KAJ PA UPORABNIKI?

Zaščita in vidljivost onkraj požarnih zidov

Stojan Rančić, CCIE

NIL d.o.o.

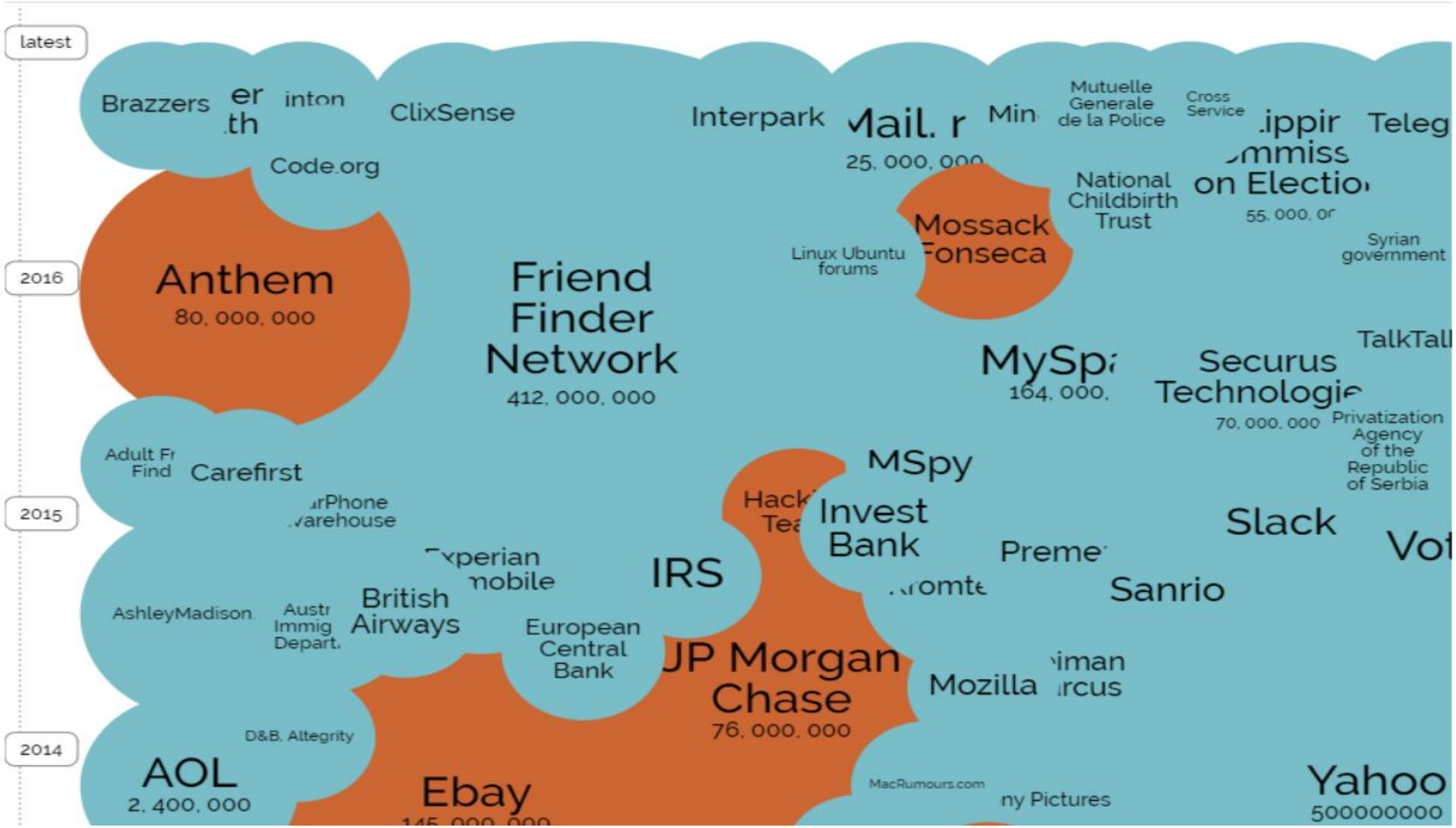
Kje je **TEŽAVA?**

NIL

Kdaj bomo NAPADENI?

Vrstijo se novice

Vrstijo se napadi



Napadi v številkah

66 % zlonamerne kode je bilo odkrite mesece ali leta po okužbi

69 % vdorov je bilo zaznanih iz zunanje strani

230k dnevno število novih vzorcev zlonamerne kode

$4M povprečna ocena stroškov zaznanega vdora

Odziv na napade je prepočasen

Napadi se zgodijo v sekundah

Do odliva podatkov pride v minutah

Napad zaznamo v mesecih

Odprava ranljivosti traja tedne

Ali je to res najbolje, česar smo zmožni?

Zaznava ranljivosti mora biti hitrejša

Odprava ranljivosti mora biti dostopnejša

Kdo je **TARČA?**

Tarča so uporabniki

“Organizations continue to spend a lot of money on network security solutions, but
it’s the endpoint that is the ultimate target of advanced threats and attacks.”

Kje so **IZZIVI?**

Pet zahtev za zaščito

1. **Slepi smo glede dogajanja pri uporabnikih in strežnikih**

2. Vnaprej **ne moremo vedeti, kaj je „slabo“**

3. **Odprava ranljivosti je prepočasna in zapletena**

4. Tradicionalna zaščita **ne zaustavi naprednih groženj**

5. **Omrežna varnost se ne integrira z varnostjo končnih točk**

Vidljivost

Imeti informacijo o tem, kaj se dogaja na končnih točkah in strežnikih, v realnem času

Zaznava

Videti in zabeležiti vse; zaznava ranljivosti v realnem času, brez podpisov

Odziv

Analiza poteka napada na podlagi zbranih podatkov; omejitev in zaustavitev napadov

Preprečevanje

Zaustavitev napadov na inovativne načine, brez podpisov

Integracija

Konsolidacija informacij o končnih točkah in omrežju, za hitrejši in natančnejši odziv

NIL

Kje je **REŠITEV?**

NIL

Poznati **DOBRO**
Zaznati **SLABO**

Cisco StealthWatch

Vaše omrežje

VSE se dotakne omrežja

Elementi

INFORMACIJA o strežnikih in uporabnikih

Revizija

SHRANITE vsako konverzacijo

Stanje

Kaj je zame **NORMALNO**

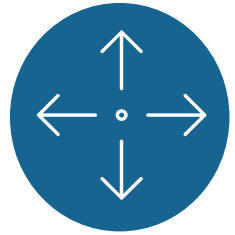
Detekcija

Opozorilo o **SPREMEMBAH**

Odziv

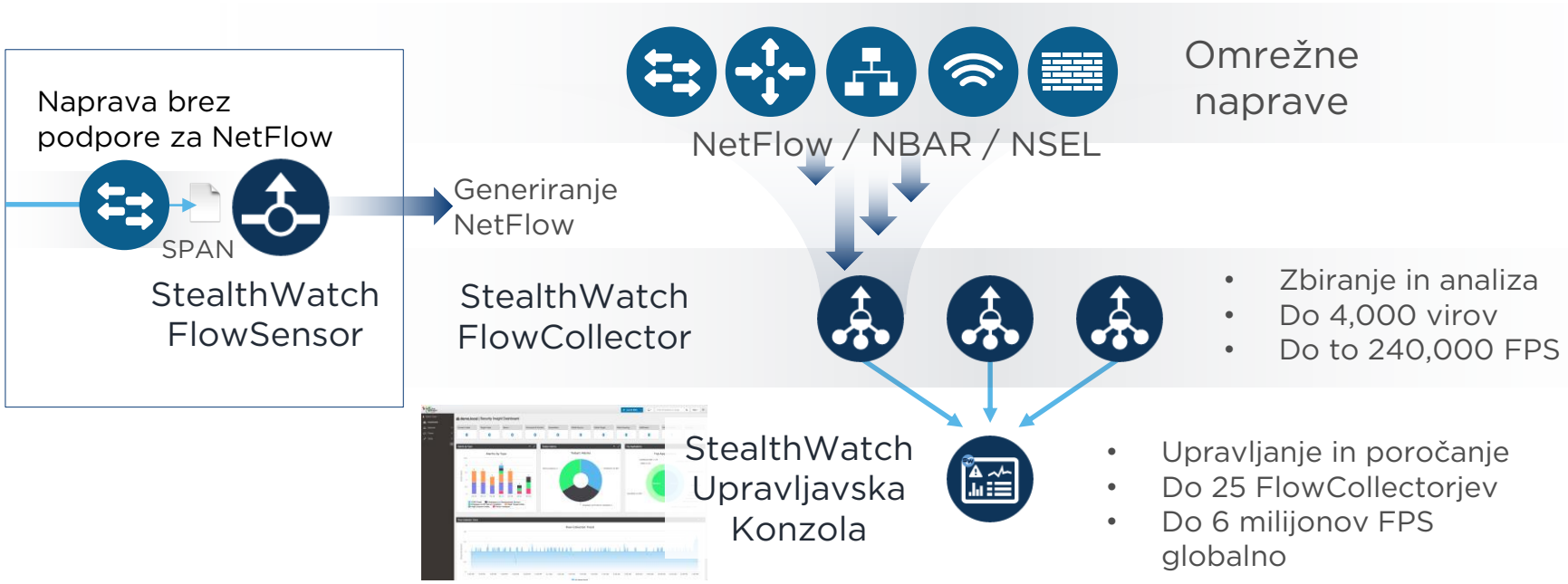
Podatke hranimo **MESECE ali LETA**

Kontekst



Kaj mi lahko omrežje še pove?

Cisco StealthWatch - Arhitektura



Kaj pa uporabniki?

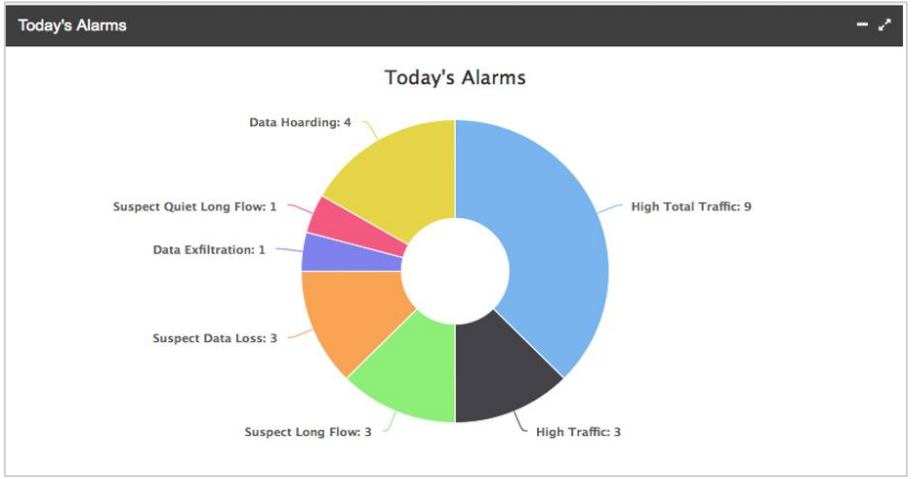
- V omrežju organizacije: zbiranje in analiza na nivoju omrežja
- Izven „domačega“ omrežja:

User Visibility | **Device Visibility**

Network Visibility

Application Visibility | **Location/Network Domain**

- Integracija v Cisco AnyConnect omogoča zbiranje podatkov:
  - Uporabnikov
  - Aplikacij
  - Naprav
  - Izvora in ponora podatkov



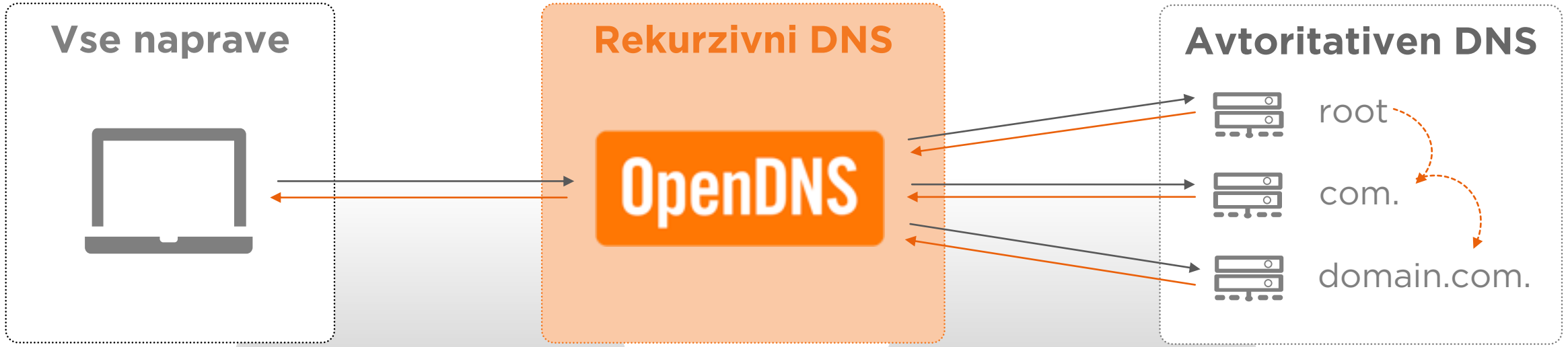
Cisco AnyConnect

V prihodu

Cisco AnyConnect

Integration with other Cisco solutions

OpenDNS



Vzorci zahtev

Za zaznavo:

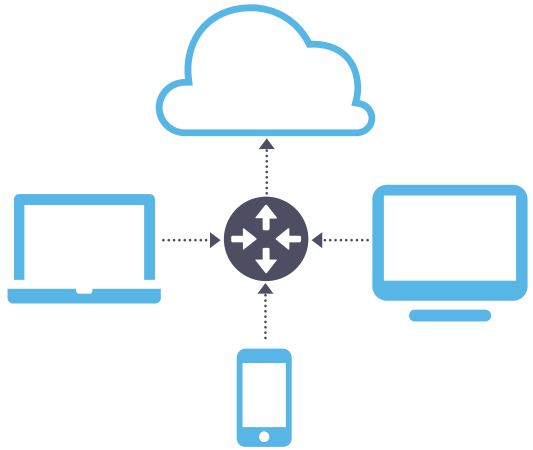
- Kompromitirani sistemi
- Povezava na C2 strežnike
- Poskusi okužbe
- Algoritemsko generirane domene
- Sorodne domene
- Novo registrirane domene

Avtoritativni logi

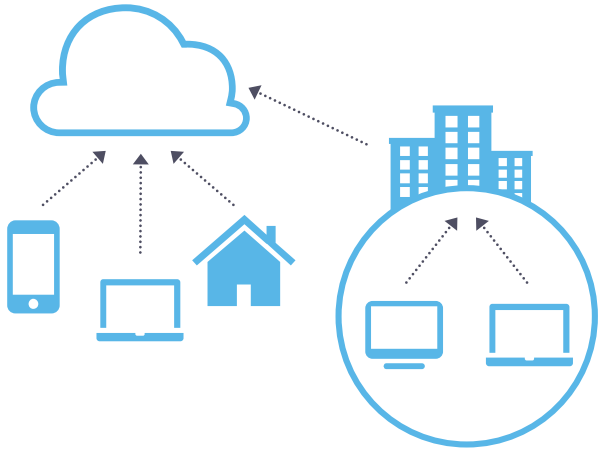
Uporabni za iskanje:

- Nova omrežja
- Zlonamerne domene, IPji, ASNs
- DNS zloraba
- Hitro bežeče domene
- Povezane domene

Zakaj DNS?



VSAKA NAPRAVA
DHCP ali DNS strežnik povesta napravi, kje je njen imenski strežnik



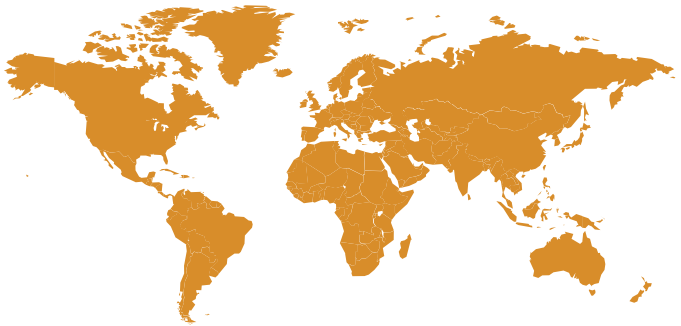
VSAKA TOPOLOGIJA
Deluje ne glede na topologijo vašega omrežja

VSI OPERACIJSKI SISTEMI
Win, Mac, iOS, Android, Linux, namenski strežniki in tudi IoT

Zakaj OpenDNS?

GLOBALNO OMREŽJE

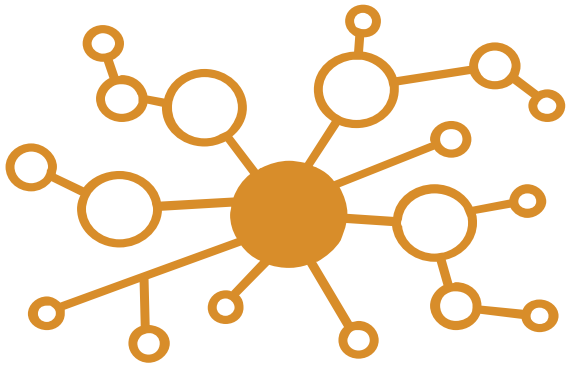
- 90B+ DNS zahtev/dan
- 25 podatkovnih centrov
- 65M+ uporabnikov
- 100% neprekinjeno delovanje
- Vsako priključno mesto in protokol



+

LASTNA ANALIZA

- raziskovalna skupina iz področja varnosti
- avtomatizirana klasifikacija
- BGP "peer relationships"
- 3D vizualizacija



=

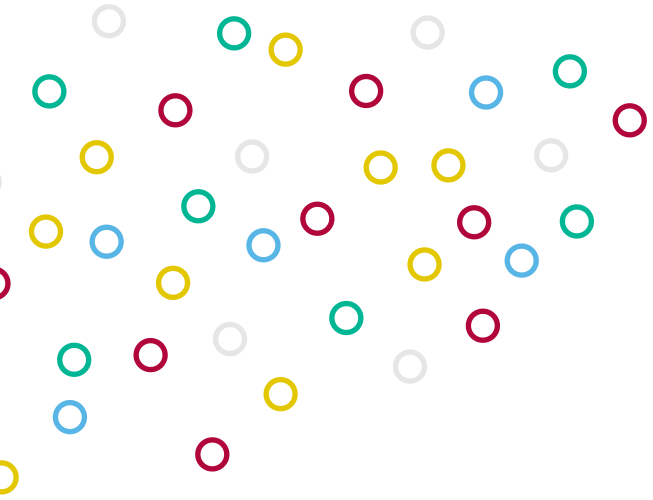
80M+

dnevno blokiranih zlonamernih zahtev

Kako pa to počne OpenDNS?

Zajem vsebin

milijoni podatkovnih točk na sekundo

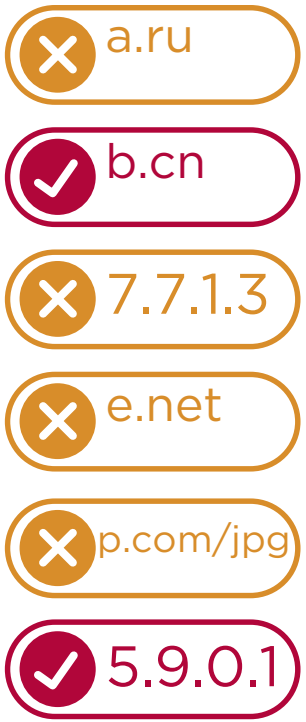


Obdelava

statistični modeli in človeška inteligenca

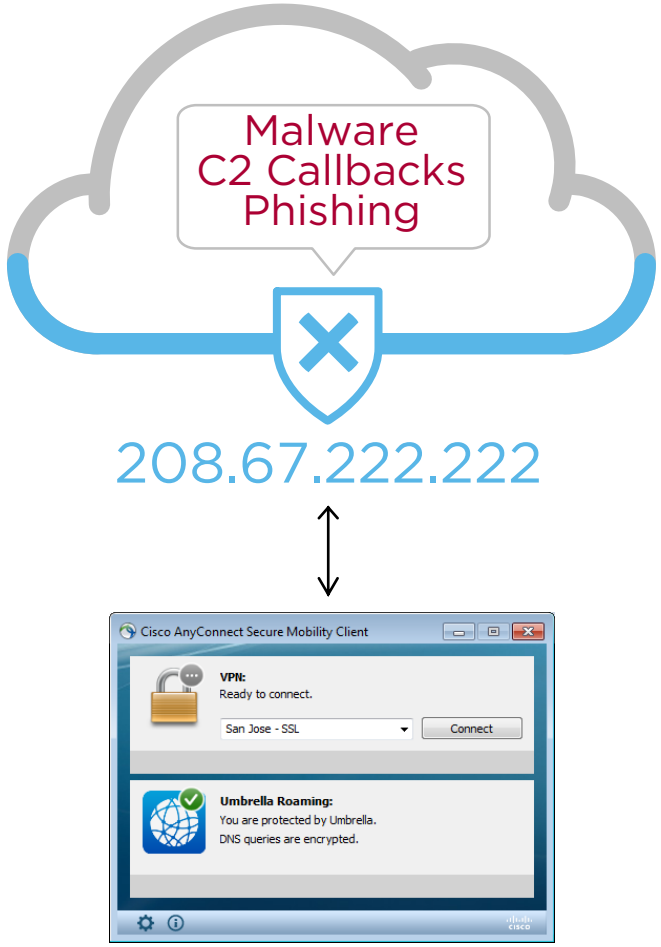
Prepoznava

verjetne zlonamerne strani

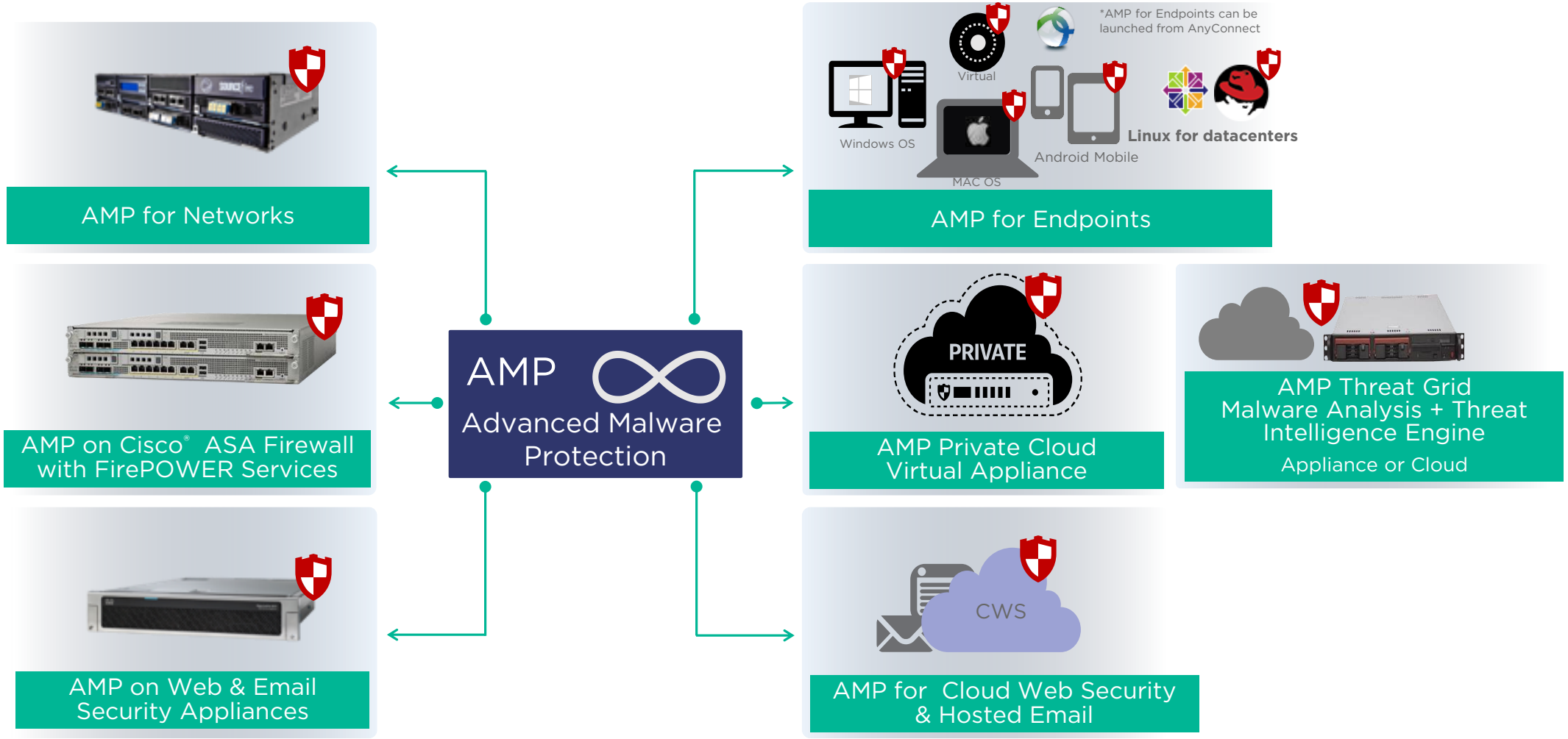


Kaj pa uporabniki?

- V omrežju organizacije: zbiranje in analiza na nivoju omrežja
- Izven „domačega“ omrežja:
  - Brez VPN povezave
  - Vidljivost in filtriranje
  - Blokiranje dostopa do škodljivih domen in IP naslovov
  - Vgrajena inteligenca z analizo aktualnih in novih groženj



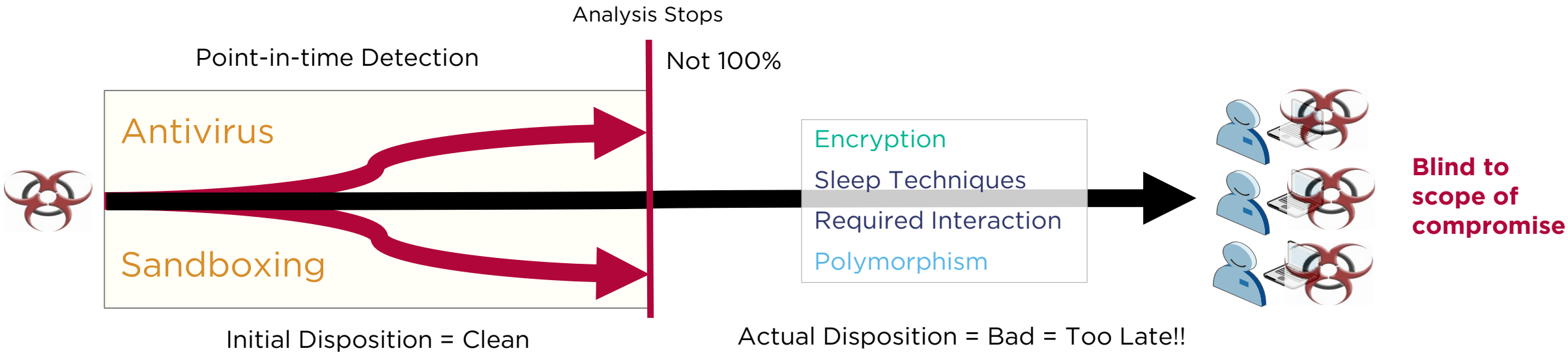
Zaščita pred zlonamerno kodo: Cisco AMP

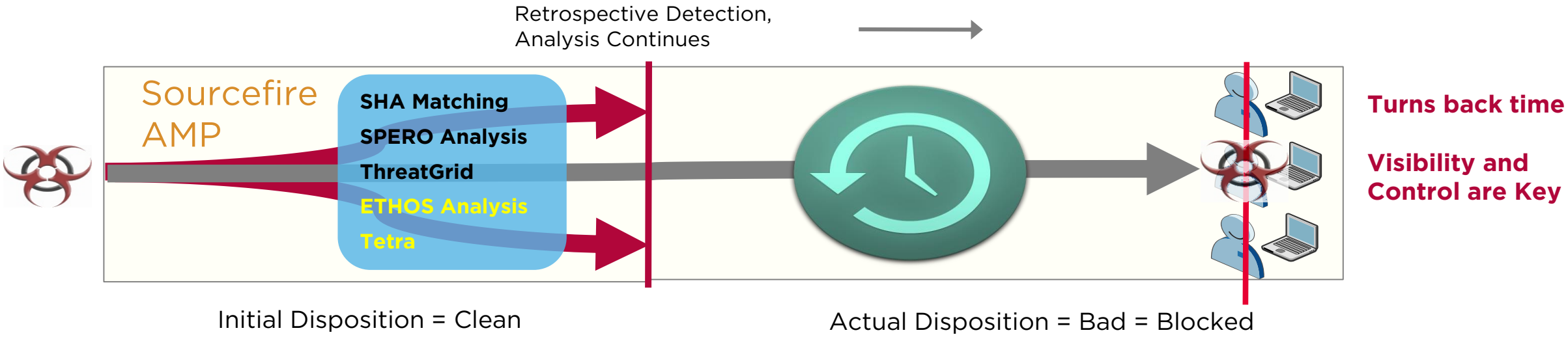


Cisco AMP - Gradniki

- **Javni oblak** – oblačna rešitev, ki ocenjuje ‘‘ugled‘‘ datotek
- **Threat Grid (TG)** – File Intelligence Gathering
- **AMP poizvedbe**:
  - 1-1 SHA: Straight SHA256 – no PII
  - ETHOS: Fuzzy SHA – no PII
  - SPERO: Machine Learning – limited PII (DLL etc)
  - PING2: Retrospective
- **The Poke** = ocena tveganja iz TG poslana v AMP Cloud

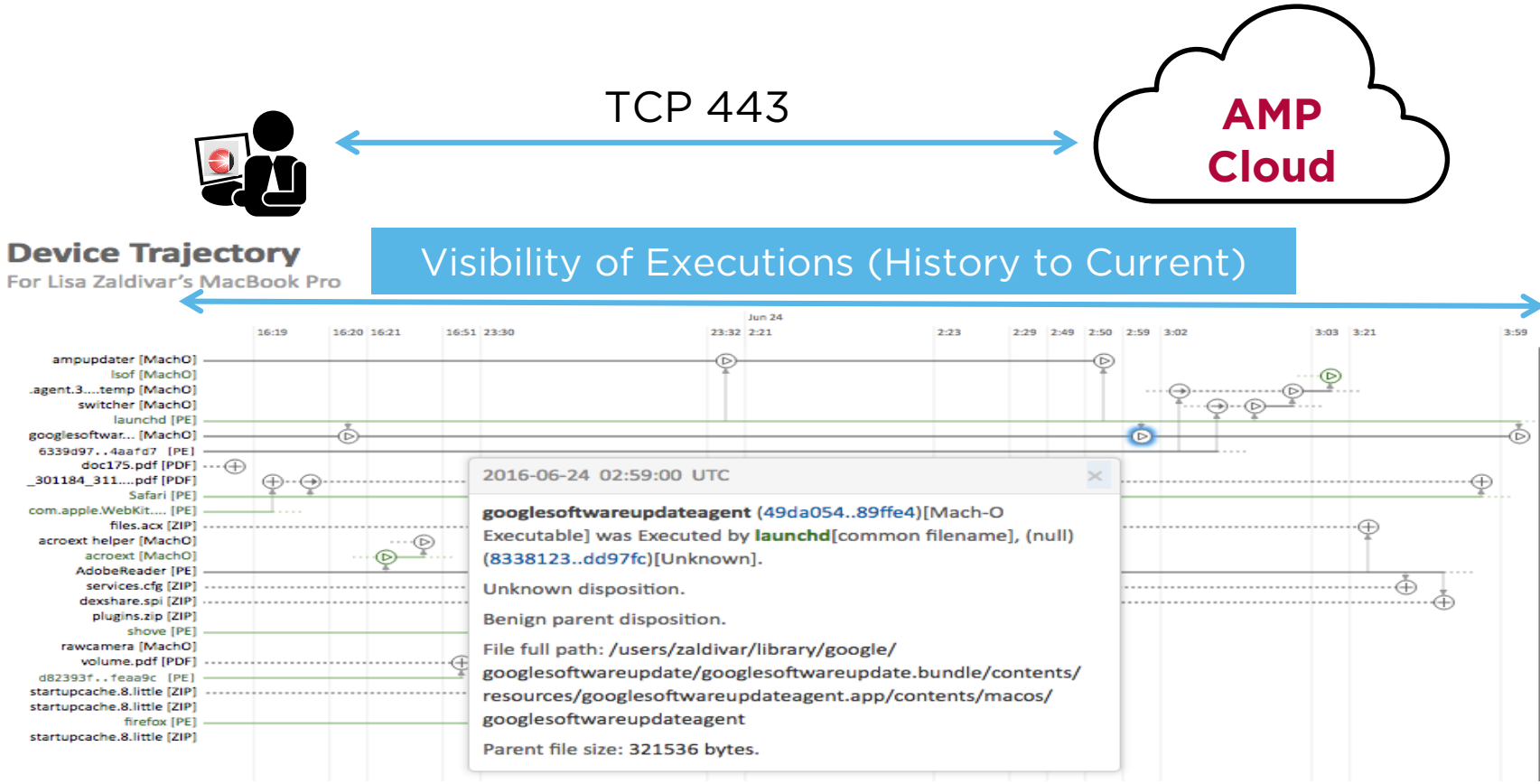
Cisco AMP omogoča polno vidljivost



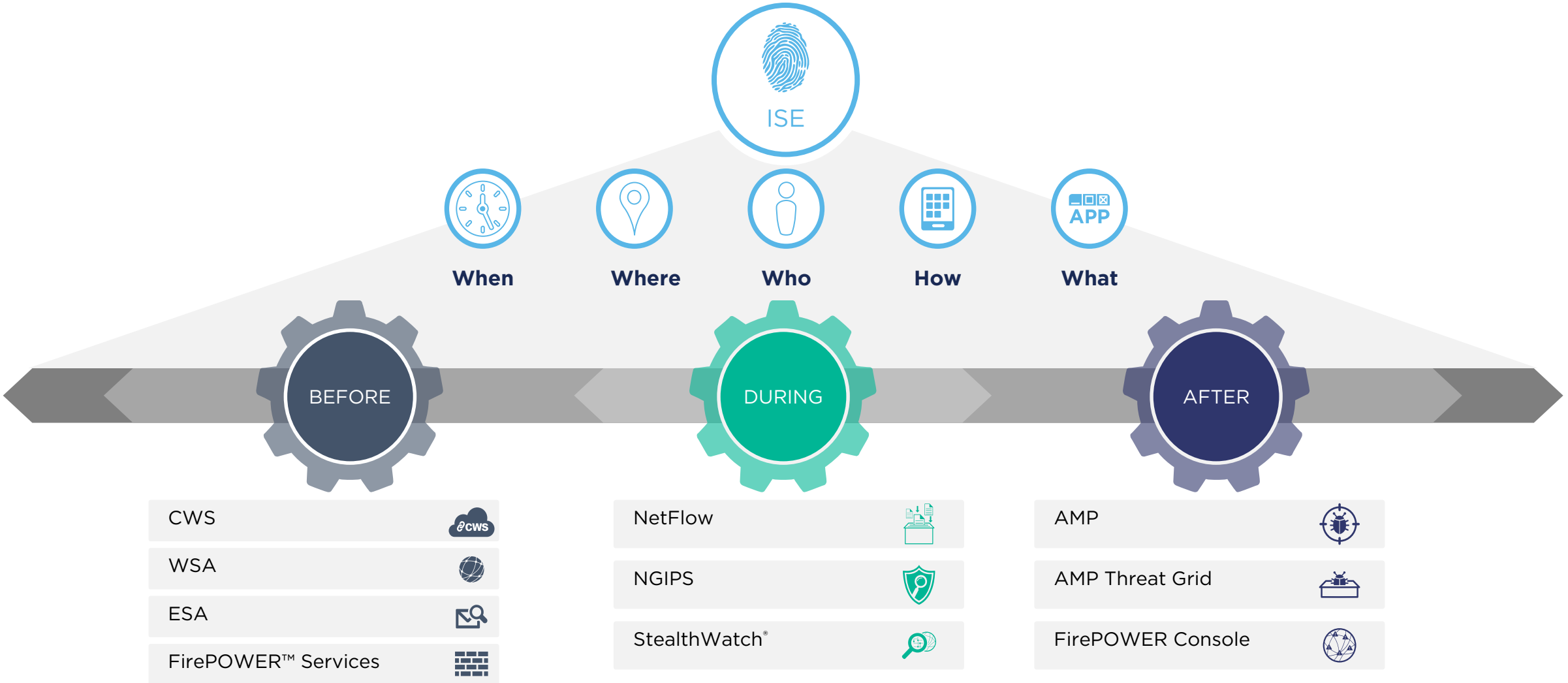


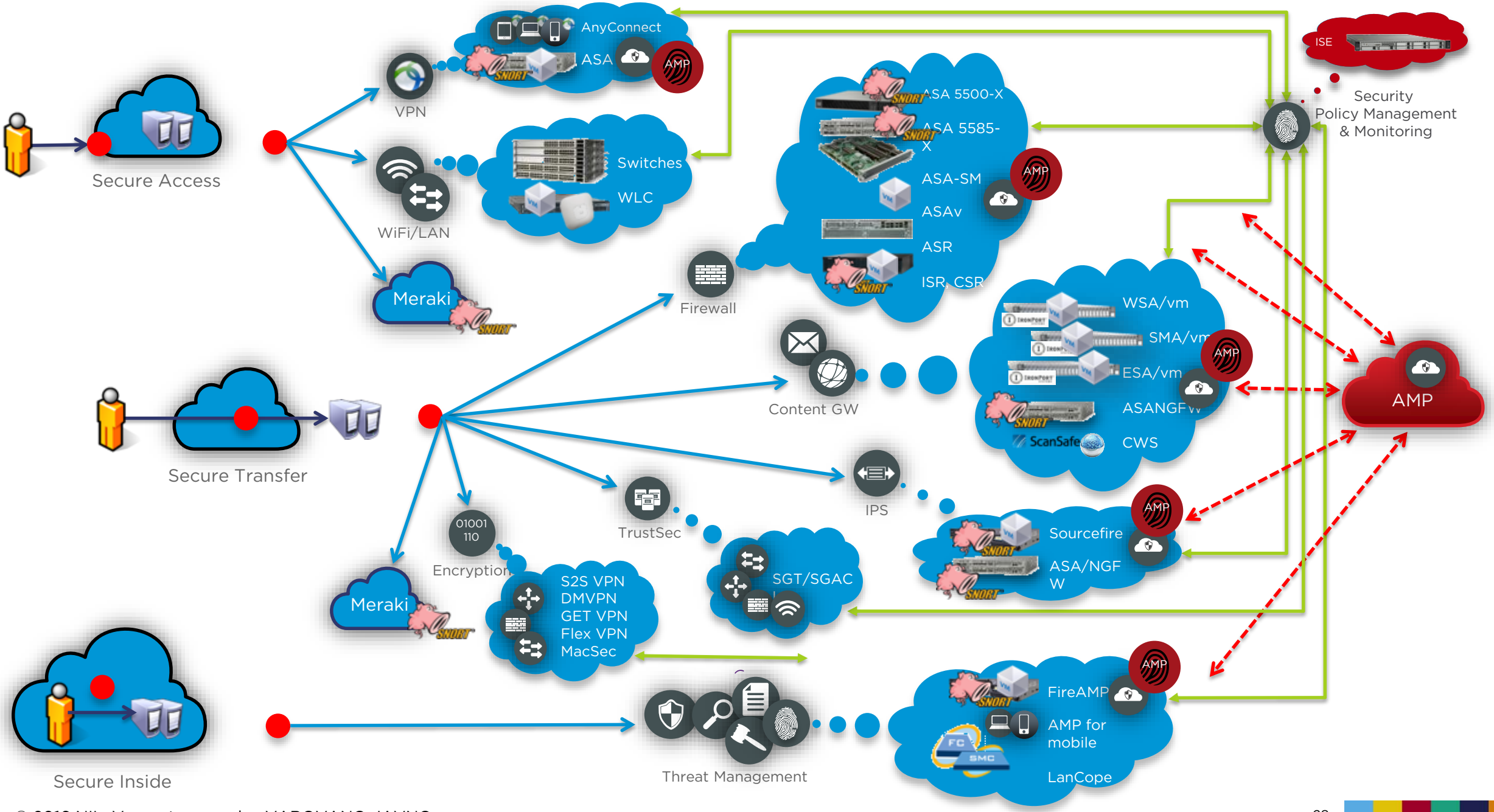
Kaj pa uporabniki?

- V omrežju organizacije: zbiranje in analiza na nivoju omrežja
- Brez vidljivosti dogajanja na končnih točkah
- AMP for Endpoints:
  - Agent, nameščen na končnih točkah
  - Brez podpisov, brez posodobitev
  - Minimalna poraba virov



Kdo pa so uporabniki?





Kaj pa uporabniki?

ENABLING IT FOR BUSINESS

nil.com