



Ridefiniamo il
concetto di
sicurezza del
network
con il NAC

BLUDIS®

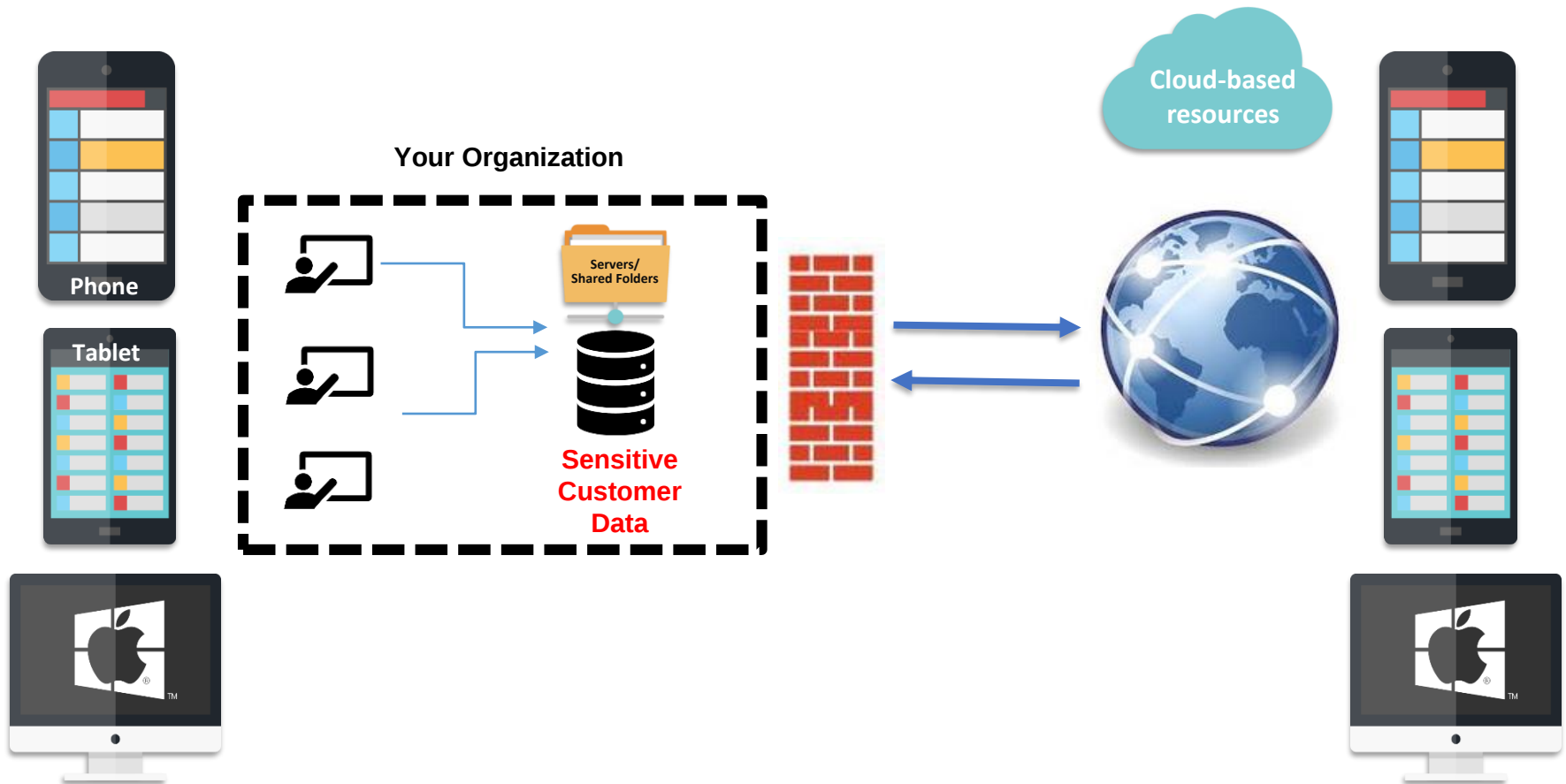
VALUE ADDED DISTRIBUTOR

AGENDA

- Perchè la sicurezza IT fallisce senza il NAC
- Il Nac nel lavoro di tutti i giorni
- La soluzione Macmon Nac



Security



IT Security Best Practices



Security Policy

Authentication

Data Classification

Data Security and Availability

Password Management

Privilege Account Management

Account Management

Router, Firewall and Network Security

Client and Server Security

Vulnerability and Hardening

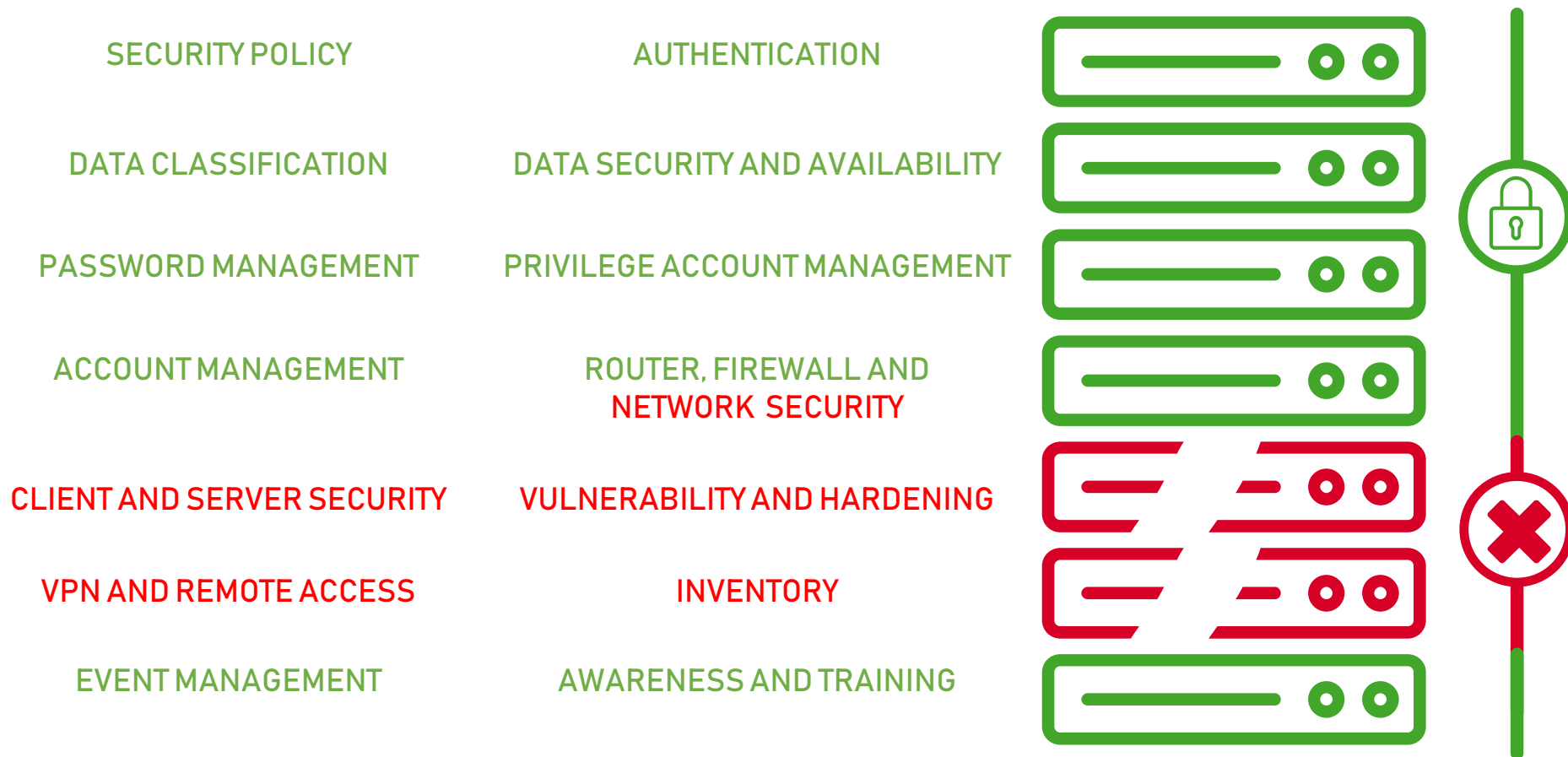
VPN and Remote Access

Inventory

Event Management

Awareness and Training

Vulnerabilità



Perchè la sicurezza IT fallisce senza NAC



Perchè la sicurezza IT fallisce senza NAC

Un consulente può collegare alla rete un pc infetto.



Perchè la sicurezza IT fallisce senza NAC

Possiamo sferrare un attacco sfruttando una vulnerabilità.



Perchè la sicurezza IT fallisce senza NAC

Un malware può infettare una macchina e propagarsi.



Perchè la sicurezza IT fallisce senza NAC

E' possibile eludere il Sistema di DLP e le policy utilizzando un dispositivo personale.



La sfida



Nuovi dispositivi, **invisibili** ai livelli di sicurezza già implementati, potranno connettersi alla rete in ogni momento.



PROPRIO DA QUESTI
DISPOSITIVI POTREBBE
PARTIRE IL PROSSIMO
ATTACCO

Regulations and NAC



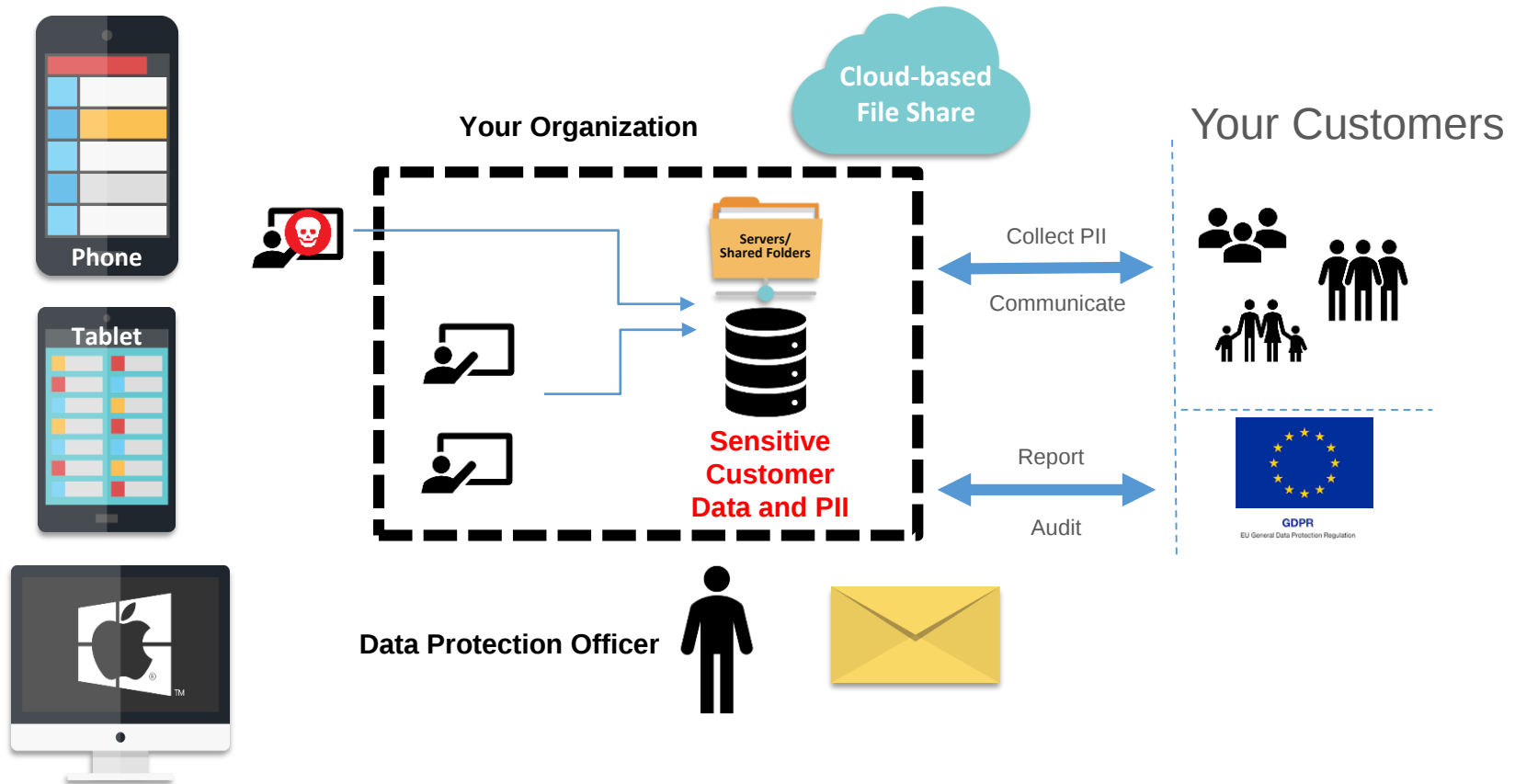
SANS
20
CRITICAL
SECURITY
CONTROLS



Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

**MISURE MINIME DI SICUREZZA ICT E
TRATTAMENTO DATI**

GDPR: Privacy e data protection by design



Global NAC Market 2018 -2022

MARKET GROWTH

The global network access control market is expected to grow at a CAGR of above 27% during the forecast period.



KEY DRIVER

Growing awareness of sophisticated data safety issues and threats.

In EMEA, the presence of some of the most advanced economies with a mature industrial as well as private sector is driving growth in the NAC market.

Source Technavio

BLUDIS | VALUE
ADDED
DISTRIBUTOR

bludis.it

IL NAC nel lavoro quotidiano

NETWORK ACCESS CONTROL - NAC

Hai **Visione** completa della tua infrastruttura di rete?



Sei **consapevole** di tutti i dispositivi connessi alla rete?



Tutti i dispositivi connessi alla rete **rispettano le policy aziendali**?



E' possibile **gestire l'accesso dei dispositivi guest e BYOD** in maniera sicura nella tua rete?



IL NAC nel lavoro quotidiano

Identificazione di tutti i dispositivi

Authorized MACs **0** Unauthorized MACs **405** Detected MACs **405** Client Compliance macmon-Agents IP-MAC assignments

Edit View **Graphic**   20 **1-20 of 95 (filtered of 412)** «

MA	Manufacturer	IP address
☐		
☐ B4	APPLE, INC.	172.30.0.103
☐ AC	SAMSUNG ELECTRO-MECHANICS(THAILAND)	172.30.0.39
☐ 3C	SAMSUNG ELECTRONICS CO.,LTD	172.30.0.120
☐ C4-86-E9-C8-B5-38	HUAWEI TECHNOLOGIES CO.,LTD	172.30.0.40
☐ C4-17-FE-15-D4-19	HON HAI PRECISION IND. CO.,LTD.	172.30.0.172
☐ C0-D3-C0-EA-1B-17	SAMSUNG ELECTRONICS CO.,LTD	172.30.0.33
☐ 2C-0E-3D-FC-2E-FF	SAMSUNG ELECTRO-MECHANICS(THAILAND)	172.30.0.74
☐ 74-67-F7-A0-E0-0D	EXTREME	

Number of MAC addresses per deactivated

Number of MAC addresses per vendor

Number of MAC addresses per network device

Number of MAC addresses per access VLAN

Number of MAC addresses per MAC VLAN

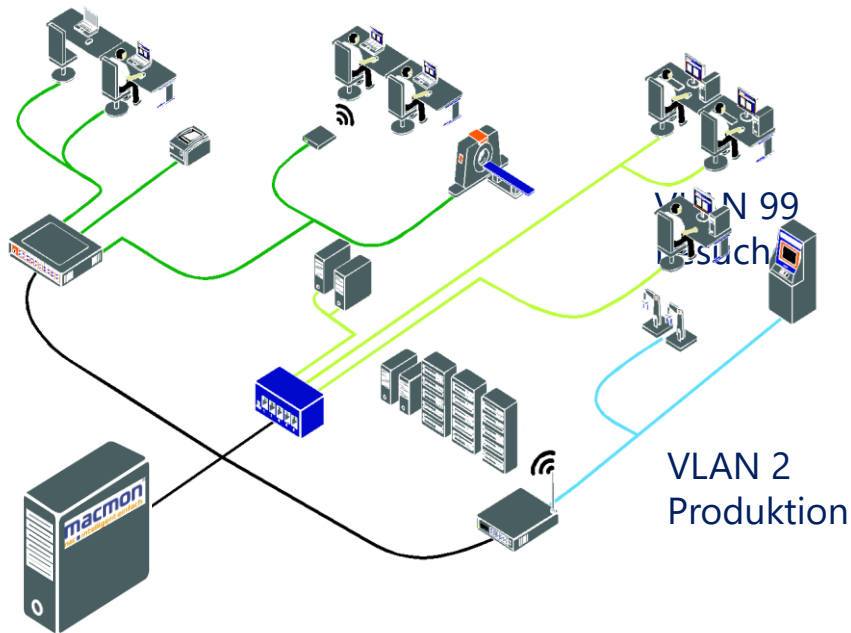
Number of MAC addresses per MAC VLAN name

Add to the dashboard



IL NAC nel lavoro quotidiano

Controllo e gestione permessi di accesso



- Mac authentication
- User and password
- Certificato



IL NAC nel lavoro quotidiano

Protezione da attacchi di livello 2

```
root@Icarus: ~  
File Edit View Search Terminal Help  
root@Icarus:~# ip route  
default via 192.168.126.2 dev eth0 proto static metric 100  
192.168.126.0/24 dev eth0 proto kernel scope link src 192.168.126.136 metric 100  
root@Icarus:~# netdiscover  
Currently scanning: 192.168.126.0/24 | Screen View: Unique Hosts  
5 Captured ARP Req/Rep packets, from 4 hosts. Total size: 300  


| IP              | At MAC Address    | Count | Len | MAC Vendor / Hostname |
|-----------------|-------------------|-------|-----|-----------------------|
| 192.168.126.2   | 00:50:56:fc:f9:c2 | 2     | 120 | Unknown vendor        |
| 192.168.126.1   | 00:50:56:c0:00:08 | 1     | 60  | Unknown vendor        |
| 192.168.126.135 | 00:0c:29:11:0c:27 | 1     | 60  | Unknown vendor        |

  
root@Icarus:~# arpspoof  
Version: 2.4  
Usage: arpspoof [-i interface] [-c own|host|both] [-t target] [-r host]  
root@Icarus:~# arpspoof -i eth0 -t 192.168.126.135 -r 192.168.126.2  
0:c:29:ab:e6:e2 0:c:29:11:c:27 0806 42: arp reply 192.168.126.2 is-at 0:c:29:ab:  
e6:e2  
0:c:29:ab:e6:e2 0:50:56:fc:f9:c2 0806 42: arp reply 192.168.126.135 is-at 0:c:29:  
:ab:e6:e2
```

IL NAC nel lavoro quotidiano

Lista delle porte aperte su ogni singolo dispositivo

ARP

DNS

DHCP

CDP

LLDP

TCP/UDP Ports

Traps

Scan data

View

20

1-20 of 2,712

MAC ^	Last IP	Last DNS name	Port	Protocol	Default service	Running service	Online since (ARP)	Date and time of the last
00-00-0C-07-AC-01	172.16.0.1		23	tcp	telnet		2018-04-24 11:09:19	2018-04-24 11:13:35
00-00-0C-07-AC-01	172.16.0.1		80	tcp	http		2018-04-24 11:09:19	2018-04-24 11:13:35
00-00-0C-07-AC-03	172.30.0.1		23	tcp	telnet		2018-04-24 11:09:19	2018-04-24 11:11:45
00-00-0C-07-AC-03	172.30.0.1		80	tcp	http		2018-04-24 11:09:19	2018-04-24 11:11:45
00-00-4E-12-30-9B	172.30.0.125		1110	tcp	webadmstart		2018-04-09 10:01:04	2018-04-09 13:43:37
00-05-1E-06-06-75	172.16.8.123		22	tcp	ssh		2018-04-26 15:19:08	2018-04-26 15:20:20
00-05-1E-06-06-75	172.16.8.123		23	tcp	telnet		2018-04-26 15:19:08	2018-04-26 15:20:20
00-05-1E-06-06-75	172.16.8.123		80	tcp	http		2018-04-26 15:19:08	2018-04-26 15:20:20
00-05-1E-06-06-75	172.16.8.123		111	tcp	sunrpc		2018-04-26 15:19:08	2018-04-26 15:20:20
00-05-1E-06-0A-EC	172.16.8.124		22	tcp	ssh		2018-04-26 15:20:07	2018-04-26 15:21:40
00-05-1E-06-0A-EC	172.16.8.124		23	tcp	telnet		2018-04-26 15:20:07	2018-04-26 15:21:40



IL NAC nel lavoro quotidiano

Gestione degli accessi degli ospiti e dei dispositivi personali



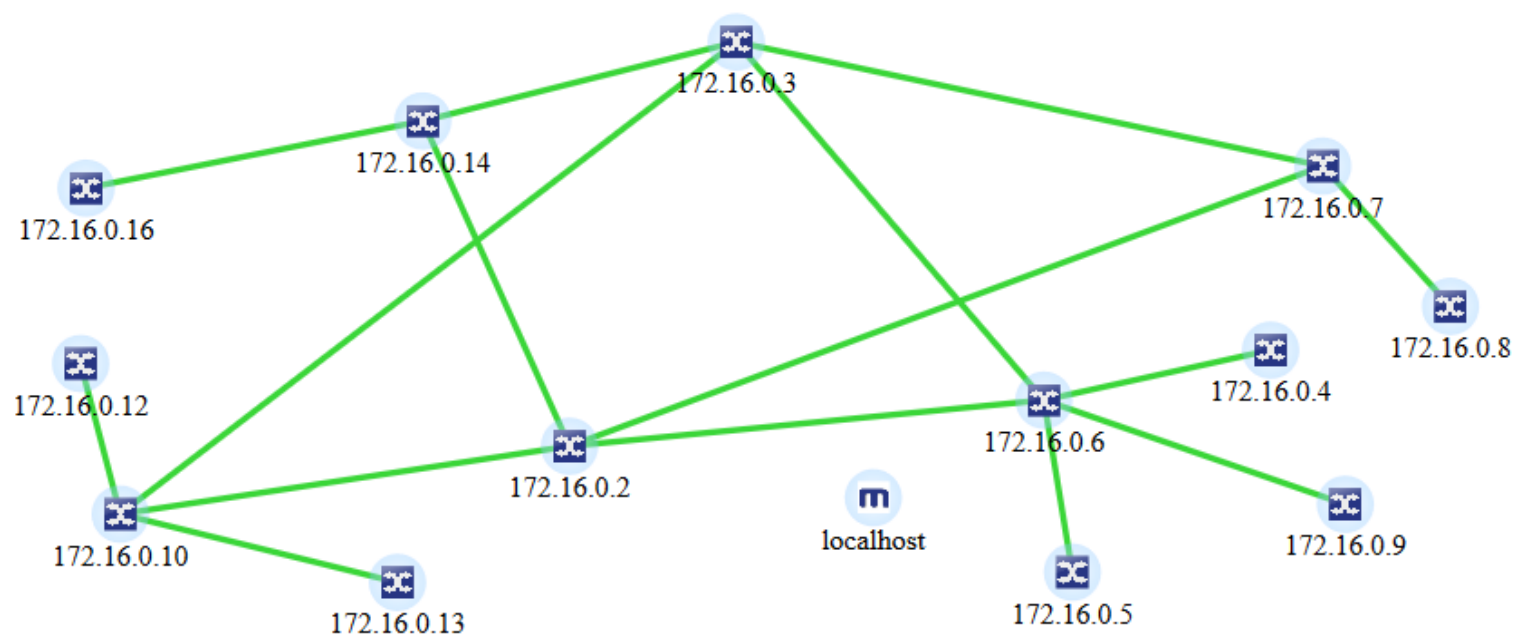
IL NAC nel lavoro quotidiano

Integrazione con sistemi di sicurezza di terze parti



IL NAC nel lavoro quotidiano

Topologia interattiva della rete



IL NAC nel lavoro quotidiano

Modifica delle vlan da GUI o VLAN Dinamiche

Interfaces of network device 172.16.0.2

Action	View	C	T	ifIndex	ifName	ifType	ifStatus	Flag	802.1X	A	Connections	Last usage
☐						Eth, wlan						
☐				10101	Gi0/1	Eth 1 Gbit/s	0/0 0/0	Uplink_CDP				
☐				10102	Gi0/2	Eth 1 Gbit/s	0/0 0/0	Uplink_CDP			172.16.0.14 / 26	2017-02-03 09:21:04
☐				10103	Gi0/3	Eth 100 Mbit/s	0/0 0/0	Uplink_CDP			172.16.0.10 / 26	2017-02-03 09:23:05
☐				10104	Gi0/4	Eth 1 Gbit/s	0/0 0/0	Uplink_CDP			172.16.0.6 / 23	2017-02-03 09:21:04
☐				10105	Gi0/5	Eth 1 Gbit/s	0/0 0/0				172.16.0.7 / 26	2017-02-03 09:21:04
☐				10106	Gi0/6	Eth 1 Gbit/s	0/0 0/0					
☐				10107	Gi0/7	Eth 1 Gbit/s	0/0 0/0					
☐				10108	Gi0/8	Eth 10 Mbit/s	0/0 0/0					
☐				10109	Gi0/9	Eth 10 Mbit/s	0/0 0/0					
☐				10110	Gi0/10	Eth 10 Mbit/s	0/0 0/0					
☐				10111	Gi0/11	Eth 10 Mbit/s	0/0 0/0					
☐				10112	Gi0/12	Eth 10 Mbit/s	0/0 0/0					

default

PUB

DMZ

SERVER

Management

Backup

clienti

Client_PC

GUEST_DEVICE

GUEST_WAN

Stampanti

LABORATORIO

Training Center

Pearson View

Client_Wired

Client_Wireless

WiFi_Dipendenti

WiFi_Guest

fdi-default

token-ring-default

default

201-20 of 52 (filtered of 63)

Connections

Last usage

172.16.0.14 / 26

2017-02-03 09:21:04

172.16.0.10 / 26

2017-02-03 09:23:05

172.16.0.6 / 23

2017-02-03 09:21:04

172.16.0.7 / 26

2017-02-03 09:21:04

2018-01-25 10:20:03

2018-01-25 10:20:03

Status overview

Action status

VLANs

Credentials

SNMP

Statistics

MIB probe



IL NAC nel lavoro quotidiano

Statistiche del traffico

Status overview

Action status

VLANs

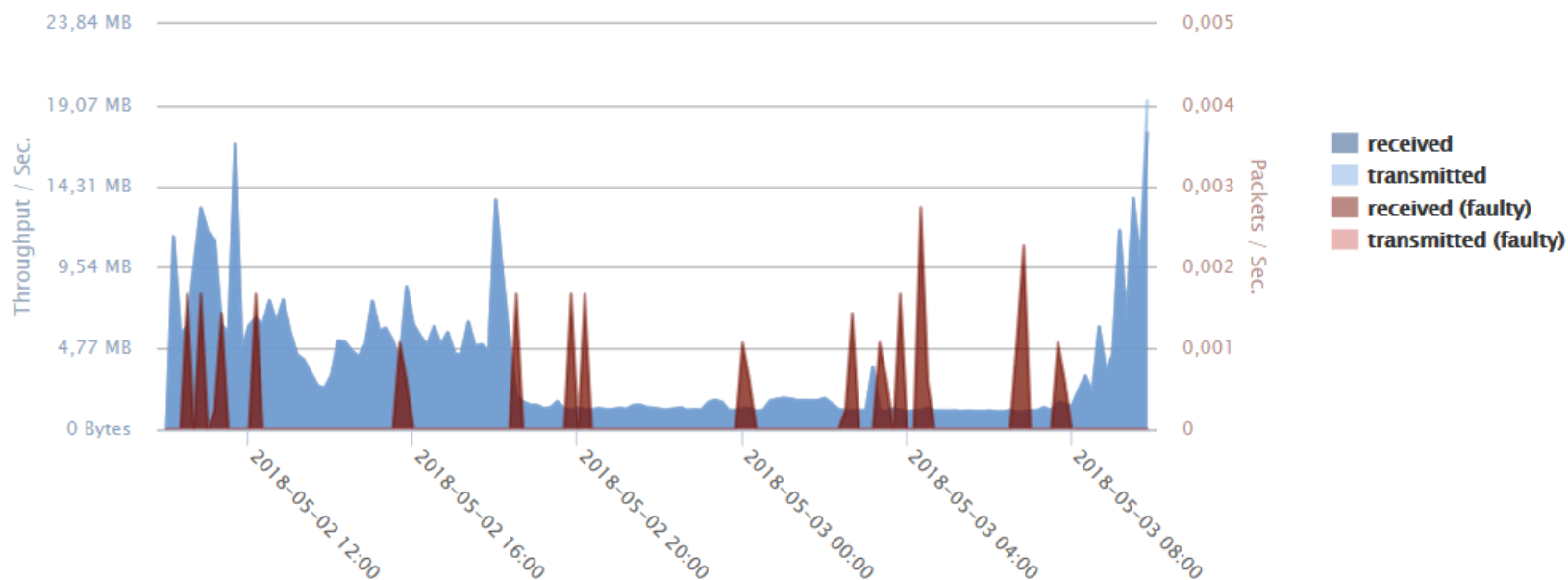
Credentials

SNMP

Statistics 

MIB probe

Interface statistic accumulated – 172.16.0.2



IL NAC nel lavoro quotidiano

Controllo stato delle porte

Network devices14

Interfaces421

Device status

Disabled interfaces

Links

Device VLANs

Interface VLANs

Edit

View

20

1-20 of 426

«

<

1

>

»

	Device ^	ifIndex	ifName	ifType	ifSpeed	ifStatus	Flag	Device group	Device location	Last usage	ifDesc
	172.16.0.2	1	VI1	VLAN	1 Gbit/s	connected	Ignore	Switch-Router			Vlan1
	172.16.0.2	10	VI10	VLAN	1 Gbit/s	free	Ignore	Switch-Router			Vlan10
	172.16.0.2	17	VI17	VLAN	1 Gbit/s	unknown	Ignore	Switch-Router			Vlan17
	172.16.0.2	30	VI30	VLAN	1 Gbit/s	disabled	Ignore	Switch-Router			Vlan30
	172.16.0.2	90	VI90	VLAN	1 Gbit/s	connected	Ignore	Switch-Router			Vlan90
	172.16.0.2	200	VI200	VLAN	1 Gbit/s	free	Ignore	Switch-Router			Vlan200
	172.16.0.2	201	VI201	VLAN	1 Gbit/s	free	Ignore	Switch-Router			Vlan201



I pregiudizi sul NAC

- **Cambiamenti radicali** all'infrastruttura
- Grandi **investimenti**
- **Effort** amministrativo
- **Pochi benefici** difficili da determinare
- Argomento complesso – grosso investimento nella **formazione**
- **Paura di bloccare** traffico e sistemi trusted



macmon
nac ■ smartly simple



BLUDIS | VALUE
ADDED
DISTRIBUTOR

bludis.it

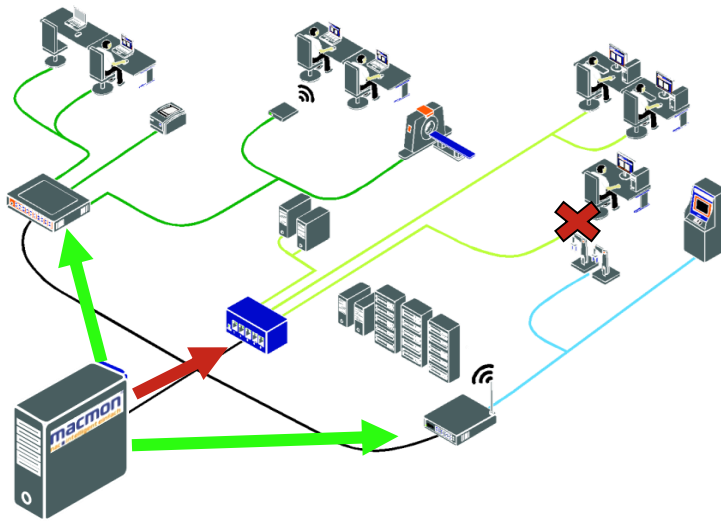
Macmon NAC

- HQ a Berlino
- 100% di ingegneria tedesca
- Sviluppatori di tecnologie e standard di sicurezza
- Collabora con diversi istituti di ricerca ed università
- Grande esperienza di integrazione di progetti NAC con clienti di differenti settori e differenti dimensioni
- Collabora con i vendor leader nelle tecnologie di sicurezza
- Membro di 



Macmon NAC

VISIBILITA' E SICUREZZA DELLA RETE



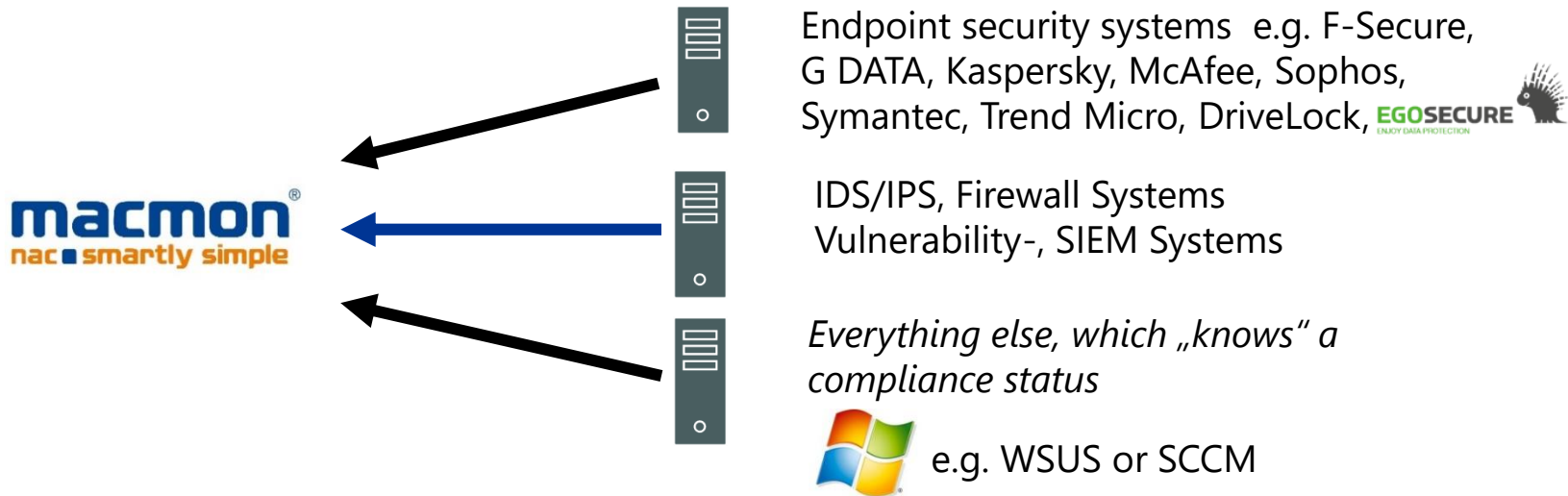
- Nessun Agent
- Nessuna modifica alla rete
- Semplice da implementare e gestire
- Vendor agnostic
- Mixed operation con e senza 802.1X

Identificazione dei dispositivi connessi alla rete attraverso protocolli standard (**SNMP, Telnet/ SSH or 802.1X**)

Macmon NAC

COMPLIANCE

- open API : connessione con soluzioni di terze parti
- antivirus connector : Con i principali sistemi anti-virus
- macmon compliance agent : controllo basilare dei dispositivi



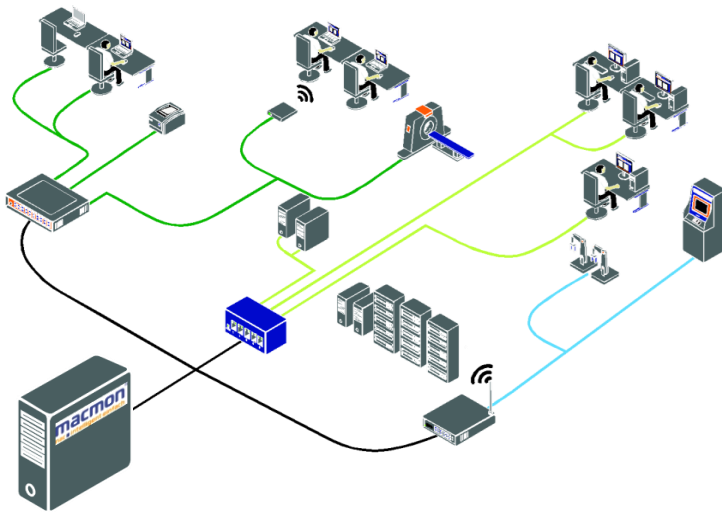
Macmon NAC

VLAN MANAGER

La VLAN è definita tramite l'associazione (MAC address VLAN-ID).

L'utente ha accesso alla vlan configurata dall'amministratore, indipendentemente dalla porta fisica.

- Semplicità, nessuna riconfigurazione manuale
- Non è necessario il know-how tecnico per amministrare gli switch



 Guest-VLAN  Office-VLAN  Production-VLAN

Macmon NAC

GUEST e BYOD Management

macmon
nac smartly simple

Welcome!

🔒 Login

User

Username / Voucher number

Password

Password / Voucher code

Login

- ✓ Captive portal completamente personalizzabile
- ✓ Diversi livelli di permessi per l'accesso alla rete
- ✓ Indipendente dal vendor dell'infrastruttura WLAN
- ✓ Localizzazione dei dispositivi sugli access-point
- ✓ Self registration con indirizzo mail
- ✓ Voucher code via SMS sul dispositivo mobile
- ✓ Creazione di una lista di voucher
- ✓ Sponsor Portal & BYOD-Portal
- ✓ Integrazione AD / LDAP

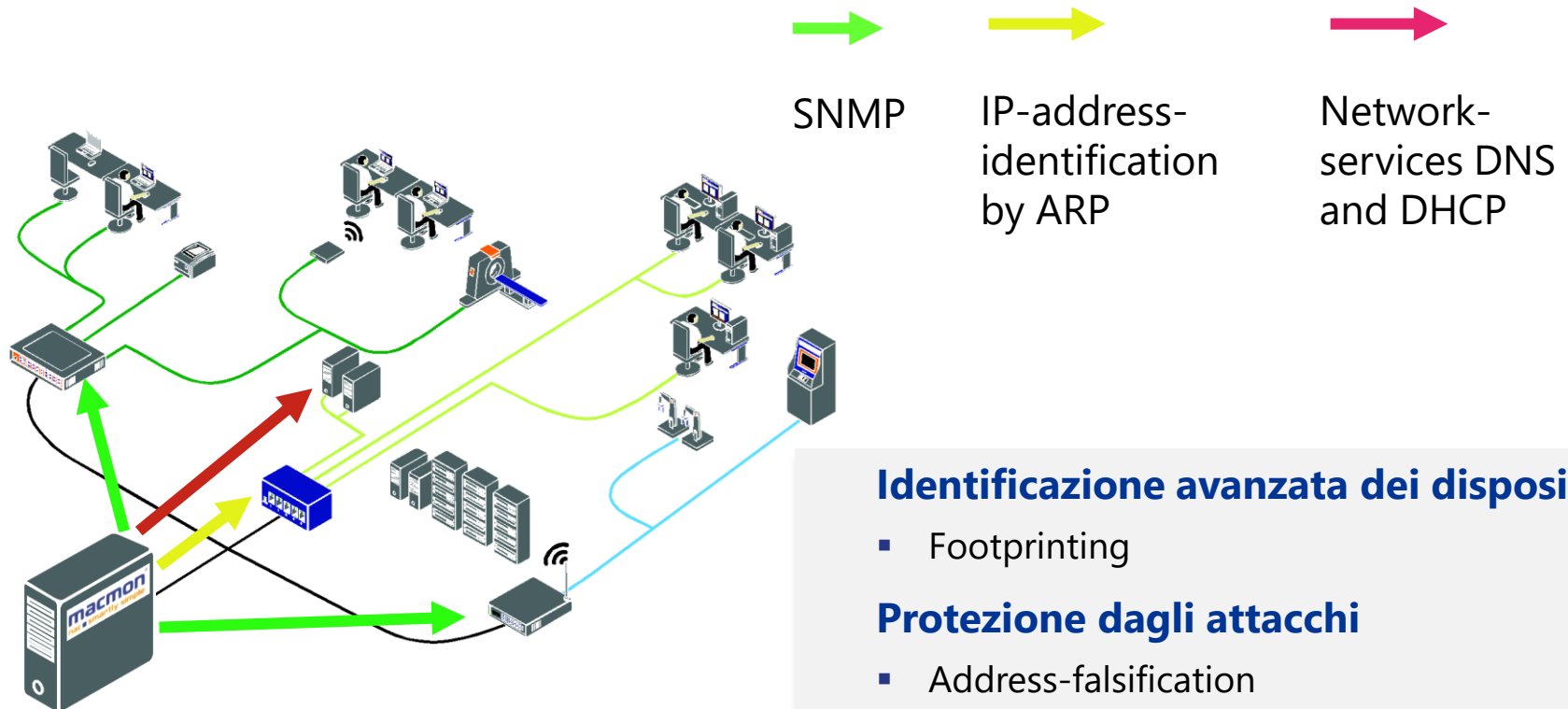


BLUDIS | VALUE
ADDED
DISTRIBUTOR

bludis.it

Macmon NAC

Advanced Security



Identificazione avanzata dei dispositivi

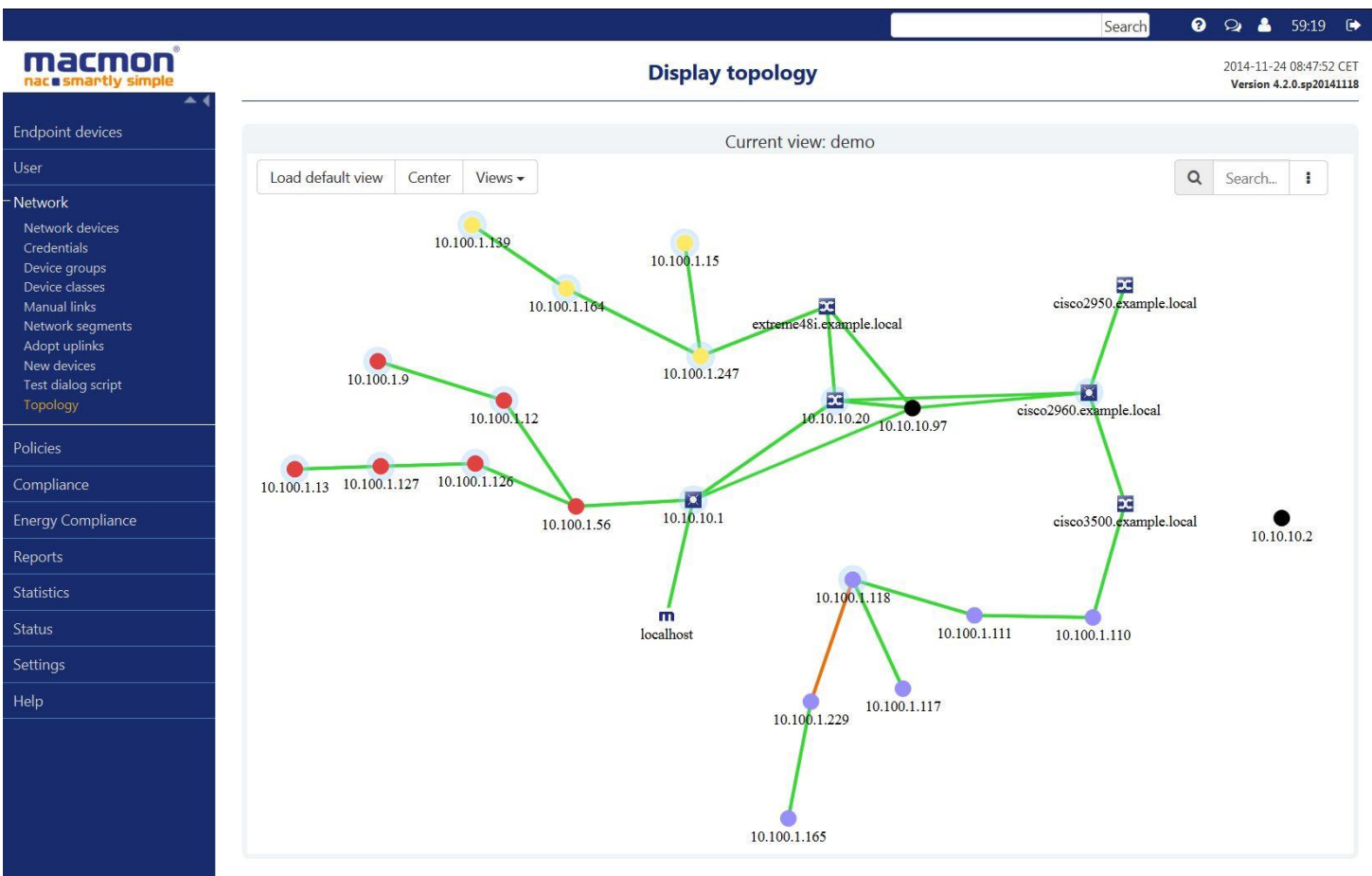
- Footprinting

Protezione dagli attacchi

- Address-falsification
- Attacks to switches
- ARP-Spoofing / MAC-Spoofing

Macmon NAC

GRAPHICAL TOPOLOGY



Macmon NAC

BENEFICI DI MACMON

- ✓ **Semplicità** di utilizzo e di implementazione (console web)
- ✓ **Non richiede modifiche** all'infrastruttura esistente
- ✓ **Vendor neutral** – compatibile con tutti gli switch managed
- ✓ **Non richiede installazione di agent** sui dispositivi
- ✓ **Protezione e visibilità** completa del network e dei dispositivi
- ✓ **Blocco o isolamento** dei dispositivi non autorizzati
- ✓ Controllo accesso dispositivi visitatori e **BYOD** con captive portal
- ✓ **Single point of view** infrastruttura di switching
- ✓ **Storico degli accessi** alla rete
- ✓ Autenticazione sicura con **802.1X e Hybrid mode**
- ✓ Integrabile con sistemi di **sicurezza di terze parti**



Caso di successo



Designing Energy

Dal 1997 leader nel mercato della raffinazione **del petrolio e del gas**, con oltre 500 progetti implementati in tutto il mondo.

OBIETTIVI RAGGIUNTI

- ✓ **Integrazione** con tutti gli apparati di rete
- ✓ **Inventario** di tutti i dispositivi corporate
- ✓ **Visione** completa dell'infrastruttura
- ✓ Integrazione con server **LDAP**
- ✓ Abilitazione **regole per isolare dispositivi** non autorizzati
- ✓ **Gestione avanzata della segmentazione** di rete Lan/Wlan
- ✓ Utilizzo **WMI, footprinting, integrazione DNS e DHCP**
Utilizzo **guest portal** per registrazione Guest attraverso lo **sponsor**
- ✓ Utilizzo guest portal per **registrazioni dispositivi BYOD**

EVOLUZIONI FUTURE

Integrazione con:

- ✓ Soluzioni Cybersecurity **Sophos**
- ✓ Suite IT Management **Manage engine**



GRAZIE

