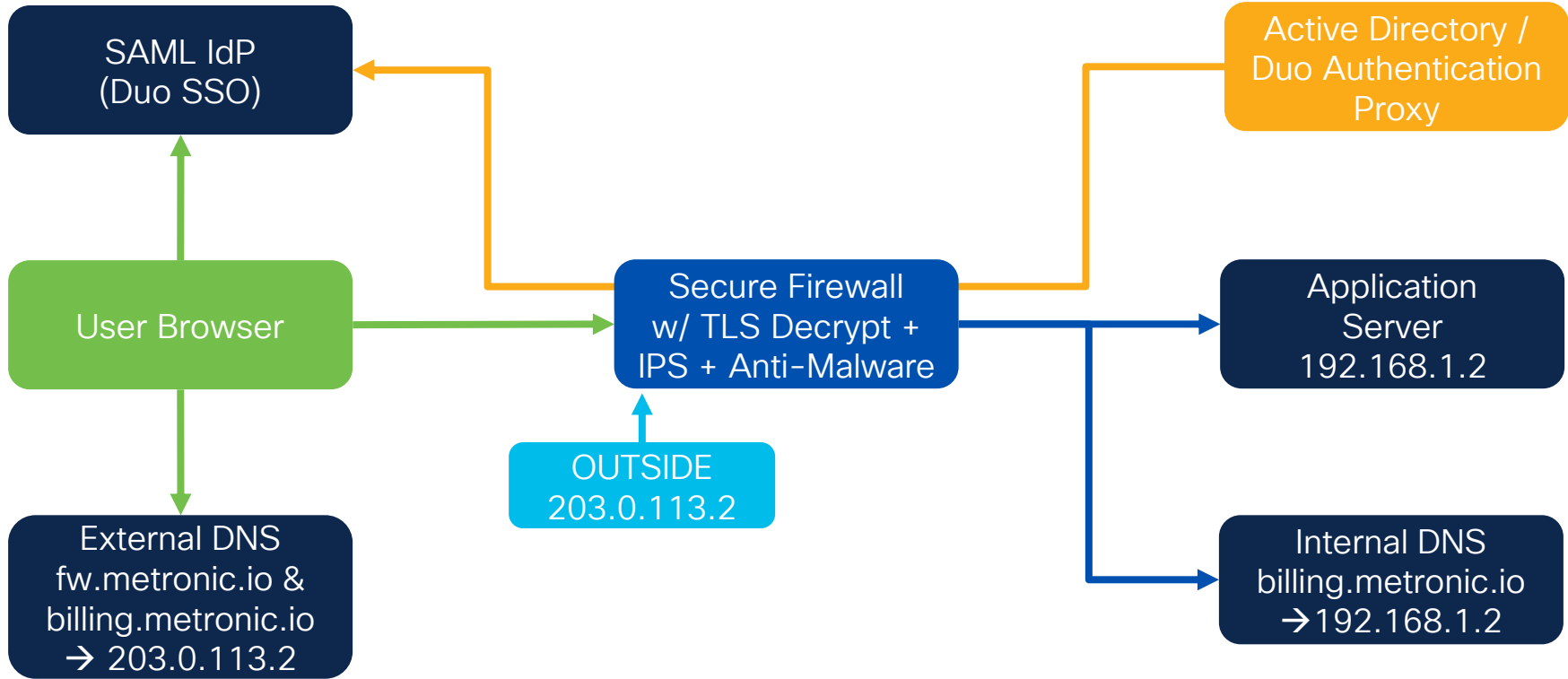
Prevent Push Phishing Attacks

Ensures users don't fall victim to push phishing attacks

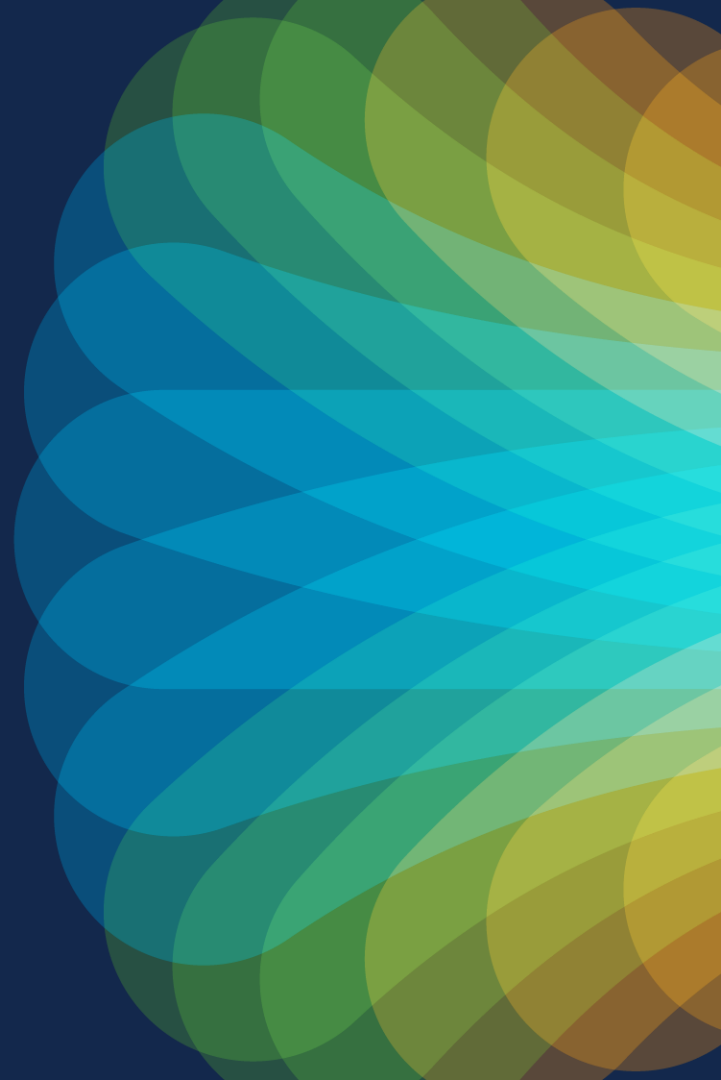
Demo Setup: Secure Firewall ZTA w/ AD FS

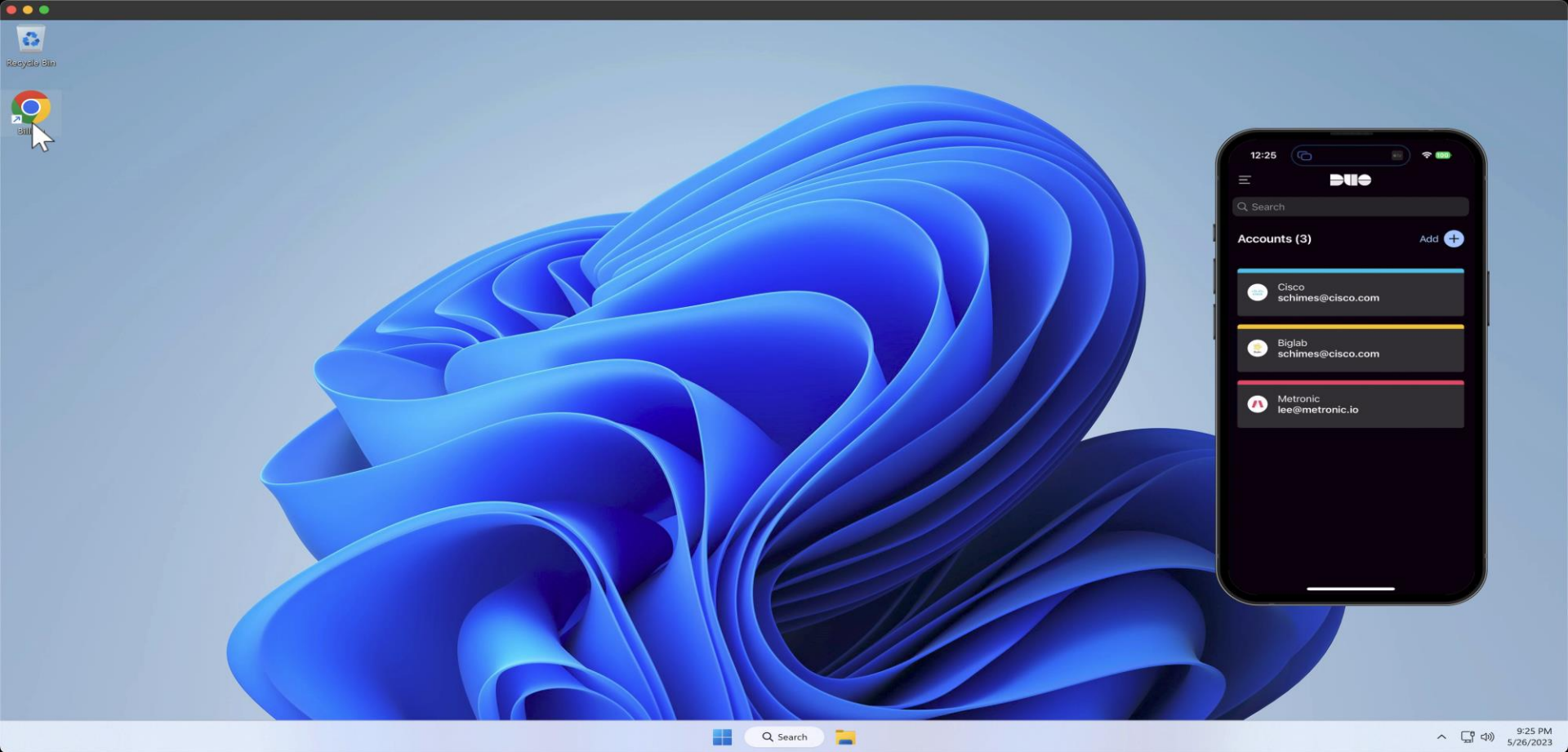


Demo Setup: Secure Firewall ZTA w/ Duo SSO

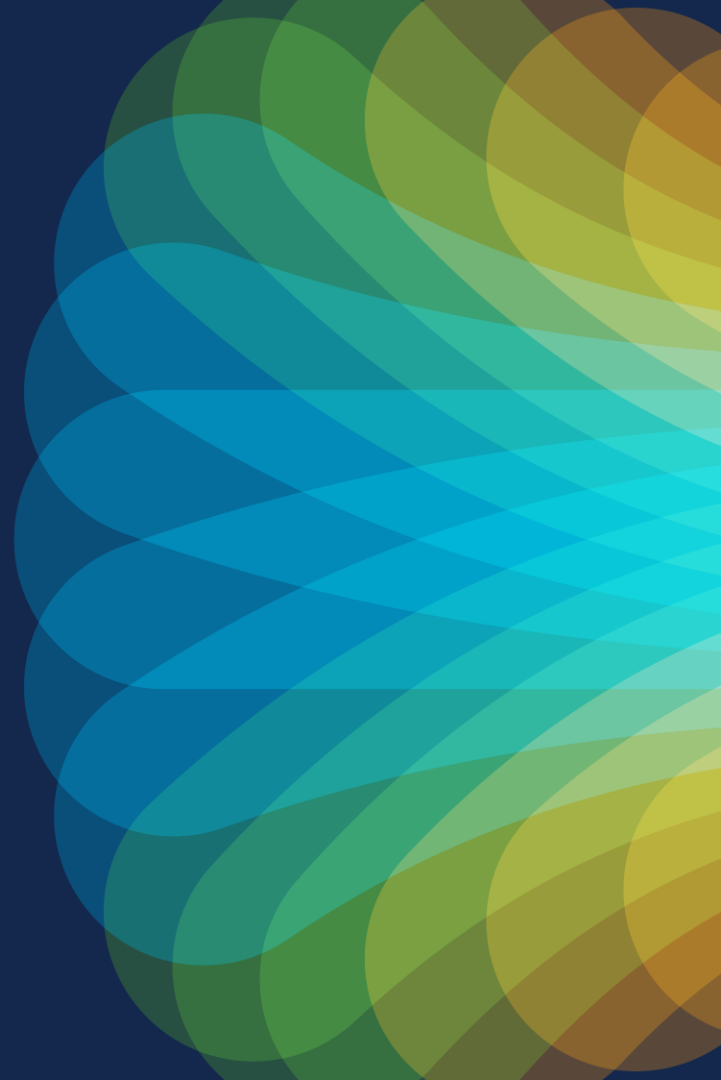


User Demo: Cisco Secure Firewall ZTA + Duo MFA





Victim Demo: Push Phishing Attack

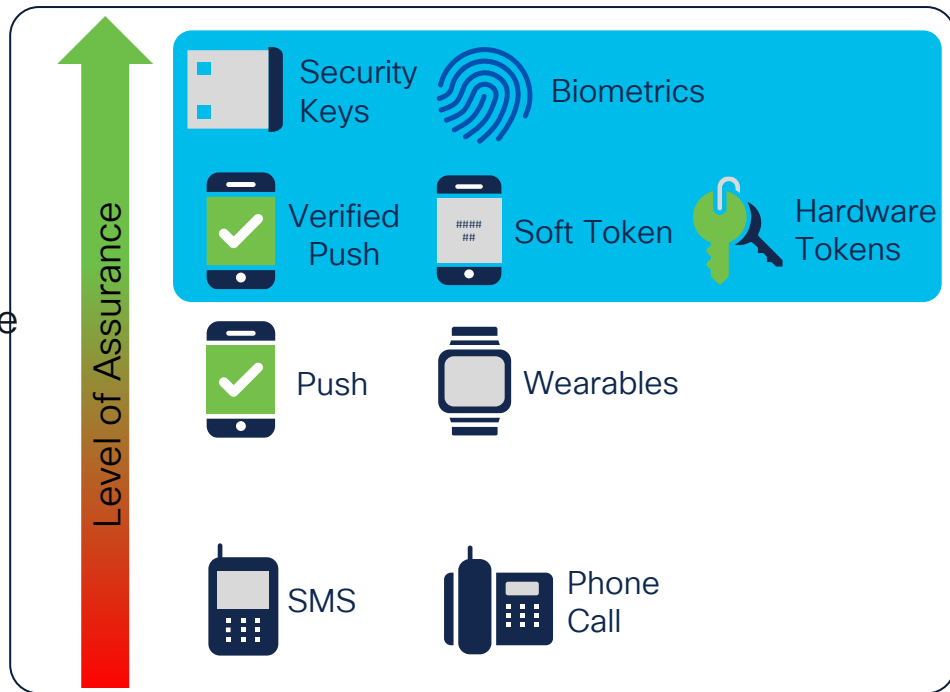


Strong Multi-Factor Authentication (MFA) Options

Flexible MFA for every use case

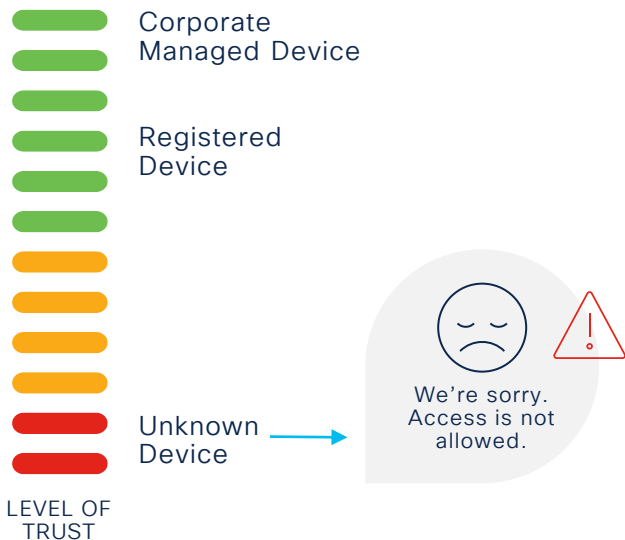
- Configure authentication options for each application or group of users
- Require phishing-resistant MFA (FIDO2) for critical applications and privileged users
- Enable multiple option for users for ease of use and flexibility

Authentication Methods



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

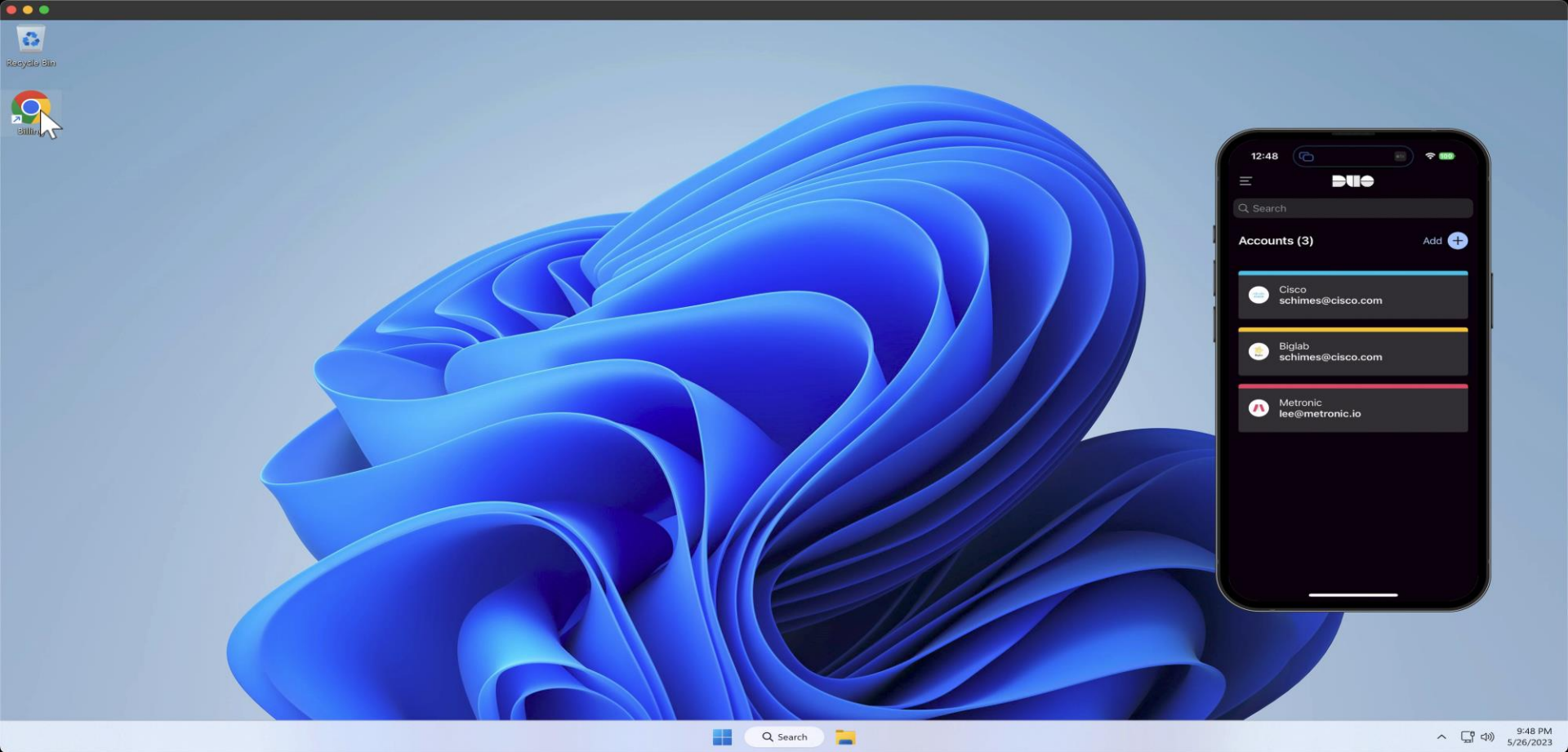
Give organizations control over which devices can access corporate apps and resources



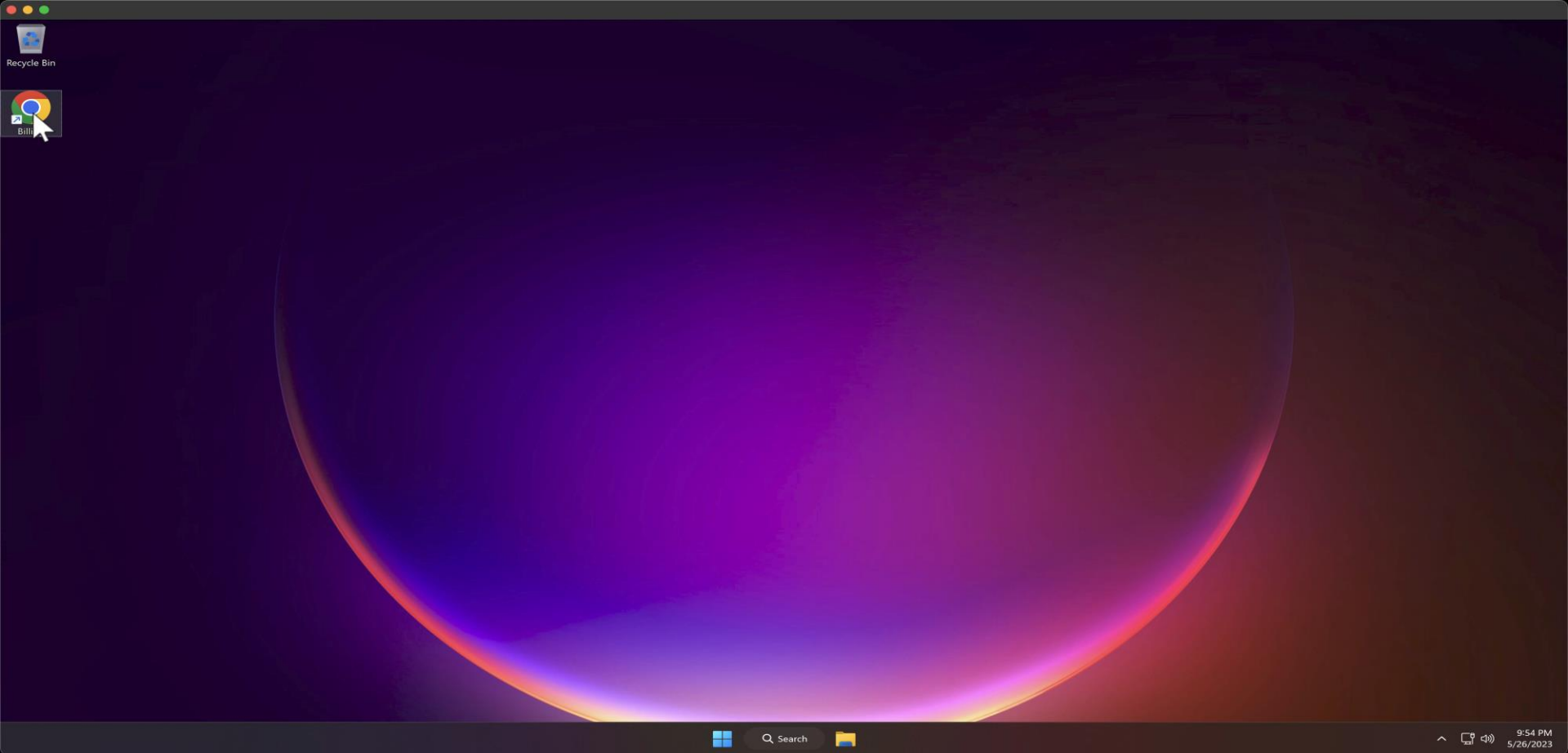
Mitigate Risk

When limited authenticator options are available

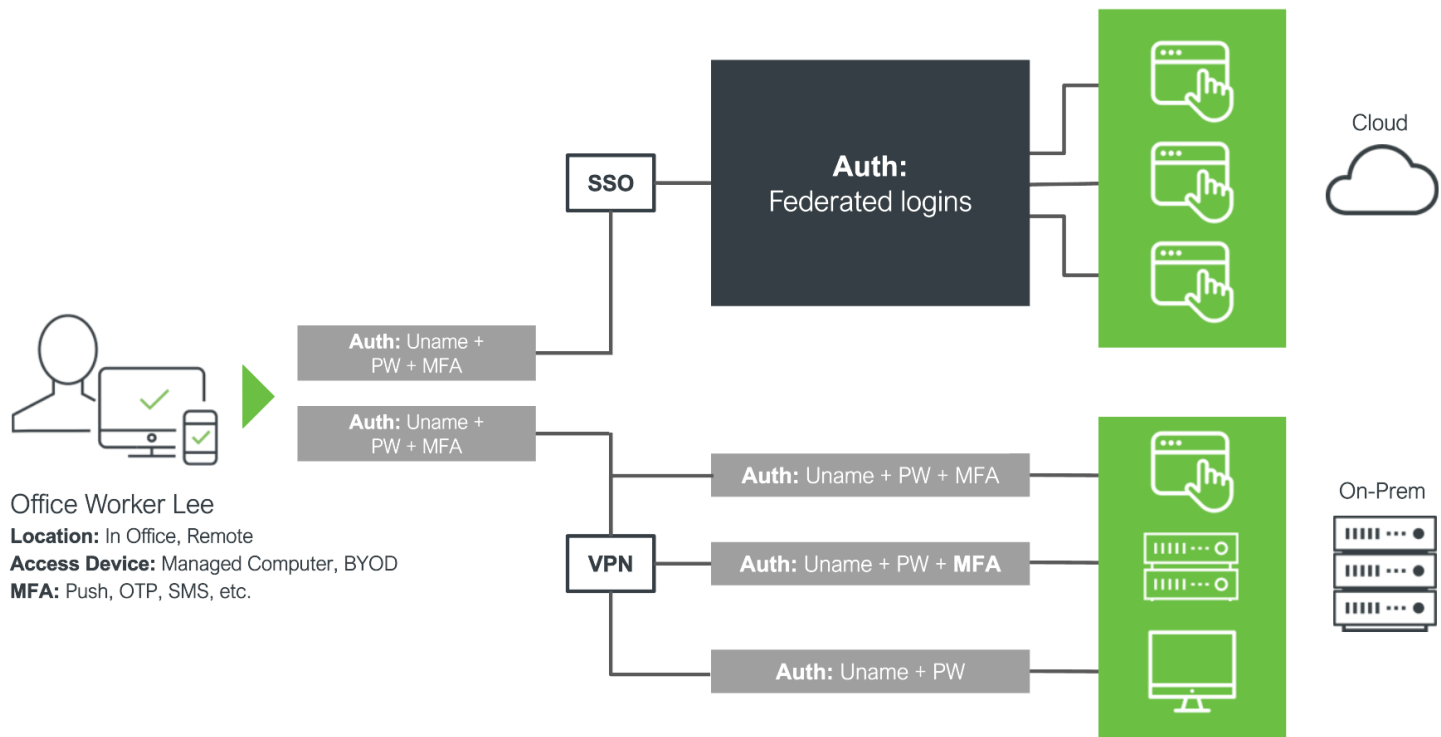
User Demo: Cisco Secure Firewall ZTA + Duo Verified Push + Duo Trusted Endpoints (AD Domain)



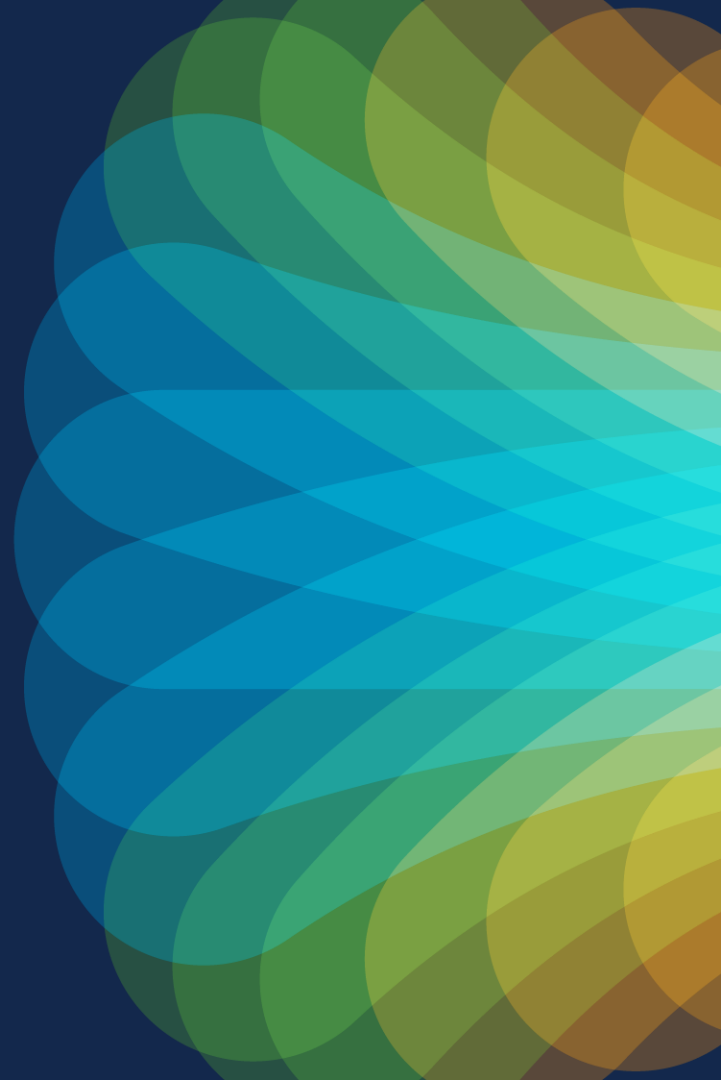
Attacker Demo: Cisco Secure Firewall ZTA + Duo Verified Push + Duo Trusted Endpoints (AD Domain)

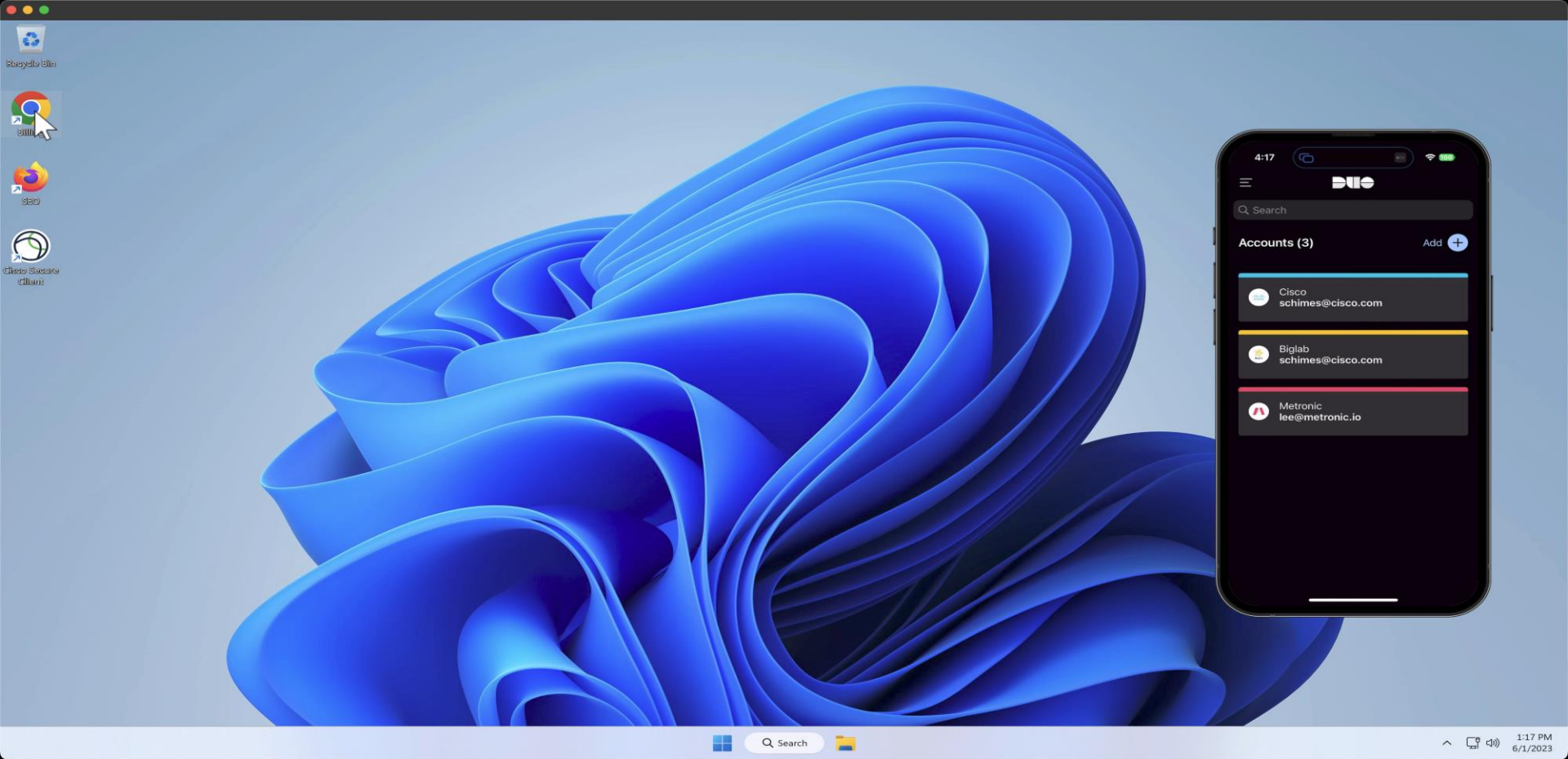


The Friction is Real – Authentication Fatigue



User Demo: Cisco Secure Firewall ZTA + Duo Verified Push + Multiple Browsers



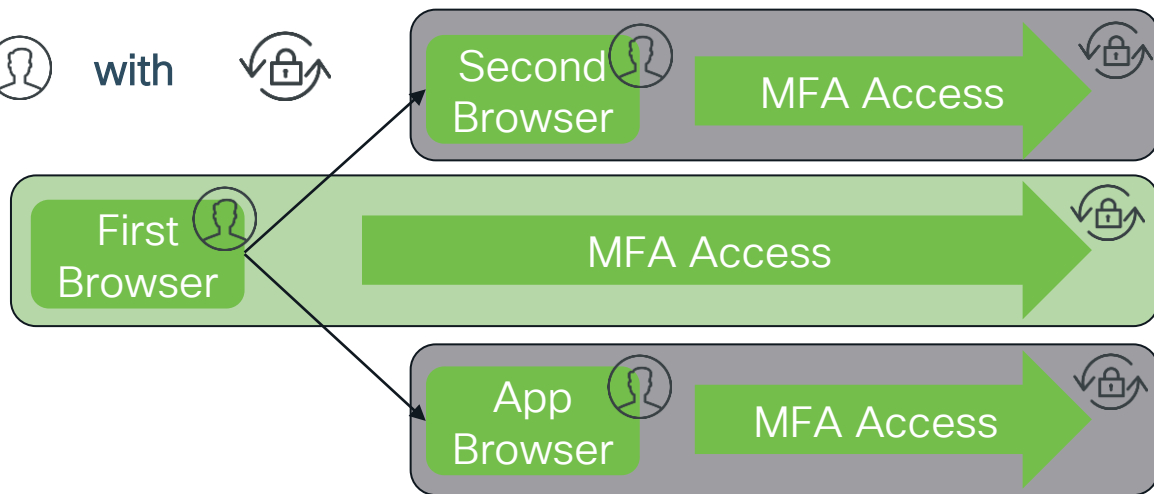


Before: Remembered Device Session Boundaries

Replace



with



Device Desktop

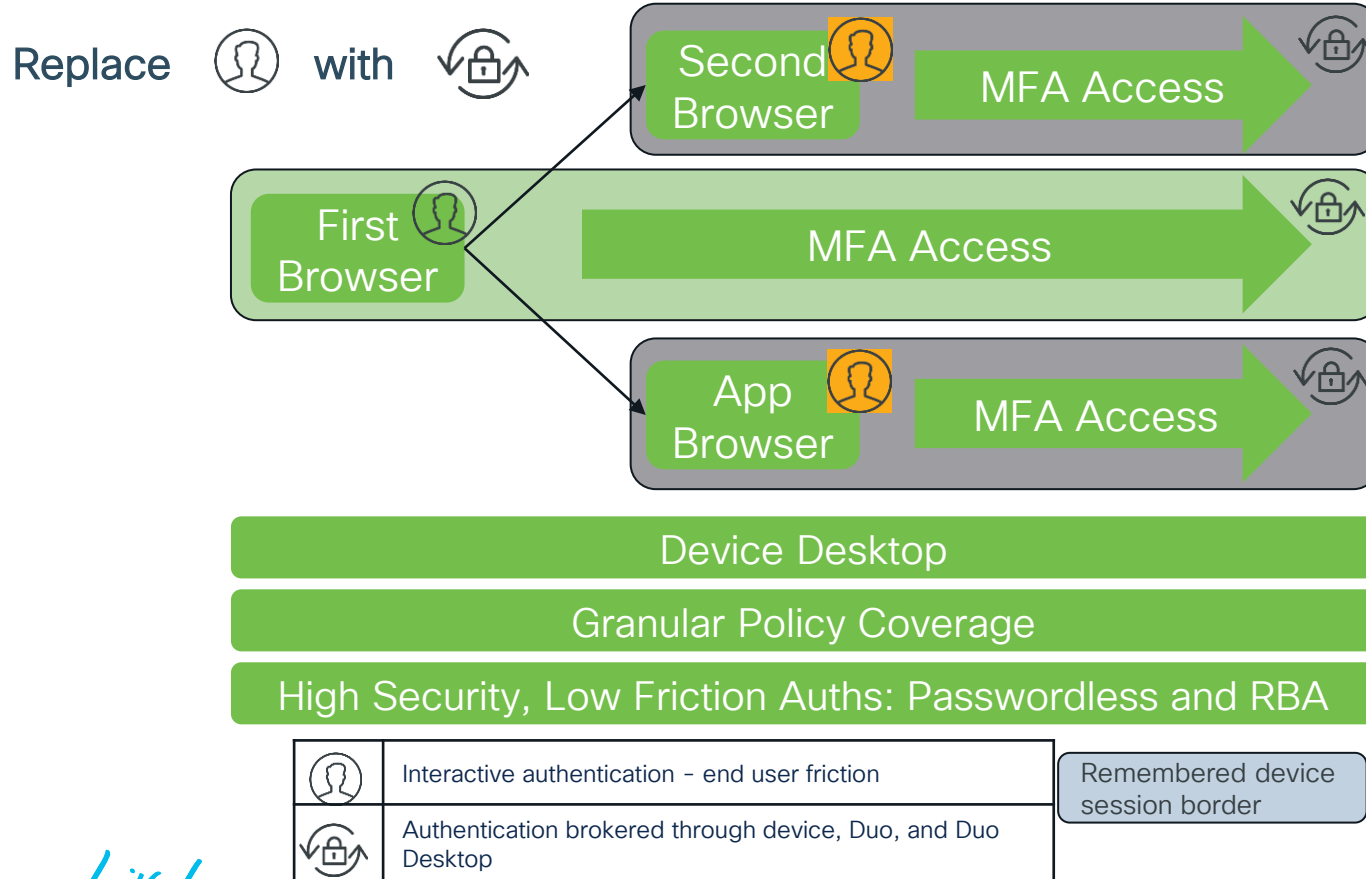
Granular Policy Coverage

High Security, Low Friction Auths: Passwordless and RBA

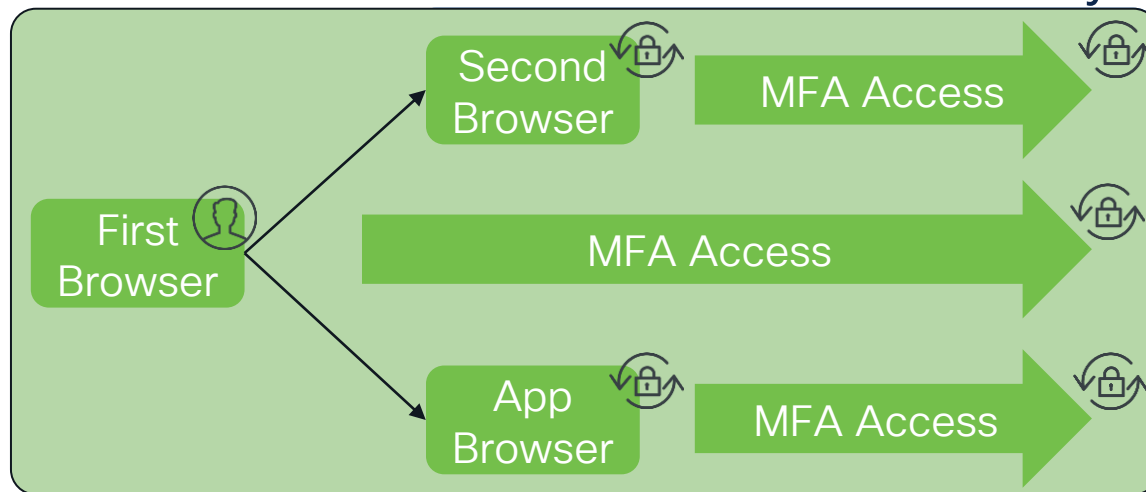
	Interactive authentication - end user friction
	Authentication brokered through device, Duo, and Duo Desktop

Remembered device session border

Before: Remembered Device Session Boundaries



After: Remembered Device Session Boundary



Device Desktop

Granular Policy Coverage

High Security, Low Friction Auths: Passwordless and RBA

	Interactive authentication - end user friction
	Authentication brokered through device, Duo, and Duo Desktop

Remembered device session border

Admin Experience: Enable "Remember Sessions"

Remembered devices

Remembered devices allow users to skip subsequent 2FA requests.

☒ Remember devices for browser-based applications

Allow users to remember their device for

☐ Users will be asked to confirm for each application, then their device will be remembered for that application only.

☒ **After a user has confirmed for any application, their device will be remembered for all applications.**

☐ Remember devices for Windows Logon

Allow users to remember their device for

Note: 2FA will be enforced after users sign-out, reboot, or change networks

Preferences

Duo Device Health

Version 3.2.1.0 (Alpha) [Release notes](#)

Updated on Dec 1, 2022

[Privacy statement](#)

[Data FAQ](#)

☒ Automatically download and install updates

The app will automatically download and install updates in the background.

☒ Launch Duo Device Health automatically when I log in

☒ Enable detailed diagnostic reports

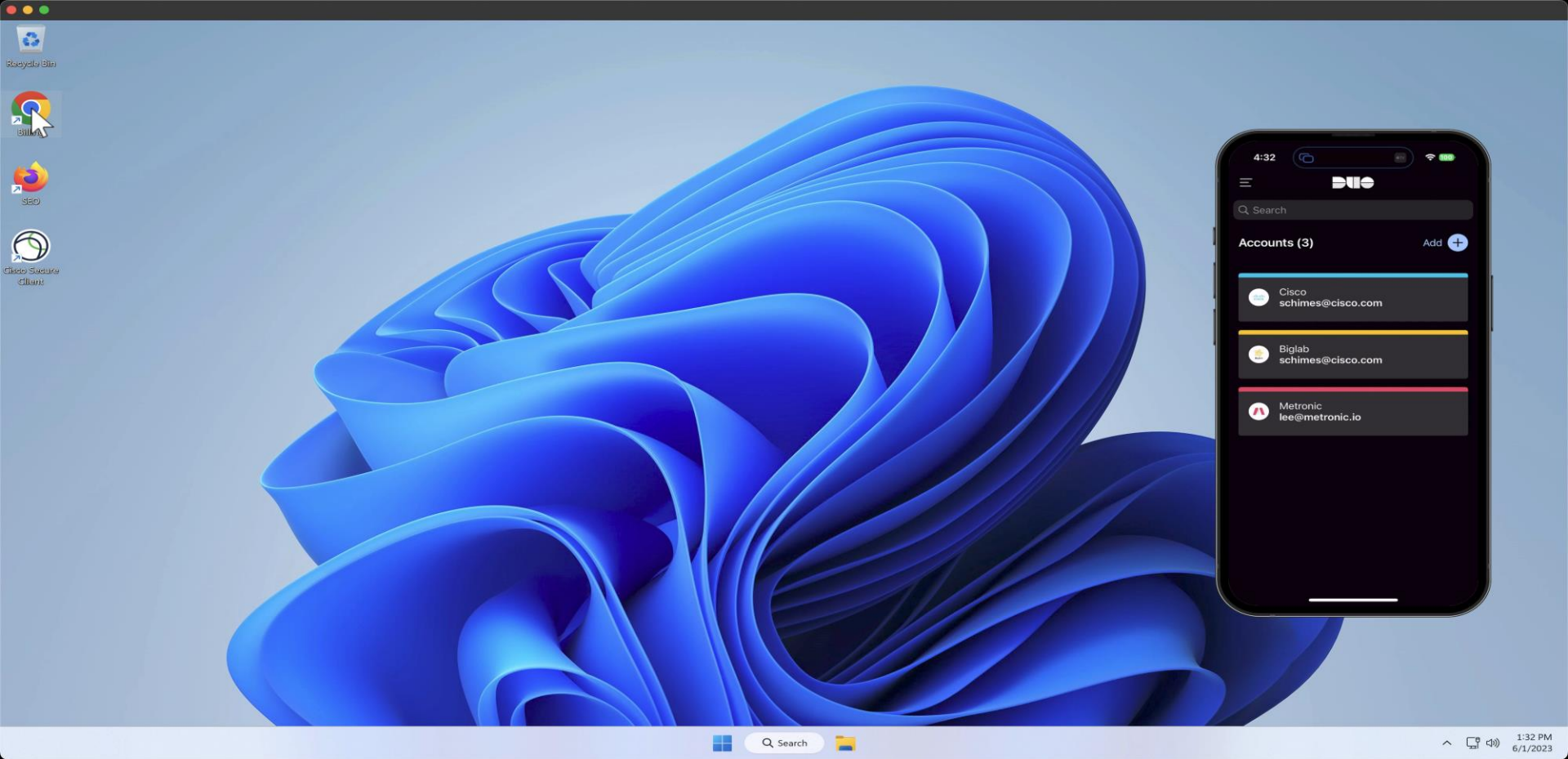
☒ Remember sessions in Duo Device Health

Uninstall Device Health

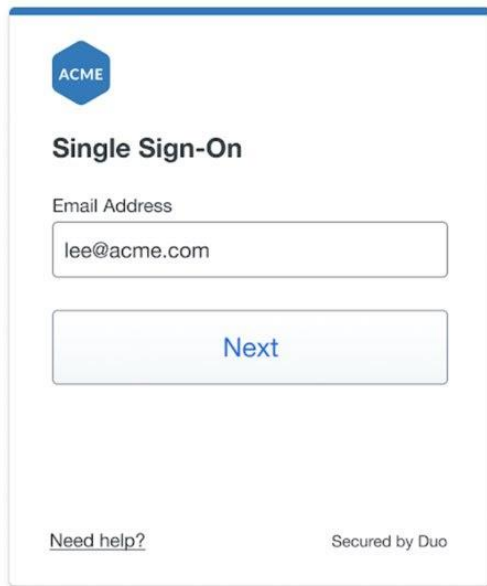
Uninstall

Uninstalling may block you from accessing your applications. Check with your administrator before proceeding.

User Demo: Cisco Secure Firewall ZTA + Duo Verified Push + Multiple Browsers + Duo DHA Remembered Sessions



Duo Passwordless. 1, 2, 3...you are in!



ACME

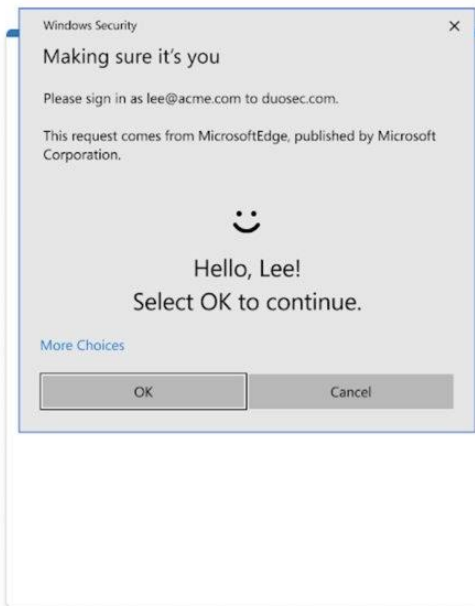
Single Sign-On

Email Address

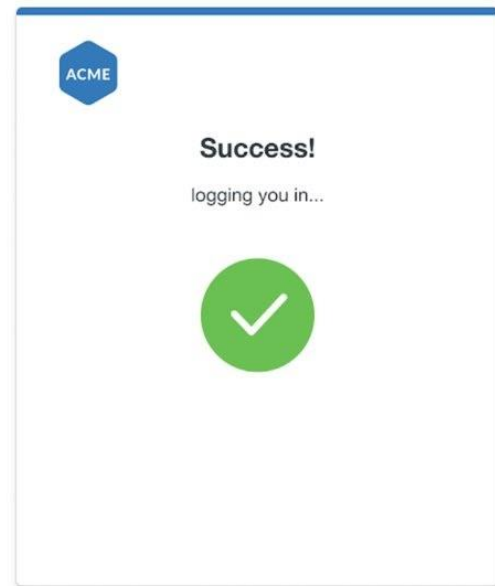
Next

[Need help?](#) Secured by Duo

Enter your current username

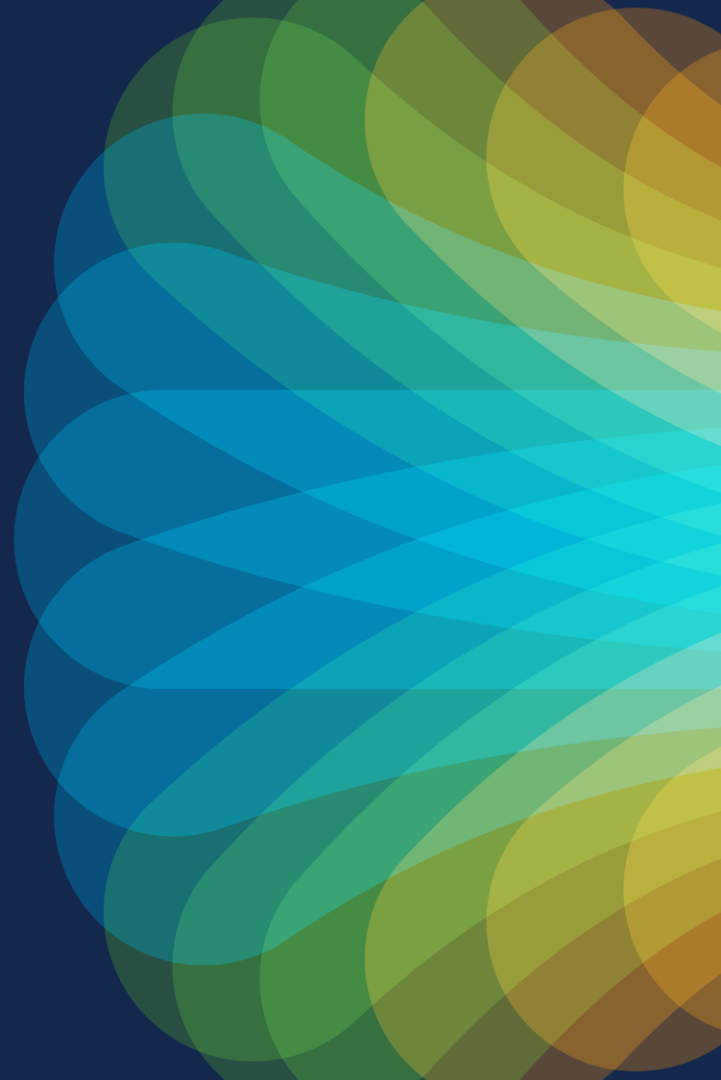


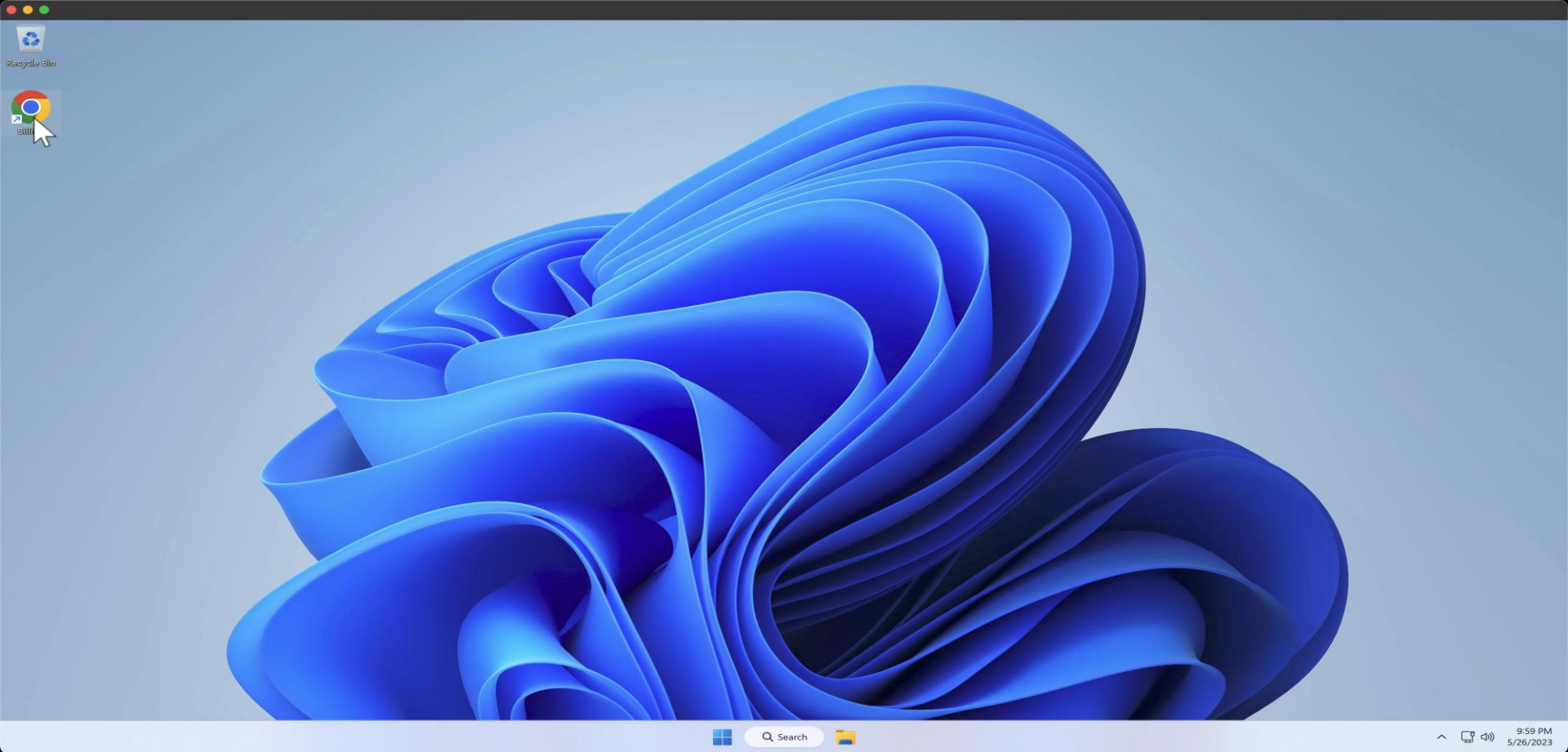
Use Passwordless Authenticators:
Platform Biometrics (Touch ID, Windows Hello)
FIDO2 security Keys (YubiKey, Feitian)
Duo Mobile (passwordless push)



That's it!

User Demo: Cisco Secure Firewall ZTA + Duo Passwordless

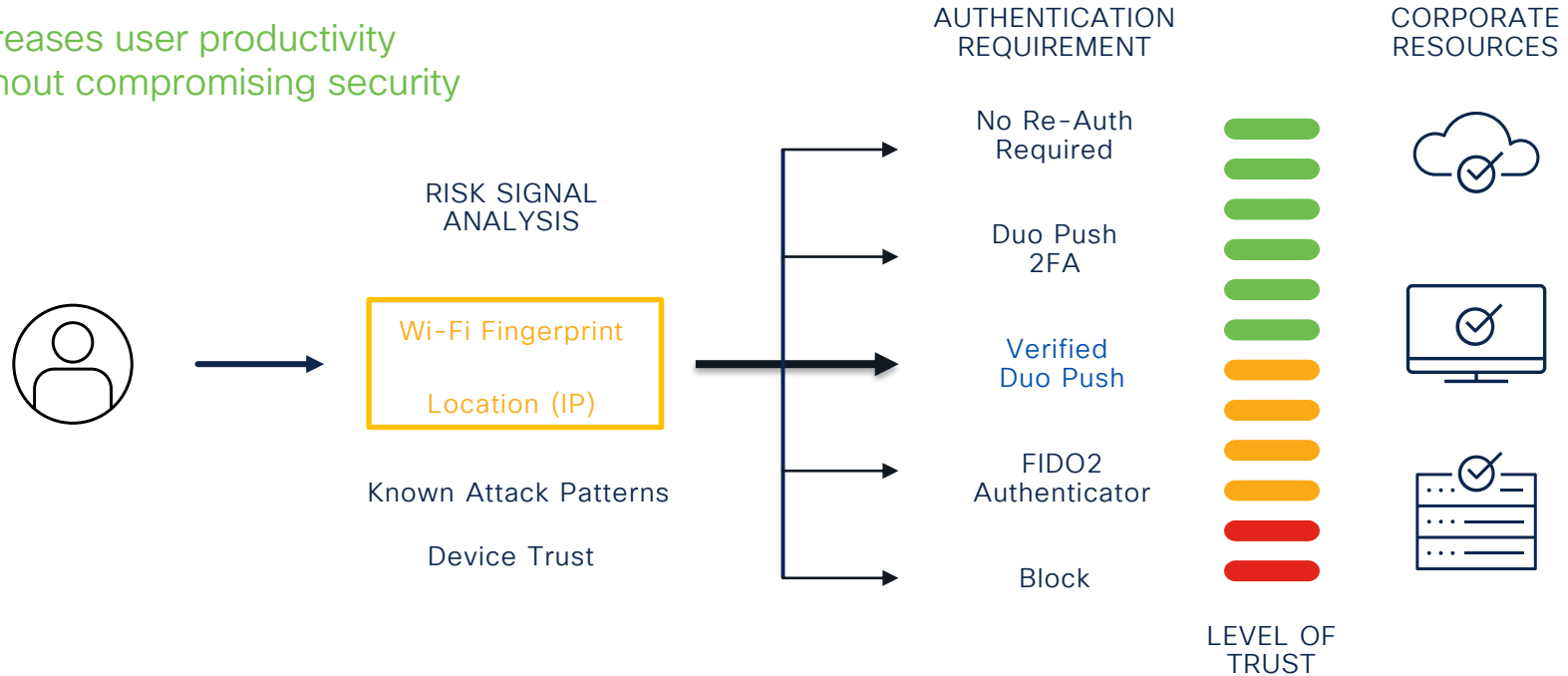




Risk-Based Authentication

Dynamically adjust requirements based on risk level

Increases user productivity
without compromising security



Risk-Signal: Wi-Fi Fingerprint

Wi-Fi Fingerprint analysis requires Duo Desktop on Windows and macOS access devices.

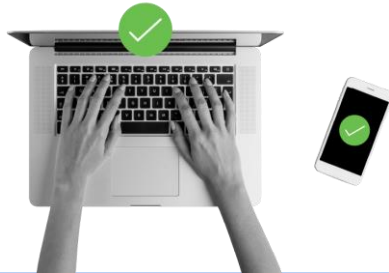
Network 1



Network 2



Network 3



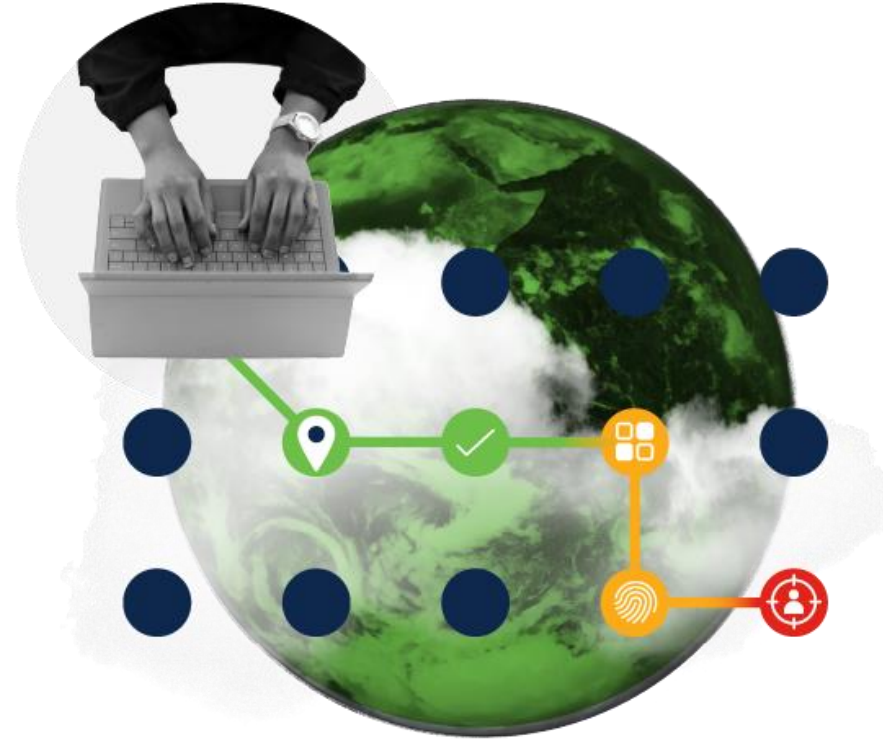
Anonymized Wi-Fi network data provides a strong risk signal.

Low Risk: Familiar network fingerprint

High Risk: Novel network fingerprint

Risk-Signal: Known Attack Patterns

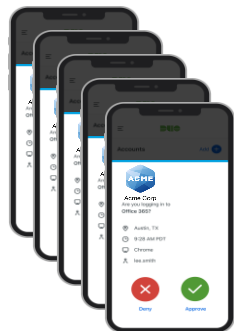
1. **User Marked Fraud:** A user has indicated they weren't responsible for a login.
2. **Anomalous and suspicious activity:** There are unusual authentication attributes, such as repeated authentication failures.
3. **Push spray:** Authentications show characteristics of an adversary performing a non-targeted push attack across multiple users.
4. **Push phishing:** Authentications show characteristics of an adversary performing a targeted push harassment attack.
5. **Unrealistic travel:** A user appears to authenticate from a new location that would be impossible to reach based on the past authentication location.
6. **Country code mismatch:** The authentication device and access device appear to be in two different countries.



Risk-Based Authentication: Factor Selection

Enhances security without compromising user experience by stepping up to more secure factors only when required

Push Phishing Attack Pattern



Risk-Based Authentication

No Re-Auth
Required

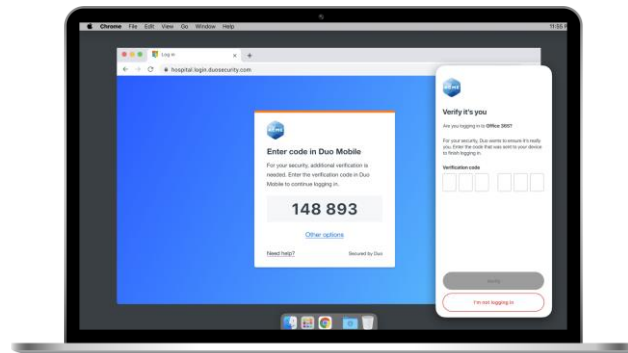
Passcodes /
Token
required

Verified
Duo Push
required

FIDO2
Authentication
required

Access Denied

Verified Duo Push



Fends off push phishing attacks while preserving user experience
by only requesting additional interaction for high-risk logins

Low Risk: Normal Push requests patterns

High Risk: Duo recognizes patterns from
common MFA targeted attacks

Risk-Based Authentication: Remembered Devices

Remembered Device
No re-authentication
required



No change to IP address /
Wi-Fi Fingerprint



Risk-Based Authentication

No Re-Auth
Required

Duo Push
2FA required

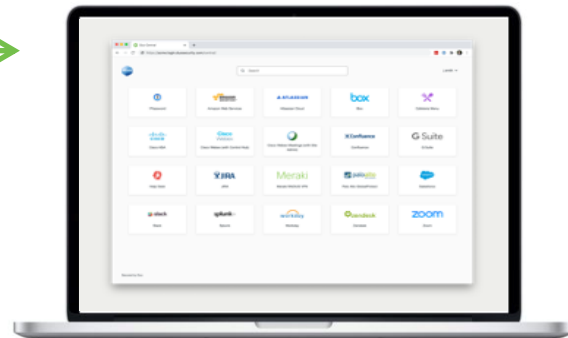
Verified
Duo Push
required

FIDO2
Authentication
required

Access Denied



Frictionless Access

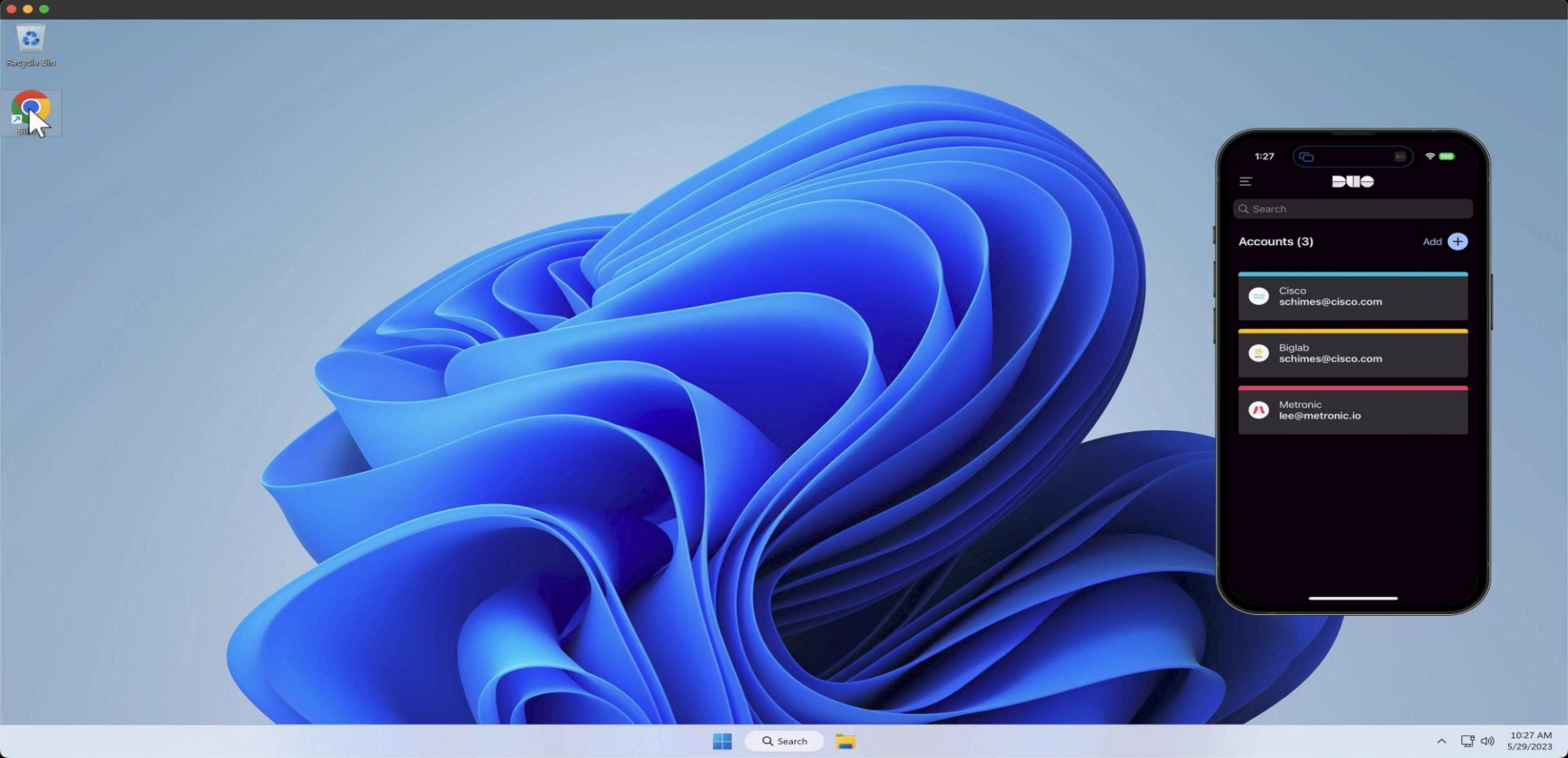


Enhanced protection for remembered devices.
Dynamically require authentication when change in risk is detected.

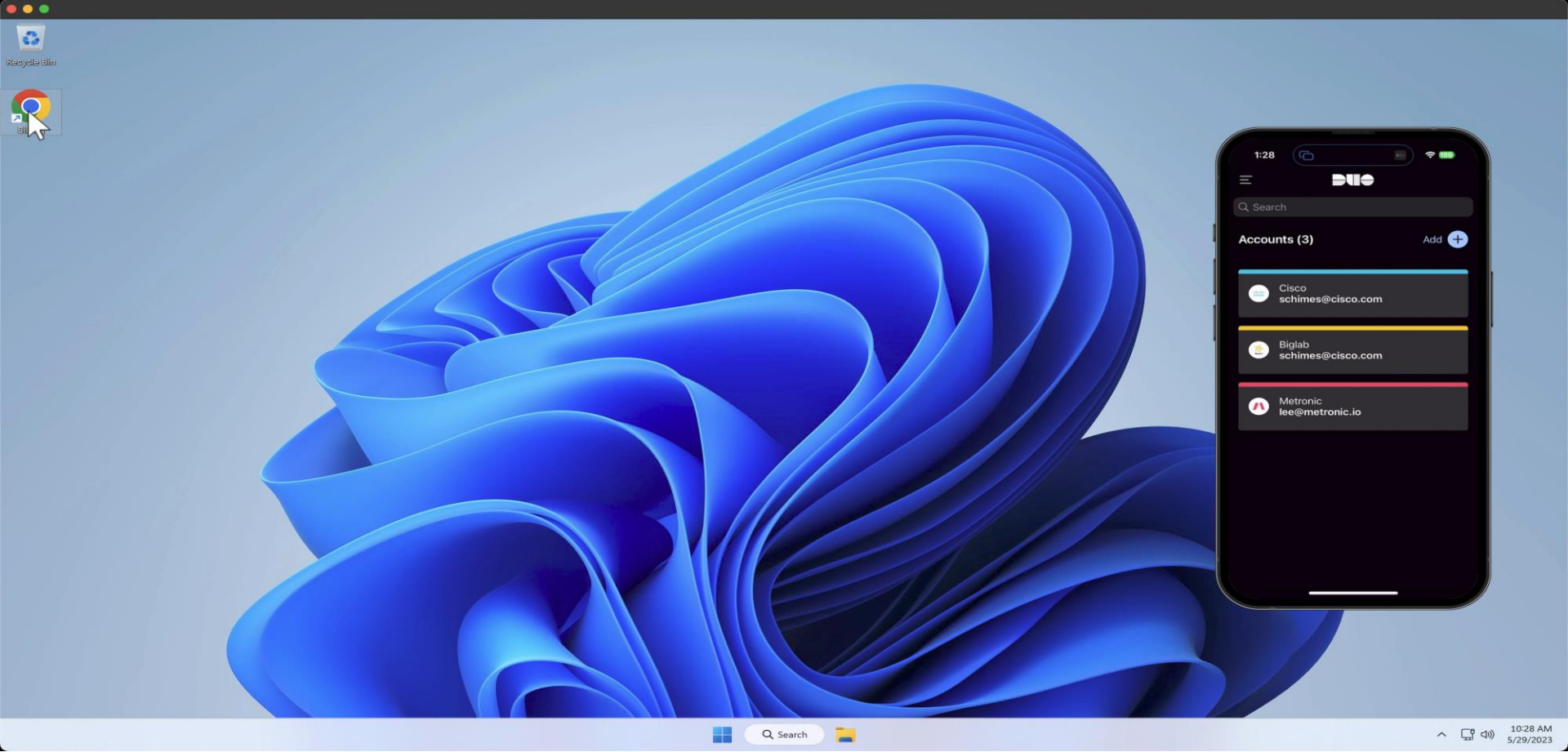
Low Risk: Device is remembered, no change,
no re-authentication required for X days

High Risk: Device is remembered, change
in network fingerprint, risk level increased,
re-authentication required

User Demo: Cisco Secure Firewall ZTA + Duo Risk-Based Auth (High Risk)

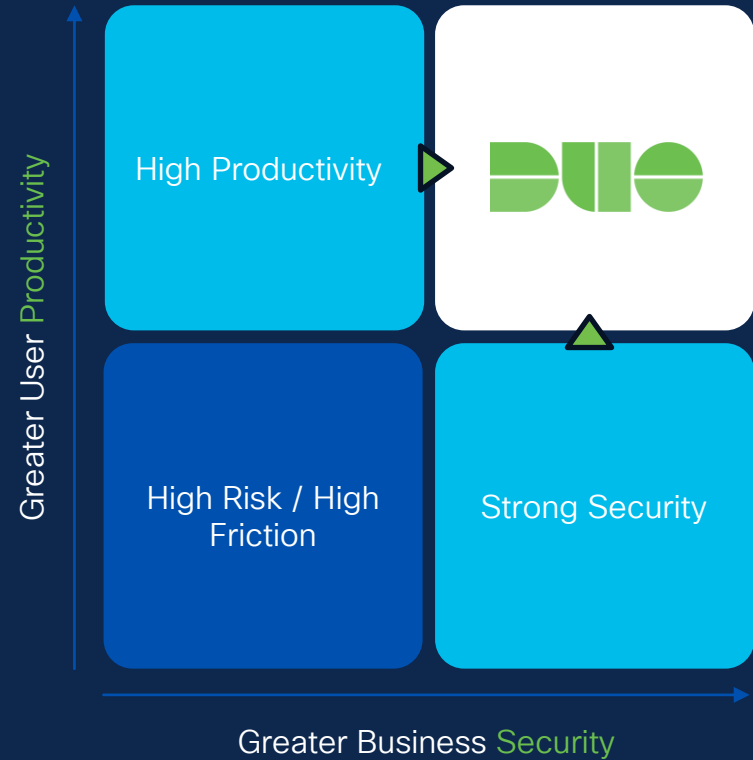


User Demo: Cisco Secure Firewall ZTA + Duo Risk-Based Auth (Low Risk)

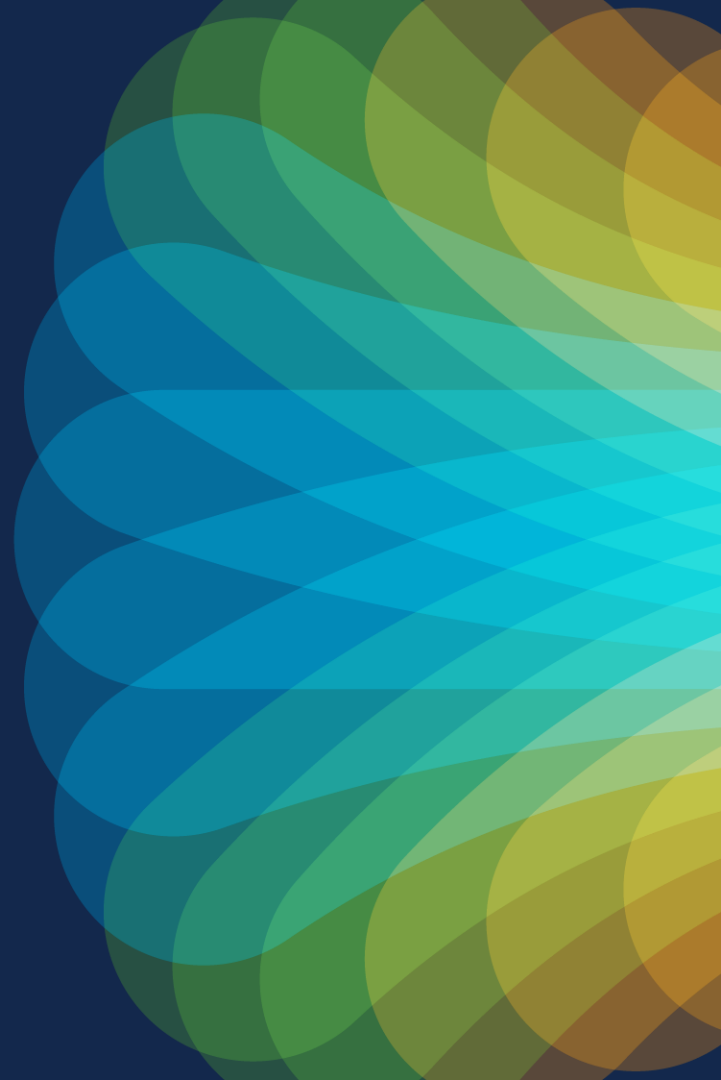


Eliminate the trade-off

Frustrate attackers, not users

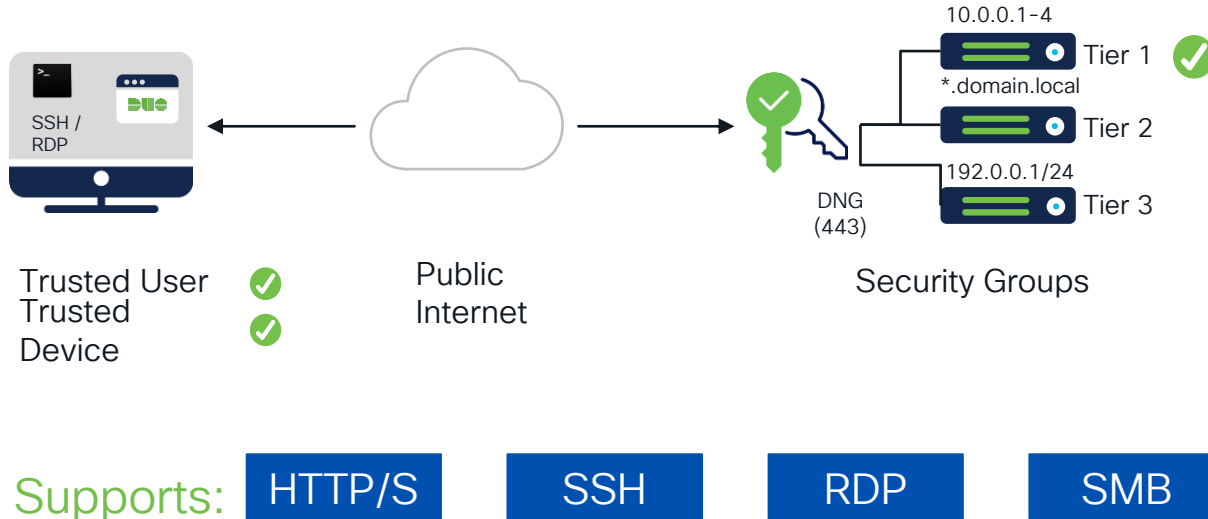


Duo Network Gateway (DNG)



VPN-less Remote Access to Private Applications

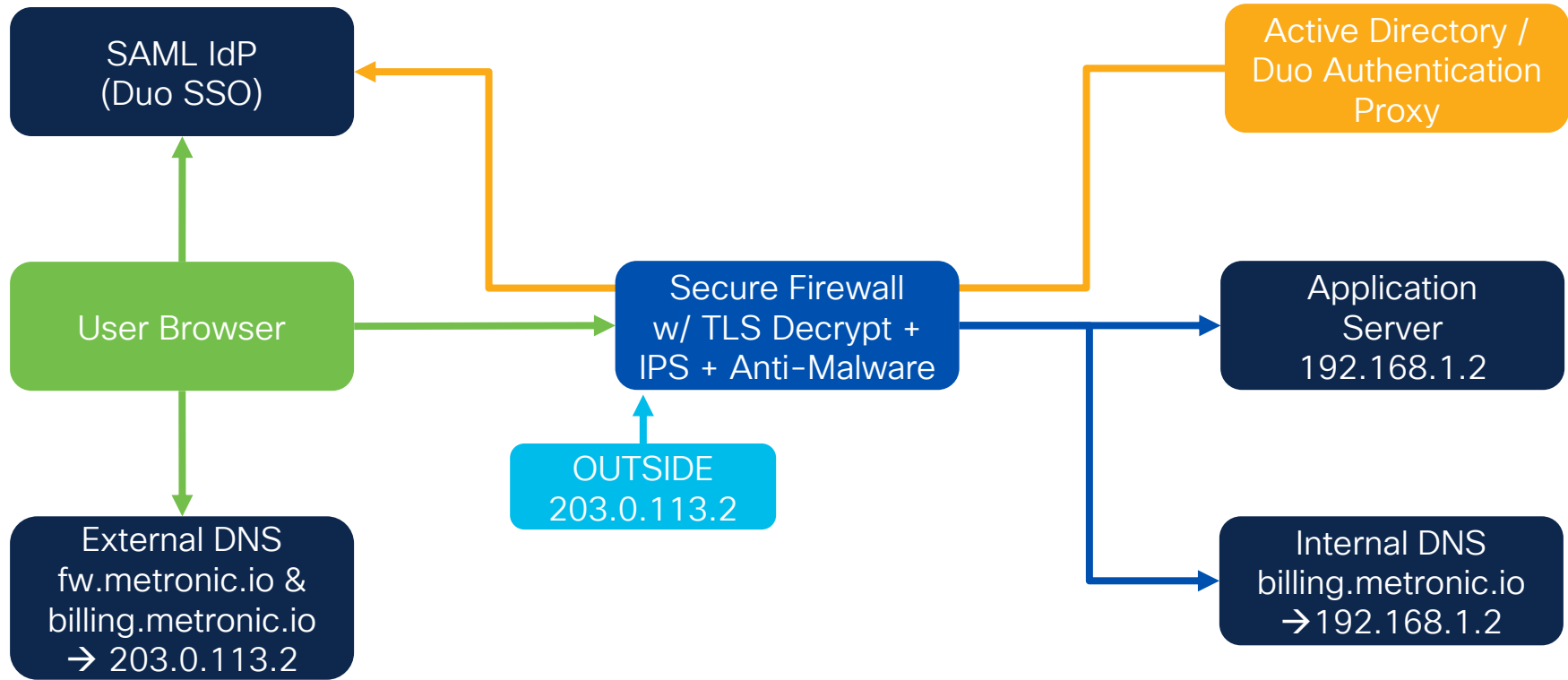
Detect user & device context for internal apps with the Duo Network Gateway



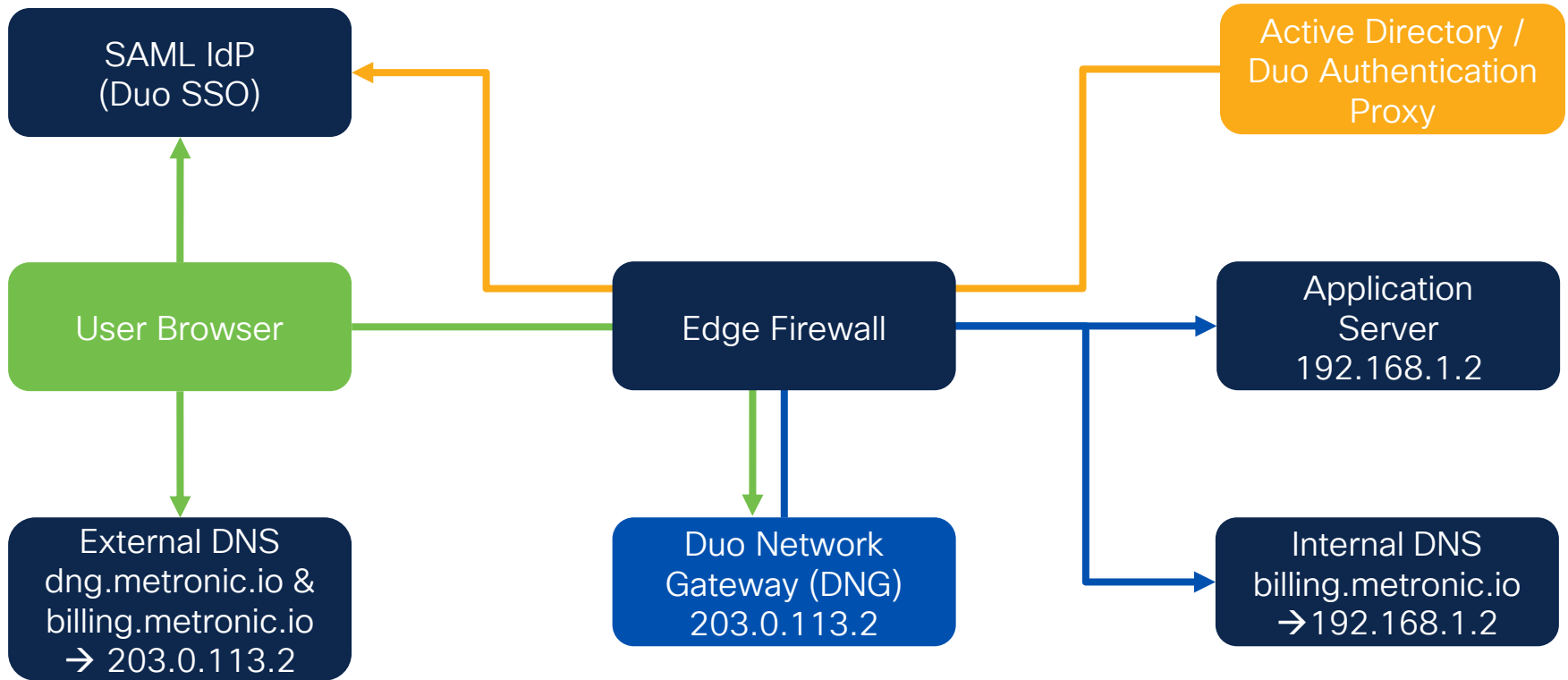
Use Cisco Duo Premier to secure access to private applications on-premises or in the public cloud.



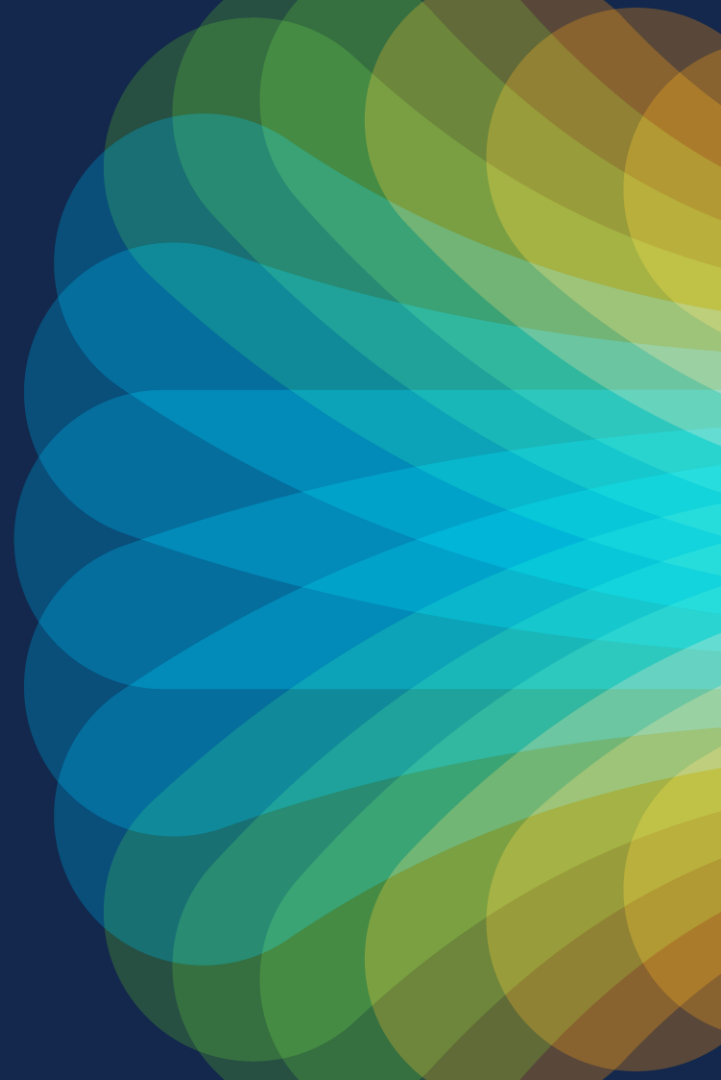
Demo Setup: Secure Firewall ZTA w/ Duo SSO

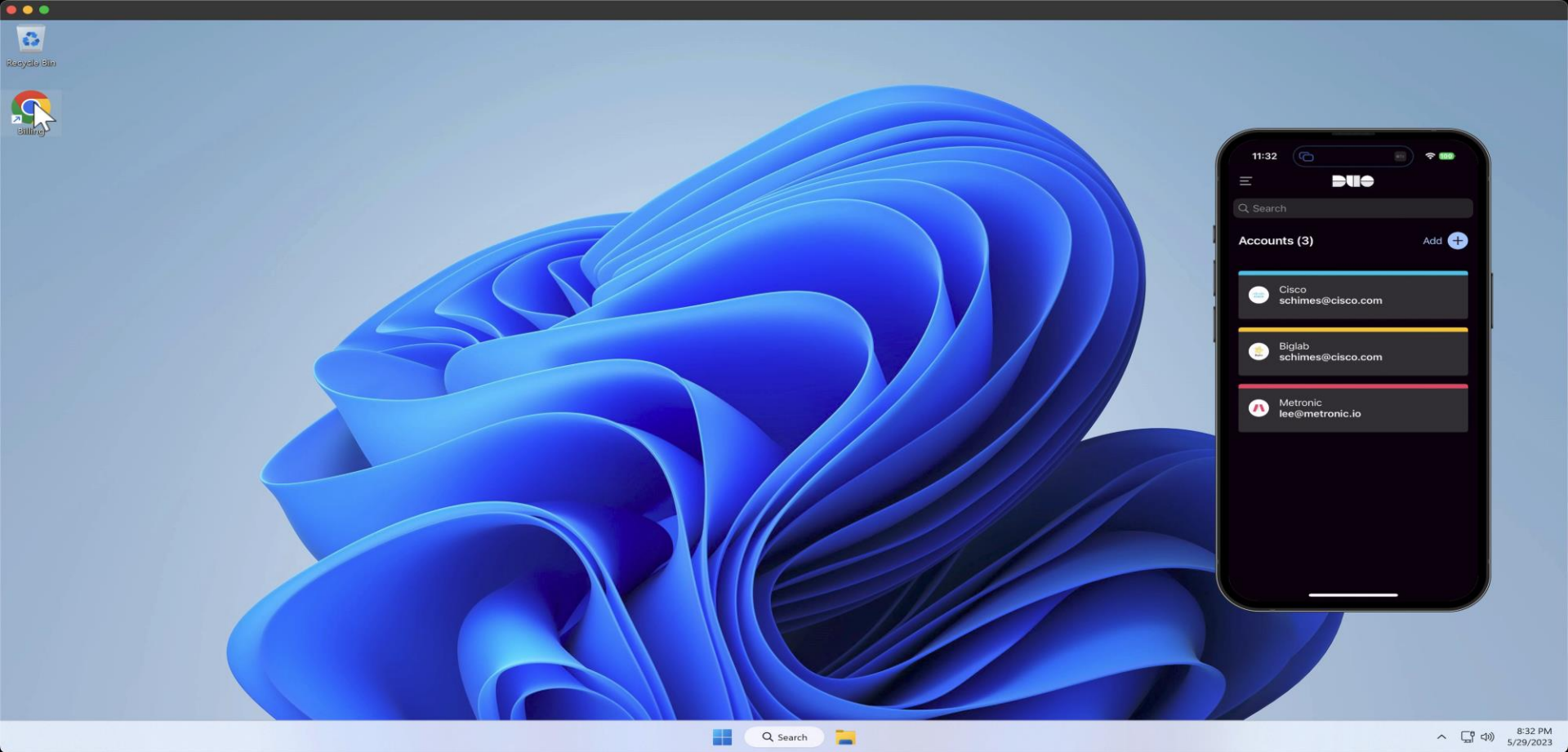


Demo Setup: Duo Network Gateway w/ Duo SSO



User Demo: Duo Network Gateway (DNG)

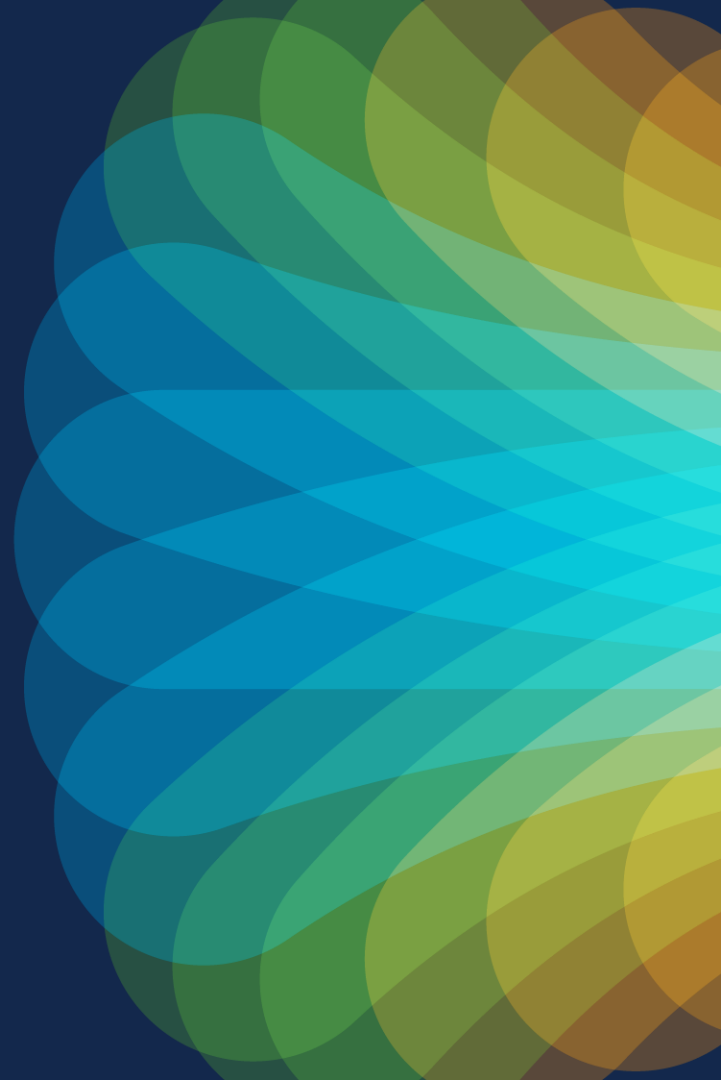




Cisco Zero Trust Access Options

	Secure Firewall	Duo Network Gateway	Cisco Secure Access
Hosting	Hardware / VM	Docker Container	
Type	Clientless	Clientless	
Client	Web browser	Web browser and/or Duo Connect	
Supported Traffic	Client-to-server	Client-to-server	
Supported Apps	HTTPS	HTTP, HTTPS, RDP, SSH, SMB	
Client Protocol(s)	TLS	TLS	
Controls	Per-App Policy, TLS Decrypt, IPS, Anti-Malware	Per-App Policy, Identity, Access Control, Device Posture, Geolocation	

Cisco Secure Access



Cisco Secure Access

Go beyond core Security Service Edge (SSE) to better connect and protect your business

Core SSE



Secure Web
Gateway (SWG)



Cloud Access Security
Broker (CASB) and
DLP



Zero Trust Network
Access (ZTNA)



Firewall as a
Service (FWaaS)
and IPS



Cisco delivers the core and more in a single subscription...



DNS
Security



Multimode
DLP



Advanced
Malware
protection



Sandbox



Talos
Threat
Intelligence



VPN as a
Service



Digital
Experience
Monitoring*



Remote
Browser
Isolation*

Add-on solutions



SD-WAN



XDR



Duo MFA/
SSO



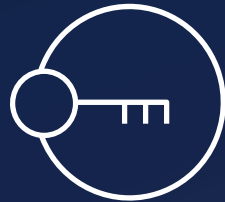
CSPM

* Included in the unified experience / separate license (optional)

Cisco Secure Access

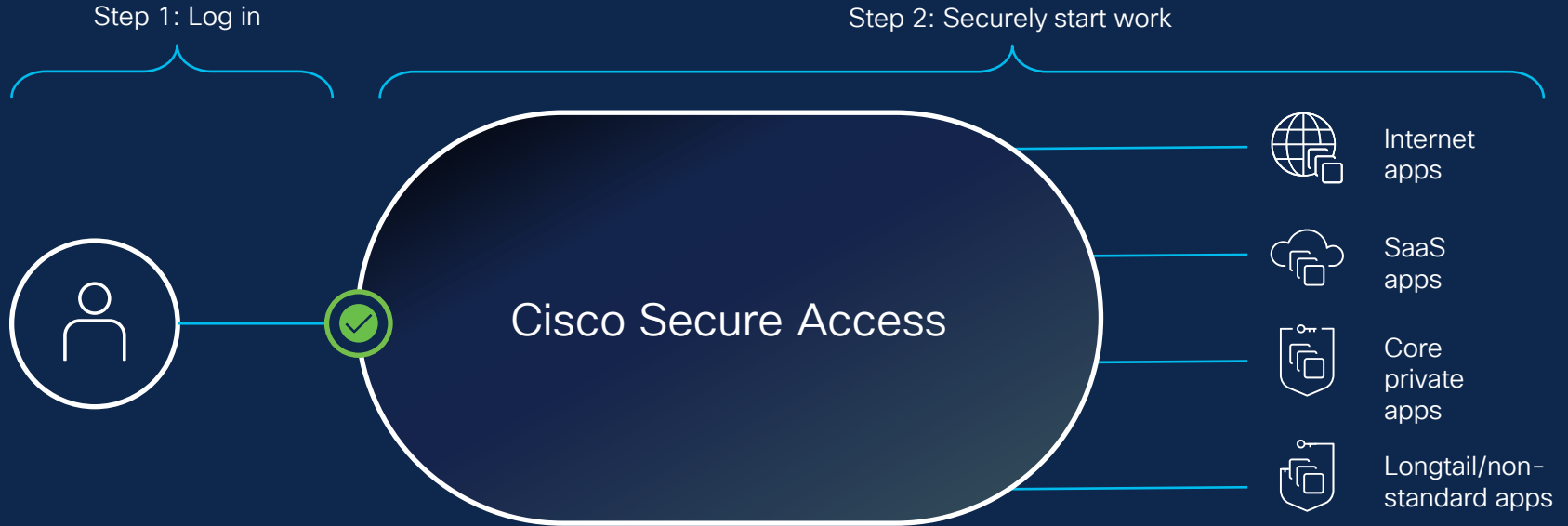
Go beyond core Security Service Edge (SSE) to better connect and protect your business

Core SSE

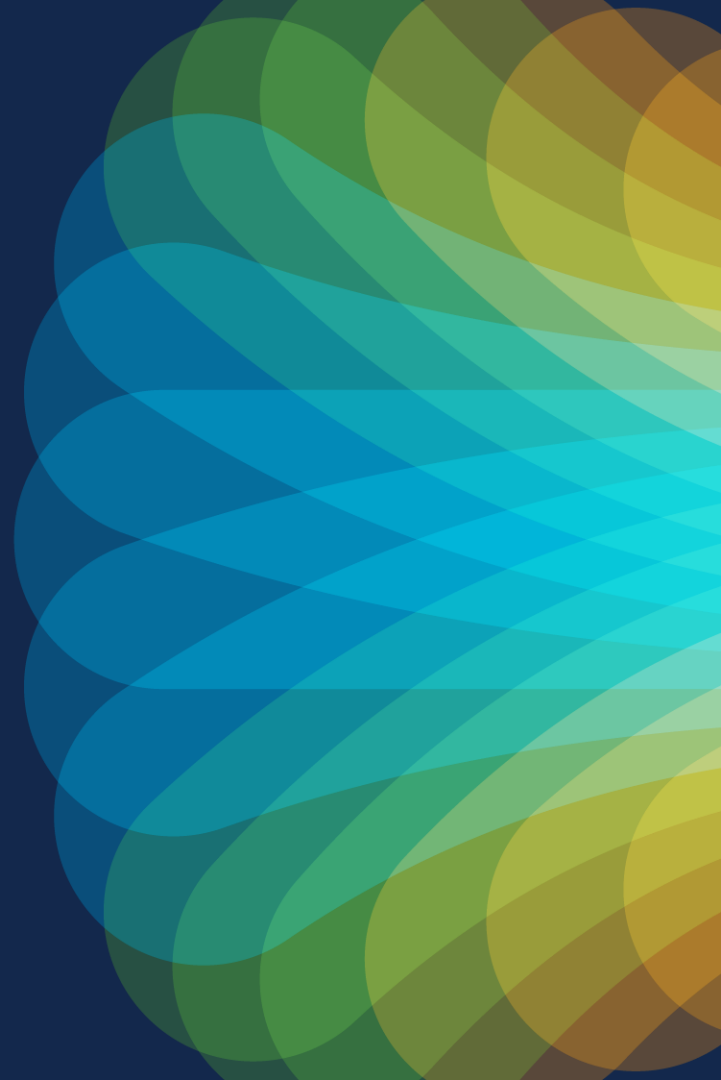


Zero Trust Network
Access (ZTNA)

Easy, frictionless user experience

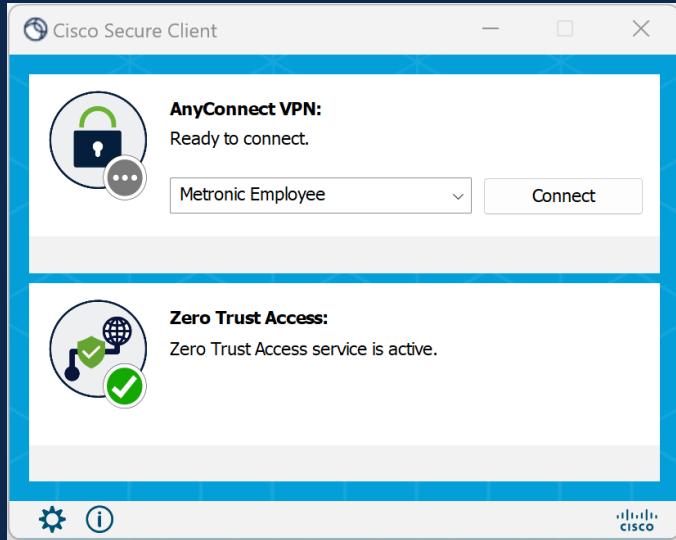


User Demo: Cisco Secure Access + Client-Based Zero Trust Access





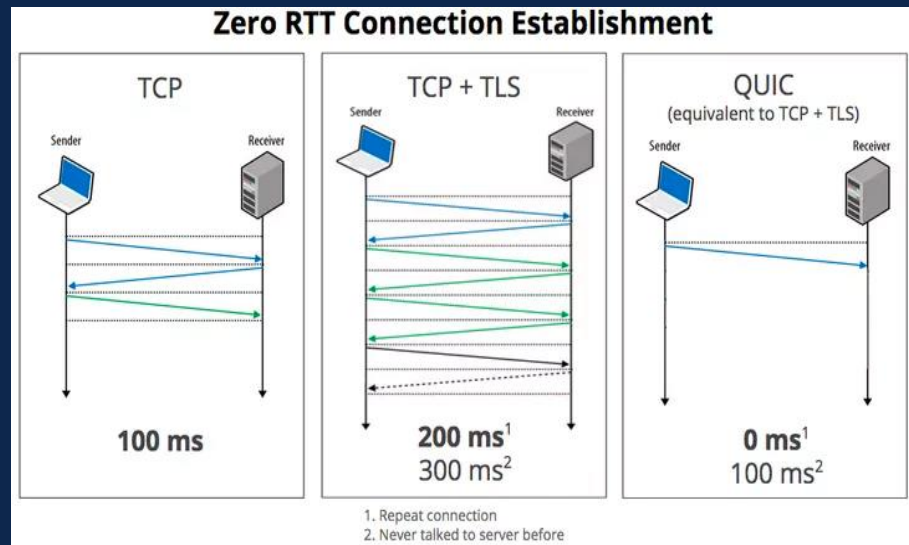
Cisco Secure Client Zero Trust Access Module



- Transparent user experience
- Proxied resource access with coarse-grained or fine-grained access control
- Service managed client certificates with TPM/hardware enclave key storage
- Support for both TCP and UDP applications
- Cisco and third-party VPN client interop
- Next-generation protocol (MASQUE + QUIC)

What is QUIC and MASQUE?

- **QUIC (not an acronym):**
 - UDP-based, stream-multiplexing, encrypted transport protocol.
 - First used in Google Chrome in 2012.
 - Used for HTTP/3, iCloud Private Relay, SMB over QUIC, DNS over QUIC, etc.
 - Optimized for the next generation of internet traffic with reduced latency compared to TLS over TCP.
- **MASQUE (Multiplexed Application Substrate over QUIC Encryption):**
 - IETF working group focused on next generation proxying technologies on top of the QUIC protocol.
 - Provides the mechanisms for multiple proxied stream and datagram-based flows inside HTTP/2 and HTTP/3.
 - Used by iCloud Private Relay since 2021.
 - HTTP/2 and HTTP/3 extensions allow for the signaling and encapsulation of UDP and IP traffic.



Why QUIC?



Fast connection establishment (0-RTT)



Ability to change IPs without renegotiation (Connection migration)



No waiting for partially delivered packets (Individually encrypted packets)



Not vulnerable to TCP meltdown (UDP transport)



No head-of-line blocking (Stream multiplexing)



Can simultaneously use multiple interfaces (Multipath)

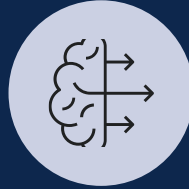
Why MASQUE?



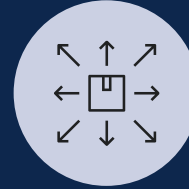
No direct resource access (Proxy architecture)



Broad application support (TCP, UDP and IP)



Fallback to HTTP/2 (TCP 443) if QUIC (UDP 443) is blocked

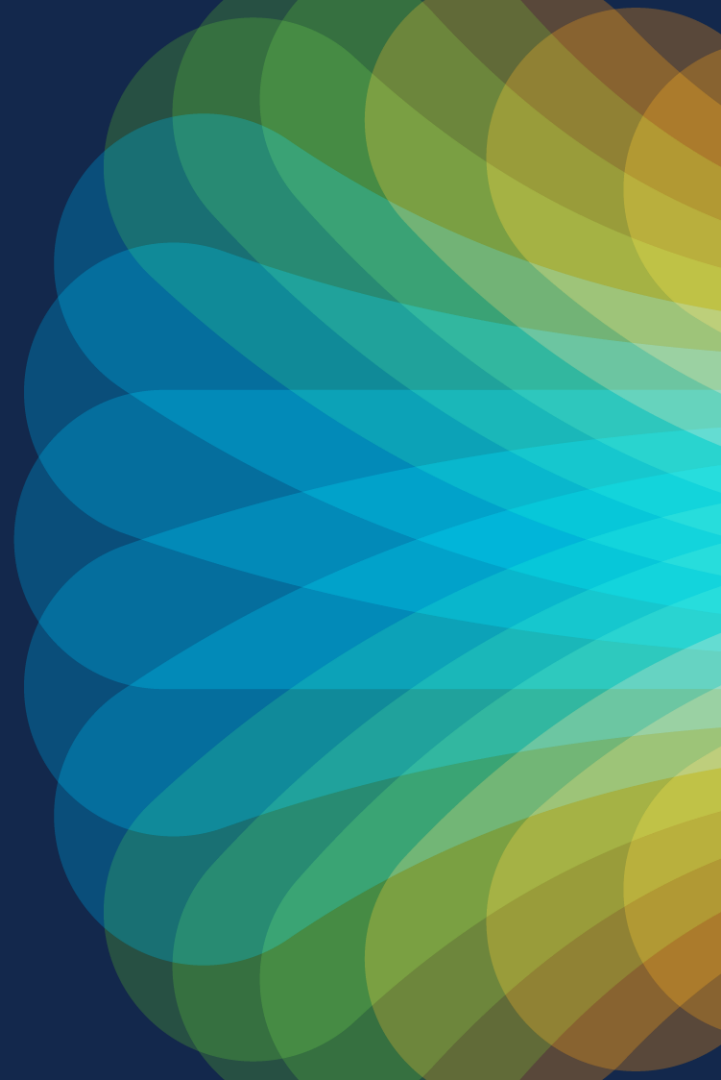


Flexibility to support per-connection, per-app or per-device tunnels



Native OS support

Demo: Cisco Zero Trust Access on Apple iOS





AnyConnect



Duo Mobile



Okta Verify



Billing



Dashboard



SEO



Owlfiles



RD Client



Billing (PWL)



Dashboard (PWL)



SEO (PWL)

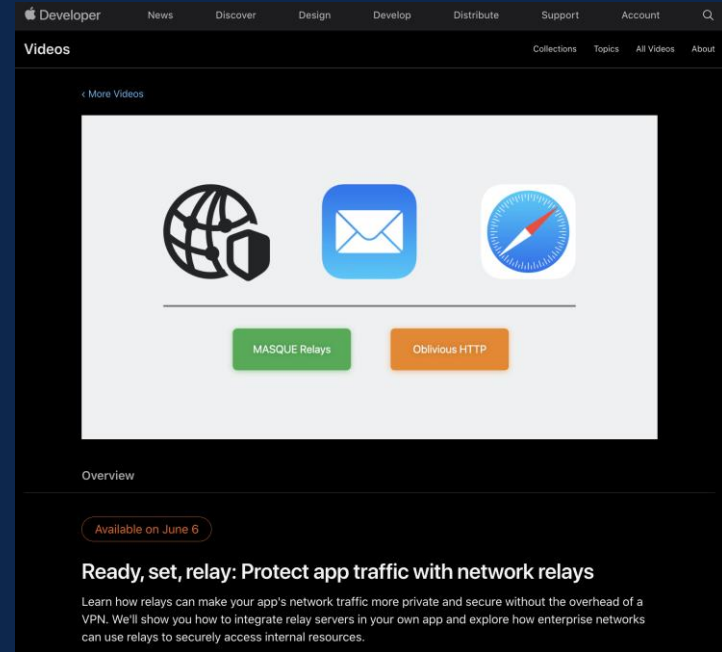


Settings



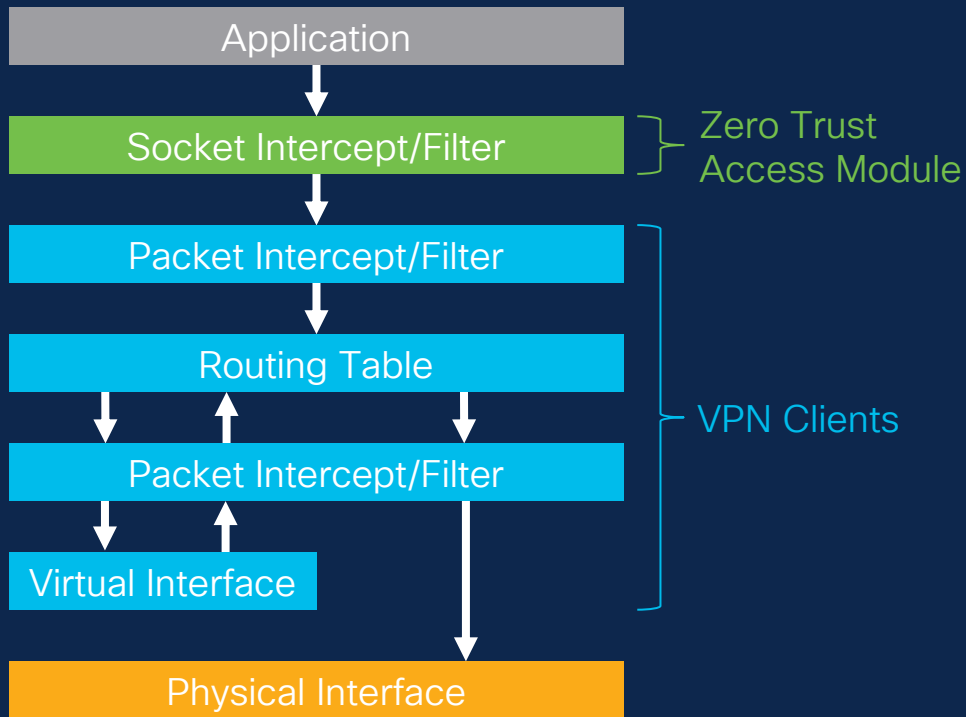
More on Apple's Native OS Support of MASQUE

*“Learn how relays can make your app's network traffic **more private** and **secure** without the overhead of a **VPN**. We'll show you how to integrate relay servers in your own app and **explore how enterprise networks can use relays to securely access internal resources.**”*



<https://developer.apple.com/videos/play/wwdc2023/10002/>

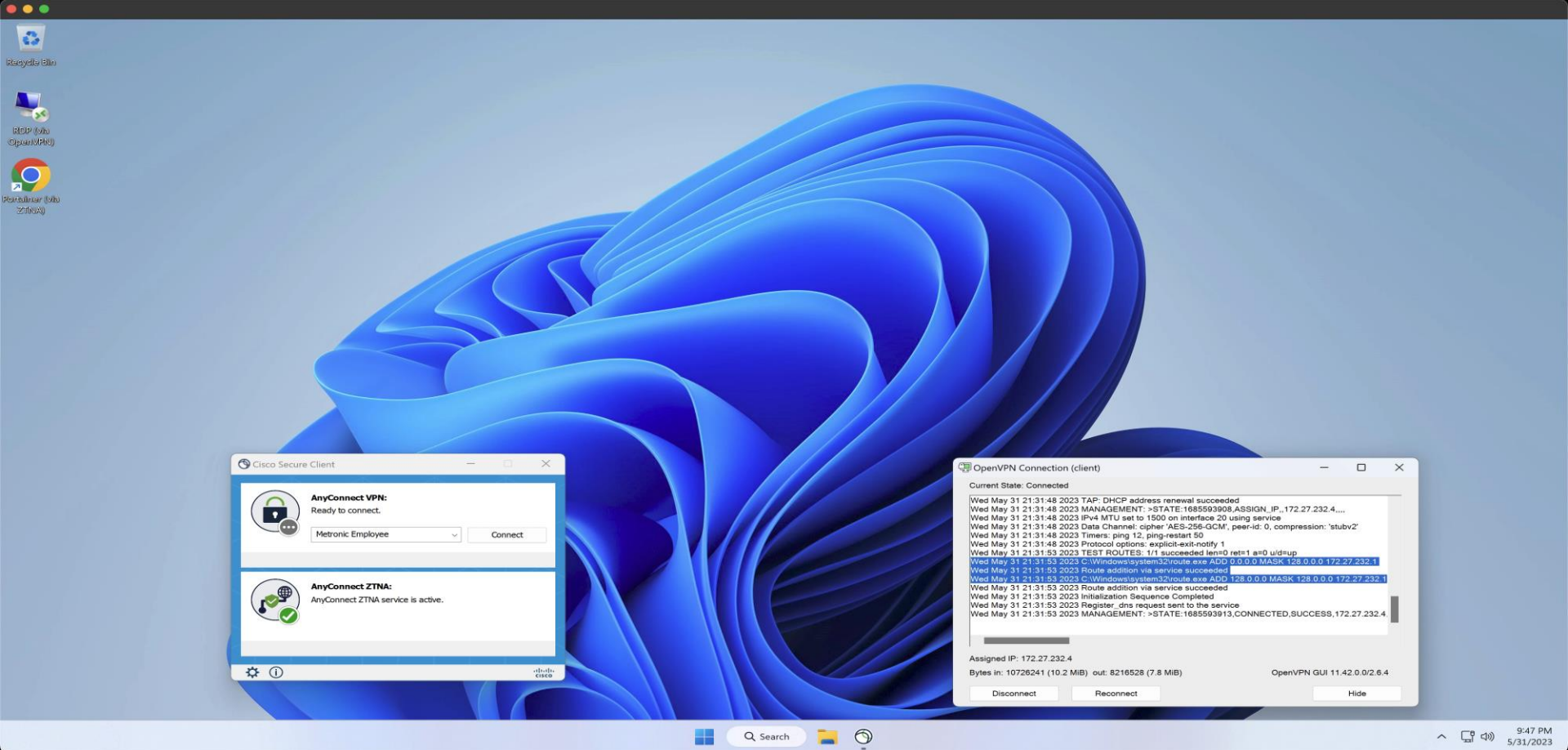
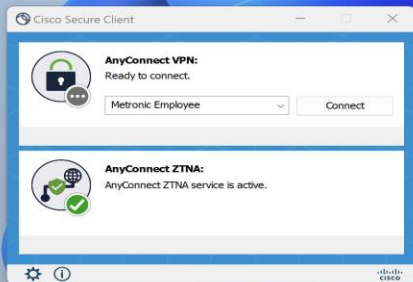
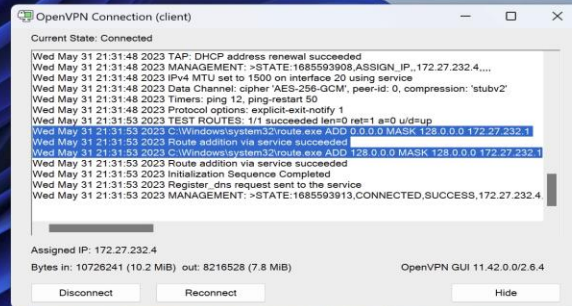
Zero Trust Access Module – Socket Intercept



Why Socket Intercept?

- Control of DNS and application traffic *before* VPN clients
- No route table manipulation
- Ability to capture traffic by IP, IP subnet, FQDN and FQDN wildcard
- Interoperability with Cisco and non-Cisco VPNs

User Demo: Cisco Secure Access + Client-Based Zero Trust Access + Third-Party VPN (OpenVPN)



Zero Trust Access Journey

Pragmatic migration to more control – direct to private apps

Take control of all your private apps with precision

Traditional VPN

Network level access – cannot control at app level – difficult to deploy and manage

VPN as-a-Service

Lift and shift your VPN to the cloud – more control and easier to manage

- Zero Trust Access does not work for non-standard apps
- Setting up Zero Trust Access for every app and user can be arduous
- Move apps to Zero Trust Access over time

Unified Zero Trust Access + VPNaaS

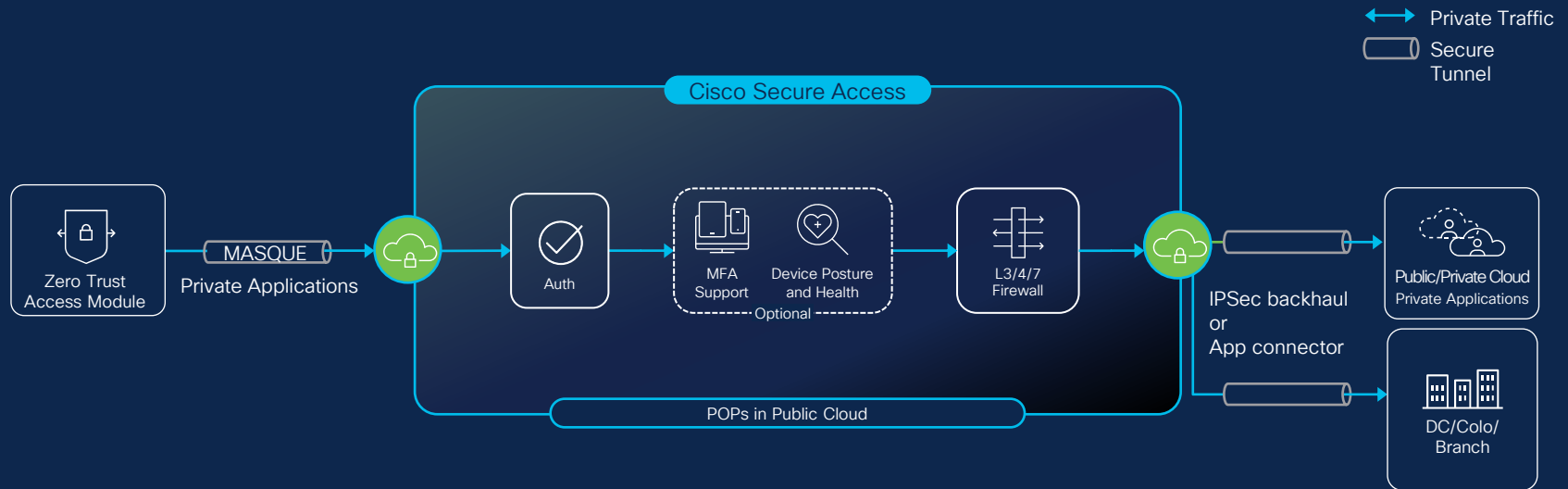
Granular controls at the application level. VPNaaS for non-standard apps

Success

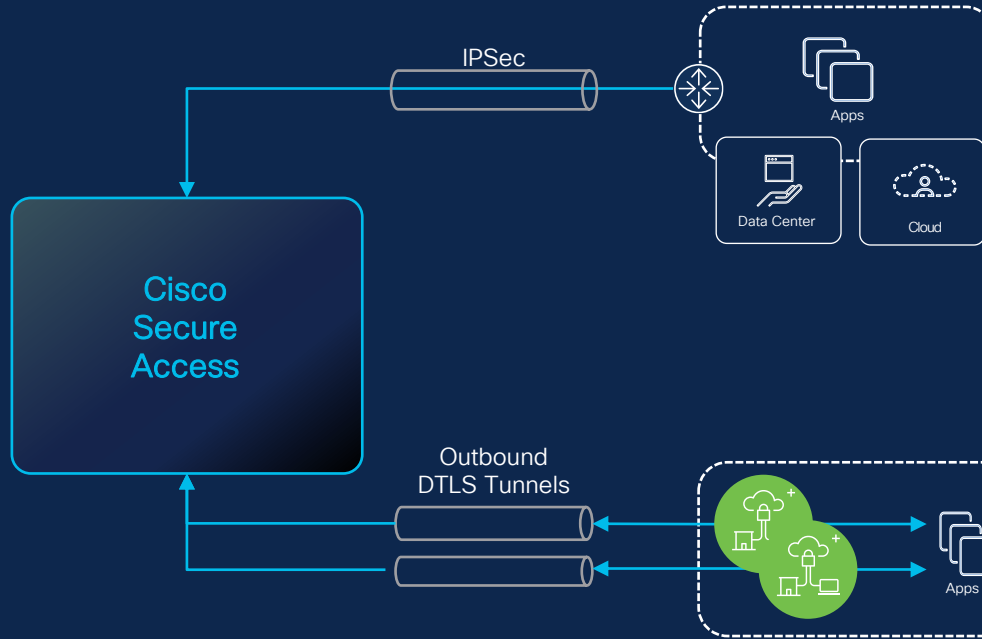
Benefits

- Reduced threat surface
- Posture verification
- App-specific access
- Least privileged access

Zero Trust Access Traffic Flow



Zero Trust Access App Connections



Network Tunnel

- IPSec Backhaul
- Static or BGP based routing
- Auto Failover/ Redundancy

Application Connector (AC)

- Software deployment (VM or Cloud Instance)
- Deploy closest to application
- Outbound connectivity (no holes in firewall)
- Auto failover / load balancing

Cisco Zero Trust Access Options

	Secure Firewall	Duo Network Gateway	Cisco Secure Access		
Hosting	Hardware / VM	Docker Container	SaaS		
Type	Clientless	Clientless	Clientless	Client-Based	
Client	Web browser	Web browser and/or Duo Connect	Web browser	Zero Trust Access Module OS Native Clients	VPN Module
Supported Traffic	Client-to-server	Client-to-server	Client-to-server	Client-to-server	Client-to-server, Client-to-client, Server-to-client
Supported Apps	HTTPS	HTTP, HTTPS, RDP, SSH, SMB	HTTP, HTTPS	TCP, UDP	TCP, UDP, ICMP
Client Protocol(s)	TLS	TLS	TLS	MASQUE over QUIC or TLS	TLS, DTLS, IPSec
Controls	Per-App Policy, TLS Decrypt, IPS, Anti-Malware	Per-App Policy, Identity, Access Control, Device Posture, Geolocation	Per-App Policy, Access Control, Device Posture, Geolocation, TLS Decrypt, IPS		

CISCO *Live!*

Did you know?

You can have a
one-on-one session with
a technical expert!

Visit Meet the Expert in The HUB
to meet, greet, whiteboard & gain
insights about your unique questions
with the best of the best.



Meet the Expert Opening Hours:

Tuesday	3:00pm – 7:00pm
Wednesday	11:15am – 7:00pm
Thursday	9:30am – 4:00pm
Friday	10:30am – 1:30pm

Session Surveys

We would love to know your feedback on this session!

- Complete a minimum of four session surveys and the overall event surveys to claim a Cisco Live T-Shirt



Continue your education



- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

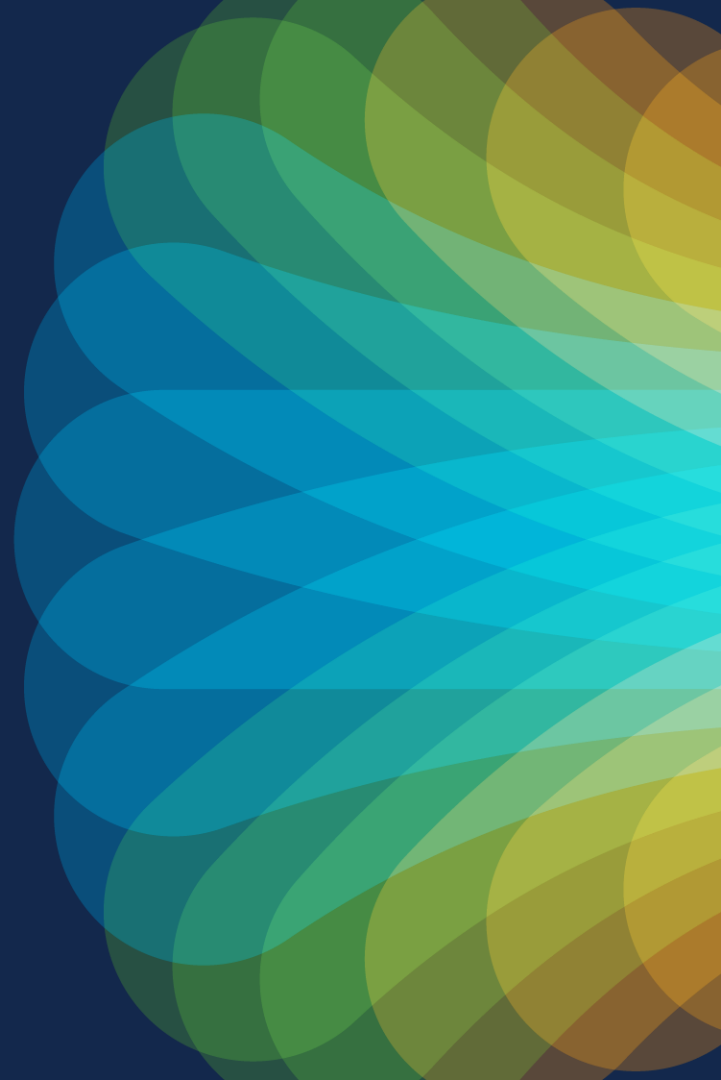


The bridge to possible

Thank you



#CiscoLive



The background is a vibrant, abstract graphic. It features a central bright white light source from which numerous colorful rays emanate, creating a sunburst or starburst effect. The rays transition through a spectrum of colors including yellow, orange, red, and various shades of blue and green. Overlaid on this are several large, semi-transparent, wavy shapes in similar color tones, giving the overall image a sense of motion and energy.

cisco *Live!*

Let's go

#CiscoLive