



# Introducing Cisco Secure Access to Umbrella users

Upasna Gandhi & Michael Neibert

Technical Customer Success Specialists

April 2025

# Agenda

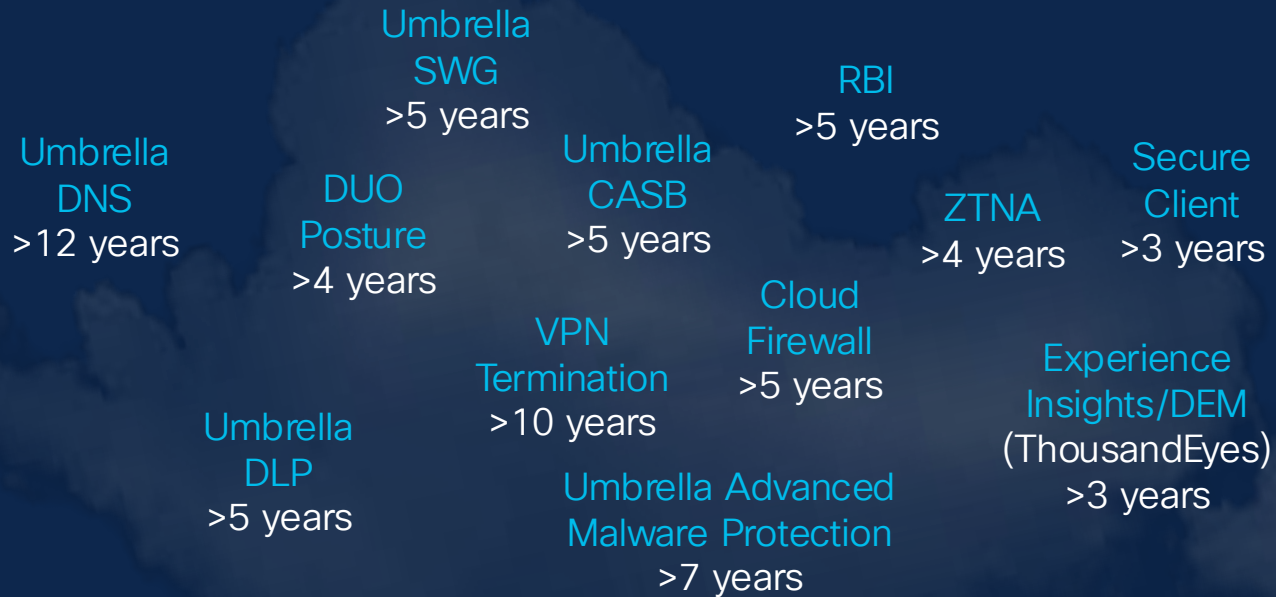
- Introduction
- Secure Access Packaging
- Secure Access Architecture
- Secure Access Use-cases ( SIA & SPA)
- Support
- 6 Demo and Q&A

# Cisco Secure Access Packaging

Category	Features	Essentials	Advantage
Secure Access	Secure Internet Access (SIA) <ul style="list-style-type: none"> <li>Roaming module (DNS/Web)</li> <li>SD-WAN DIA</li> <li>Roaming firewall</li> <li>IPSEC tunnels, PAC, Proxy Chain</li> </ul>	✓	✓
	Secure Private Access (SPA) <ul style="list-style-type: none"> <li>Client-based ZTNA</li> <li>Clientless ZTNA</li> <li>VPN access (private app)</li> </ul>	✓	✓
Foundational Security	DNS protection	✓	✓
	Cloud Delivered Firewall for layer 3 & layer 4 controls of web and private apps	✓	✓
	Secure web gateway (proxy web traffic, URL filtering, content filtering, advanced app controls)	✓	✓
	CASB - Cloud app discovery, risk scoring, blocking, cloud malware detection; tenant controls	✓	✓
	Remote Browser Isolation (License type - Risky traffic only)	✓+	✓+
	Secure Malware Analytics (sandbox)	Limited	Unlimited
Advanced Security	Layer 7 Cloud Delivered Firewall		✓
	IPS protection		✓
	Data Loss Prevention (DLP) for web applications		✓
	Remote Browser Isolation (License type - Any traffic)		✓+
Support	Cisco 24x7 enhanced support access via email and phone (required Enhanced attach, optional Premium upgrade)	+	+

# Introducing Cisco Secure Access

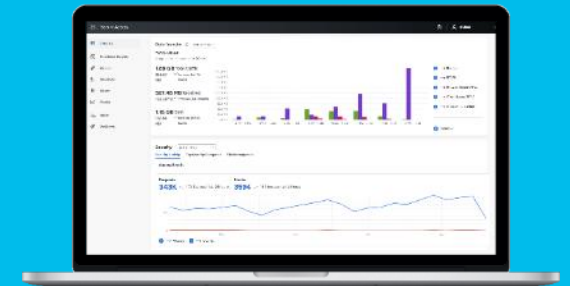
Proven Network and Cloud security converged into one service



Protecting 70,000+ customers

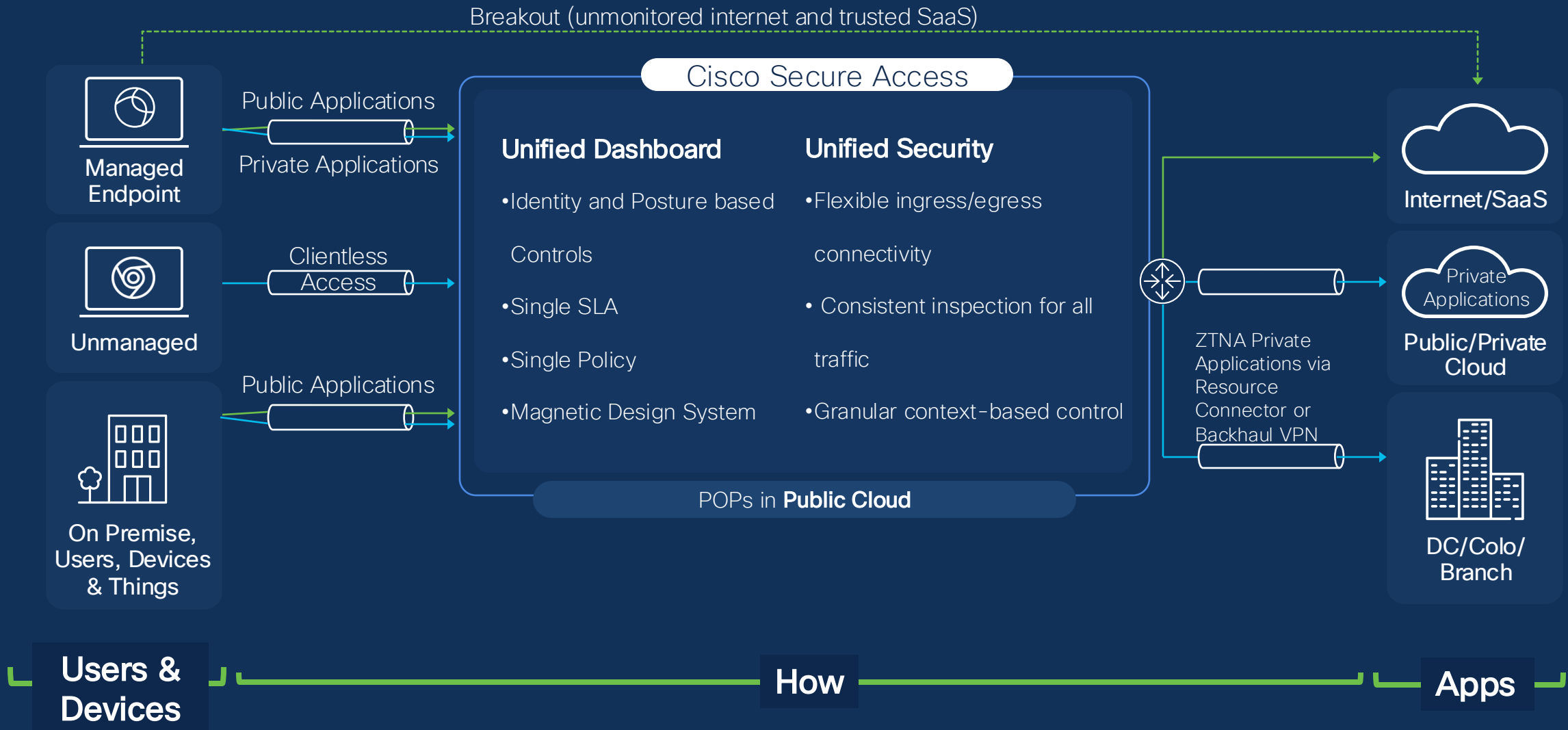
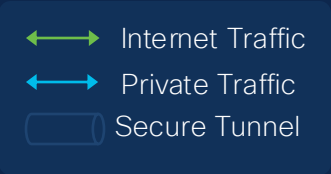
More than 220M endpoints

## Cisco Secure Access

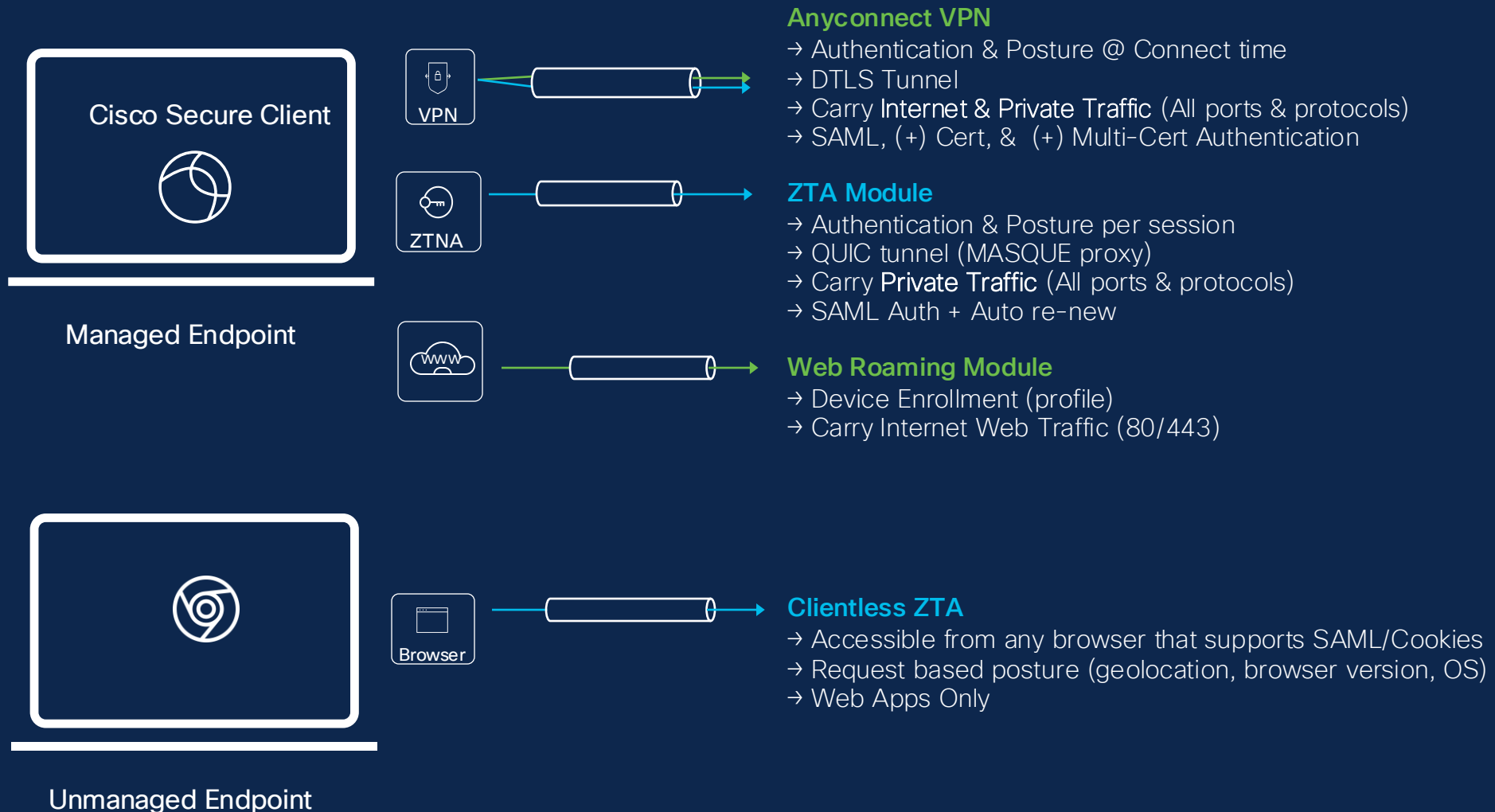
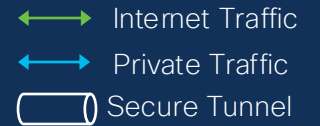


- Single Console
- Single Client
- Unified Policies

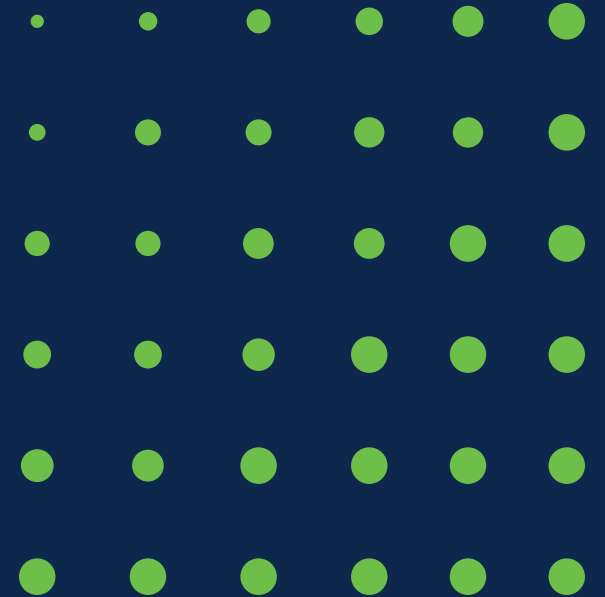
# Architecture Overview



# Who: Remote User Connectivity



# Use Cases



# Cisco Secure Access

## Secure Internet Access



Secure Web Gateway (SWG)



Cloud Access Security Broker (CASB) and DLP



Firewall as a Service (FWaaS) IPS



DNS Security



Sandbox



Multimode DLP



Advanced Malware protection



Digital Experience Monitoring\*



Remote Browser Isolation\*

## Secure Private Access



Client-based Zero Trust Network Access (ZTNA)



Clientless Zero Trust Network Access (ZTNA)



VPN as a Service



Firewall as a Service (FWaaS) IPS

## Both use cases



Talos Threat Intelligence

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



# Use Cases Connectivity Options

- Secure Internet Access

- Network Protection
- Branch (IPsec Tunnel)
- Roaming Module
- Pac File
- RA VPN (Secure Client – VPN Module)

- Secure Private Access

- RA VPN (Secure Client – VPN Module)
- Client-Based ZTNA (Secure Client – ZTNA Module)
- ZTNA Clientless (Browser-Based)
- Branch (IPsec Tunnel)

# SIA Connection options/Deployment Methods

## Types of Deployments

## Capabilities

### Network Protection

1. First line of defense
2. Deployed with in minutes
3. Policy enforcement (Security and Content Access controls)

### Secure Branch

1. User come online
2. Secure Client detects in office network connection, so VPN not required
3. Private application traffic is routed via optimized SDWAN, Internet bound traffic is routed through SIA tunnel

### Roaming Module (Secure Client – Roaming Module)

1. DNS/Web Traffic (80/443) Redirection
2. Policy Enforcement
3. Trusted Network Detection
4. Domain/IP proxy bypass and User Identity visibility

# SIA Connection options/Deployment Methods

## Types of Deployments

## Capabilities

### PAC File

1. Browser Web Traffic (80/443) Redirection
2. Policy Enforcement
3. Domain/IP proxy bypass
4. User Identity visibility( If SAML is configured)

### Secure Internet Access (typically coupled with Secure Private Access via VPN)

1. User authenticates, MFA & posture optional, identity determined
2. Authorization based traffic match
3. Traffic determined as Internet vs Private traffic and forwarded to firewall
4. Firewall applies identity-based access control
5. Firewall applies TLS decryption and IPS on the traffic (if enabled)
6. Web traffic sent to SWG; non-web traffic sent to SSE egress
7. SWG applies security policy and advanced scanning (DLP, CASB..) as controlled by the policy.
8. Egress traffic NAT prior to egress

# Use Cases Connectivity Options

- Secure Internet Access

- Network Protection
- Branch (IPsec Tunnel)
- Roaming Module
- Pac File
- RA VPN (Secure Client – VPN Module)

- Secure Private Access

- RA VPN (Secure Client – VPN Module)
- Client-Based ZTNA (Secure Client – ZTNA Module)
- ZTNA Clientless (Browser-Based)
- Branch (IPsec Tunnel)

# SPA Connection options/Deployment Methods

## Types of Deployments

## Capabilities

RA VPN ( Secure Client – VPN Module)

1. SAML 2.0 + cert-based authentication
2. Posture verification (optional)
3. Trusted Network Detection
4. Start before logon
5. IPS
6. Granular context-based control

ZTNA Client-Based (Secure Client – ZTNA Module)

1. SAML 2.0 authentication
2. Posture verification (optional)
3. Supports most TCP/UDP protocols
4. Masque over QUIC or TLS
5. IPS
6. Granular context-based control

# SPA Connection options/Deployment Methods

## Types of Deployments

## Capabilities

ZTNA  
(Browser-Based)

Clientless

1. Clientless
2. App specific access
3. Undiscoverable IP address
4. Least privileged user access
5. Reduced threat surface

Branch (IPsec Tunnel)

1. Branch connectivity through tunnel
2. Traffic flows through cloud firewall
3. Traffic gets routed to private apps

# ZTA Clientless, ZTA Client-Based and RAVPN comparison

	Cisco Secure Access		
Hosting	SaaS		
Type	Clientless	Client-Based	
Client	Web Browser	ZTA Module OS Native Clients	VPN Module
Supported Traffic	Client-to-server	Client-to-server	Client-to-server, Client-to-client, Server-to-client
Supported Apps	HTTP, HTTPS	TCP & UDP	All TCP, UDP & ICMP
Client Protocol(s)	TLS	MASQUE over QUIC or TLS	TLS, DTLS, IPsec
Device Posture	Per-Rule	Per-Rule	On Connect
Per-App Controls	User/Group-Based Access Control, TLS Decrypt, IPS		

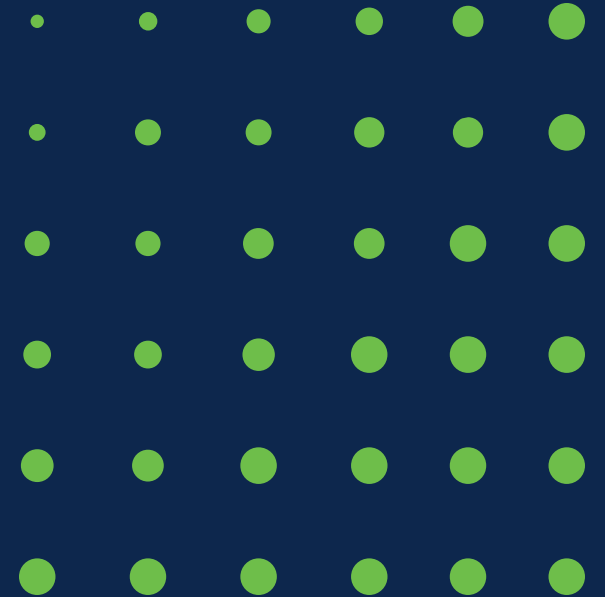
# Migration tool Update

Cisco is working on Migration tool ( for DNS ONLY) from umbrella to secure access which will be available soon.

More details to come!!



# Support & Documentation



# Support Services for Cisco Secure Access

Deliverables	Software Support Enhanced (Required for all packages)	Software Support Premium (Optional Upgrade)
Technical support (24x7 access to Cisco Cloud Security Support – phone/online)	✓	✓
Initial response target (Severity 1 and 2 cases)	30 minutes for phone	15 minutes for phone
Software updates	✓	✓
Prioritized case handling		Prioritized over Enhanced Support
Primary point of contact with software expertise	✓	✓
Technical onboarding including configuration guidance	✓	✓
Technical adoption including periodic system risk evaluations and guidance for software usage	✓	✓
Support case analytics		✓
Designated service management: assigned expert who provides incident, case, and change management plus consultation and recommendations		✓

To learn more about Cisco Support Services for Security Software, click [here](#).

# Support

- Technical Support (24x7 access to Cisco Cloud Security Support - phone/online).

Contact TAC by  
Phone US/Canada  
1 800 553 2447  
1 408 526 7209

Email Support  
[tac@cisco.com](mailto:tac@cisco.com)

[Open a TAC Case](#)  
[Online](#)

Cisco Worldwide Support Contacts:

<https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>

Additional Resources

[Manage Support Cases](#)

[Cisco Community](#)

[Cisco Support Assistant](#)

[Cisco - Secure Access Service Status](#)

# Documentation

Cisco Secure Access Help Center: <https://docs.sse.cisco.com/>

The screenshot shows the Cisco Secure Access Help Center interface. At the top left is the Cisco logo. At the top right, it says "Secure Access Help Center" with a settings icon. Below the header is a search bar with a magnifying glass icon, the text "Search", and a keyboard icon. On the left side, there is a navigation menu under the heading "Cisco Secure Access Help". The menu items are: "Welcome to Cisco Secure Access" (highlighted in blue), "Sign into Secure Access with Security Cloud Sign On", "Find Your Organization ID", "Determine Your Current Package", "View Cloud Security Service Status", "Contact Cisco Secure Access Support", "Secure Access Single Sign-On Authentication", "Get Started", "Quickstarts", "Limitations and Range Limits", "Manage Network Connections", "Manage Network Tunnel Groups", "Network Tunnel Configuration", "Secure Access Regions", "Manage Users and Groups", "Provision Users and Groups from Active Directory", "Configure Integrations with SAML Identity Providers", "Manage End User Connectivity", "Manage DNS Servers", "Traffic Steering for Zero Trust Client-Based Connections", and "Manage Virtual Private Networks". The main content area on the right is titled "Welcome to Cisco Secure Access". It contains three sections: "Secure Access is Cisco's cloud-based platform that provides you with multiple levels of defense against internet-based threats. Cisco Secure Access enables you to connect securely to the internet, Software-as-a-Service (SaaS) apps, and your private digital resources, whether you connect from your organization's network or roaming off a network."; "In Secure Access, you can apply and enforce comprehensive security controls on collections of resources, users, and devices. The Secure Access policy is a container for your security configuration rules. Organize your policy rules to protect your users and permit access to resources. The Secure Access policy manages the connections and resources for users and devices in your organization, and the network components that forward traffic to resources."; and "Secure Access collates various reports and logs. The Secure Access Overview dashboard and Security Activity report show snapshots of user and device traffic and connection events over distinct time periods. You can audit digital behaviors and observe top network and security activities in your organization." Below these sections are three more sections: "Sign in to Secure Access" (with a link to "Sign into Secure Access"), "Find Your Organization" (with a link to "Find Your Organization ID"), and "Determine Your Current Package" (with a link to "Determine Your Current Package"). At the bottom, there is a "Contact Support" section with a link to "Contact Cisco Secure Access Support".

# Demo and Q&A.



SECURE