

# Digitalizacija, Mobilnost.



Kaj pa varnost in nadzor dostopa uporabnikov?

---

Damir Benedičič, Samo Kotnik  
S&T Slovenija



# Multi-device user experience

A photograph of a desk setup illustrating multi-device user experience. In the center is a large Samsung monitor displaying a website. To its right is a silver laptop showing a gallery of images. In the foreground, a tablet and a smartphone are visible. A white tower PC is on the left. The text 'Multi-device user experience' is overlaid in white on a red background.



**500B**

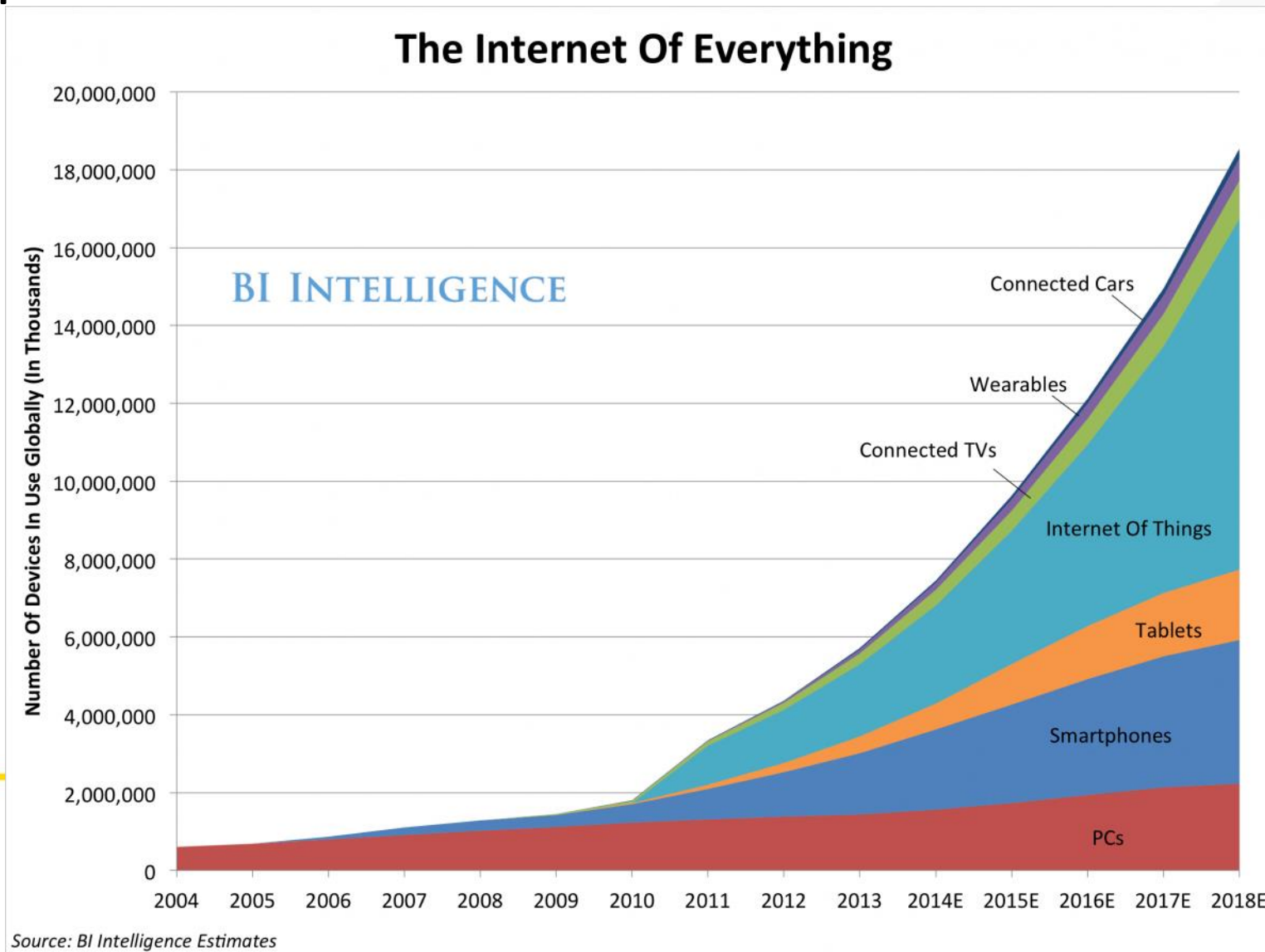
devices will be connected worldwide

**70%**

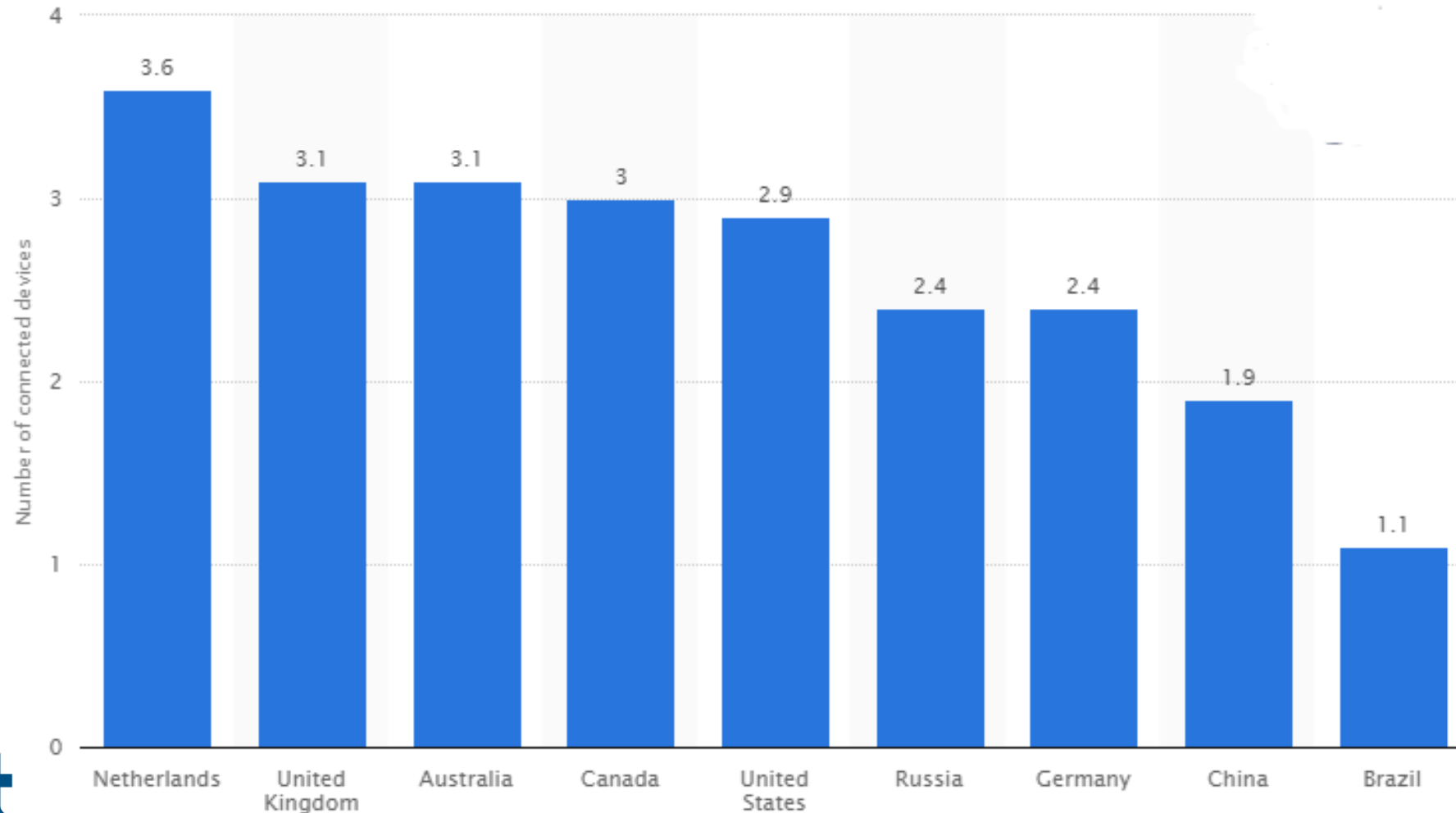
of professionals will conduct their work on personal smart devices by 2018



# Kaj pa trendi?



# Število naprav na uporabnika 2016



# Digitalna Transformacija je vroča



“A century ago the average person could only create and access a small amount of information. Now, ordinary people not only have access to huge amounts of data, but are also able to create gigabytes of data themselves and, potentially, publish it to the world via the Internet, if they choose to do so.”

University of California, Berkeley

# Grozijo nove nevarnosti



„The interconnection of billions of devices with IT and operational systems will introduce a new world of security risks for business, consumers and governments.“

PWC, State of Cybercrime Survey

# Internet of Things



- Connected Car
- Connected House
- Connected Fridge
- Connected TV
- Connected Pet
- Werables...
- Connected machines (proizvodnja)
- Green energy (objekti, retail)
- Logistika (transport)
- SCADA (proizvodnja, energetika)
- IDM (banke, zavarovalnice)
- Inventar (npr. bolnice)



# 100% varnosti ni (sta pa 2 ekstrema)



Vse je odprto

Vse je zaprto



Veliko tveganje

Veliko administracije



90% podjetij ne pozna naprav, ki se povezujejo v omrežje



# Smo pripravljeni?

- Upoštevati zahteve uporabnikov
- Upoštevati zahteve standardov in regulative
- Zaščititi informacije podjetja
- Upoštevati bistveno povečanje števila naprav
- Upoštevati M2M komunikacije, ki prihajajo in bodo del nas

Bomo še vedno zaupali stari arhitekturi in konceptom?

---

# Direktor



- Sem videl kolega, ki ima vse podatke na tablici tudi jaz želim tako
- Zakaj moram vedno vnašati geslo kamorkoli se prijavim ali se ne da bolje urediti



# Marketing



- Želijo captive portal
- Želijo nagovarjati kupce
- Želijo promovirati „brand“ kjerkoli je možno
- Želijo informacije



# CSO



- Skladnost
- Varnost
- Birokracija



CISCO  SEC

# R&D



- Vedno nekaj hoče
- K njemu vedno hodijo zunanji izvajalci
- Stalno potrebuje strežnike, nove aplikacije, nove zahteve

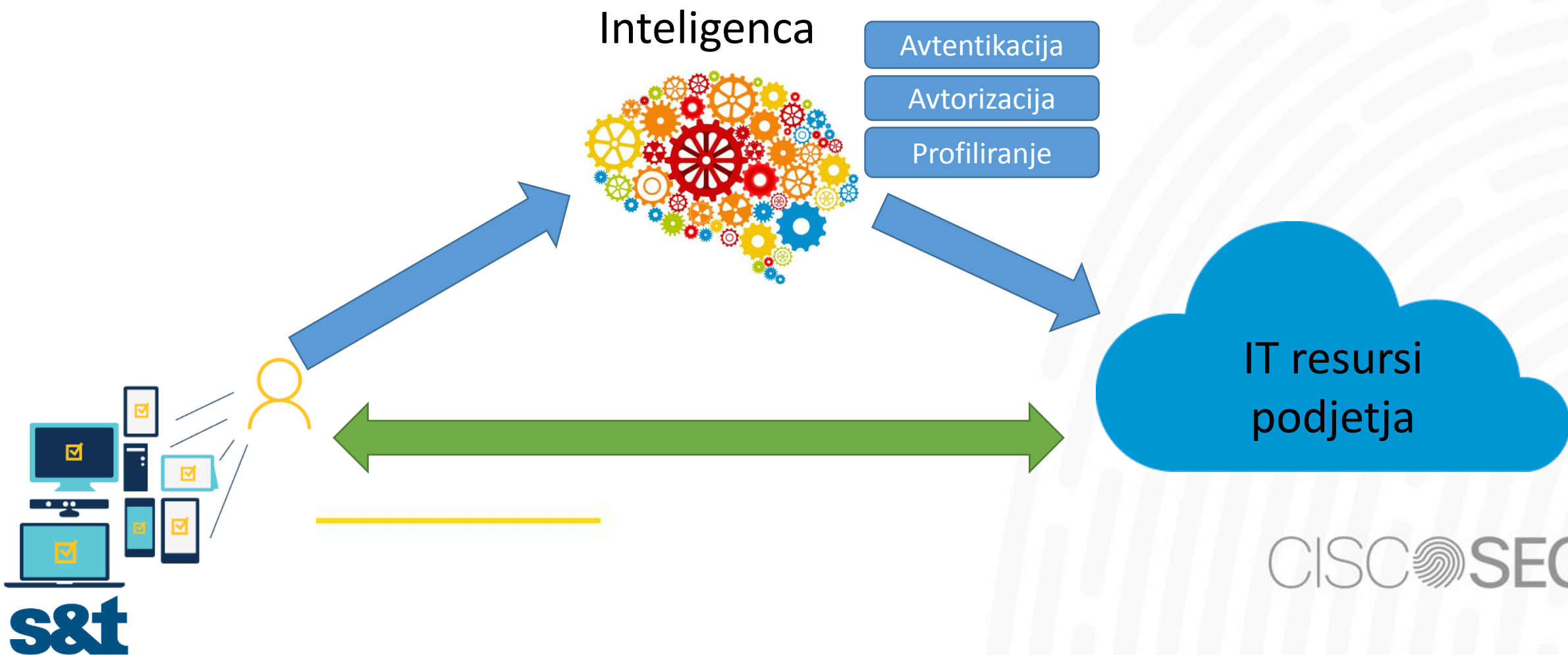


# Inženýr



CISCO  SEC

# Sodobni pristop dostopa



# Cisco ISE



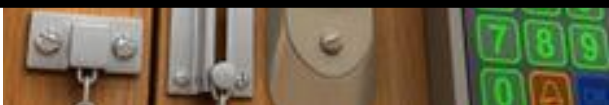


# Kolikšna je prava raven varnosti?



“Those who surrender freedom for security will not have, nor do they deserve, either one.”

— Benjamin Franklin



# Kolikšen je pravi pristop?

- Enostavna uporaba
- Učinkovit
- Varen
- Centraliziran
- Visoko razpoložljiv



# Tipi dostopa do omrežnih virov?

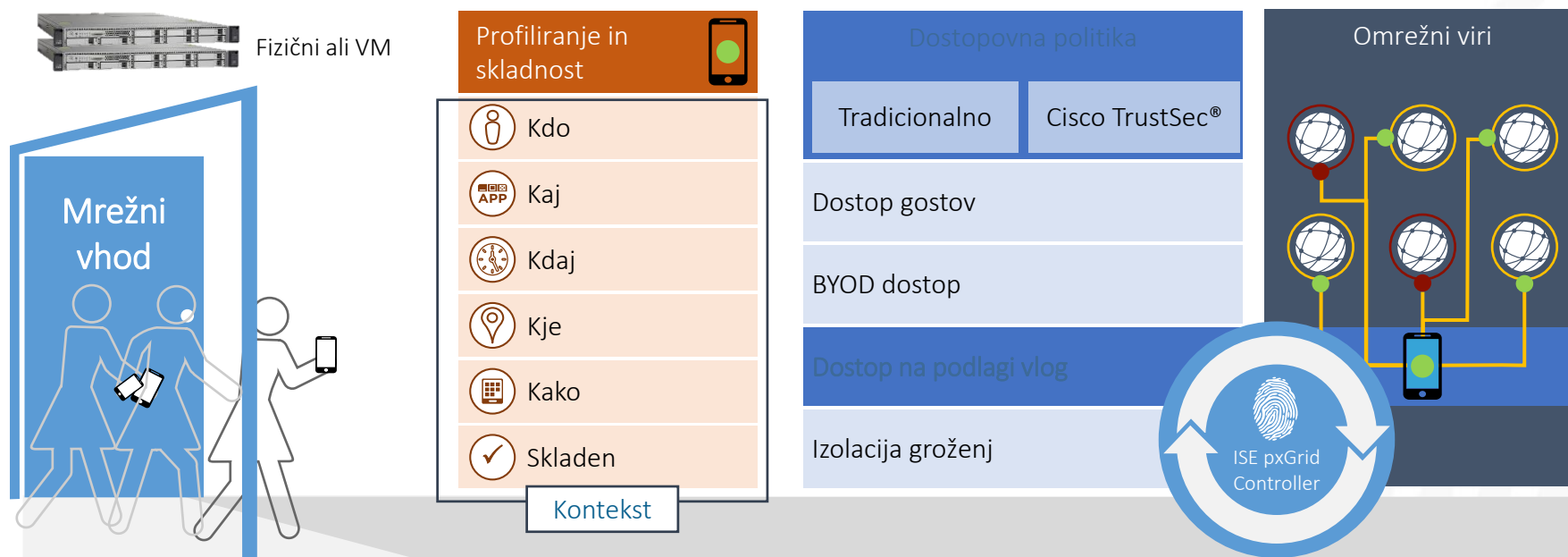
- Brezžični
- Žični
- VPN
- Gosti



# ISE splošno



Centralizirana varnostna rešitev, ki avtomatizira dostop na podlagi različnih podatkov o uporabnikih/napravah do omrežnih virov in deli pridobljene podatke z drugimi napravami



# Odločitev na podlagi informacije



Pomanjkljiva informacija	Kontekst	Obširna informacija
IP naslov 192.168.1.51	Kdo	Zvonko
Neznano	Kaj	Tablica, iOS, v. 9.1x
Neznano	Kje	Prvo nadstropje
Neznano	Kdaj	12:40, 4.4.2016
Neznano	Kako	Brezžični dostop
Katerikoli uporabnik, naprava, na katerikoli lokaciji dobi dostop do omrežja	Rezultat	Znan uporabnik, na dovoljeni napravi, iz prave lokacije dobi <b>pravilen dostop</b>



# ISE komponente:



# Avtentikacija



<input checked="" type="checkbox"/>	MAB-Continue	: If Wired_MAB <b>OR</b> Wireless_MAB	Allow Protocols : Default Network Access	and	Edit   ▾
<input checked="" type="checkbox"/>	Default	: use Internal Endpoints			
<input checked="" type="checkbox"/>	Dot1X	: If Wireless_802.1X	Allow Protocols : PEAP_OR_EAPTLS	and	Edit   ▾
<input checked="" type="checkbox"/>	Default	: use ID_src_sequence			
<input checked="" type="checkbox"/>	Default Rule (If no match)	: Allow Protocols : Default Network Access	and use : Guest		Edit   ▾

**Authentication Search List**

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available		Selected
Internal Endpoints	>	AD
OTP_Server	<	Internal Users
	>>	Guest Users
	<<	

**Identity Source Details**

NameID\_src\_sequence

**Options**

- If authentication failed **REJECT**
- If user not found **REJECT**
- If process failed **DROP**

# Avtorizacija



## Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

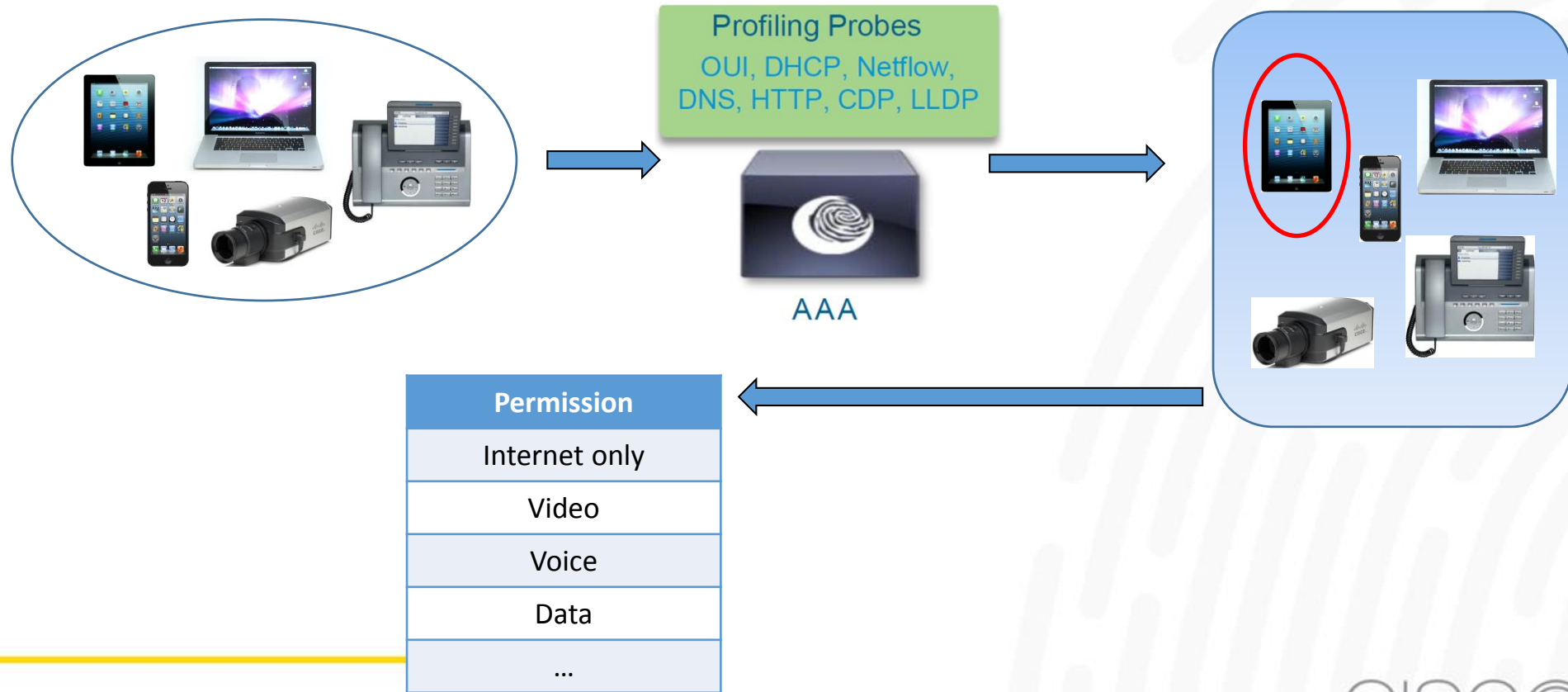
First Matched Rule Applies

### Exceptions (0)

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Profiled Cisco IP Phones	if <b>Cisco-IP-Phone</b>	then Cisco_IP_Phones
✓	Employees	if demo.local:ExternalGroups EQUALS demo.local/Users/employees	then Employee
✓	Contractors	if demo.local:ExternalGroups EQUALS demo.local/Users/contractors	then Contractor
✓	Default	if no matches, then DenyAccess	

Authorization result	Policy
Employee	VLAN / dACL / SGA
Contractor	VLAN / dACL / SGA

# Profiliranje



# Profiliranje



Rule Name	Conditions (identity groups and other conditions)	Permissions
Employee - Smart Phones	if (HTC-Phone OR BlackBerry OR Apple-iPhone OR Android) AND ADusers	then V601
Employee - CorpPC	if Workstation AND ADusers	then V603

Permission	Description	Policy
V601	Employee – Smart Phone	dACL = 601 (VLAN, SGA)
V603	Employee – CorpPC	dACL = 603 (VLAN, SGA)

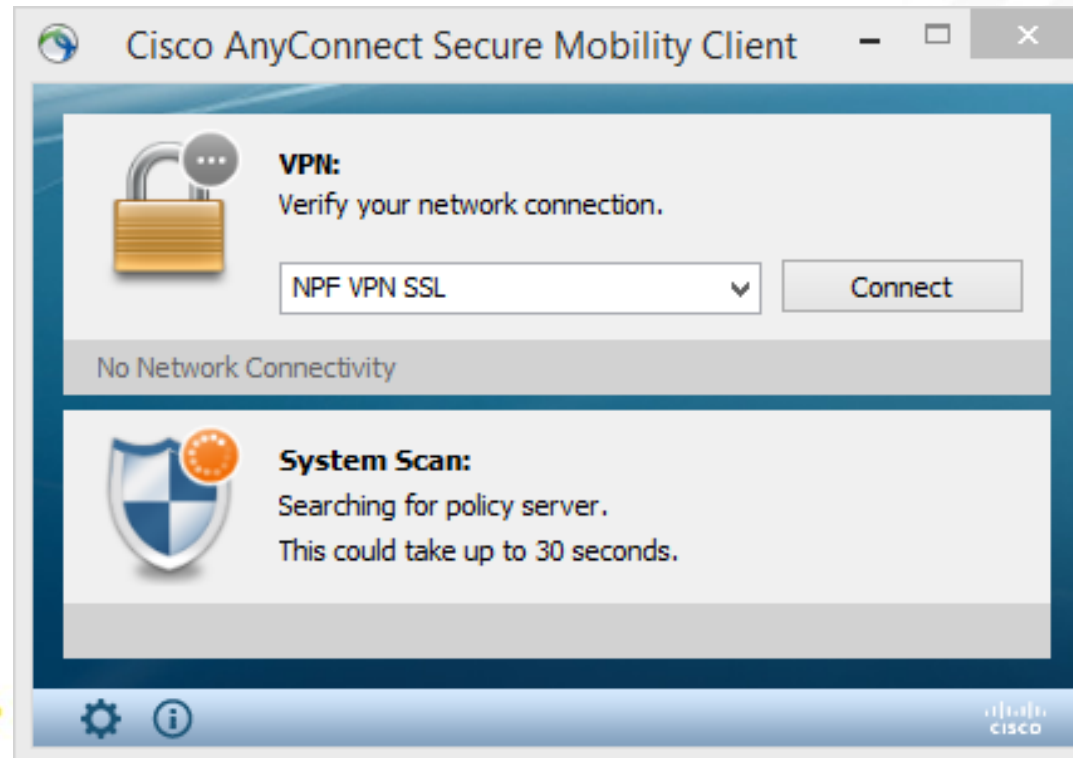


# Preverjanje skladnosti



**Preverjanje skladnosti** = ali kandidat izpolnjuje zahtevane varnostne standarde?

- Antivirus
- Antispyware
- Registry vnosi
- Datoteke, Procesi
  - prisotnost / status
- Windows Update
  - Kritični popravki,...



# Politika



Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Profiled Cisco IP Phones ISE	if <b>Cisco-IP-Phone</b>	then Cisco_IP_Phones_ISE
✓	Printers	if <b>HP-Color-LaserJet-4700 OR Xerox-Phaser-6010n</b>	then Printers
✓	Corp Workstation	if <b>Wireless_Access_ISE OR Wired_802.1X_ISE</b> AND CorpAD:ExternalGroups EQUALS cisco.com/Users/Domain Computers AND Network Access:EapTunnel EQUALS EAP-FAST AND Network Access:EapAuthentication EQUALS EAP-TLS AND Network Access:EapChainingResult EQUALS User failed and machine succeeded AND <b>Session:PostureStatus EQUALS Compliant</b> AND <b>NewYork</b>	then AD_Login
✓	Employee and Corp_Workstation	if <b>Wireless_Access_ISE AND Wired_802.1X_ISE</b> AND CorpAD:ExternalGroups EQUALS cisco.com/Users/Domain Users AND Network Access:EapTunnel EQUALS EAP-FAST AND Network Access:EapAuthentication EQUALS EAP-TLS AND Network Access:EapChainingResult EQUALS User and machine both succeeded AND <b>Session:PostureStatus EQUALS Compliant</b> AND <b>NewYork</b>	then Employee
✓	Registered Devices	if <b>RegisteredDevices</b> AND <b>Wired_802.1X_ISE</b> AND Network Access:EapAuthentication EQUALS EAP-TLS AND CERTIFICATE:Subject Alternative Name EQUALS Radius:Calling-Station-ID )	then BYOD Access
✓	Personal Devices	if <b>Employee</b> AND Network Access:EapAuthentication EQUALS EAP-MSCHAPv2	then BYOD Provisioning
✓	VPN	if <b>VPN</b>	then VPN Employee
✓	Guest	if <b>Guest</b> AND <b>Business Hours</b>	then Internet Only
✓	Default	if no matches, then <b>DenyAccess</b>	

# Nekateri možni scenariji

- ACS -> ISE
- Skladnost (PCI,DSS)
- Dostopi za goste



# Scenarij 1



- ACS -> ISE
  - Razlog:
    - ACS je proti koncu razvoja
    - ACS zahteva large deployment licenco za upravljanje več kot 500 naprav
    - ISE 2.0 TACACS+ licenca nima omejitve števila naprav
    - ISE podpira napredne funkcionalnosti
  - Rezultat: Stranka je preselila vse funkcionalnosti na ISE. Kupljene so bile dodatne licence, ki bodo uporabljene za profiliranje naprav in kreiranje politike na podlagi tipa naprave.

# Scenarij 2



- Skladnost (PCI,DSS)

- Razlog:

- Zahteva lastnika po uveljavitvi 802.1x v žično omrežje

- Rezultat:

- Avtentikacija delavnih postaj na podlagi Active Directory domene
    - Avtentikacija Citrix klientov s pomočjo certifikatov

- Nadgradnja:

- Smo v fazi testiranja preverjanja skladnosti prenosnikov



# Scenarij 3



- Dostopi za goste

- Razlog:

- K stranki prihaja več različnih tipov gostov, ki potrebujejo dostop do omrežnih storitev
    - Stranka ne želi imeti ločene infrastrukture za goste

- Rezultat:

- Implementacija portalov za brezžične in žične uporabnike
      - Uporabniki dobijo dostop, ki jim je dodeljen s strani administratorja portala gostov
      - Različni avtorizacijski profili za različne tipe strank



# Zaključek

- Pričakovanja uporabnikov za dostop do omrežnih storitev se spreminjajo
  - Poljubna naprava, lokacija, način dostopa,...
- Administratorji težko zagotovijo varnost in enostavno uporabo ob enem
  - Uporaba različnih baz uporabnikov, certifikatov, različni protokoli, pravice,...
- Možen odgovor na ta izziv je Cisco Identity Services Engine

# Zaključek

- So pa seveda tudi druge rešitve...





# Hvala

---

Damir Benedičič, Samo Kotnik  
S&T Slovenija

[Damir.benedicic@snt.si](mailto:Damir.benedicic@snt.si)

[Samo.kotnik@snt.si](mailto:Samo.kotnik@snt.si)

