



The bridge to possible

Merre tovább “Security”?

Csordás Szilárd
IT biztonsági szakértő

scsordas [at] cisco.com



Adversaries are “creative”



Malicious code embedded in UEFI firmware [Link](#)



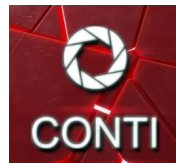
Hackers breached Microsoft to find out **what**
Microsoft knows about them January 20, 2024



Blue Team

Lapsus\$

Nvidia, Samsung, MS, EA Games, Ubisoft's services,
Okta. [src:zdnet.com](https://www.zdnet.com)

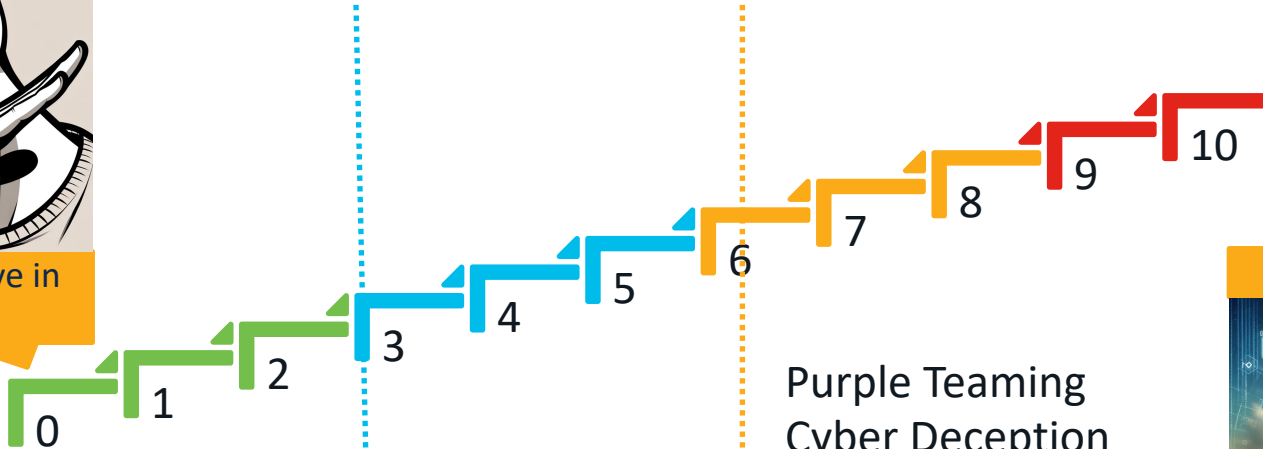


An ‘employee’ of the month’ +50% salary
pen-tester were not aware that they are hacking for real
Negotiators – 0.5%-1.00% commission
Employee referral program, with bonuses

Teljeskörű Biztonsági Állapot. Hol Állsz Most?



I do not believe in security



Purple Teaming
Cyber Deception
Threat Hunter
Detection Engineer

Security nirvana



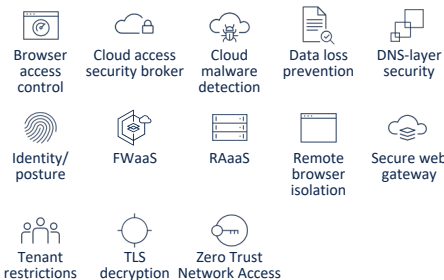
Referencia Architektúra – Zero Trust

ZERO TRUST

Client/Device Security + =Threat Intel

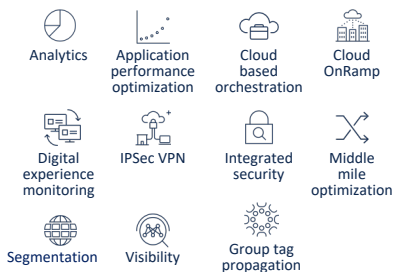


SASE / Secure Service Edge



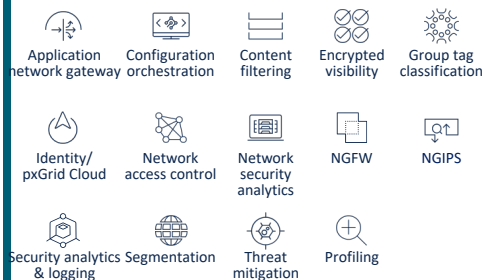
SASE/SDWAN

Meraki | Secure Firewall
ThousandEyes | Viptela



In the Office/Managed Location

Catalyst | DNAC | ISE | Meraki | Secure Firewall
Secure Network Analytics | Web Appliance



Industrial Threat Defense

DNAC | CyberVision | Industrial Networking
ISE | Secure Firewall | Secure Network Analytics

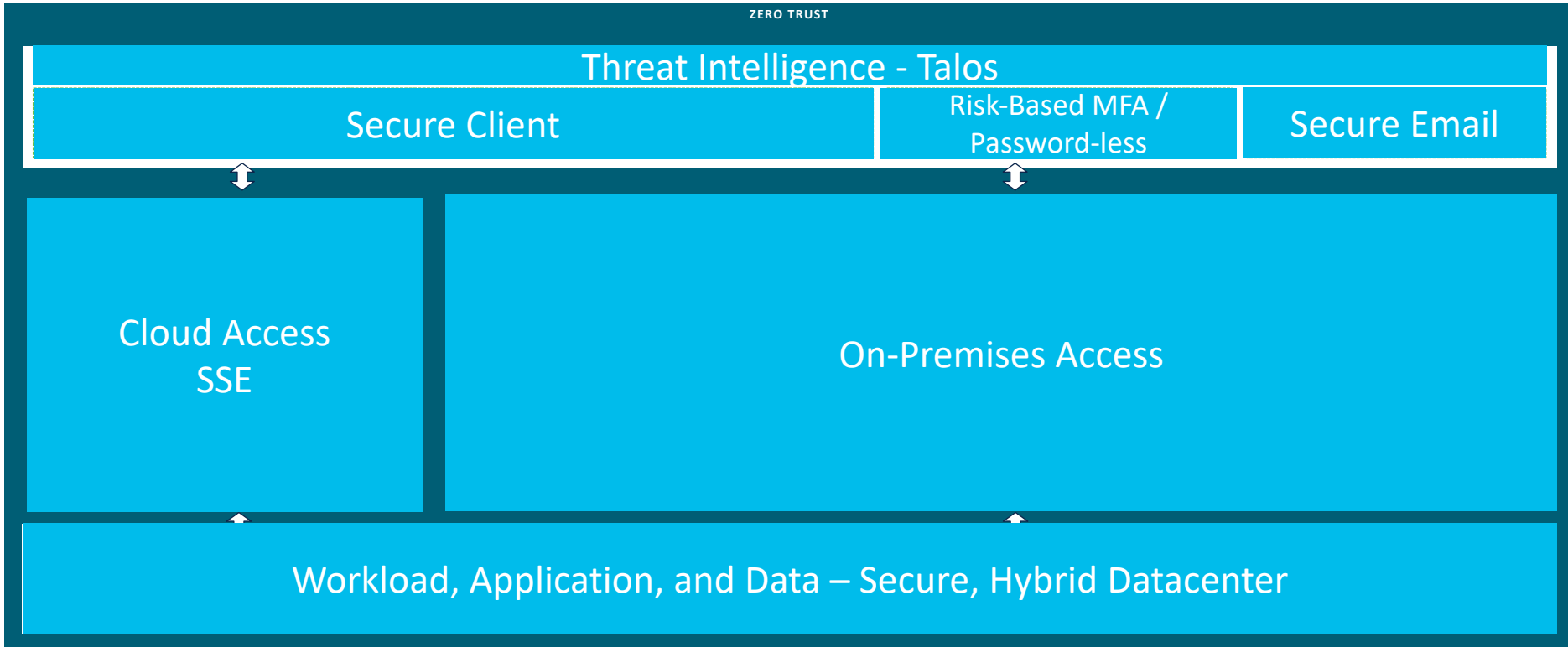


Workload, Application, and Data Security

HYBRID MULTI-CLOUD: ACI | Cloud Insights | Panoptica | Radware | Secure Application | Secure Endpoint | Secure Firewall | Secure Cloud Analytics | Secure Workload



Referencia Architektúra – Zero Trust



Az XDR megoldás előnyei

How good are we at detecting attacks **early**?

1 Detect Sooner

Where are we **most exposed** to risk? Are we **prioritizing the attacks** that represent the largest **material impacts** to our business?

3 Prioritize by Impact

How fast can we **confidently respond**? How much can SecOps **automate**? Are we **improving** our time to respond?

5 Accelerate Response

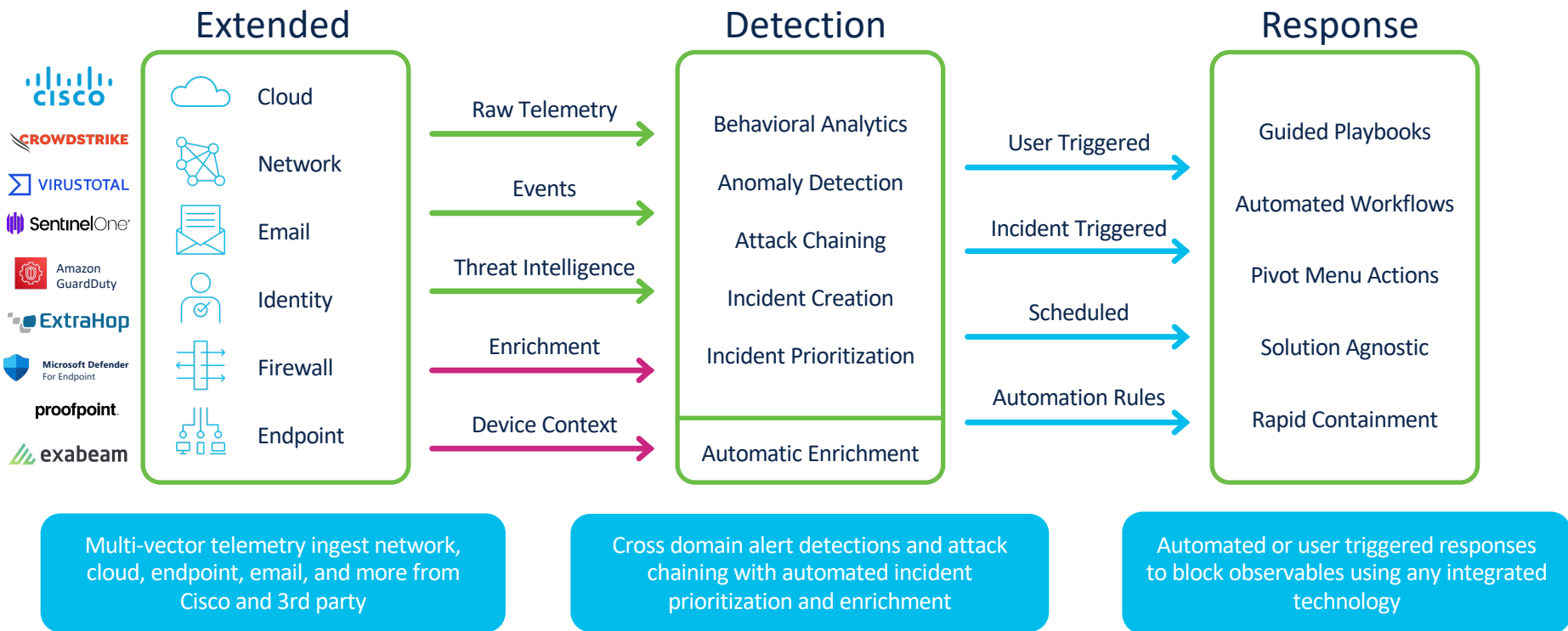
Extend Asset Context 2

How quickly are we able to understand the **entry vectors and full scope** of attacks?

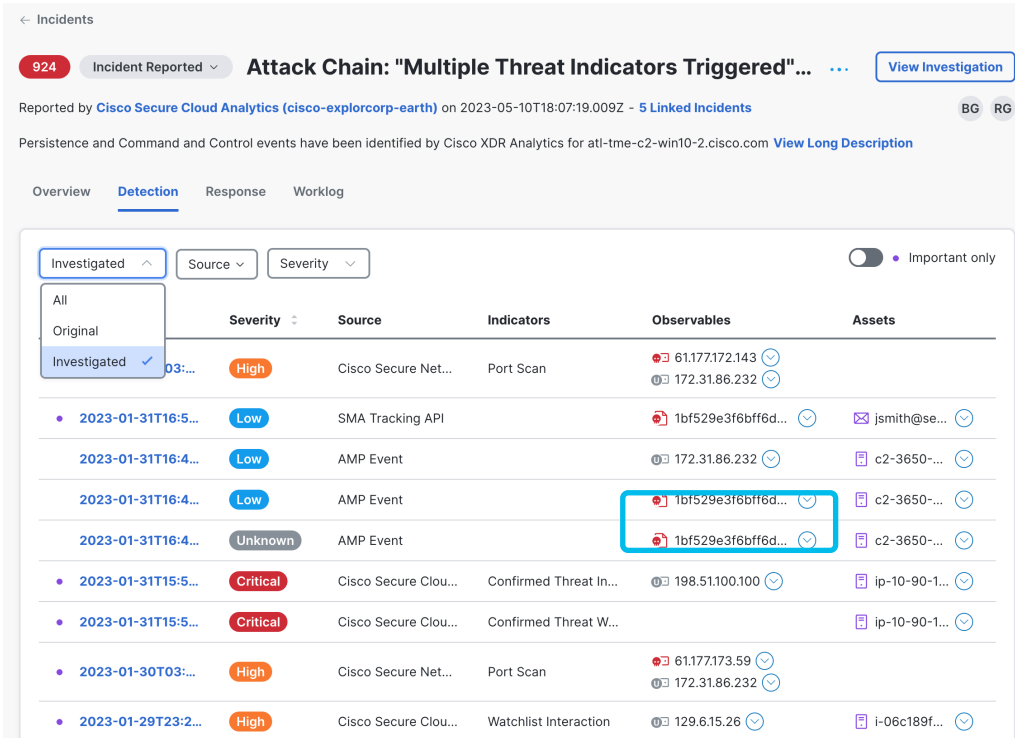
Reduce Investigation Time 4

Do we have **full visibility** into all our assets?
Can we **reliably identify** a device and who uses it?

A “motorháztető” alatt



Incidensek kontextusba helyezése



The screenshot displays a security incident management dashboard. At the top, it shows the incident count (924) and the incident title: "Attack Chain: 'Multiple Threat Indicators Triggered'...". Below this, it indicates the incident was reported by Cisco Secure Cloud Analytics on 2023-05-10T18:07:19.009Z. The interface includes tabs for Overview, Detection, Response, and Worklog. A filter menu is open, showing options for "Investigated", "Original", and "Investigated" (checked). The main table lists incidents with columns for Severity, Source, Indicators, Observables, and Assets. One incident is highlighted with a red box around its ID and indicators.

Severity	Source	Indicators	Observables	Assets
High	Cisco Secure Net...	Port Scan	61.177.172.143 172.31.86.232	
Low	SMA Tracking API		1bf529e3f6bff6d...	jsmith@se...
Low	AMP Event		172.31.86.232	c2-3650-...
Low	AMP Event		1bf529e3f6bff6d... 1bf529e3f6bff6d...	c2-3650-...
Unknown	AMP Event			c2-3650-...
Critical	Cisco Secure Clou...	Confirmed Threat In...	198.51.100.100	ip-10-90-1...
Critical	Cisco Secure Clou...	Confirmed Threat W...		ip-10-90-1...
High	Cisco Secure Net...	Port Scan	61.177.173.59 172.31.86.232	
High	Cisco Secure Clou...	Watchlist Interaction	129.6.15.26	i-06c189f...

- XDR incidents are automatically enriched when they are created.
- Enrichment uses Cisco integrations, third-party integrations, public intelligence, private intelligence, and endpoint data to add context to incidents.
- Judgments are automatically provided to analysts to help them make more informed incident response decisions with fewer steps.

Incidents nyomozásának részlete, folyamata

Progressive reveal of details

Looking into an incident is a progressive experience where the relevant data is revealed as needed without overwhelming the SOC analyst.

Priority	Name
1000	Malicious Process and Suspicious SMB/RDP Activity Detect
1000	Unusual External Server for This is localhost

Rich incident details

Incidents are enriched with data, such as assets, indicators, and observables, from multiple sources. Associated MITRE ATT&CK tactics and techniques are displayed and factored into the incident priority score.

Priority **1000** Status **New**

Malicious Process and Suspicious SMB/RDP...

Reported by **Cisco Secure Cloud Analytics (rsa)**
15 hours ago

Assigned **BM** **JF**

MITRE *********

Priority score breakdown

1000 **100** **10**
Detection Risk Asset Value at Risk

Short description

This feature is currently under active development

Long description

Alert Chain
fb56eea65af173cd7286d510722e4f8f7e5c8613

Description

[View Incident Detail](#)

MITRE | ATT&CK

View all Tactics

Tactics

TA0002: Execution **100**

The adversary is trying to run malicious code. Execution consists of techniques that result in adversary-controlled code running on a local or remote system. Techniques that run malicious code are often paired with techniques from all other tactics to achieve broader goals, like exploring a network or stealing data. For example, an adversary might use a remote access tool to run a PowerShell script that does Remote System Discovery.

TA0008: Lateral Movement **66**

MITRE ATT&CK Mapping

Incidents are mapped to MITRE ATT&CK framework Tactic categories to highlight which attack stages the detections fall under, providing a quick view and link to a common language for the SOC

Orientation

4 Assets

- virtualmachines/win-vic-2 (6 events)
- virtualmachines/win-dc-0 (5 events)
- virtualmachines/win-vic-6 (4 events)
- virtualmachines/kali (1 event)

31 Observables

- NT AUTHORITY\SYSTEM (6 events)
- C:\Windows\System32\svchost.exe (6 events)
- svchost.exe (6 events)
- SYSTEM (6 events)

Cisco Secure Access

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



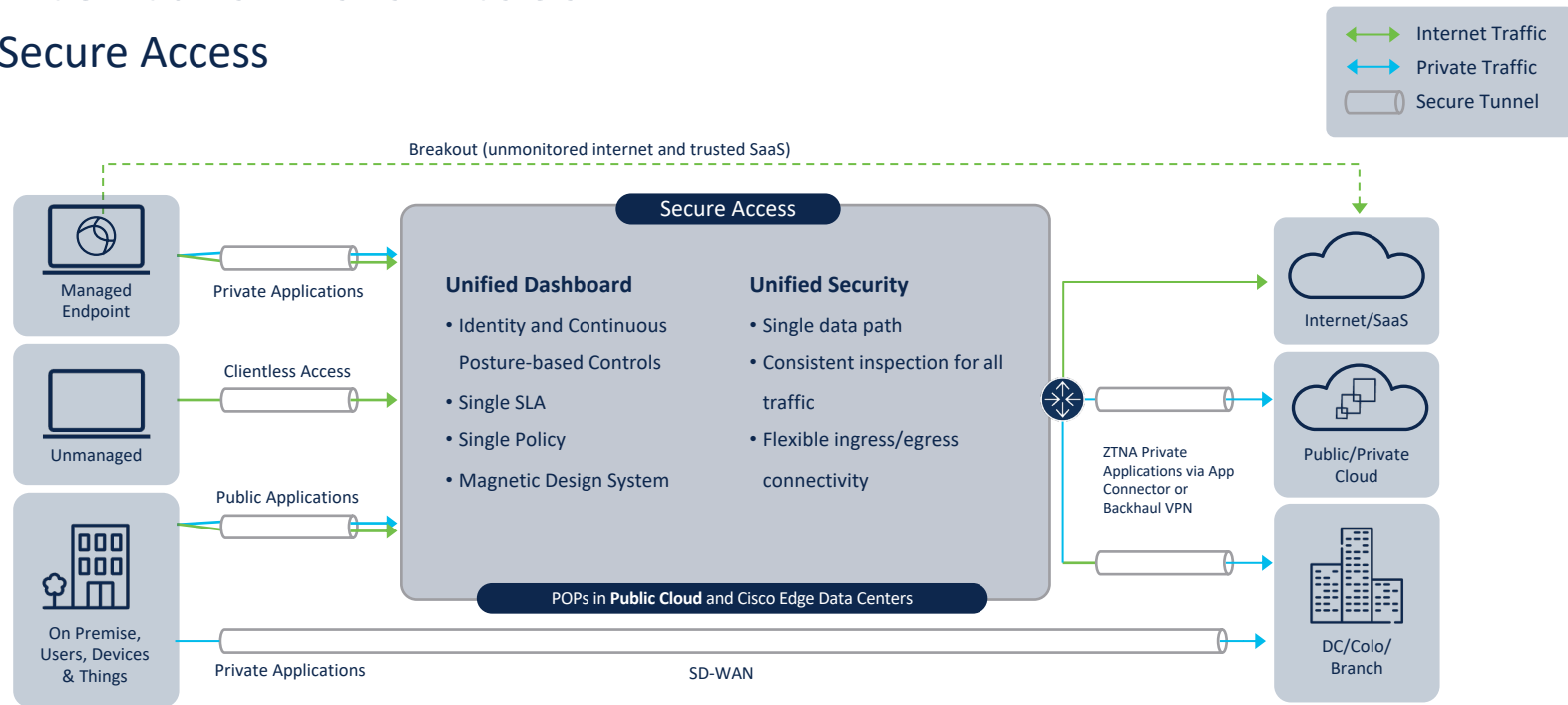
DUO MFA/SSO



CSPM

Architektúra kialakítása

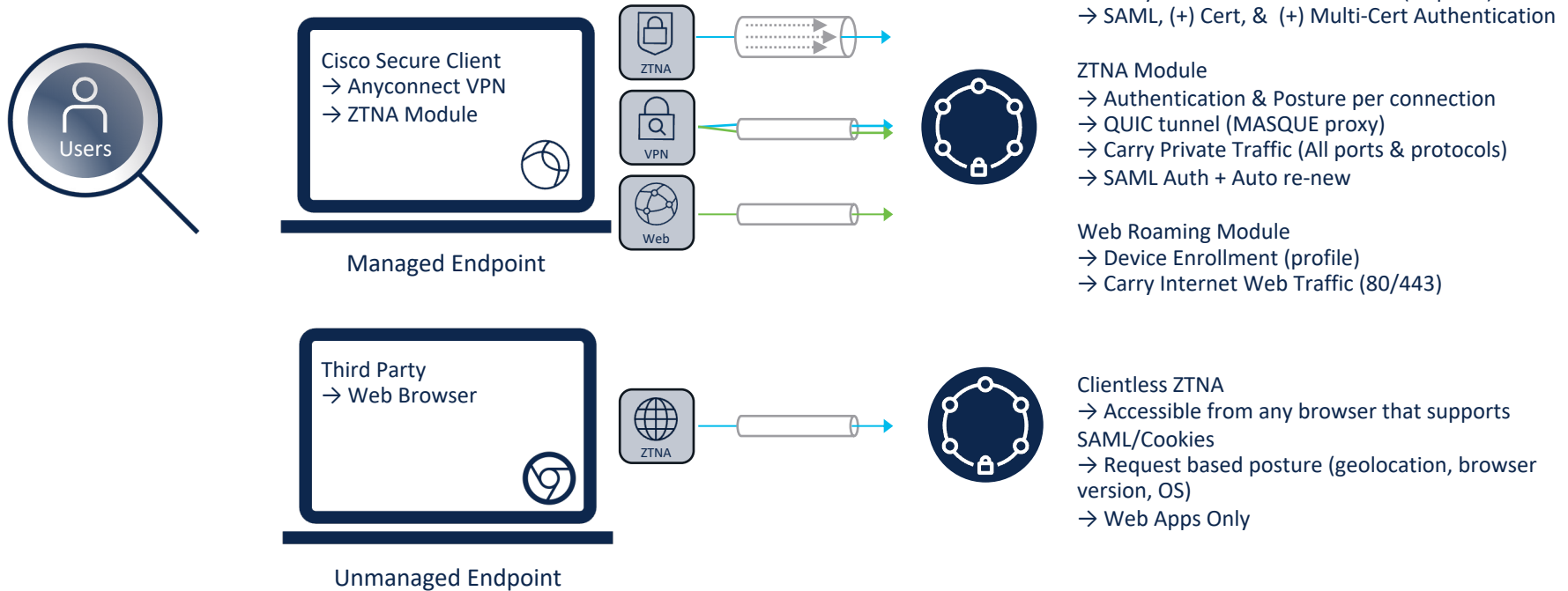
Cisco Secure Access



Who How What

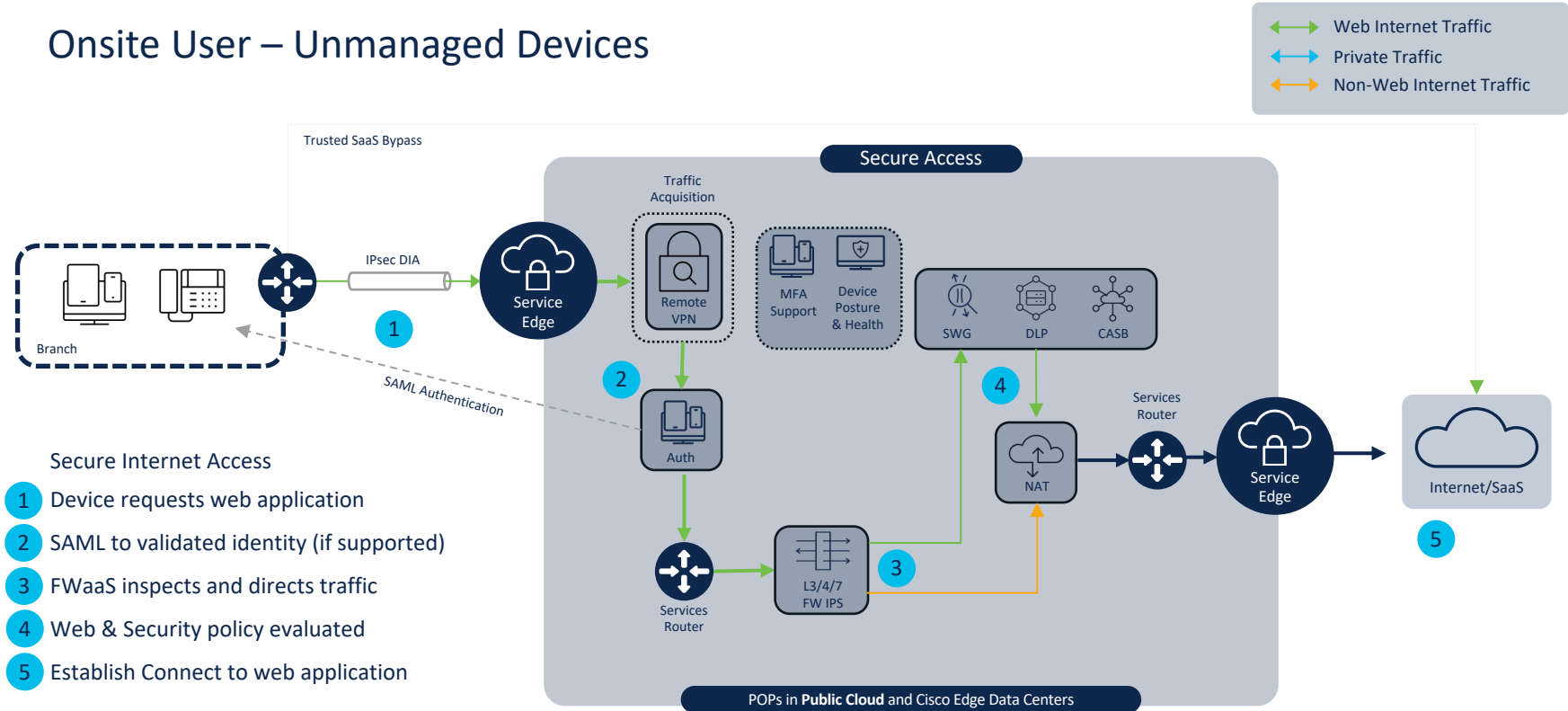
Architecture Detail

Who (is accessing)– Users & Devices



Secure Internet Access

Onsite User – Unmanaged Devices



Secure Internet Access

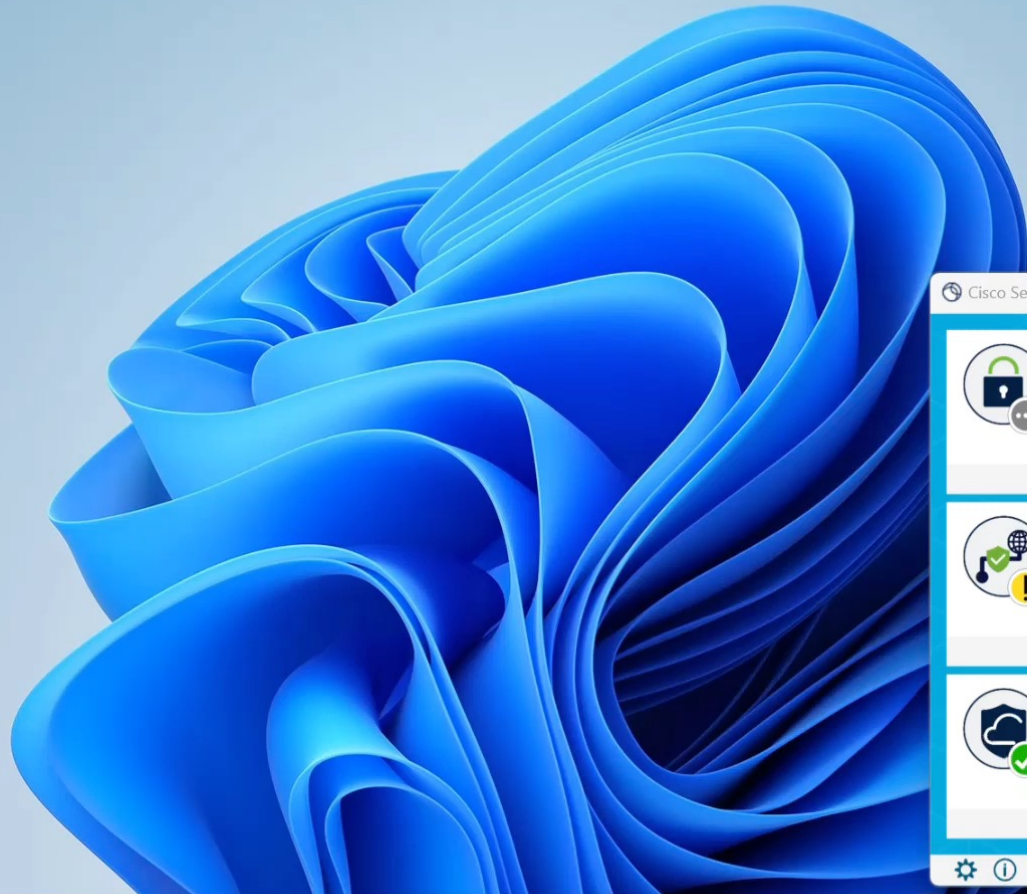
- 1 Device requests web application
- 2 SAML to validated identity (if supported)
- 3 FWaaS inspects and directs traffic
- 4 Web & Security policy evaluated
- 5 Establish Connect to web application



Recycle Bin



Google
Chrome



Cisco Secure Client

AnyConnect VPN:
Ready to connect.
346a.vpn.sse.cisco.com/PseudoC

Zero Trust Access:
Registration is required to access secure resources.

Umbrella:
Umbrella is active.



Search



Mon

Köszönöm a figyelmet!