RISK CONFERENCE 2019

BUSINESS SOLUTIONS

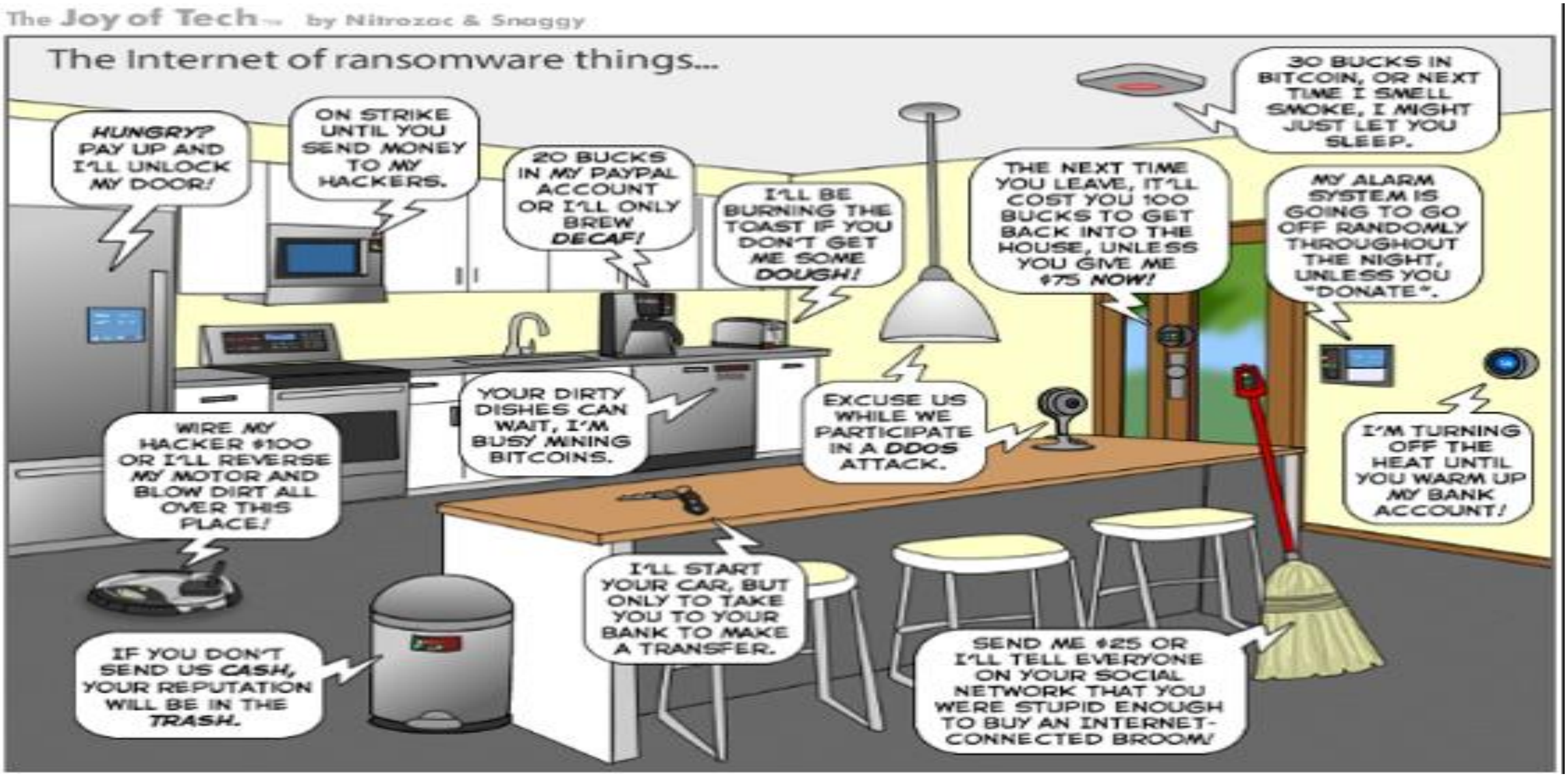
Ste prepričani, da veste, kdo ali kaj se povezuje v vaše omrežje?

Miha Petrač – ADD

Gorazd Kikelj – Selectium/HPE

29. marec 2019

Kaj se povezuje v vaše omrežje?



Nadzor nad povezovanjem v omrežje

- Tradicionalne nastavitve fizičnih vmesnikov
  - Statične ACL/VLAN nastavitve
  - MAC „whiteliste“
  - Port security
- Microsoft CA/PKI -> NPS (Network policy server)

- NAC (network access control)
  - BYOD, Guest portal, profiliranje naprav (CoA), MDM integracija, …

  - Naprave z avtentikacijo
    - 802.1x (EAP/PEAP/TLS/…)
    - MAC
    - Captive portal

Naprave brez avtentikacije

- OnConnect

Aruba ClearPass

VISIBILITY

- Know what's connected on your wired & wireless multivendor environment
- See who is authenticated by role

CONTROL

- Reduce risk and workload through Automation – All devices Authenticated or Authorized – NO UKNOWN DEVICES

RESPONSE

- Change rules for users and devices based on behavior
- Adaptive response brokering with best of breed security solutions

Aruba ClearPass - profiling

- Profiling

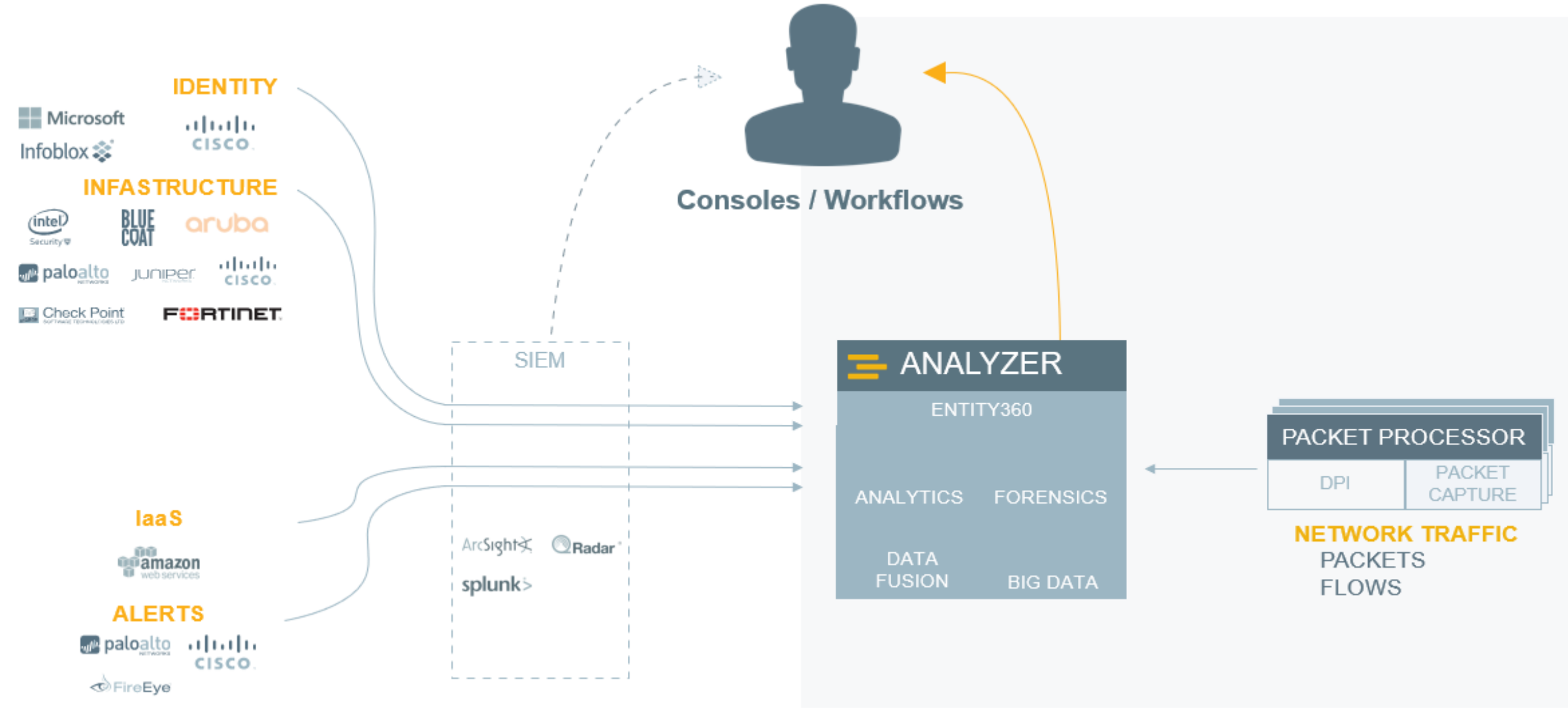
Passive Profiling

- DHCP Fingerprinting (MAC OUI & Certain Options)
  - DHCP Relay or SPAN
- HTTP User-Agent
  - AOS IF-MAP Interface, Guest and Onboard Workflows
- TCP Fingerprinting (SYN, SYN/ACK)
  - SPAN
- ARP
  - SPAN
- Cisco Device Sensor
- Netflow/IPFIX

Active Profiling

- Windows Management Instrumentation (WMI)
- Nmap
- MDM/EMM
- SSH
- ARP Table
  - SNMP
- MAC/Interface Table
  - SNMP
- CDP/LLDP Table
  - SNMP

Aruba IntroSpect - UEBA



Aruba ClearPass in IntroSpect

1. Discover and Authorize

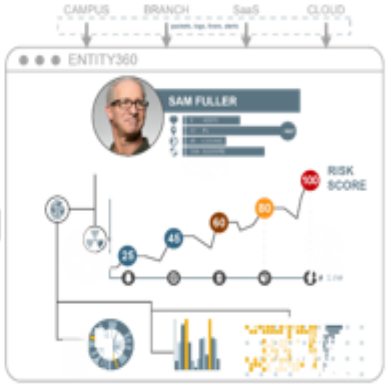
Wired/Wireless
Device Authentication

ClearPass
Policy Manager

User/Device
Context

Actionable
Alerts

IntroSpect UEBA



Entity360 Profile
with Risk Scoring

2. Monitor and Alert

3. Decide and Act

ClearPass Real-time Policy-based Actions

- Real-time quarantine
- Re-authentication
- Bandwidth Control
- Blacklist

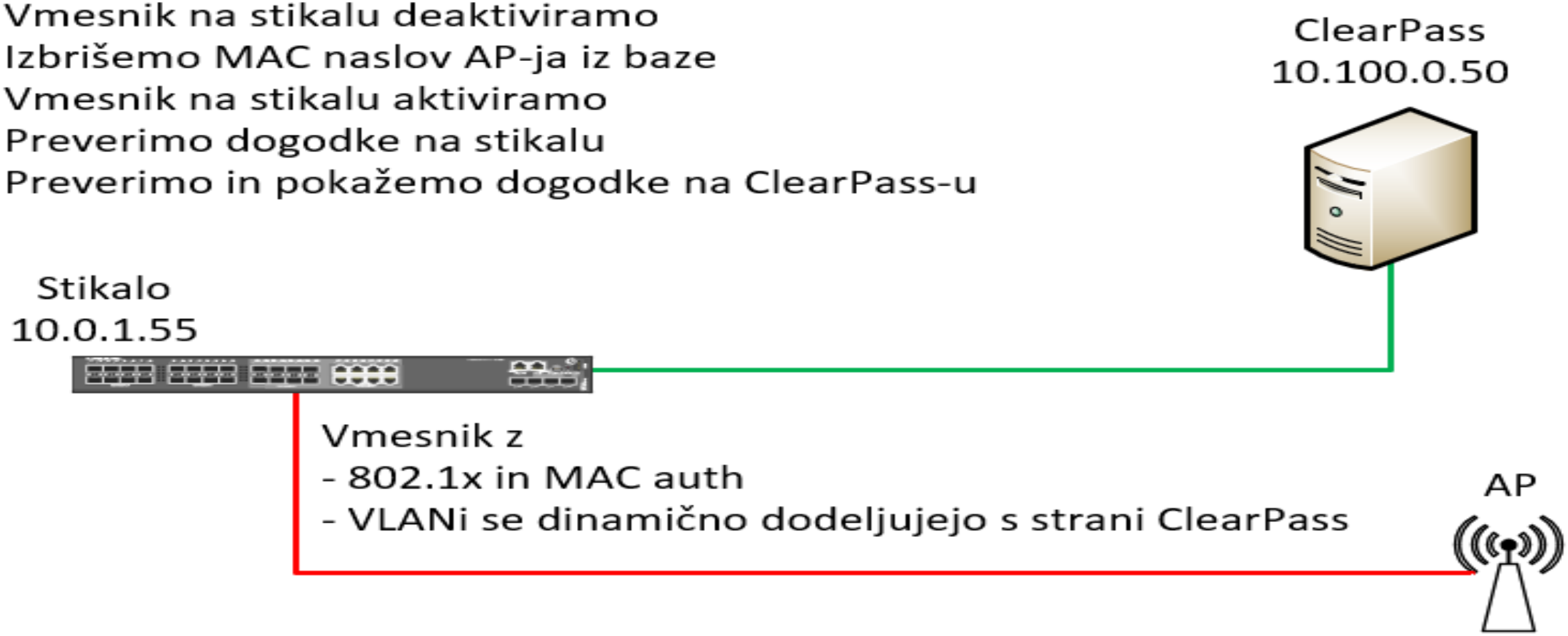
Zakaj Aruba ClearPass

- Vidljivost v realnem času, nadzor in možnost odziva (brez dodatnih agentov)
- Neodvisnost od proizvajalca opreme in integracija z drugimi ponudniki (PaloAlto, McAfee, AirWatch/MobileIron, …)
- Enostavna registracija BYOD naprav
- Razširljivost (clustering)
- Uporaba veliko dodatnih virov informacij pri pripravi politike (2FA, MDM, …)
- Profiler - IoT
- Ena rešitev za vse načine avtentikacije
  - Osnovane na AAA
    - MAC avtentikacija
    - 802.1x (uporabnik/geslo in certifikat)
    - Captive Portal
  - Brez AAA
    - OnConnect

DEMO - shema

Koraki prikaza za DEMO

- Vmesnik na stikalu deaktiviramo
- Izbrišemo MAC naslov AP-ja iz baze
- Vmesnik na stikalu aktiviramo
- Preverimo dogodke na stikalu
- Preverimo in pokažemo dogodke na ClearPass-u



?

add
BUSINESS SOLUTIONS

Tbilisijska 85
1000 Ljubljana
Slovenija

info@add.si
+386 1 1 479 00 11