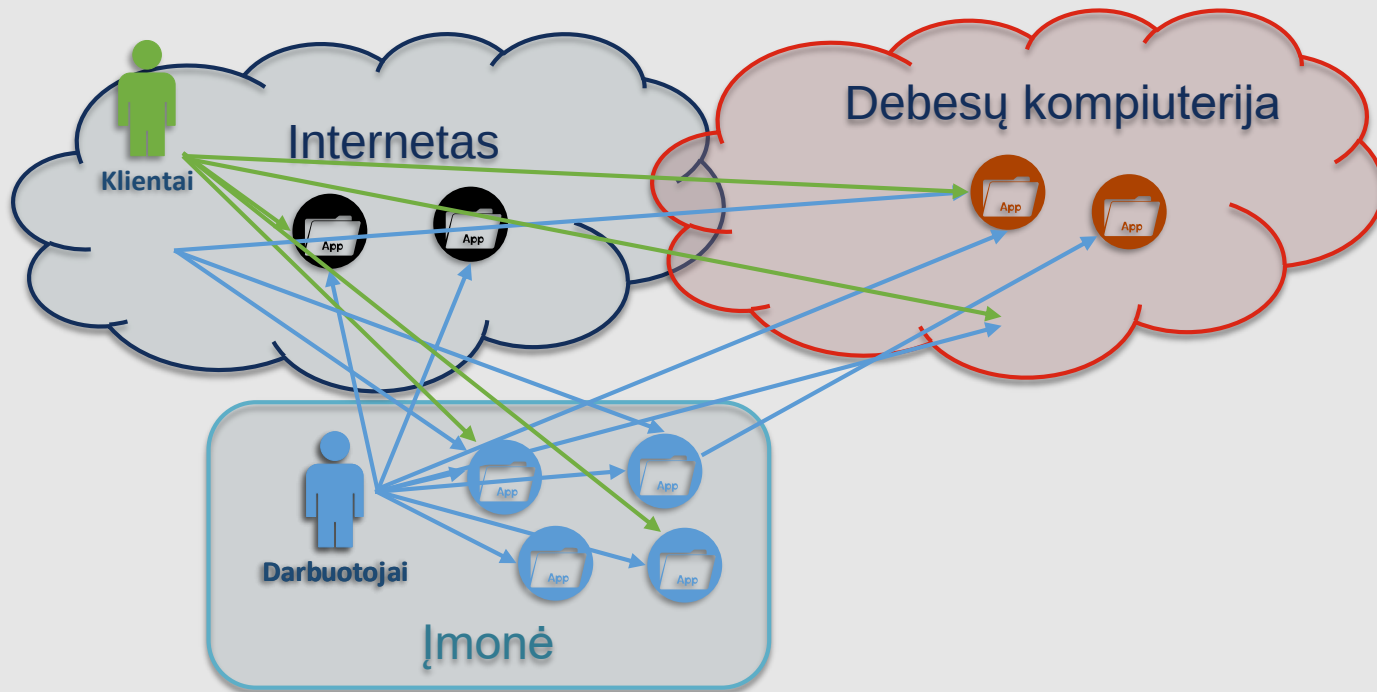


Zero Trust: kas tai?



Poreikių evoliucija



Poreikiai

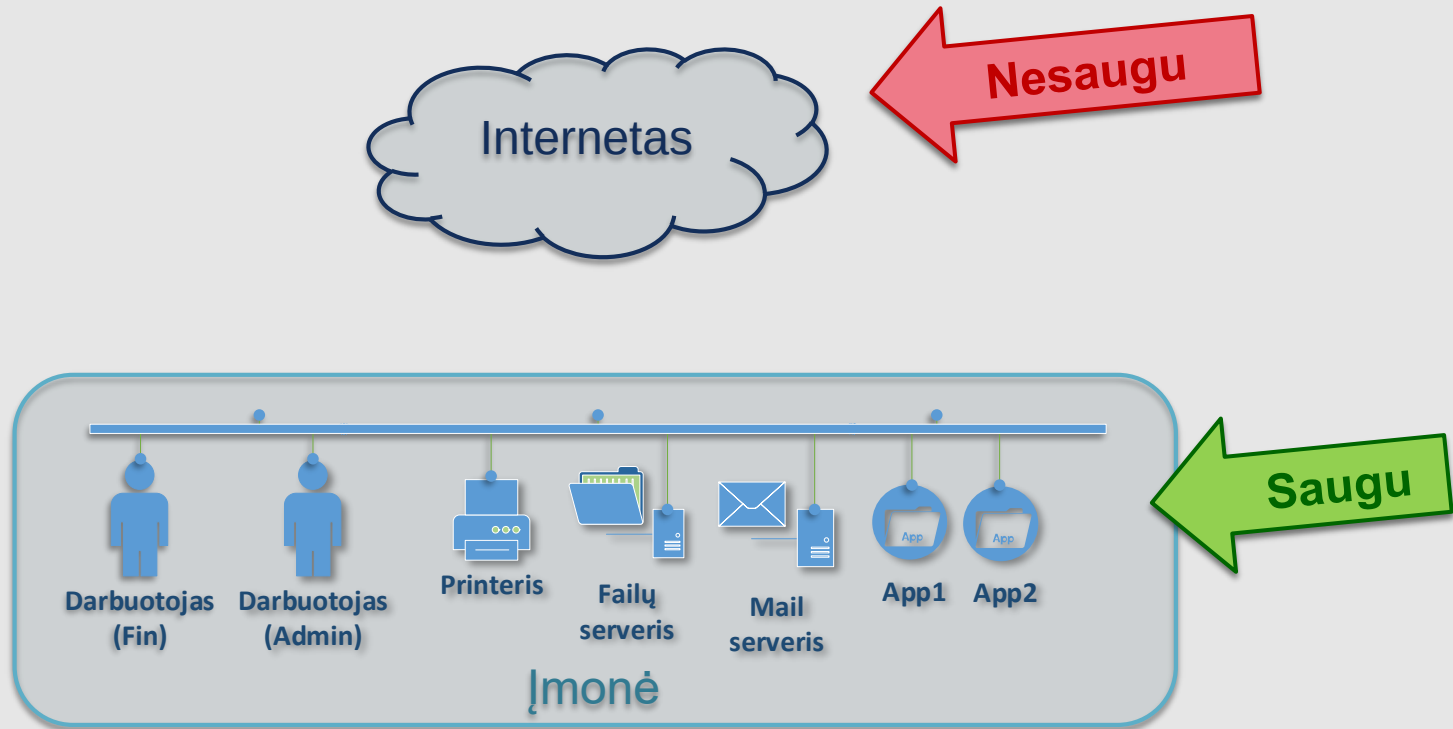
Vakar

- Aplikacijos savame duomenų centre
- Prieiga tik būnant įmonės viduje
- Darbuotojų prieiga prie interneto

Šiandien

- **Sistemų/aplikacijų mobilumas:**
Turi būti galimybė sistemas/aplikacijas talpinti bet kur
Turi būti galimybė sistemas/aplikacijas greitai perkėlinėti iš vienos vietos į kitą
- **Vartotojų mobilumas:**
Sistemos/aplikacijos turi būti prieinamos iš bet kur

Perimetro saugumas



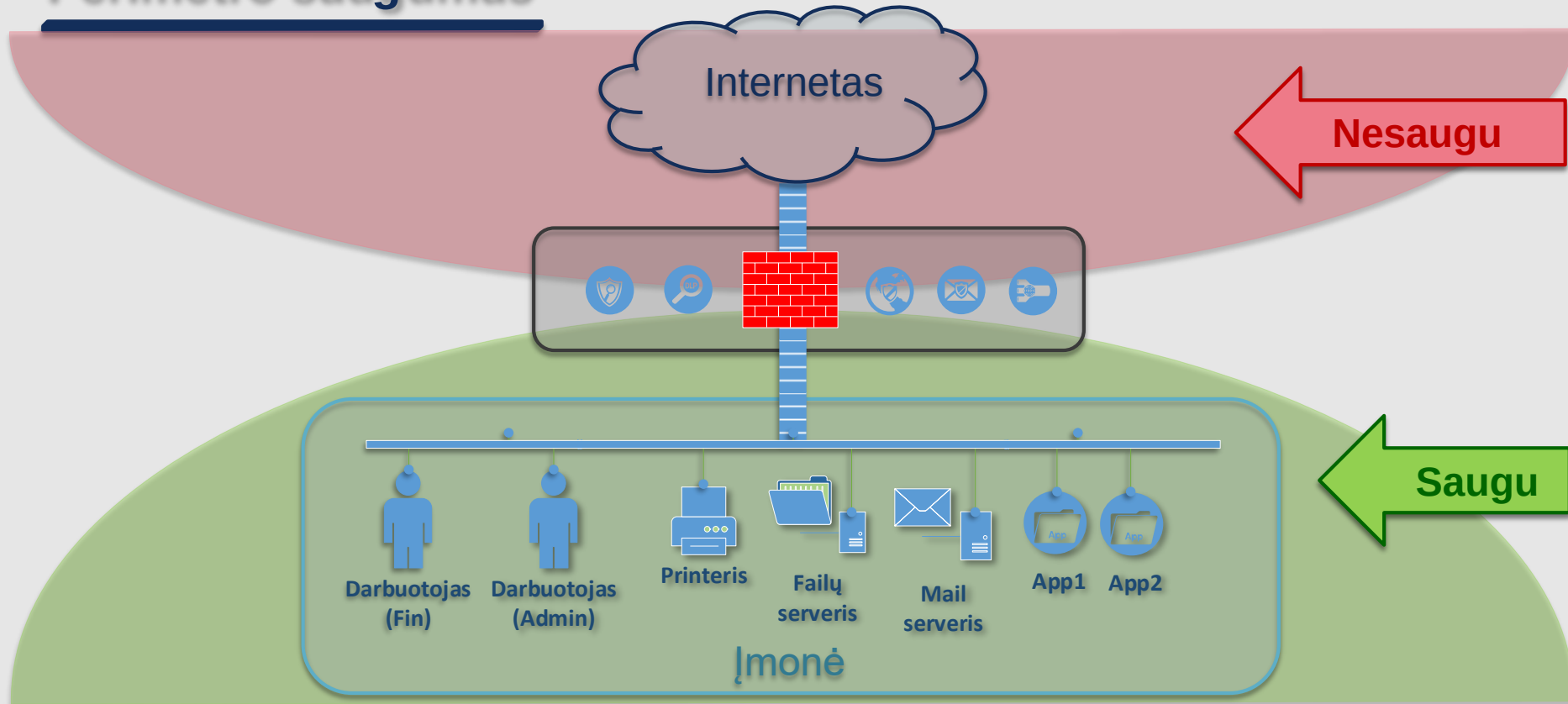
Panaudojam tai ką žinom



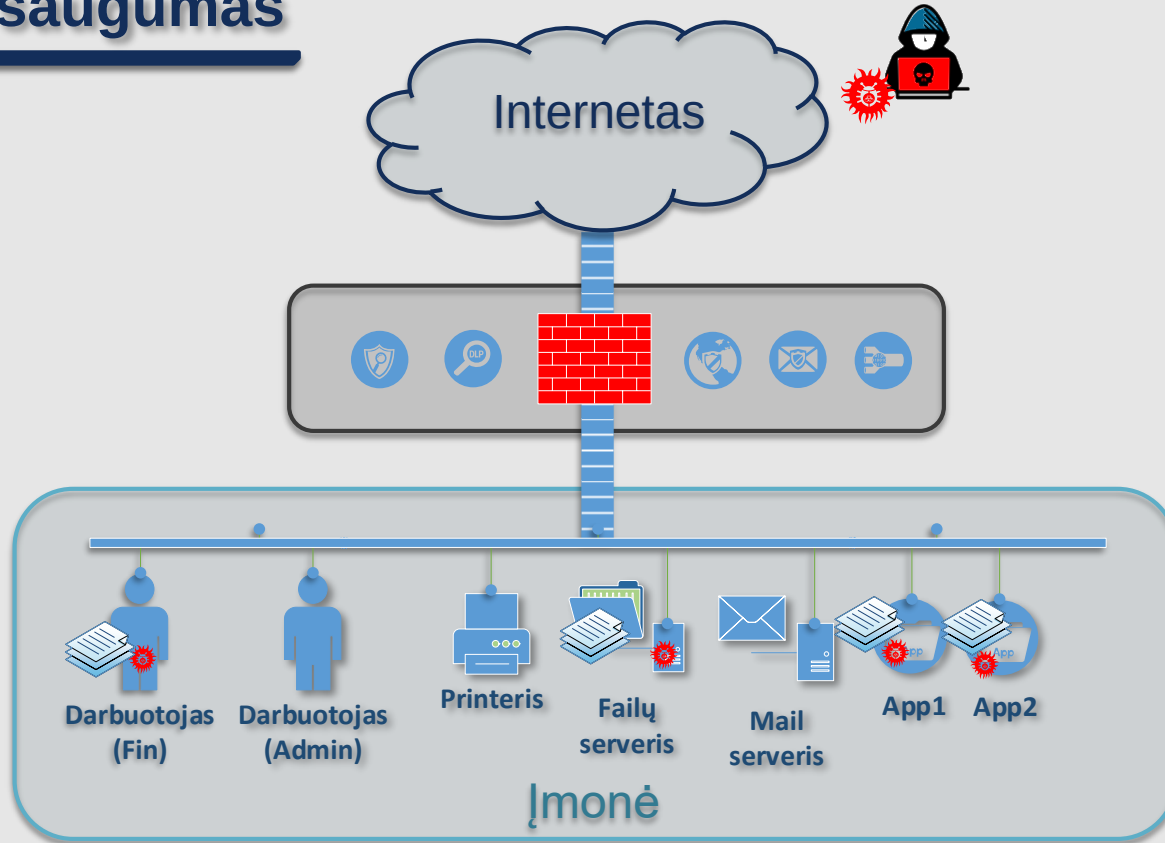
Saugu

Nesaugu

Perimetro saugumas

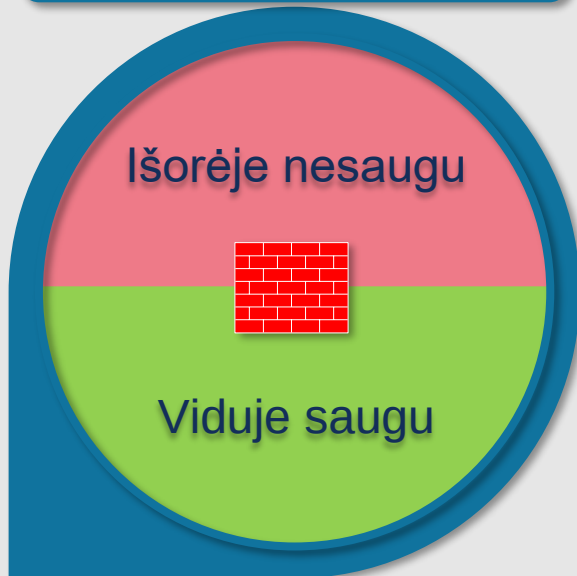


Perimetro saugumas

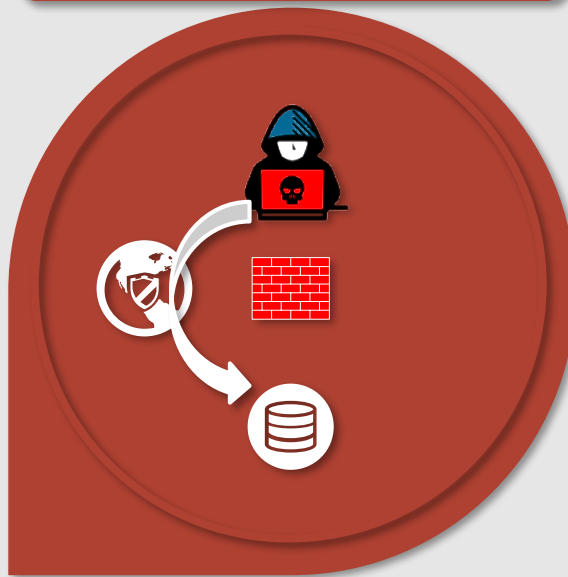


Ką turime šiai dienai

Įsitikinimas



Menamas saugumas



Pavienės sistemos



Pagrindinis dėmesys yra duomenų srautų kontrolei, būvimo vietai

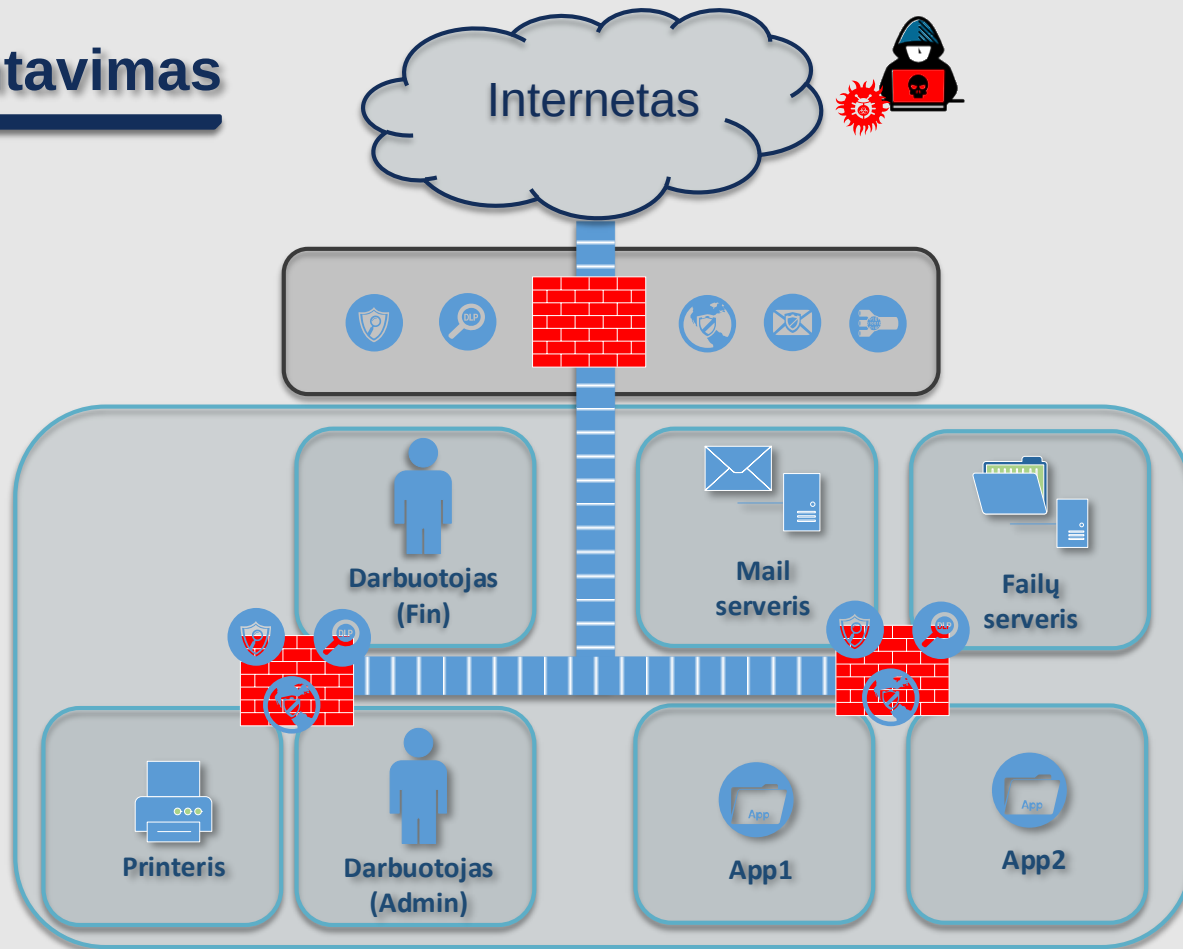
Zero trust: Istorija



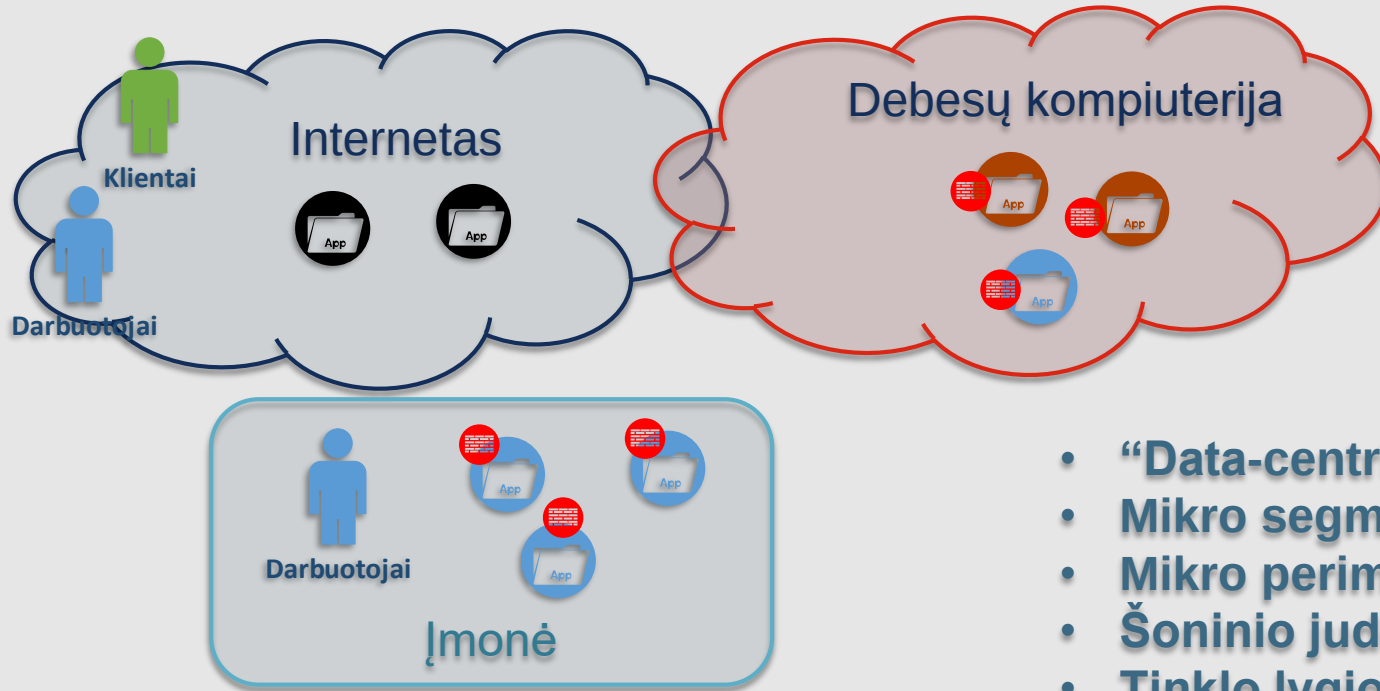
Forrester analitikas John Kindervag pasiūlė „Zero trust“ modelį, kurio pagrindinis principas – nepasitikėti niekuo. Data-centric tinklo architektūra su Micro-segmentavimu ir detalioja kontrole, šoninio judėjimo mažinimas

Data-centric

Mikrosegmentavimas

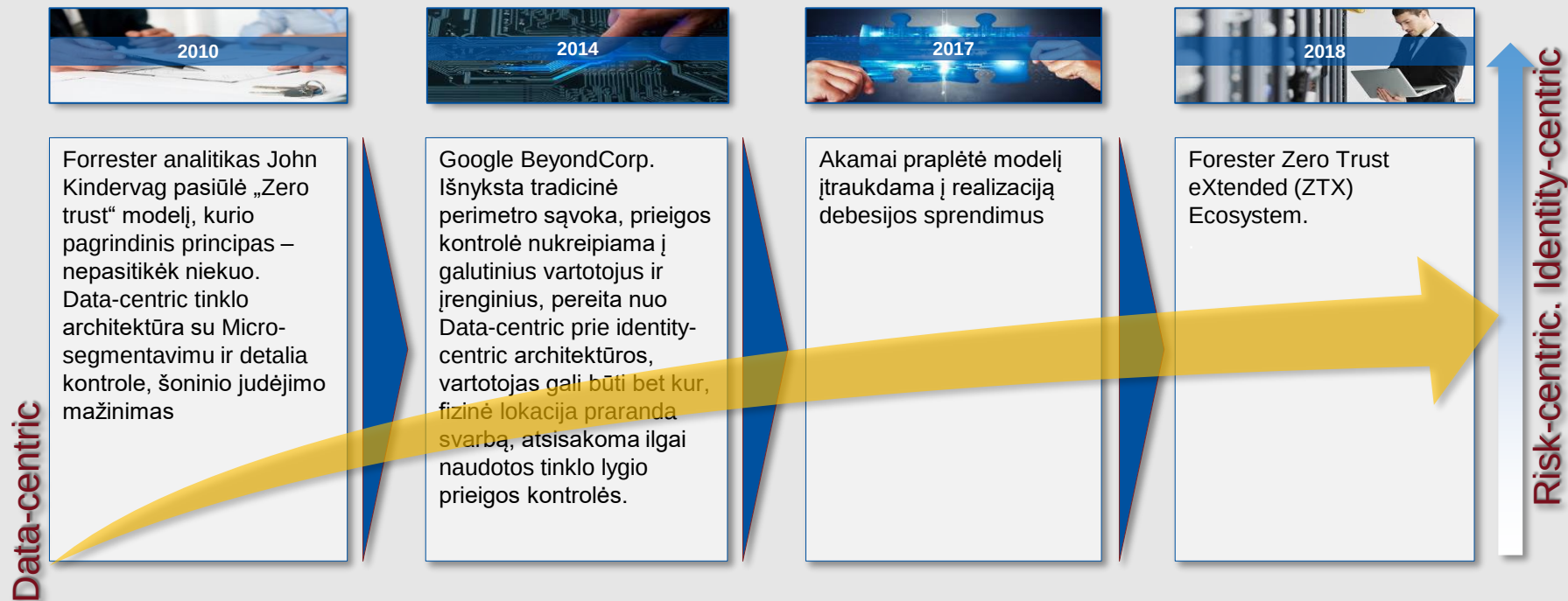


Mikro perimetras



- “Data-centric” architektūra
- Mikro segmentavimas
- Mikro perimetras
- Šoninio judėjimo kontrolė
- Tinklo lygio prieigos kontrolė
- Prisirišimas prie vietos

Zero trust: Istorija



Zero trust: pagrindiniai principai



Zero-trust: Niekuo nepasitikėk

- Tinklas visada yra priešiškas
- Tinkle visą laiką yra išorinių ir vidinių grėsmių
- Buvimo vieta nėra pakankama patikimumo įvertinimui
- Turi būti nustatyta kiekvieno įrenginio, vartotojo tapatybė
- Kiekvienas įrenginys, vartotojas, duomenų srautas turi būti autentikuotas, o veiksmai autorizuoti
- Saugumo politikos turi būti dinamiškos ir kuriamos naudojant kiek įmanoma daugiau šaltinių



Zero-trust: Komponentai

- Pasitikėjimo valdymas
- Autorizacijos sprendimų priėmimas
- Pasitikėjimas įrenginiais
- Pasitikėjimas vartotojais
- Pasitikėjimas aplikacijomis
- Pasitikėjimas duomenų srautų



Zero-trust: pasitikėjimas įrenginiais

Įrenginio inventorizacija:

fiksuojama detali informacija;
inventorizacijos duomenų bazėje (tiksliai HW
specifikacija, konfigūracijos pakeitimai, ip, OS
ir t.t.)

CMDB panaudojimas.

Naudojamos programinės įrangos
sertifikavimas:

„Golden image“;

Fiksuojama PĮ perdiegimo data;

Fiksuojama naudojamos programinės
įrangos versija;

„Secure boot“.

Įrenginio identifikacija:

Skaitmeniniai sertifikatai;

Authentication proxy seniems įrenginiams.

Tapatybės duomenų saugojimas:

paprastas saugojimas;

šifravimas;

HSM, TPM.

Tapatybę patvirtinančių duomenų diegimas,
atnaujinimas:

rankinis;

automatinis.

Pirminė įrenginių registracija ir pasitikėjimo
atnaujinimas

Įrenginių elgsena:

kas kaip dažnai jais naudojasi;

iš kur įrenginys jungiasi;

įrenginio elgsena tinkle.

Zero-trust: pasitikėjimas vartotojais

Įrenginių ir vartotojų tapatybė turi būti nustatoma atskirai

Vartotojų tapatybė patvirtinantys duomenys negali būti saugomi darbo kompiuteryje

Vartotojo inventorizacija:

fiksuojama detali informacija apie vartotoją, jo roles, tipines darbo vietas, kaip dažnai keičia būvimo vietą ir pan.

Pasitikėjimo balo naudojimas prieigai prie sistemų

SSO

Informacijos apie vartotojo elgseną rinkimas

Tinkamų tapatybės nustatymo metodų naudojimas

Tapatybės nustatymo metodų grandinių sudarymas

Kuo dažnesnis vartotojo veiksmų autorizavimas

Zero-trust: pasitikėjimas aplikacijomis

Programinės įrangos inventorizacija
Saugus aplikacijos kūrimas ir eksploatacija:

- Aplikacijas turi kurti kūrėjai, kurie yra patikimi;

- Aplikacijos kodas buvo patikimai paruoštas;

- Aplikacija buvo patikimai įdiegta į sistemą;

- Nuolatos stebimas aplikacijos patikimumas;

- Aplikacijos kodo patikimumo patvirtinimas kriptografiniais būdais;

- Aplikacijos kodo nepakeičiamumo užtikrinimas (kūrimo ir eksploatacijos metu);

- Kūrimo metu naudojamų komponentų patikimumo užtikrinimas;

- Savalaikis aplikacijoje naudojamų komponentų atnaujinimas.

- Naudojamų aplikacijų izoliavimas, resursų rezervavimas

Zero-trust: pasitikėjimas duomenų srautu

Turi būti kaupiama informacija apie duomenų srautus

Turi būti atliekama elgsenos analizė

Duomenų kontrolė turi būti atliekama

komunikacijoje dalyvaujančiuose objektuose (pvz.: VMas) arba kuo arčiau jų

Duomenų filtravimas sistemoje įėjimo ir išėjimo kryptimis

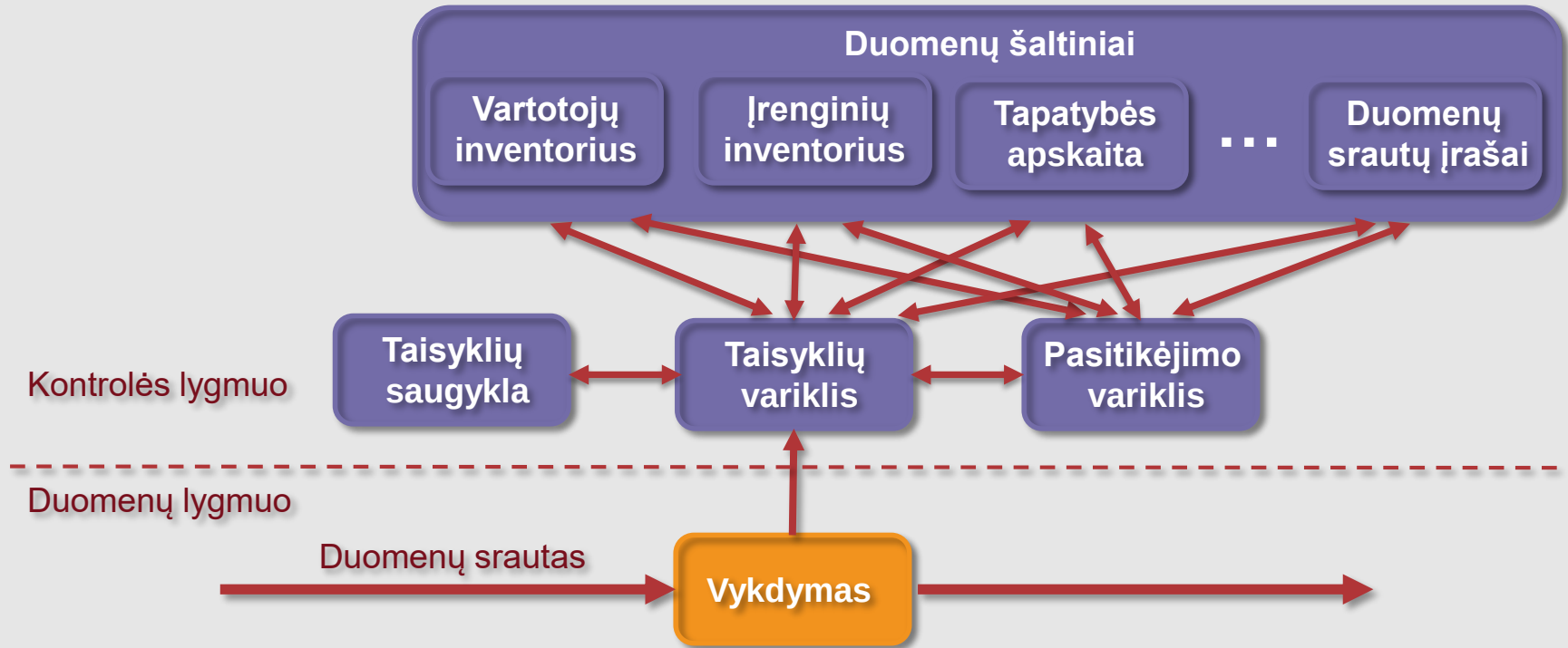
Duomenų filtravimas tarpiniame taške

Dinamiškas filtrų aktyvavimas atsižvelgiant į saugumo balus, komunikuojančius objektus, autorizacijos informaciją

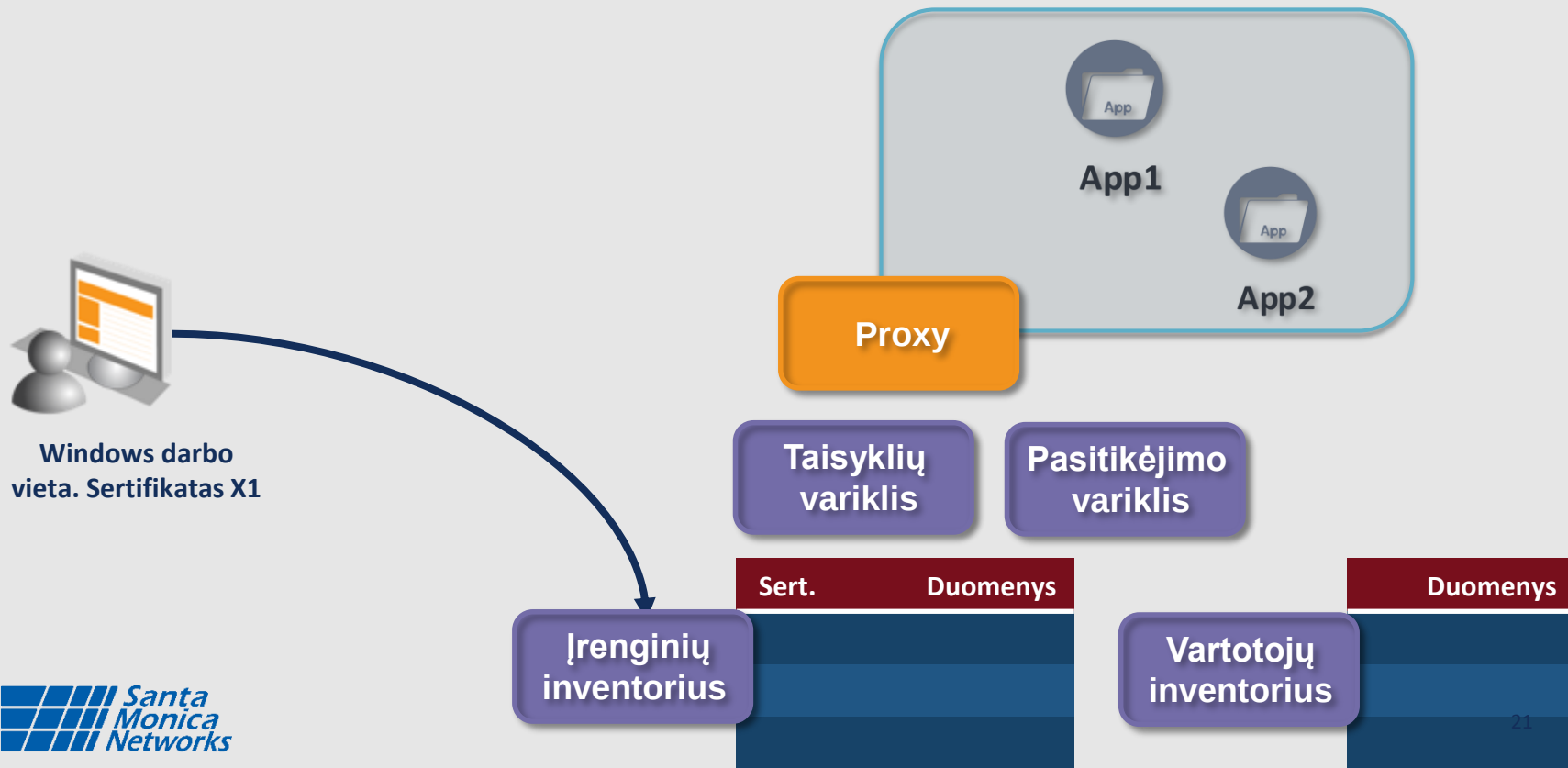
Dinamiškas maršrutizavimas atsižvelgiant į saugumo balus, komunikuojančius objektus, autorizacijos informaciją

IPSEC naudojimas duomenų centrų viduje, TLS – vartotojų prisijungimui

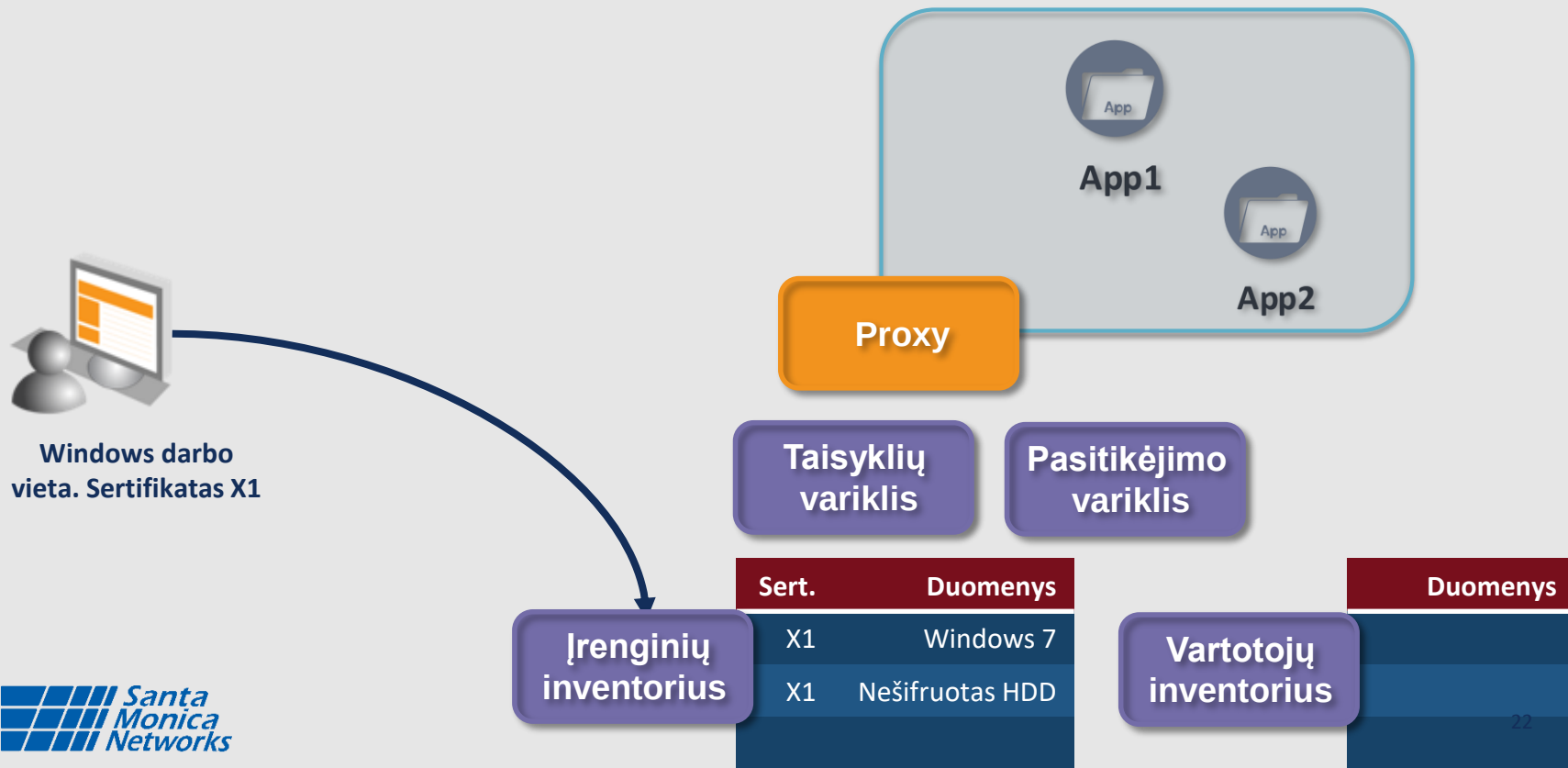
Zero-trust: sprendimų priėmimas



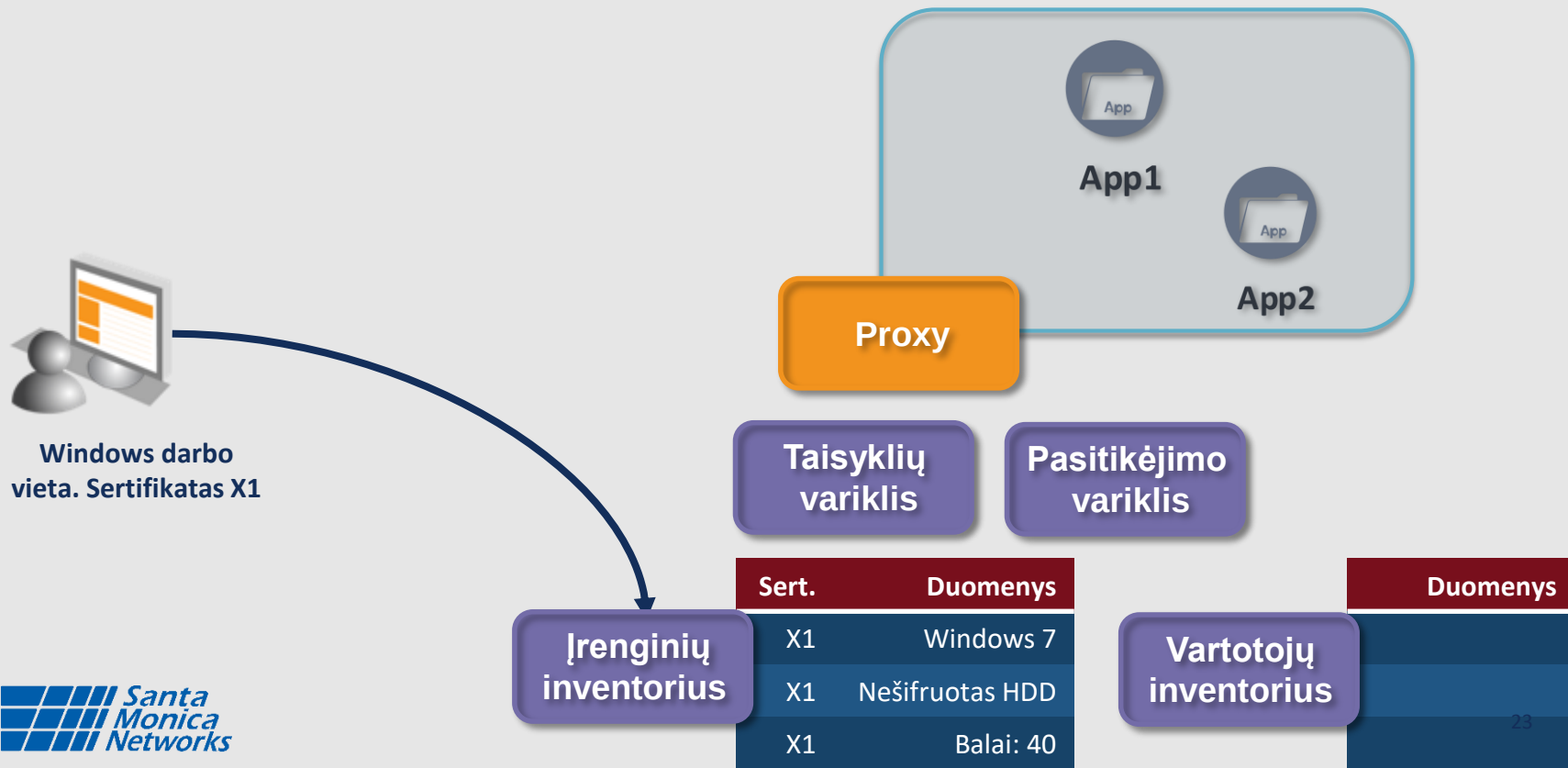
Zero-trust: veikimas



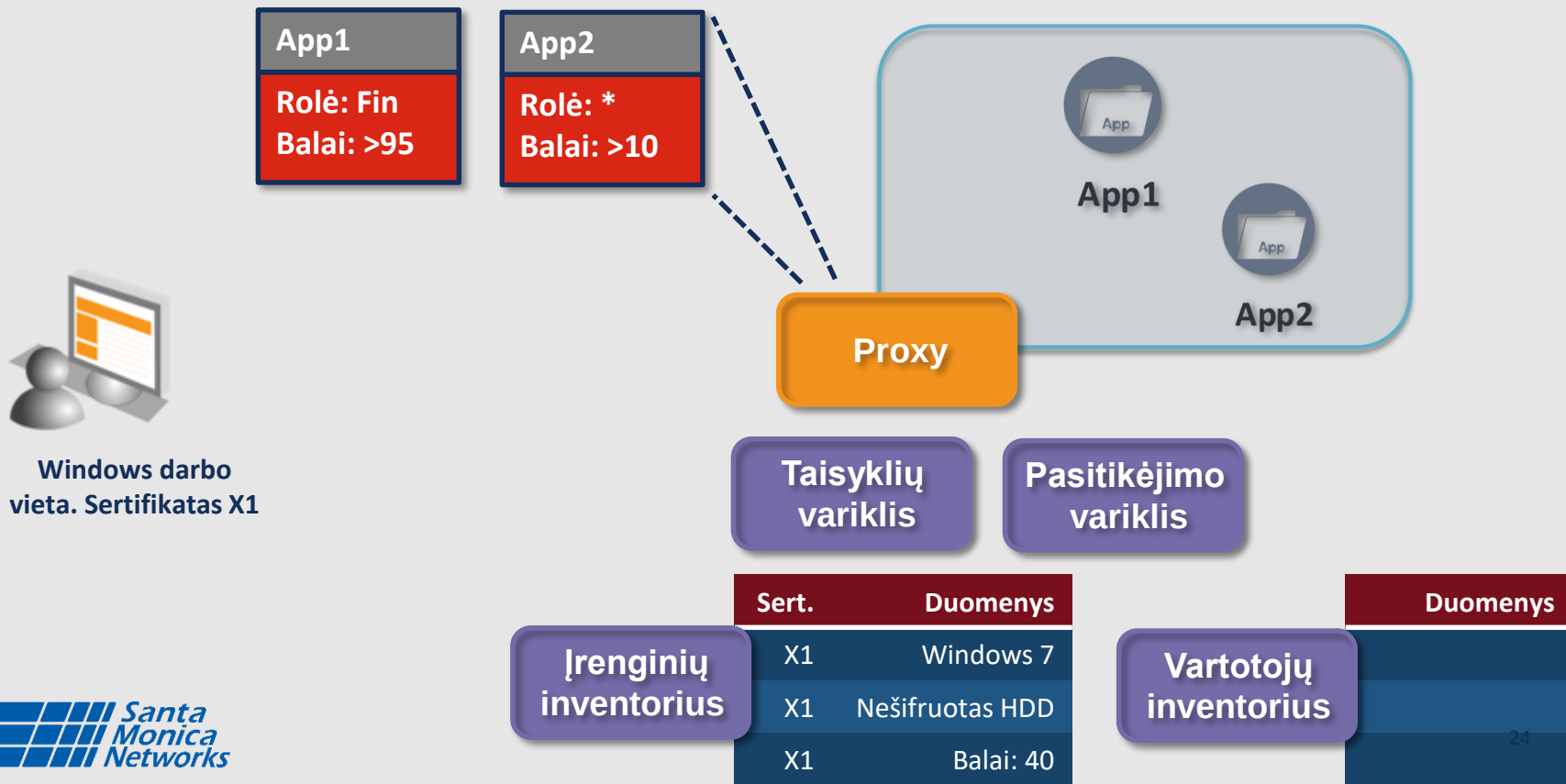
Zero-trust: veikimas



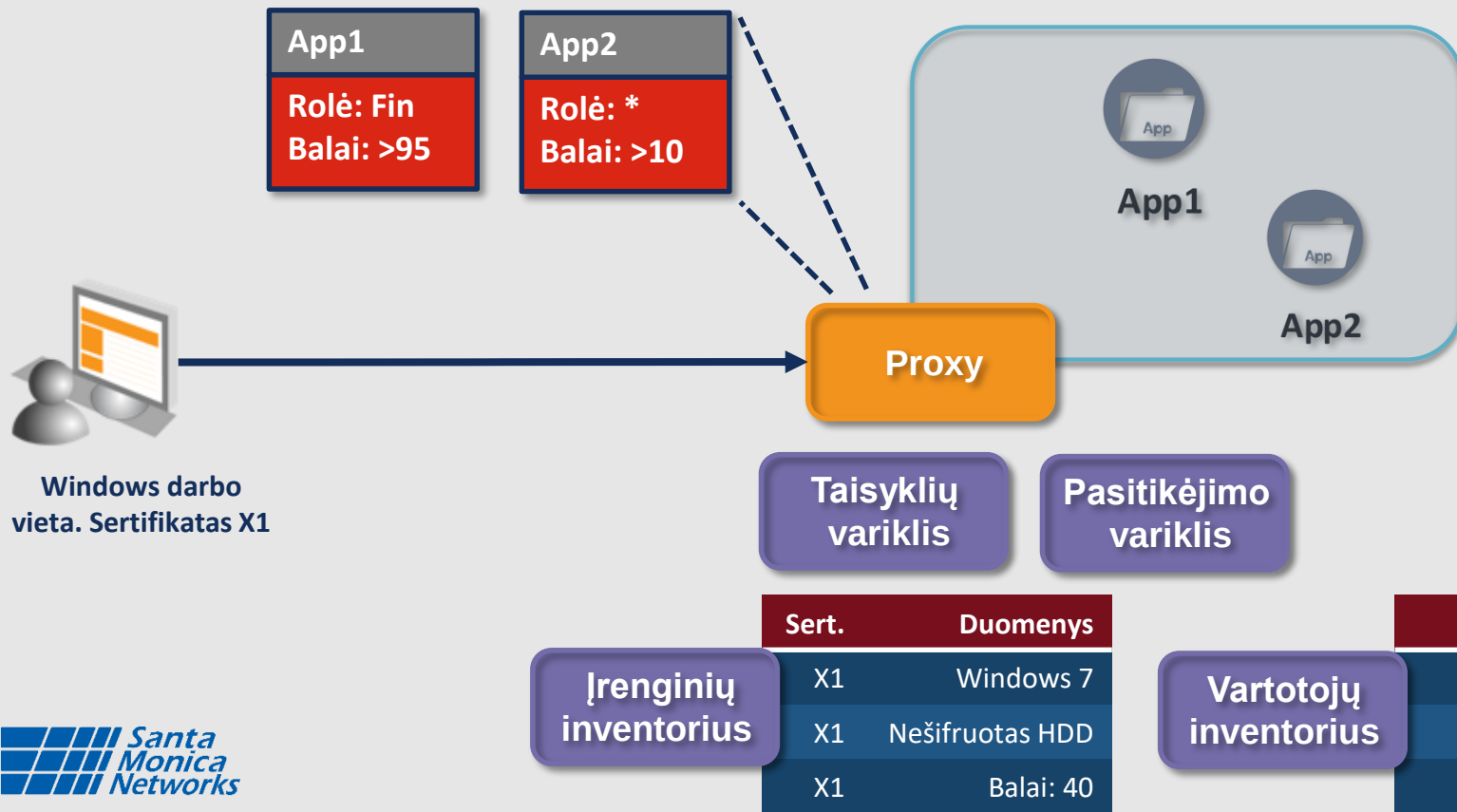
Zero-trust: veikimas



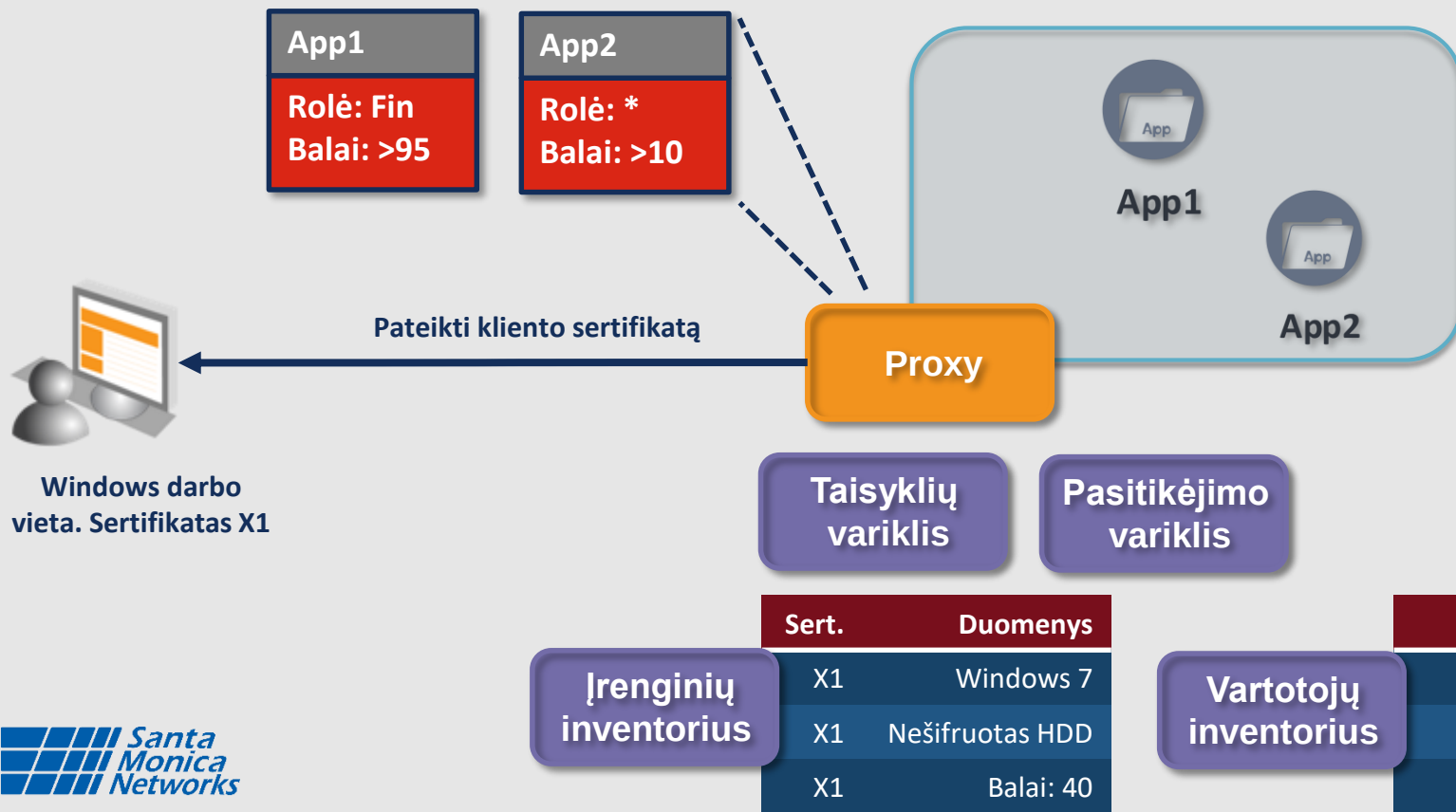
Zero-trust: veikimas



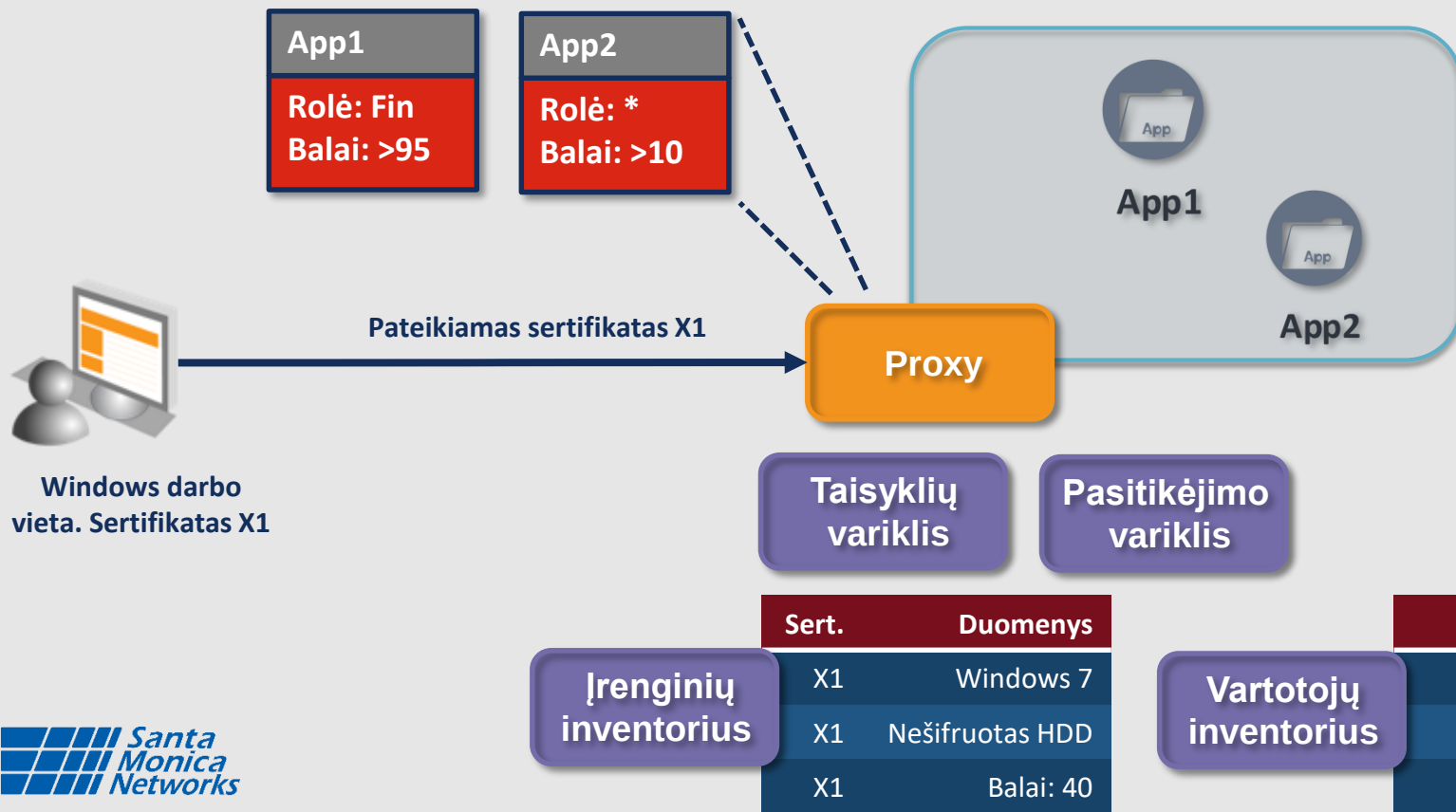
Zero-trust: veikimas



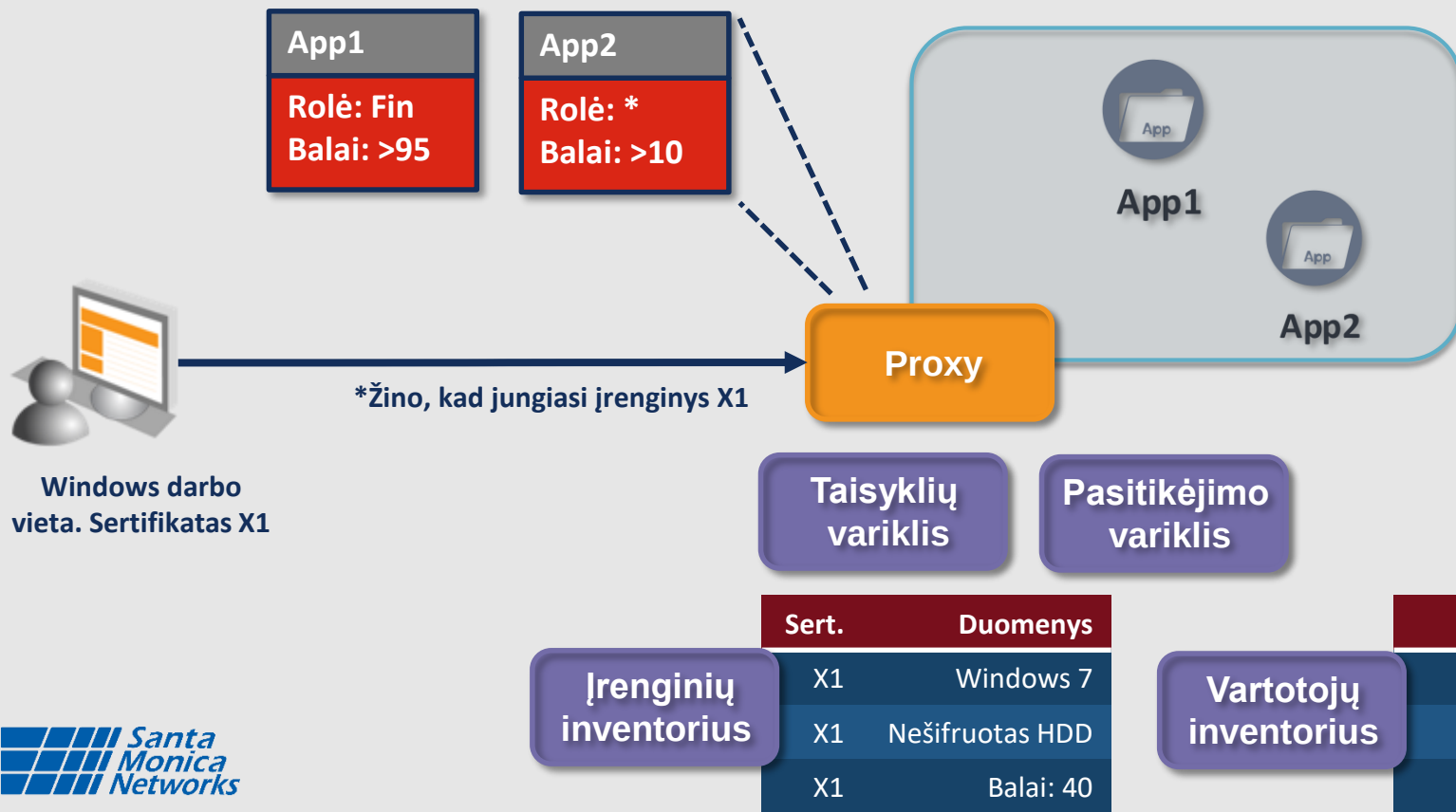
Zero-trust: veikimas



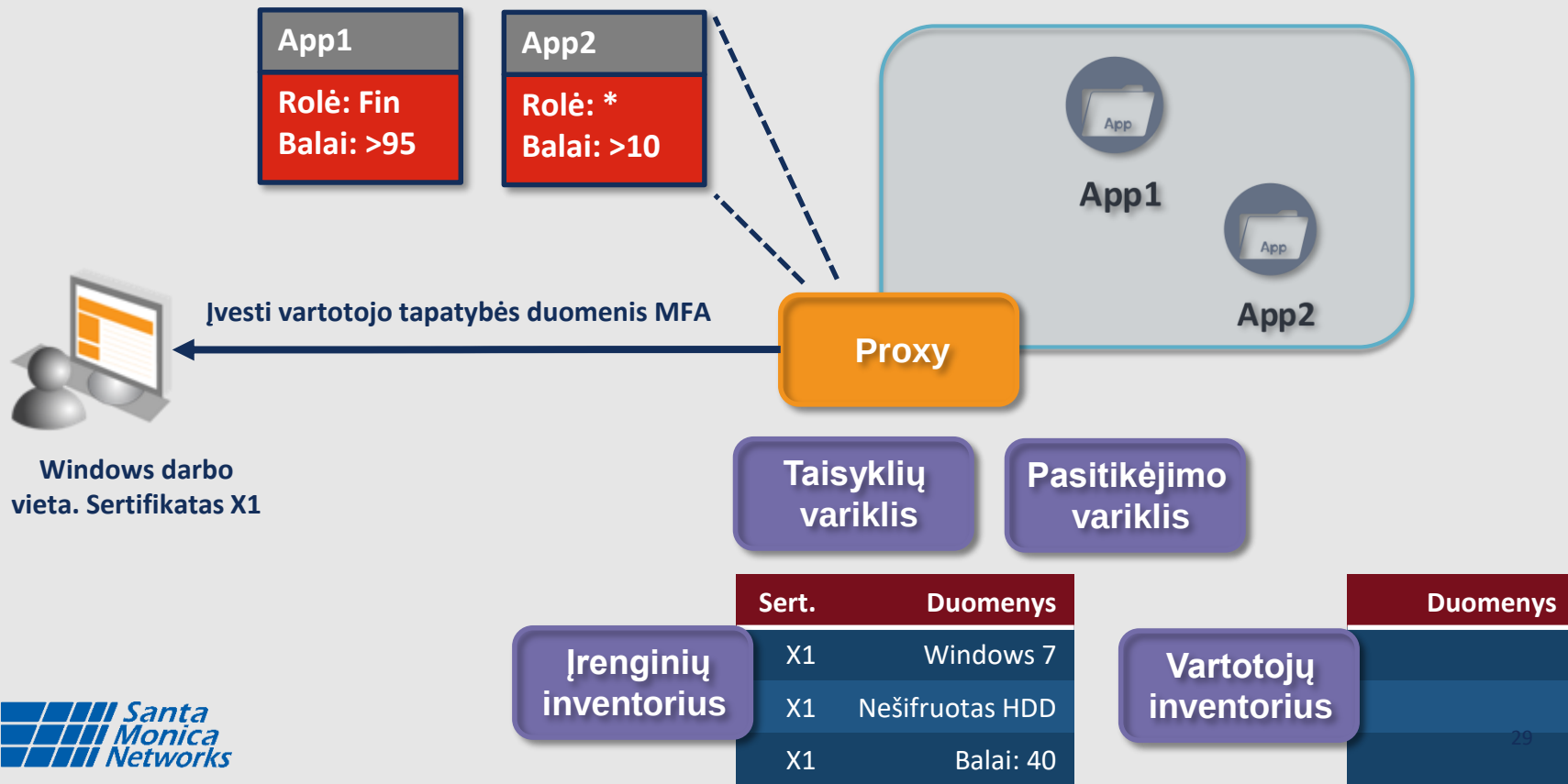
Zero-trust: veikimas



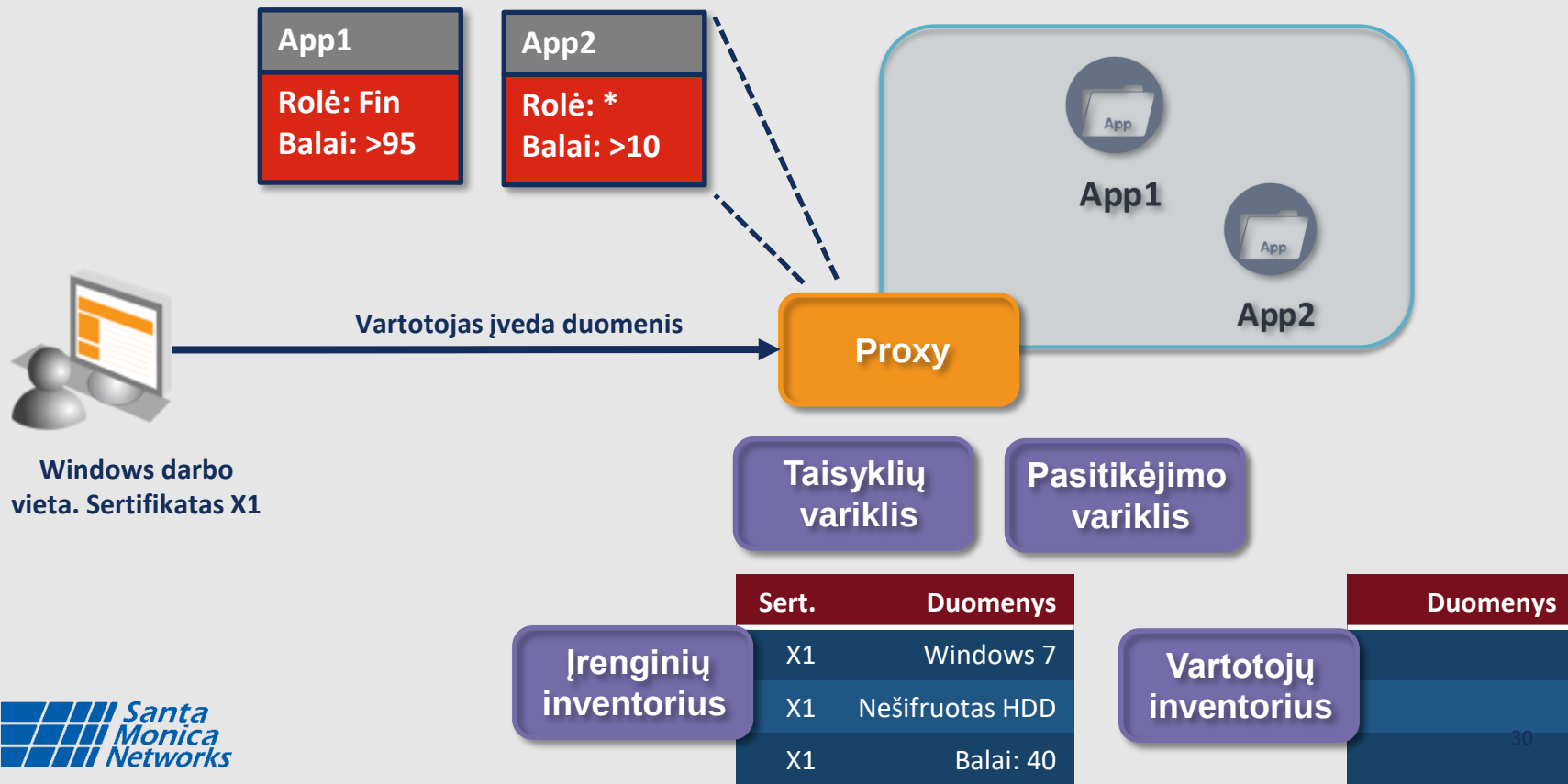
Zero-trust: veikimas



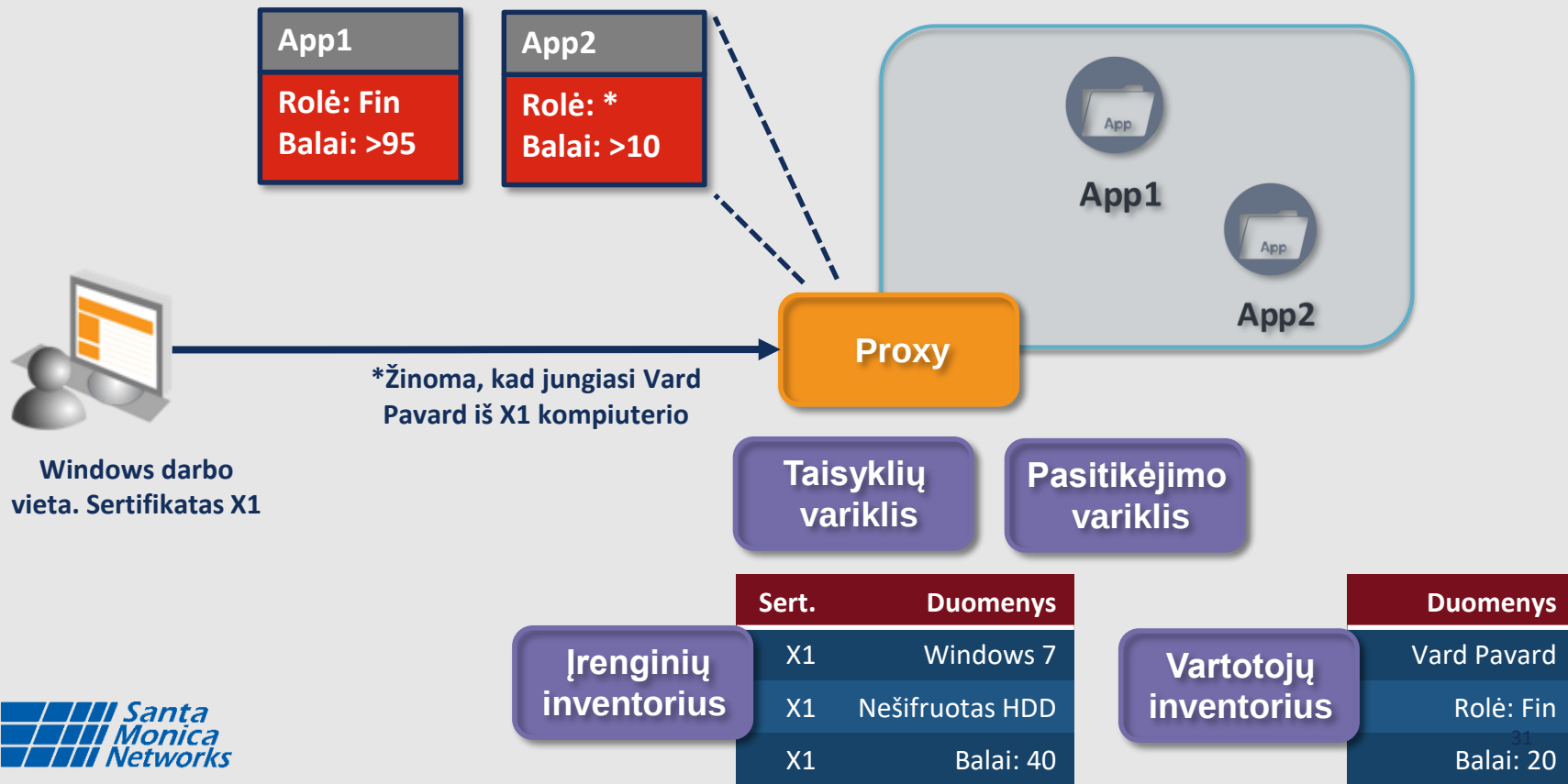
Zero-trust: veikimas



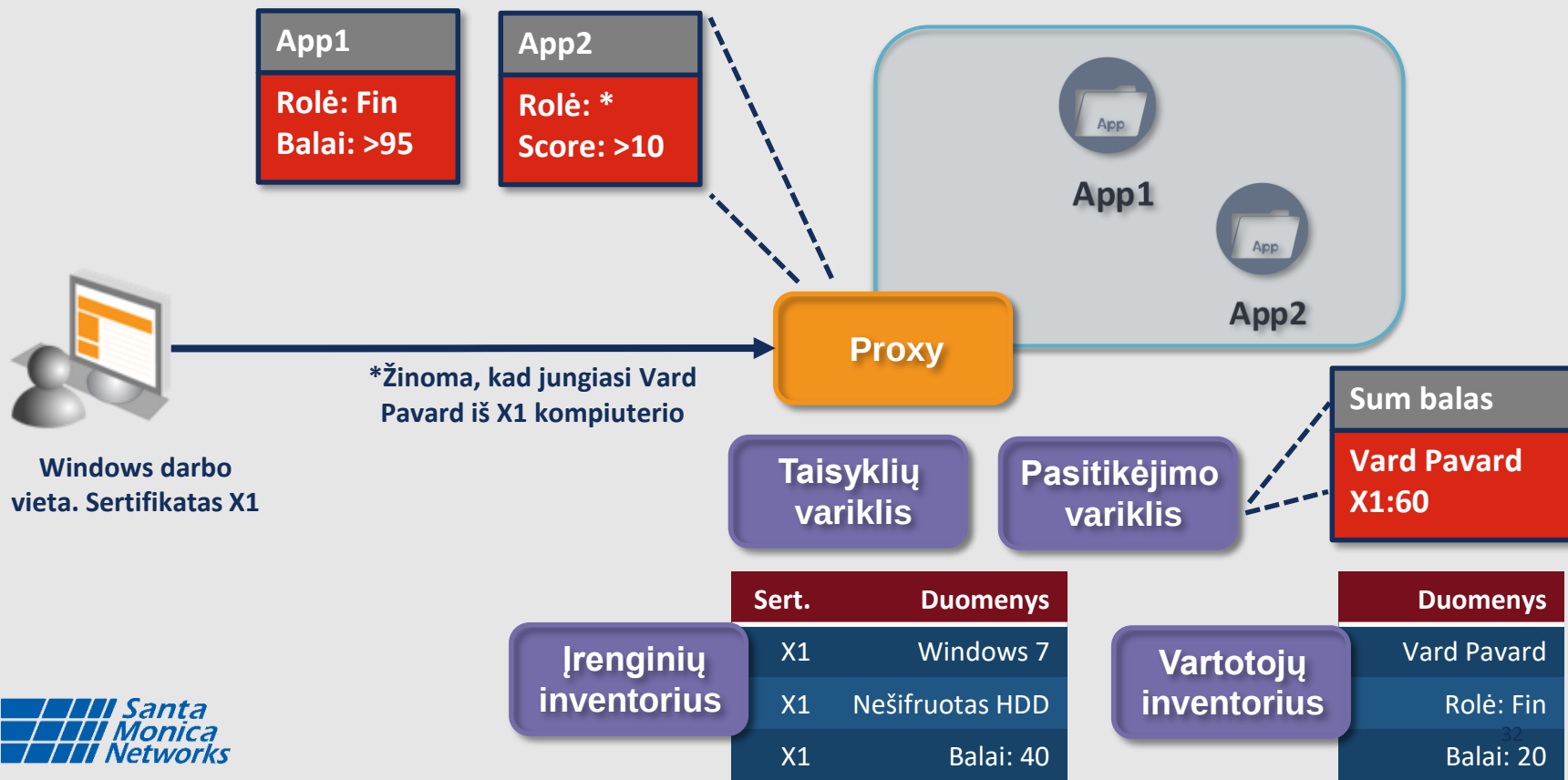
Zero-trust: veikimas



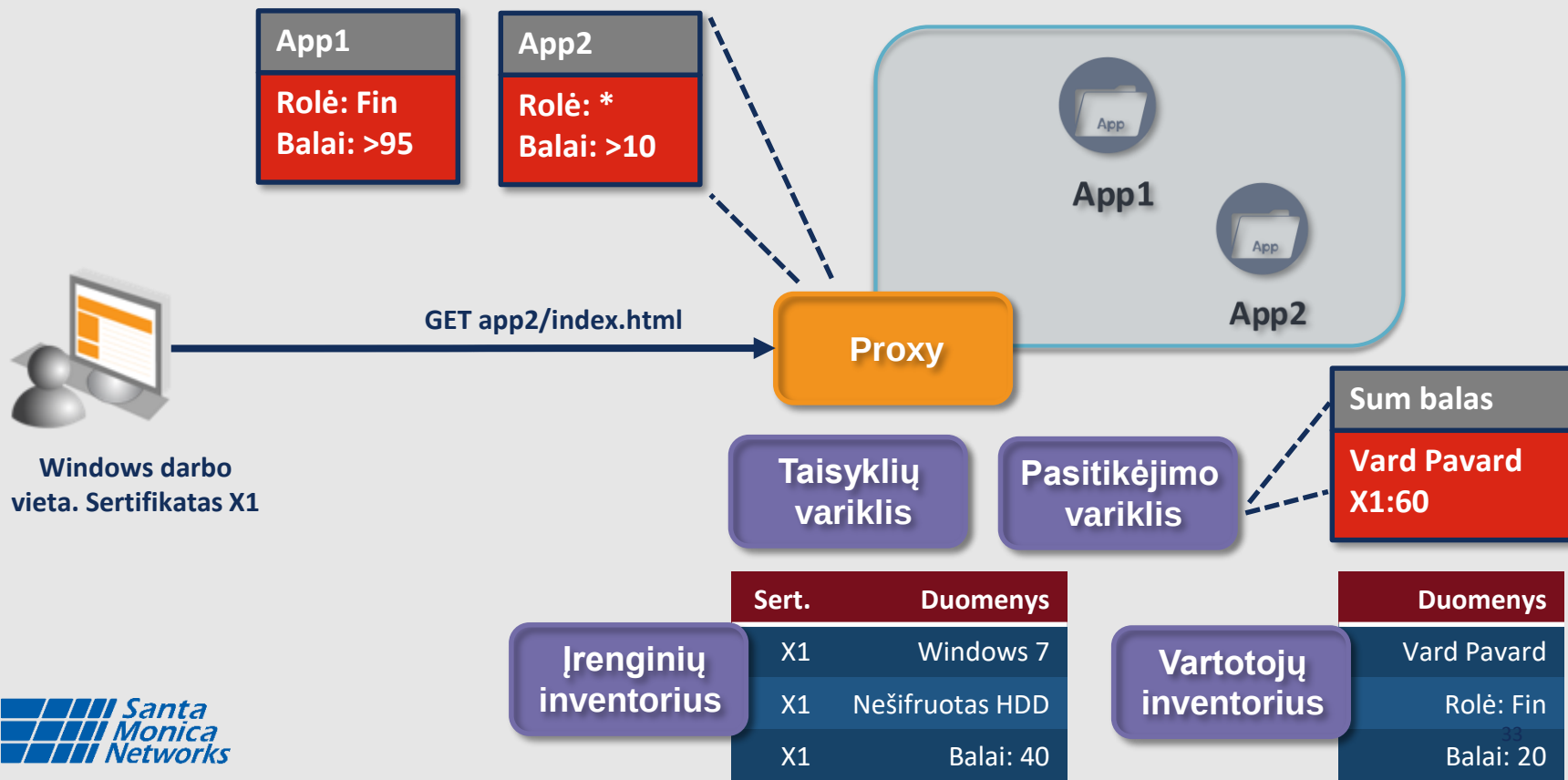
Zero-trust: veikimas



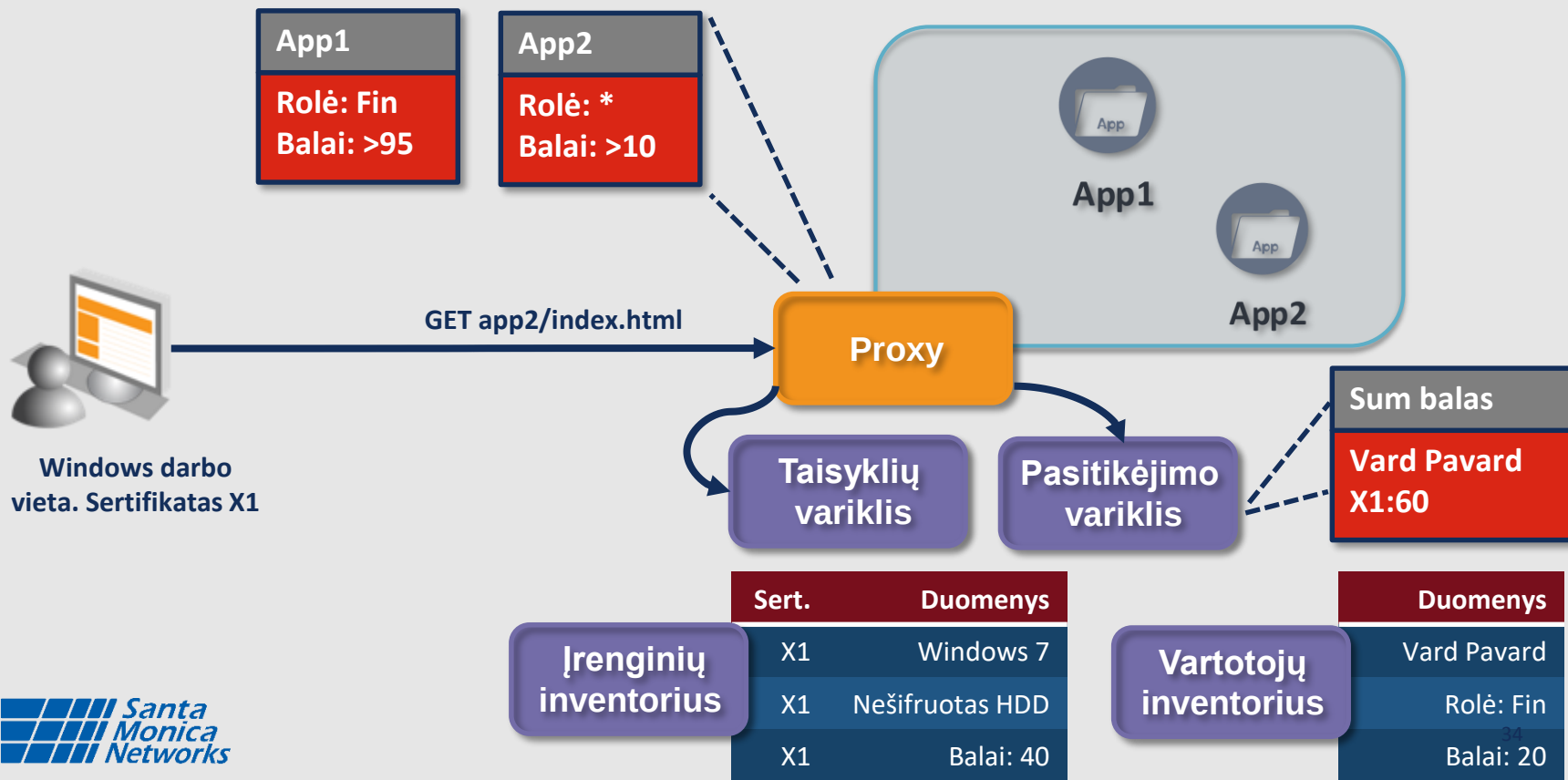
Zero-trust: veikimas



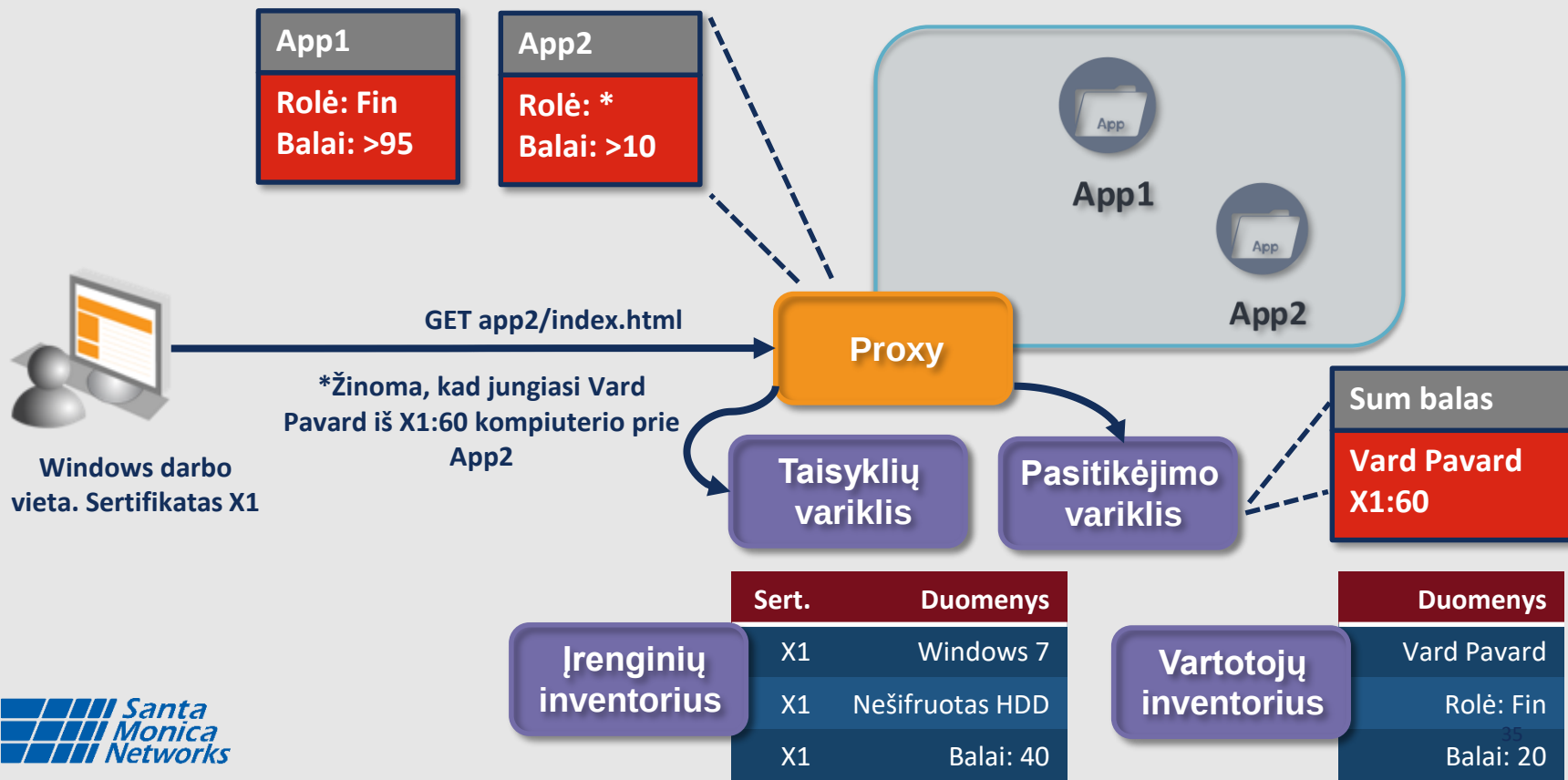
Zero-trust: veikimas



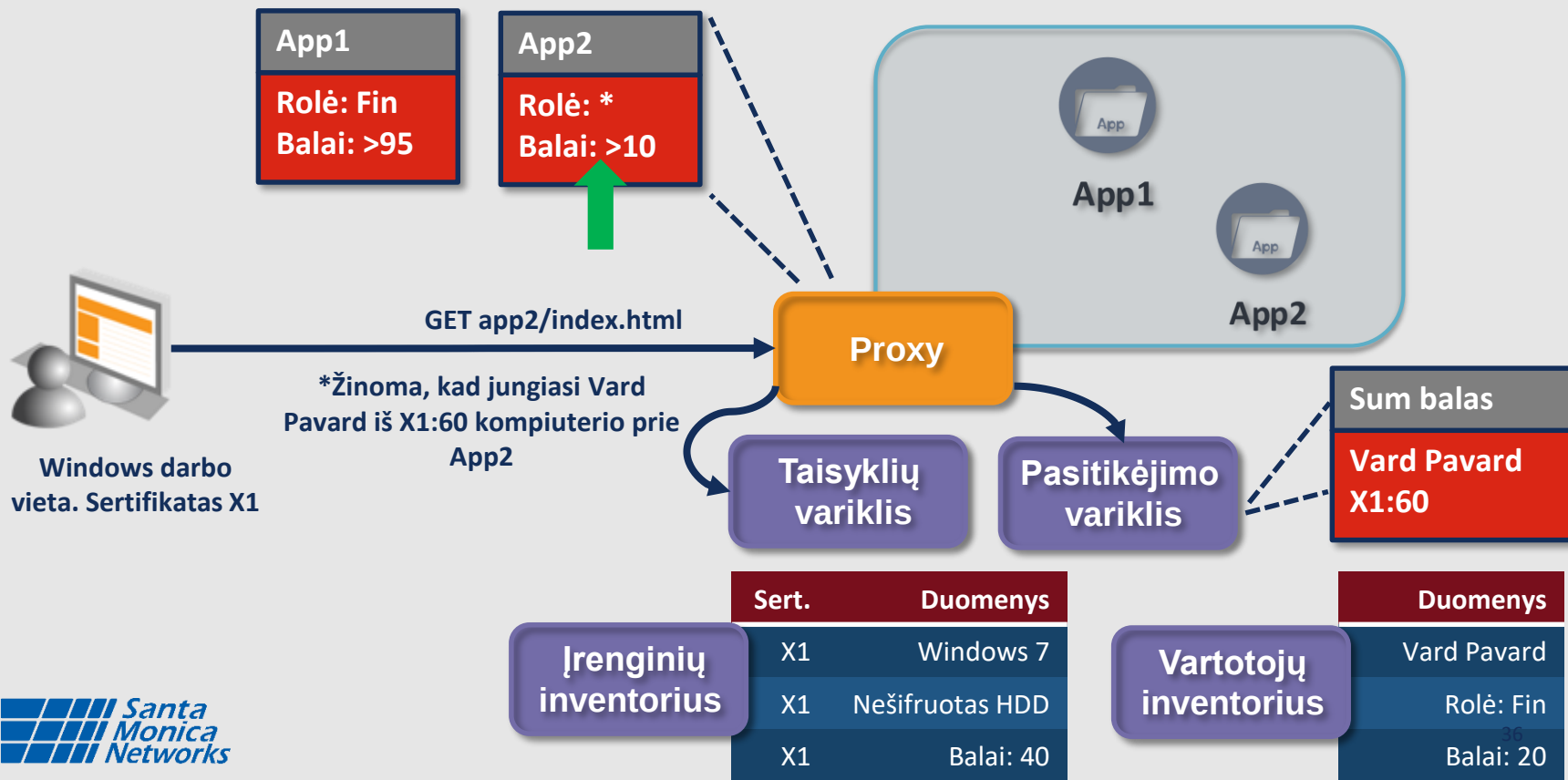
Zero-trust: veikimas



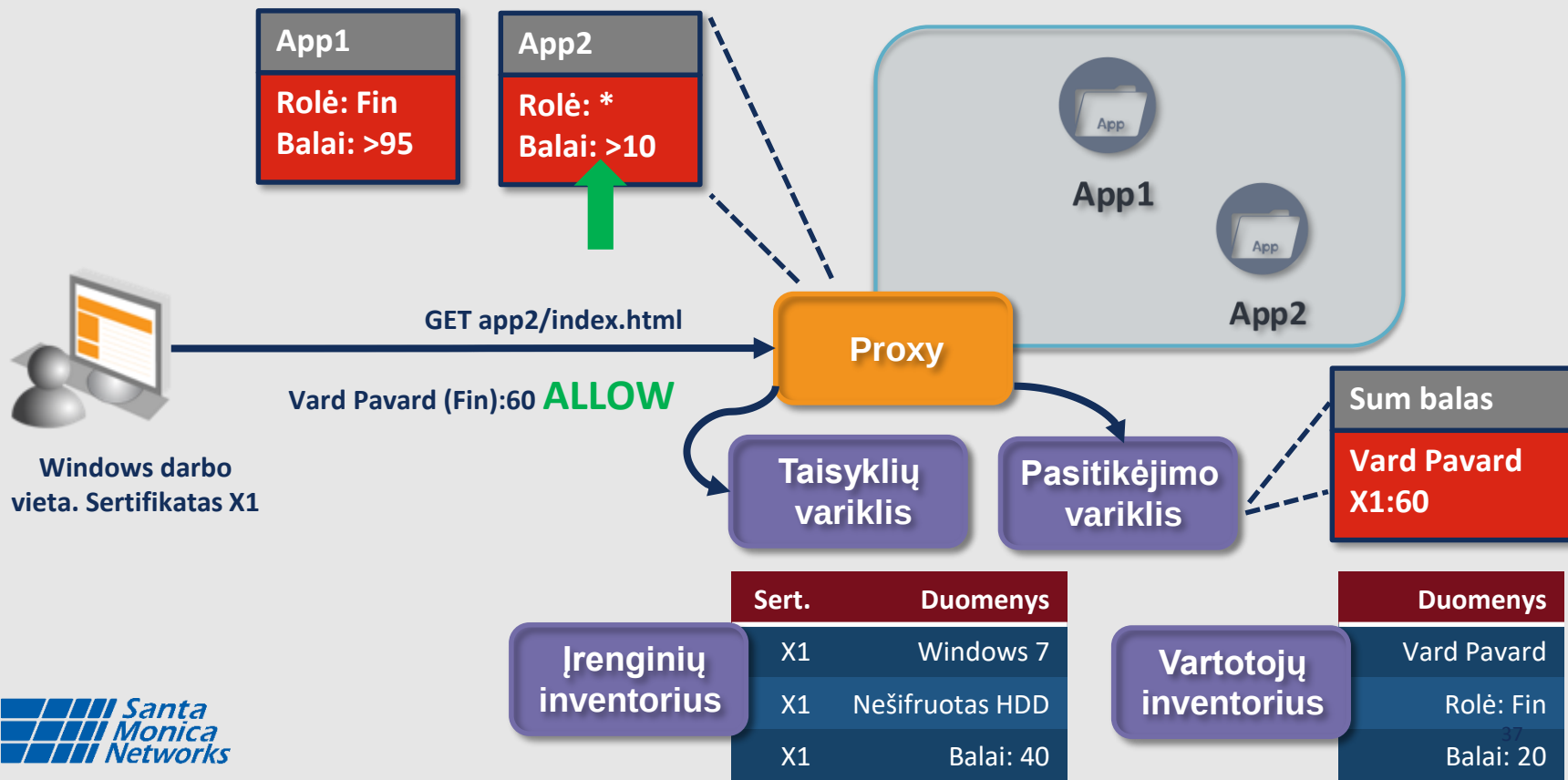
Zero-trust: veikimas



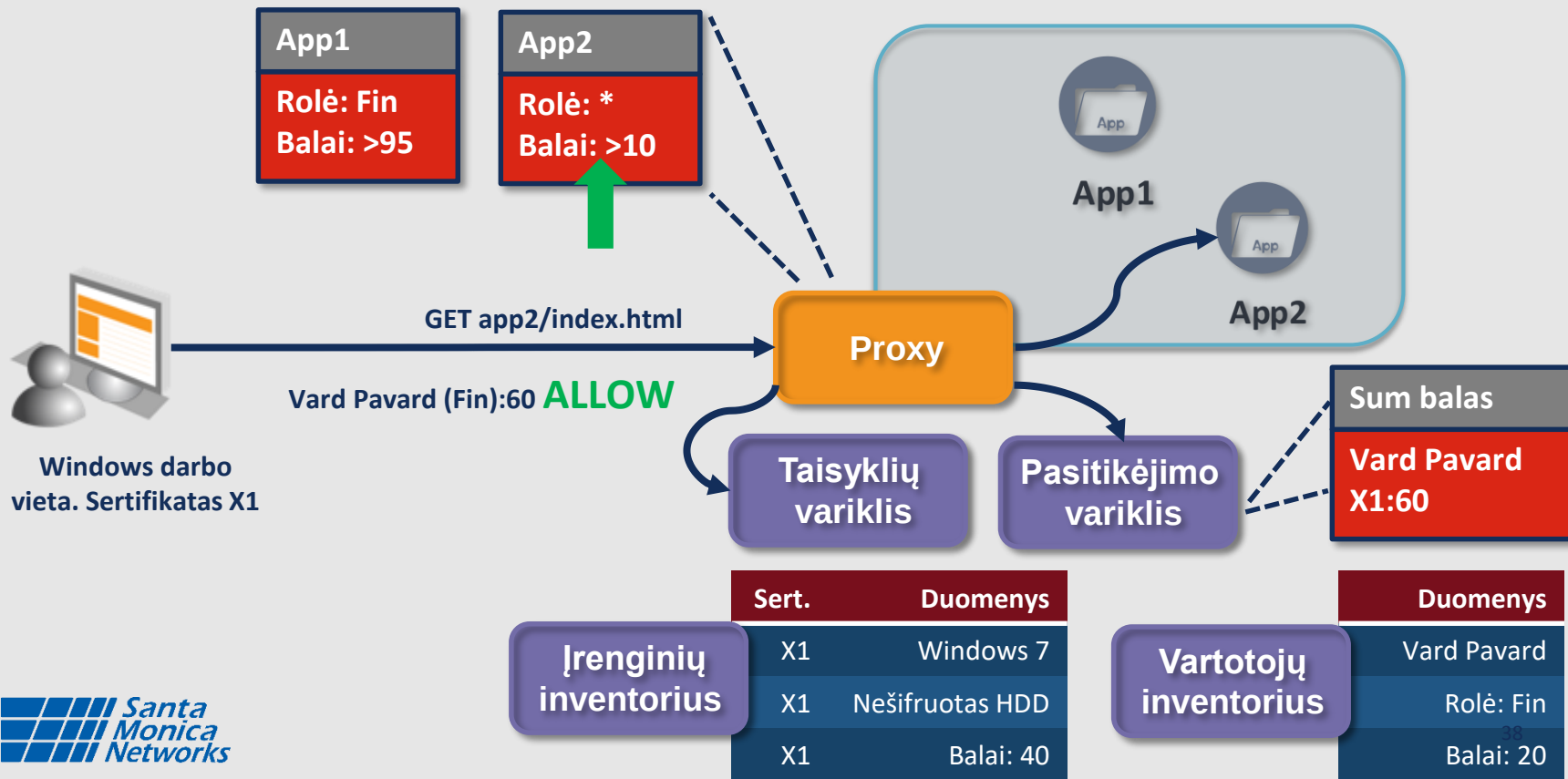
Zero-trust: veikimas



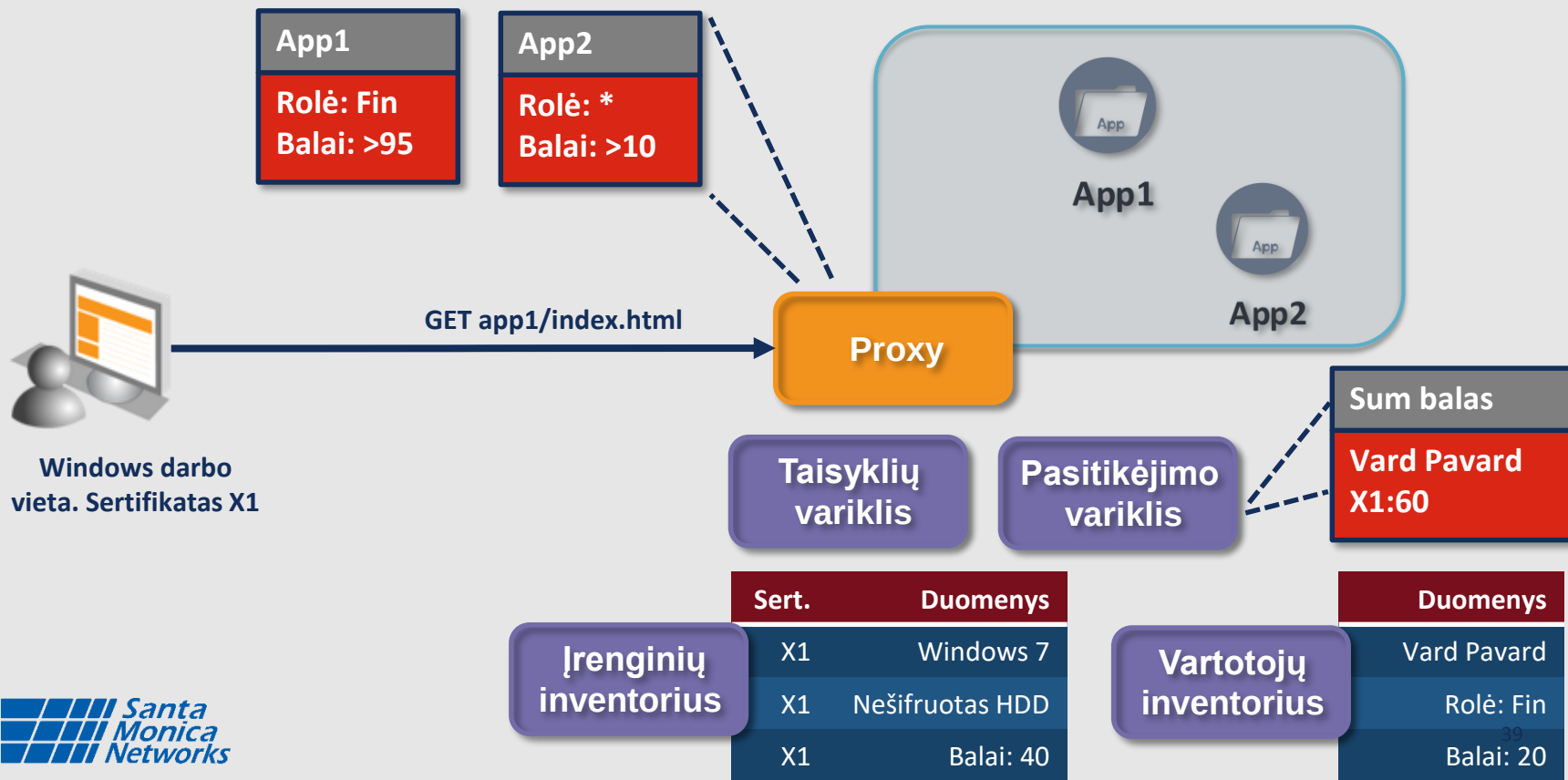
Zero-trust: veikimas



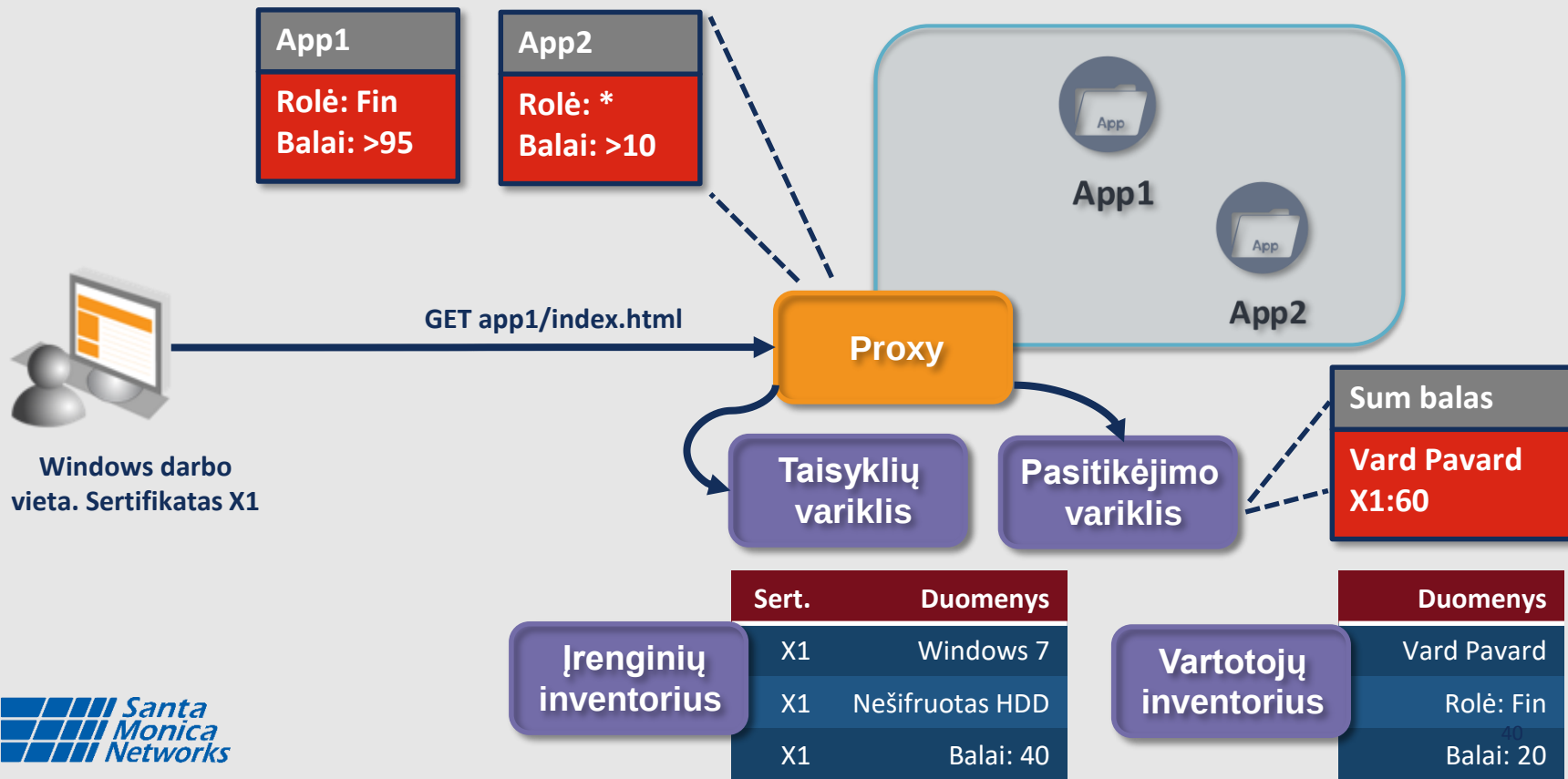
Zero-trust: veikimas



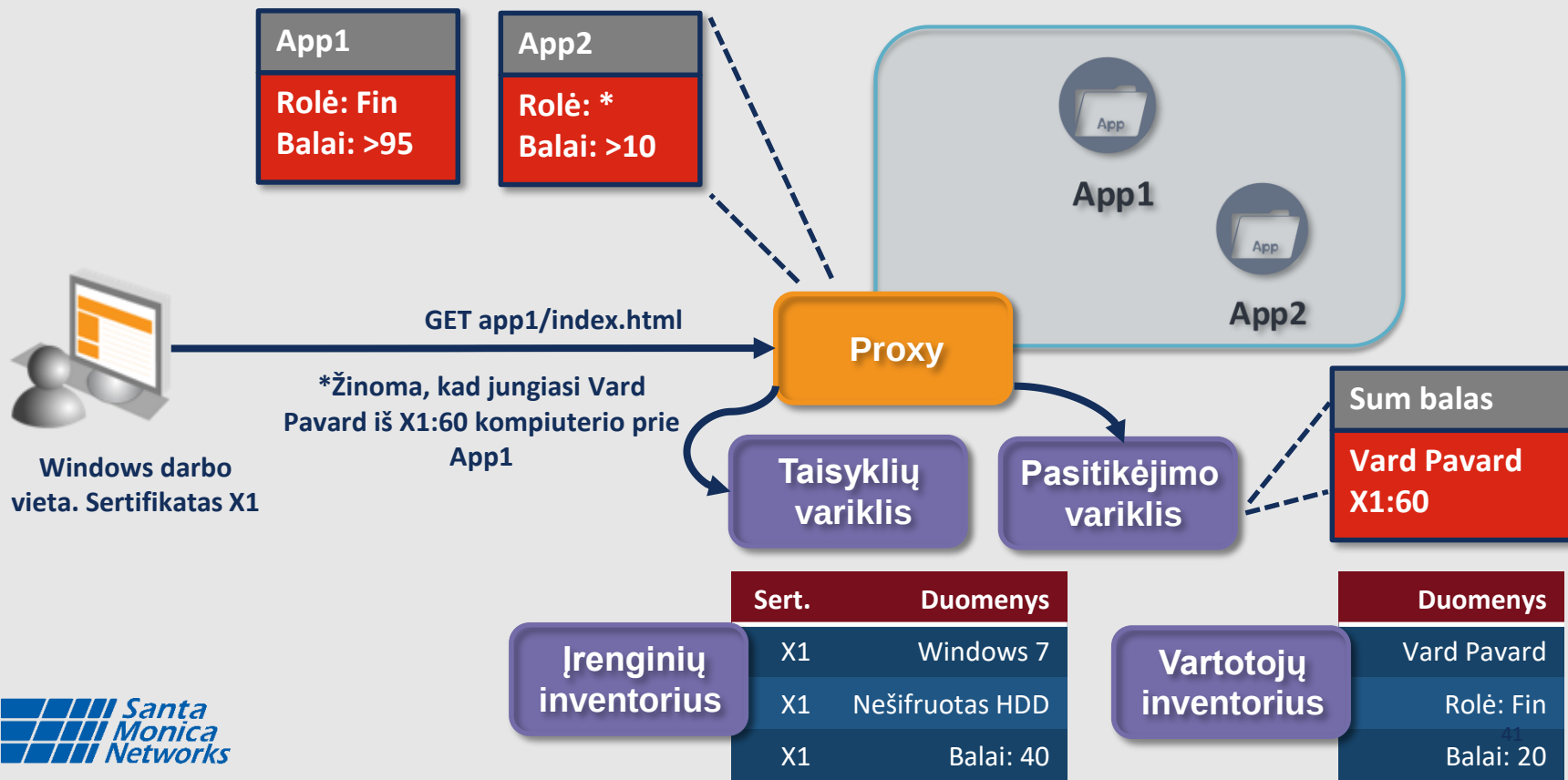
Zero-trust: veikimas



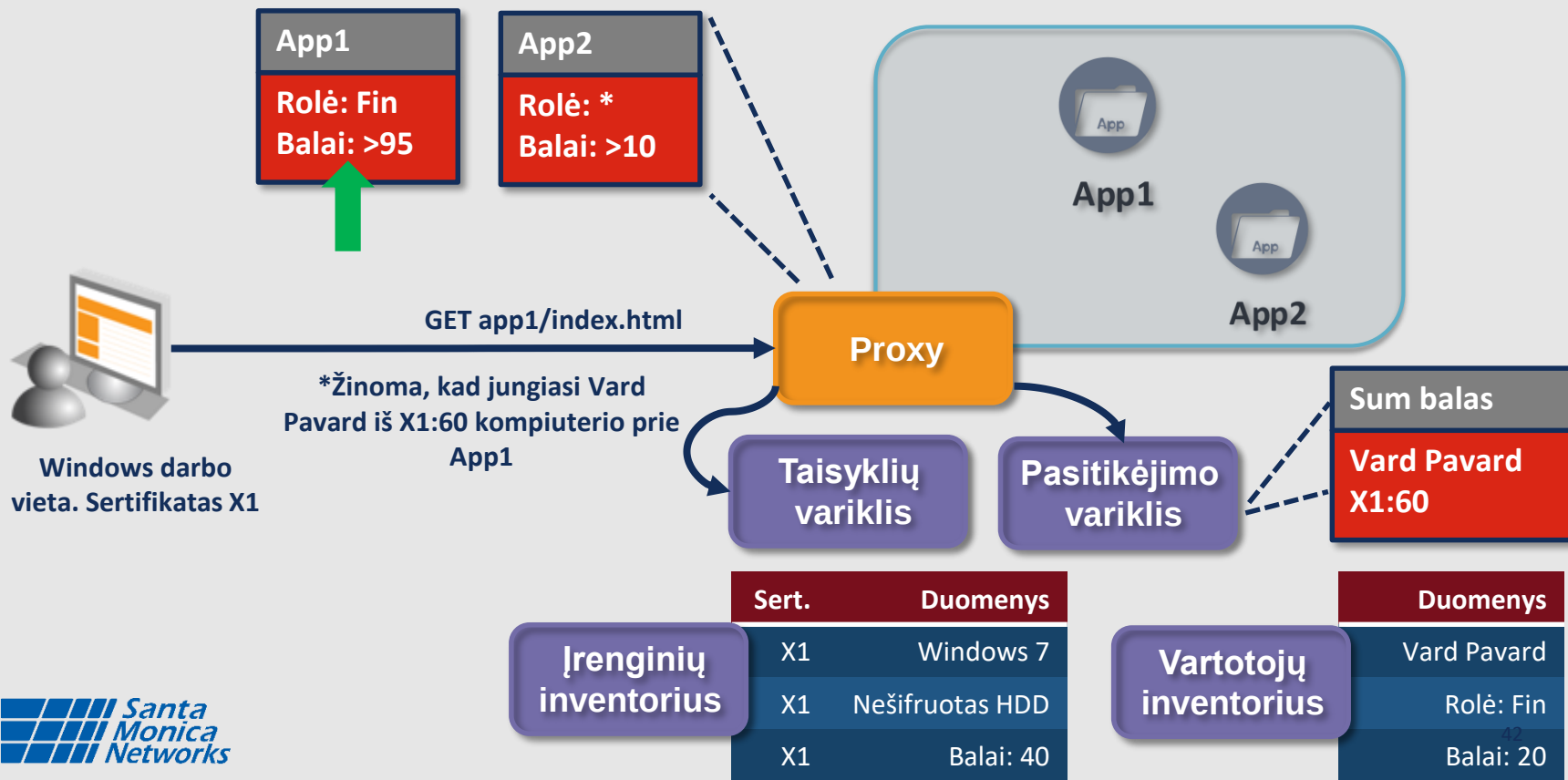
Zero-trust: veikimas



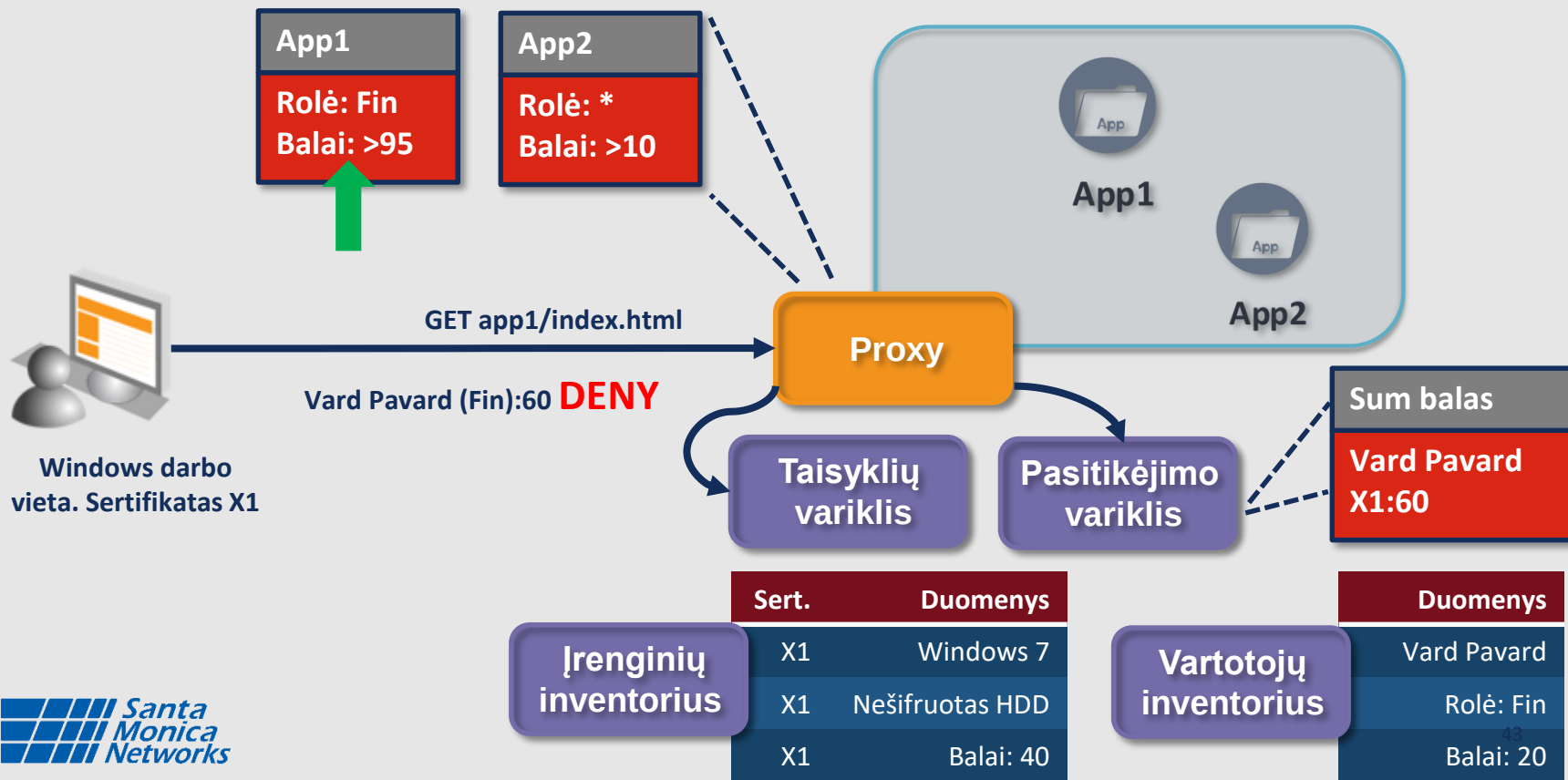
Zero-trust: veikimas



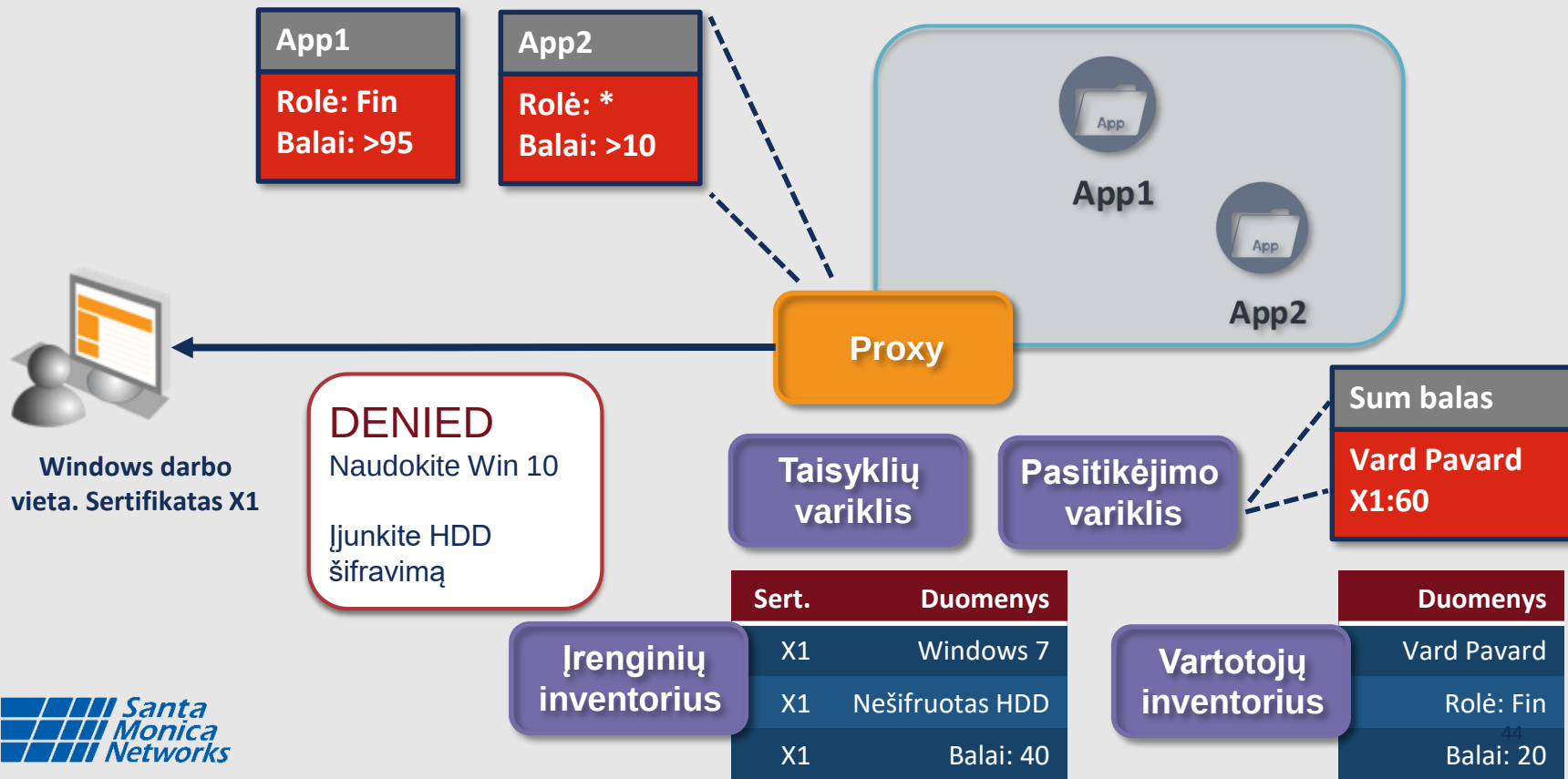
Zero-trust: veikimas



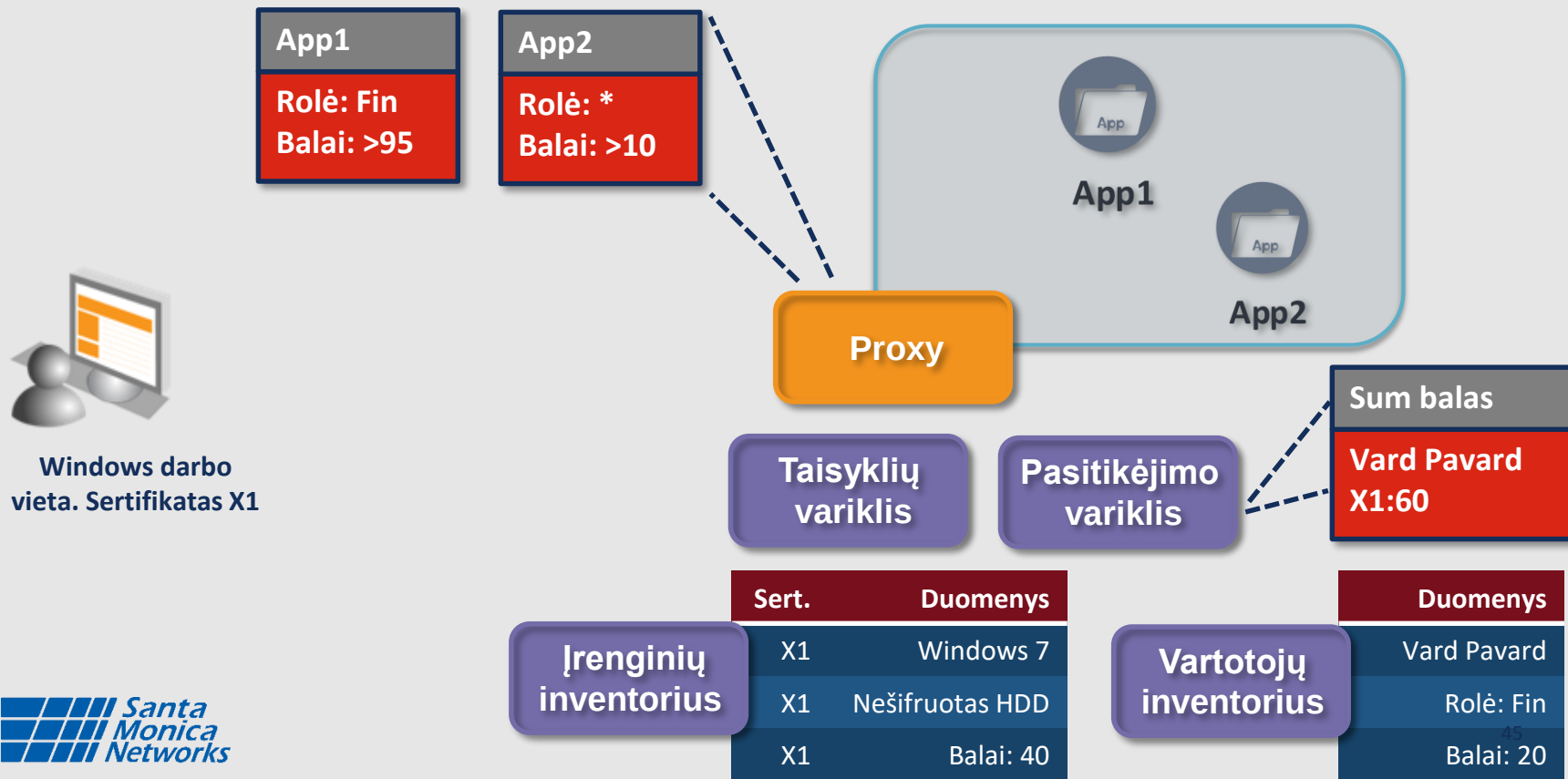
Zero-trust: veikimas



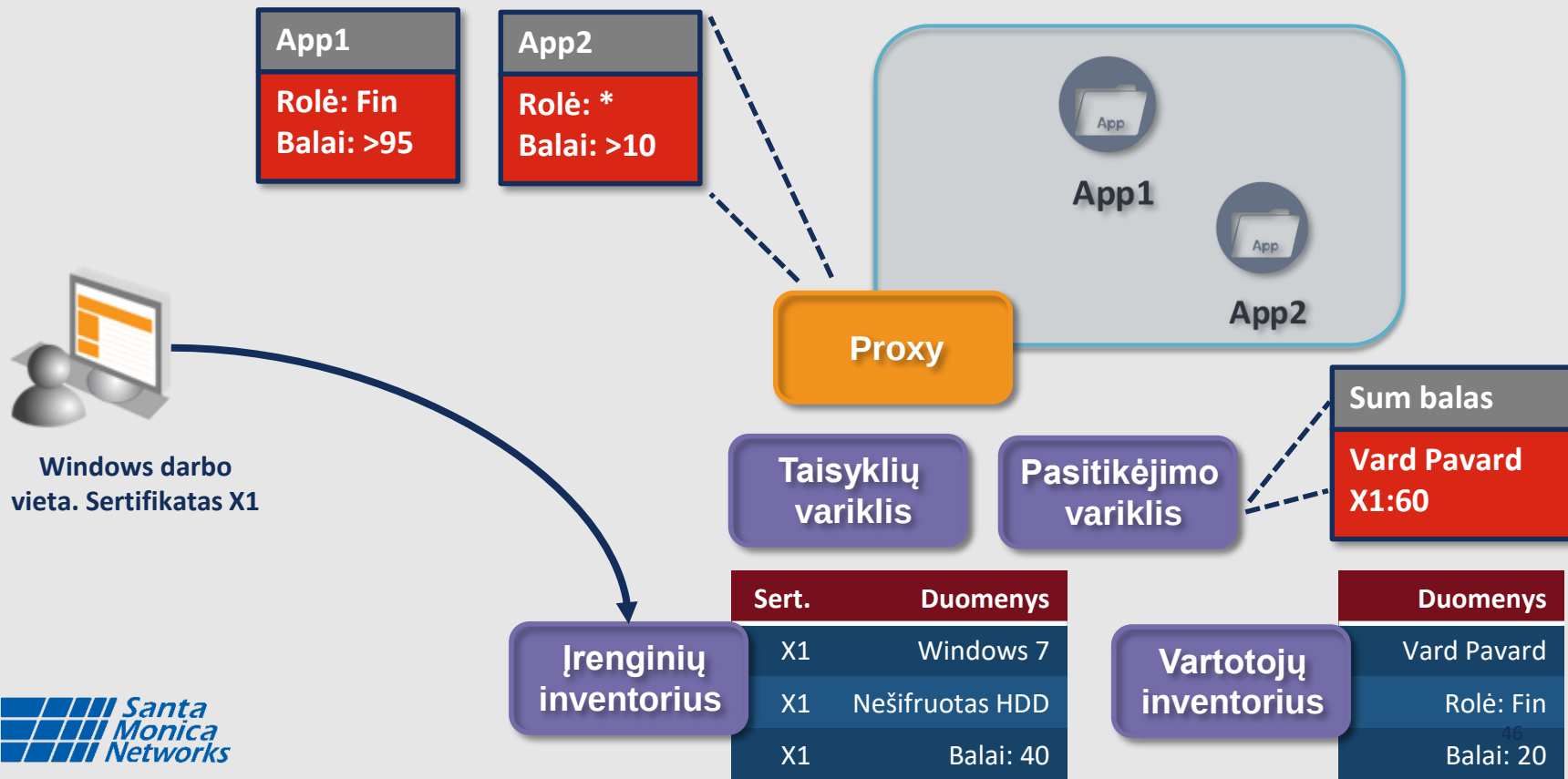
Zero-trust: veikimas



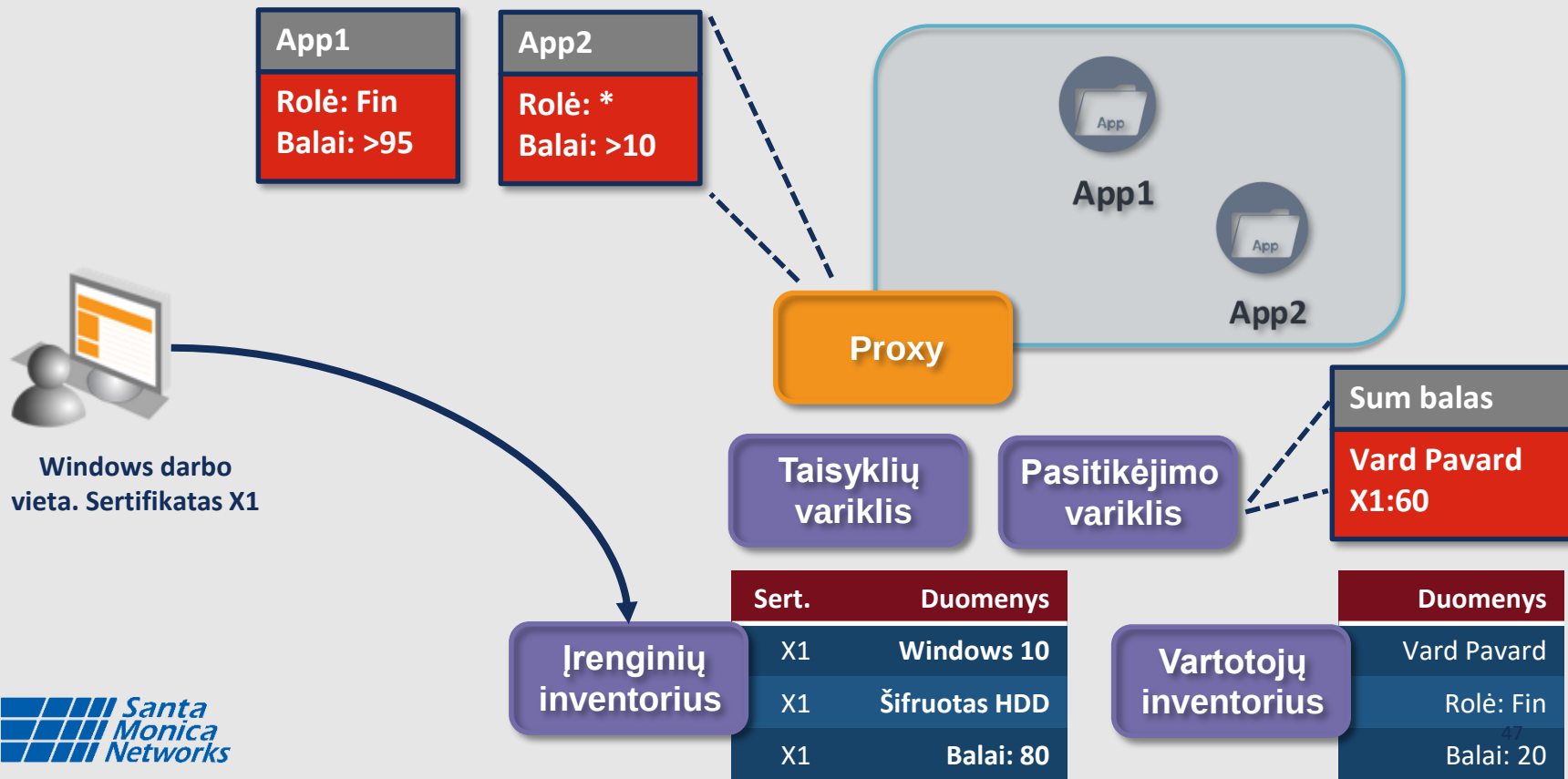
Zero-trust: veikimas



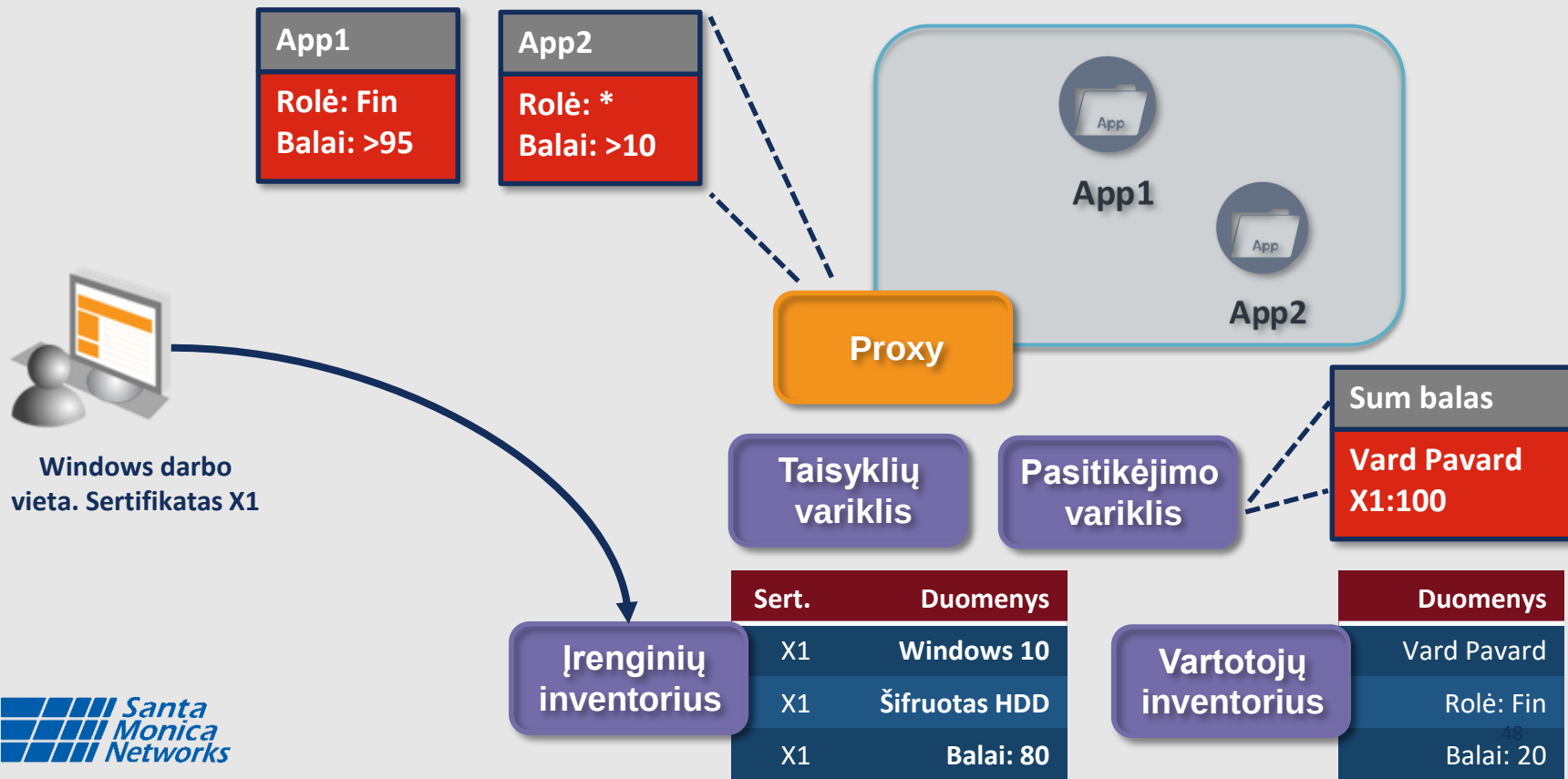
Zero-trust: veikimas



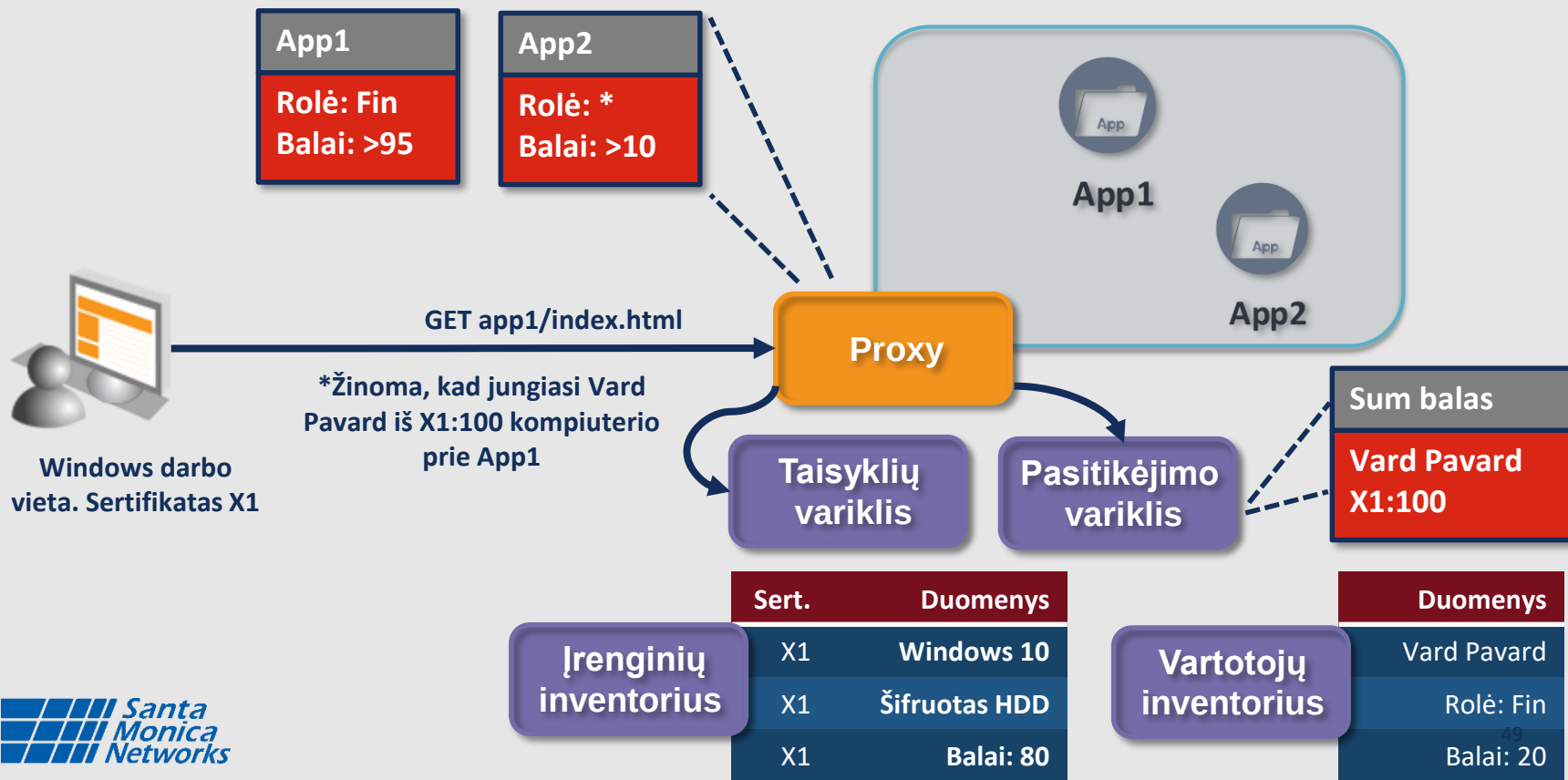
Zero-trust: veikimas



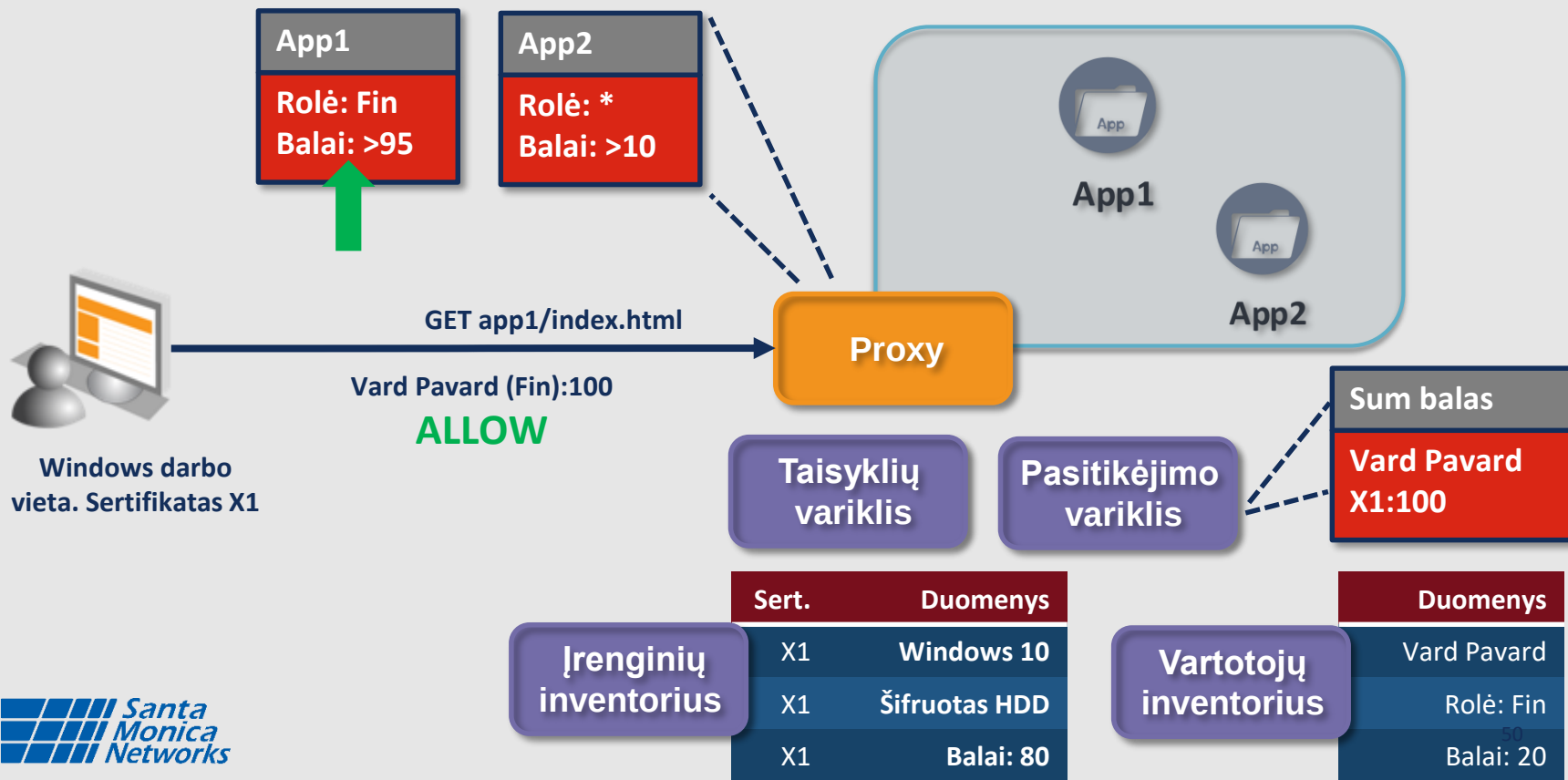
Zero-trust: veikimas



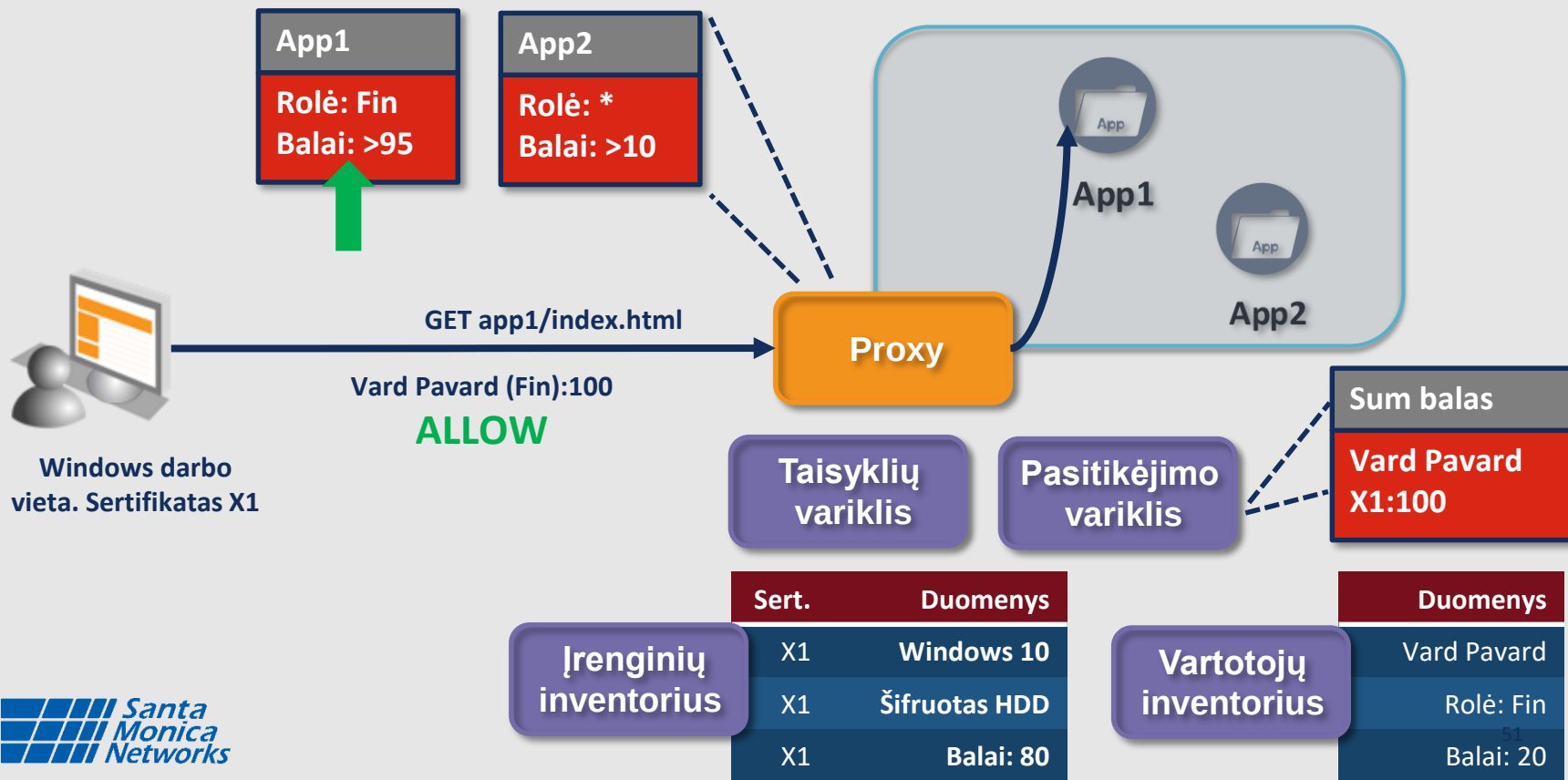
Zero-trust: veikimas



Zero-trust: veikimas



Zero-trust: veikimas



Zero-trust

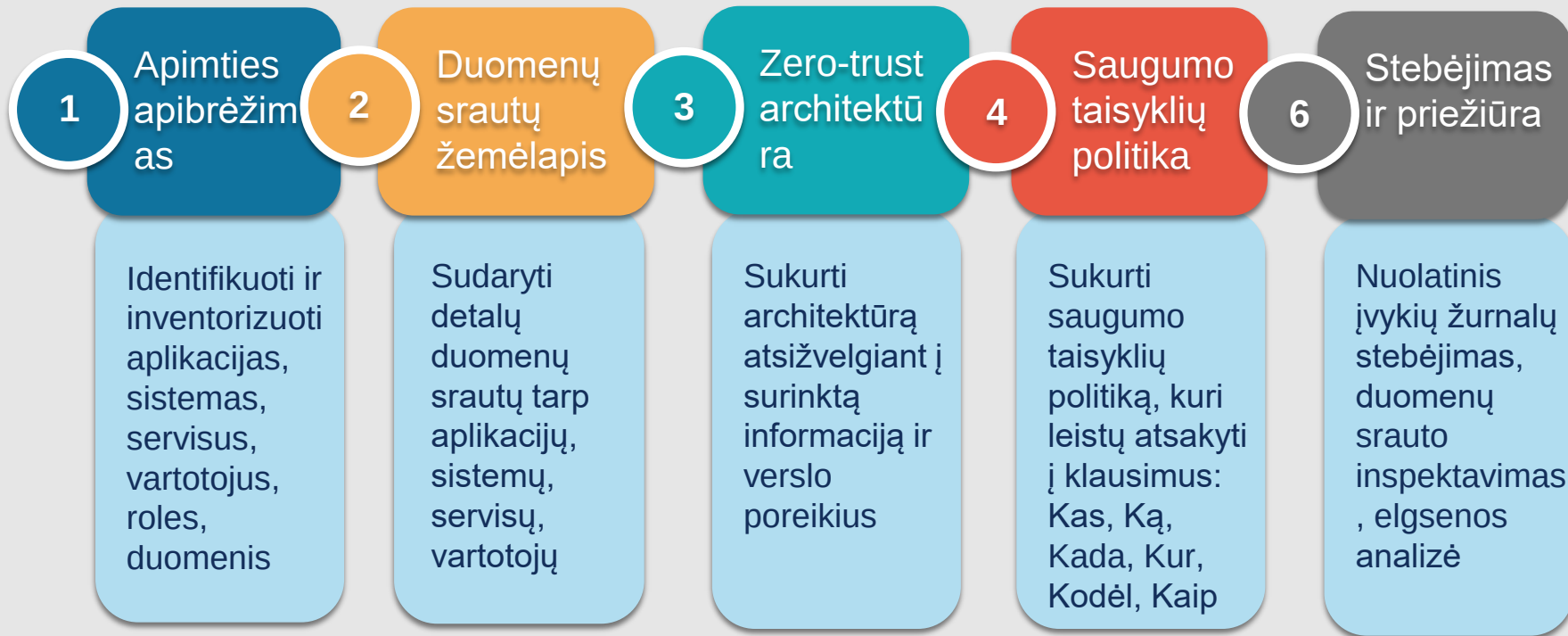
Tai nėra Zero-trust

- Vartotojų nuotolinė prieiga
- Tinklo segmentavimas
- Darbo vietų apsauga
- Įrangos, vartotojų inventorizavimas
- Įrangos, vartotojų saugumo būsenos įvertinimas
- Prieigos kontrolės valdymas
- Duomenų srauto analizė
- Pažeidžiamumų analizė
- Įvykių žurnalų valdymas
- Programinės ir aparatinės įrangos saugios konfigūracijos

Tai yra Zero-trust

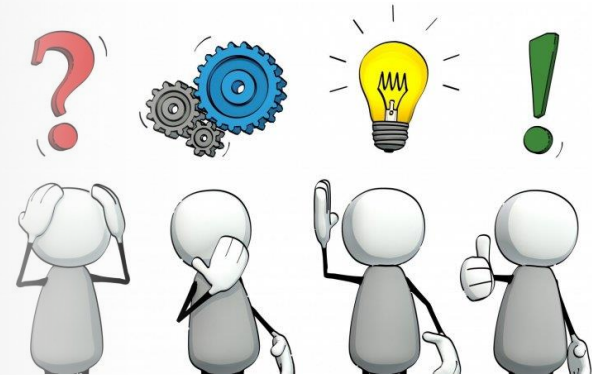
- Vartotojų nuotolinė prieiga
- Tinklo segmentavimas
- Darbo vietų apsauga
- Įrangos, vartotojų inventorizavimas
- Įrangos, vartotojų saugumo būsenos įvertinimas
- Prieigos kontrolės valdymas
- Duomenų srauto analizė
- Pažeidžiamumų analizė
- Įvykių žurnalų valdymas
- Programinės ir aparatinės įrangos saugios konfigūracijos
-
- Dinaminis reitingavimas
- Dinaminės prieigos teisės

Zero-trust: 5 žingsniai link Zero-trust



Zero-trust: klaidos

- Tai galima įdiegti per vieną naktį
- Galima įdiegti nepakeitus mąstymo ir kultūros įmonėje
- Zero-trust įgyvendinamas įdiegus tik vieną iš komponentų
- Pakanka atlikti mikrosegmentavimą
- Pakanka šifruoti duomenis
- Pakanka įdiegti WAF
- Zero-trust užsibaigia ties vartotojų mobilumo klausimo išsprendimu



Zero-trust naudos

- Padidina saugumą iš visų pusių
- Didina duomenų srautų organizacijoje matomumą ir kontrolę
- Didina saugų duomenų, sistemų mobilumą, o tuo pačių verslo mobilumą ir greitį
- Didina vartotojų (darbuotojai, klientai, partneriai) mobilumą. Vartotojai gali jungtis iš bet kur, bet tik įrodžius savo patikimumą, saugumą
- Mažinamas pažeidžiamumo domenai - vartotojai, sistemos gauna prieigą tik prie jiems asmeniškai skirtų aplikacijų
- Trumpina įsibrovimų aptikimo laiką
- Nereikia diegti ir išlaikyti vartotojų tinklų
- Kontroliuojamas šoninis duomenų judėjimas
- Duomenys/sistemos gali būti tiek tradiciniuose DC, tiek pas debesų kompiuterijos paslaugų tiekėjus
- Lengvas sistemų migravimas tarp skirtingų vietų
- Sumažinta įsibrovimo, duomenų nutekimo rizika



Zero-trust nėra technologija ar išbaigtas sprendimas. Zero-trust yra strategija, kurios įgyvendinimui turime naudoti įvairius sprendimus, apjungtus į vieną visumą.

Zero-trust tai yra perėjimas nuo „data-centric“ prie „identity-centric“ architektūros.

Nepasitikėk niekuo, stebėk kiekvieną