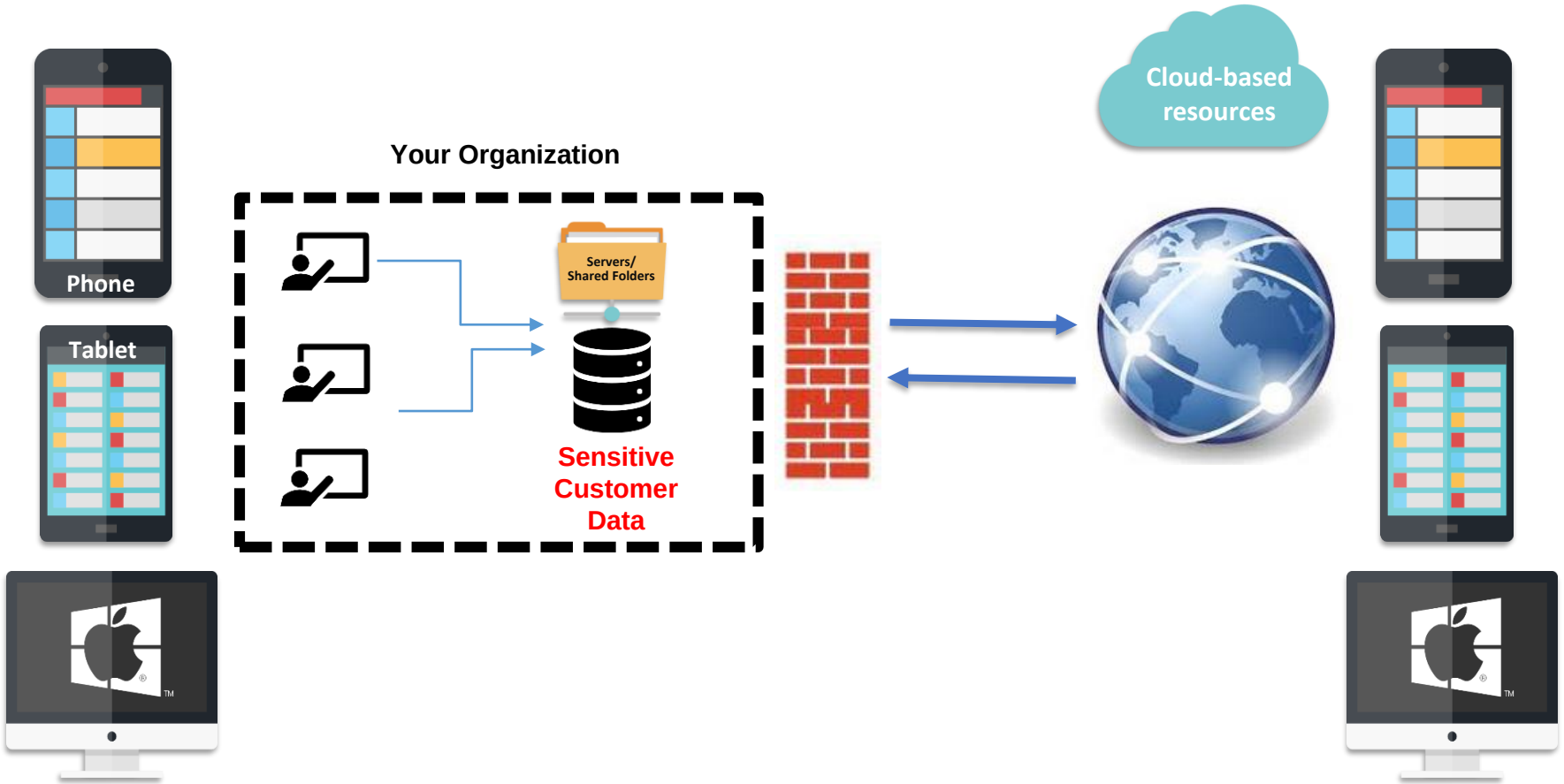
Ridefiniamo il concetto di sicurezza del network con il NAC

BLUDIS®
VALUE ADDED DISTRIBUTOR

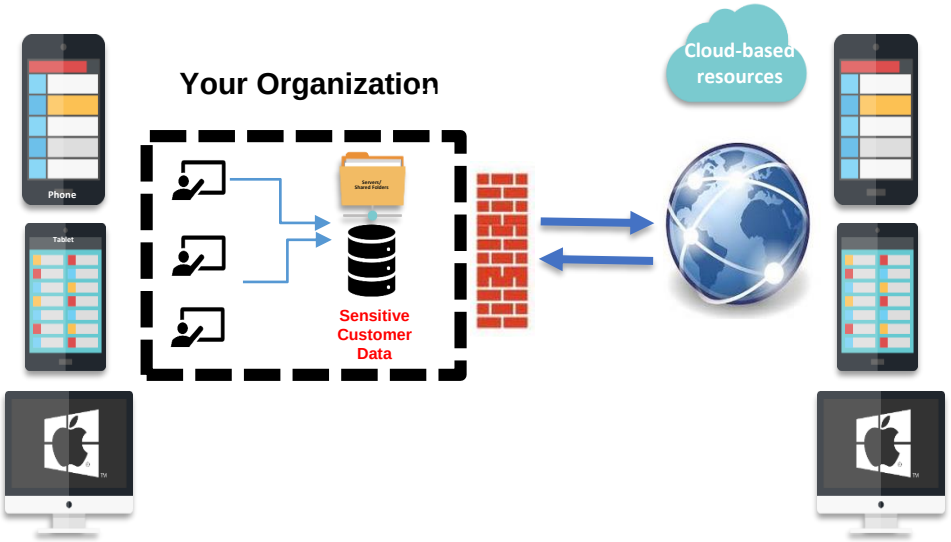
AGENDA

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

Security


Phone
Tablet
Your Organization
Servers/
Shared Folders
Sensitive
Customer
Data
Cloud-based
resources

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

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

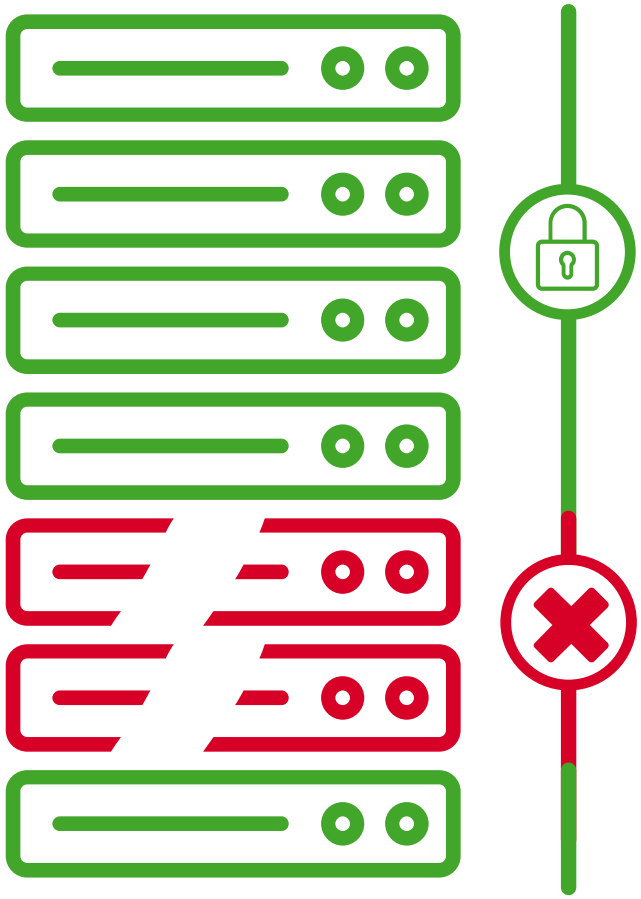
VULNERABILITY AND HARDENING

VPN AND REMOTE ACCESS

INVENTORY

EVENT MANAGEMENT

AWARENESS AND TRAINING



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

PCI

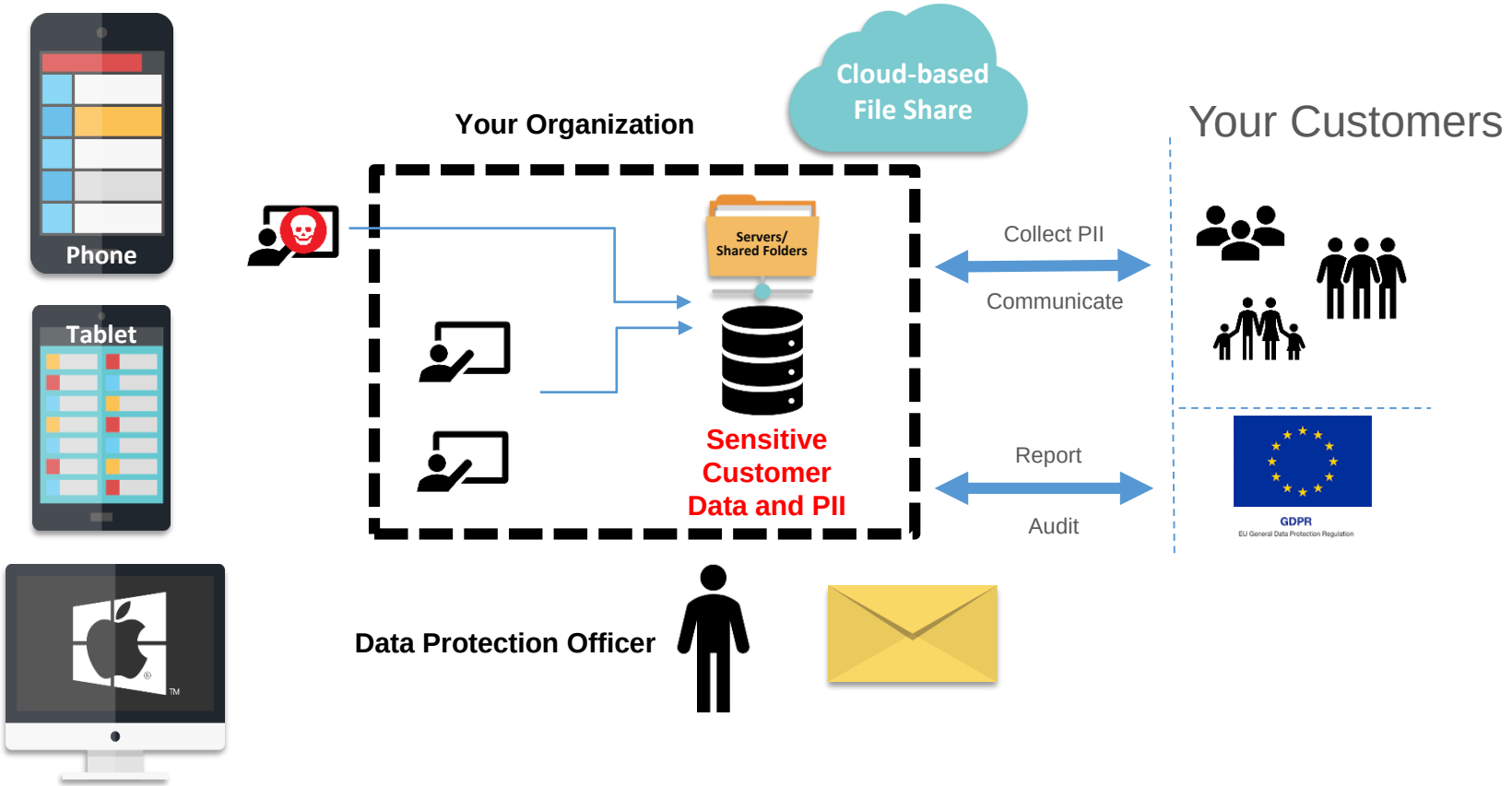
ISO 27001

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

IL NAC nel lavoro quotidiano

NETWORK ACCESS CONTROL - NAC

Hai Visione completa della tua infrastruttura di rete?

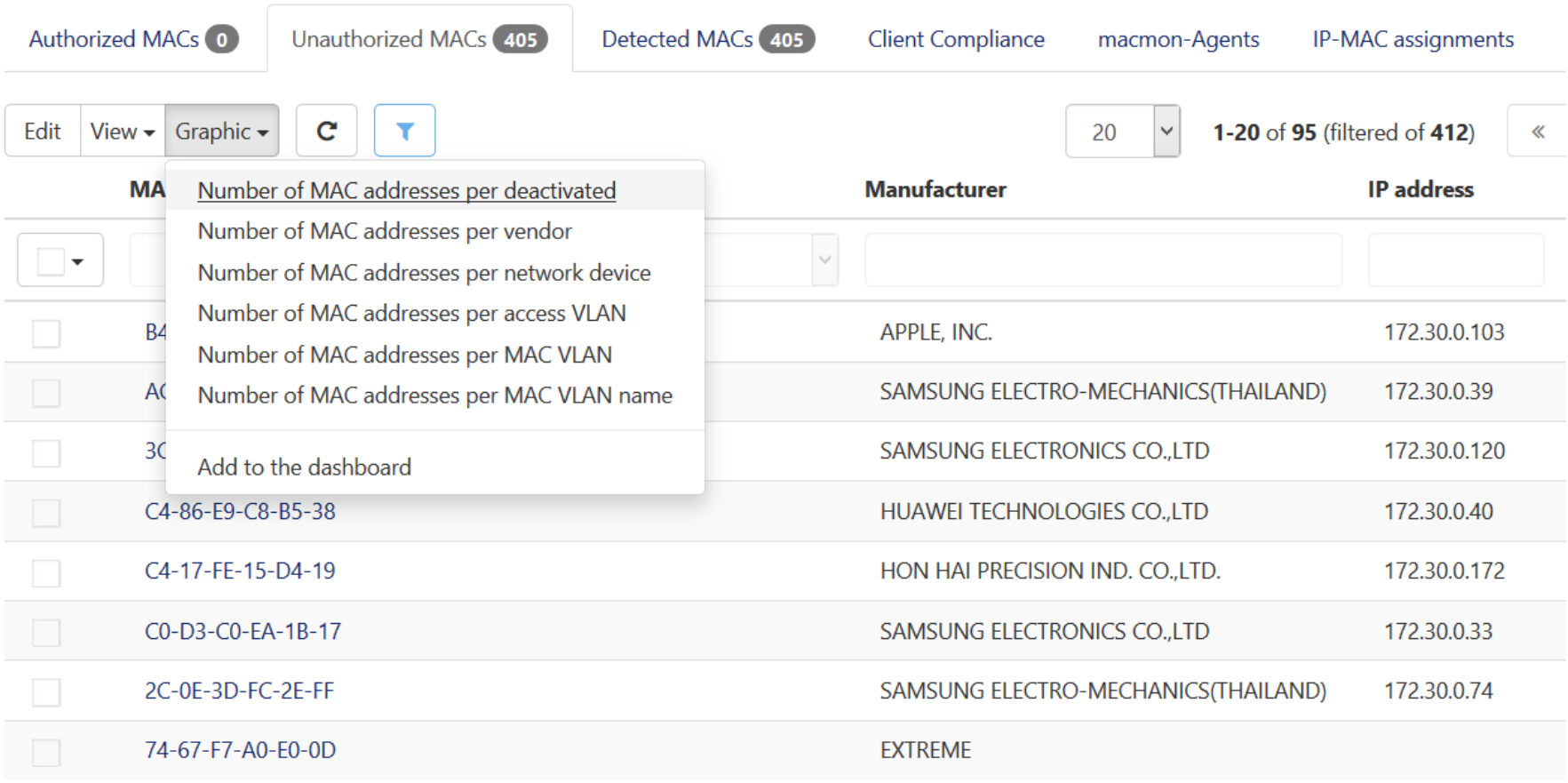
Sei **consapevole** di tutti i dispositivi connessi alla rete?

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?

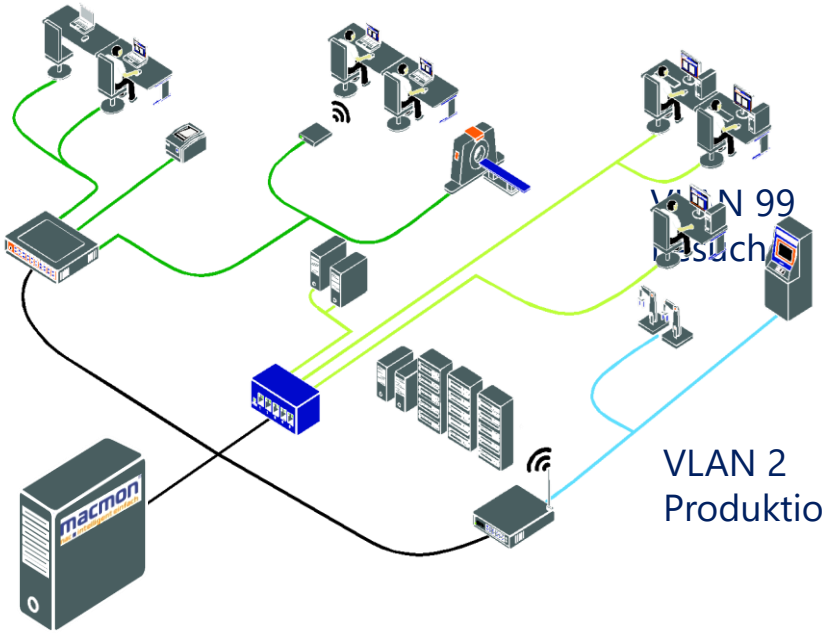
IL NAC nel lavoro quotidiano

Identificazione di tutti i dispositivi



IL NAC nel lavoro quotidiano

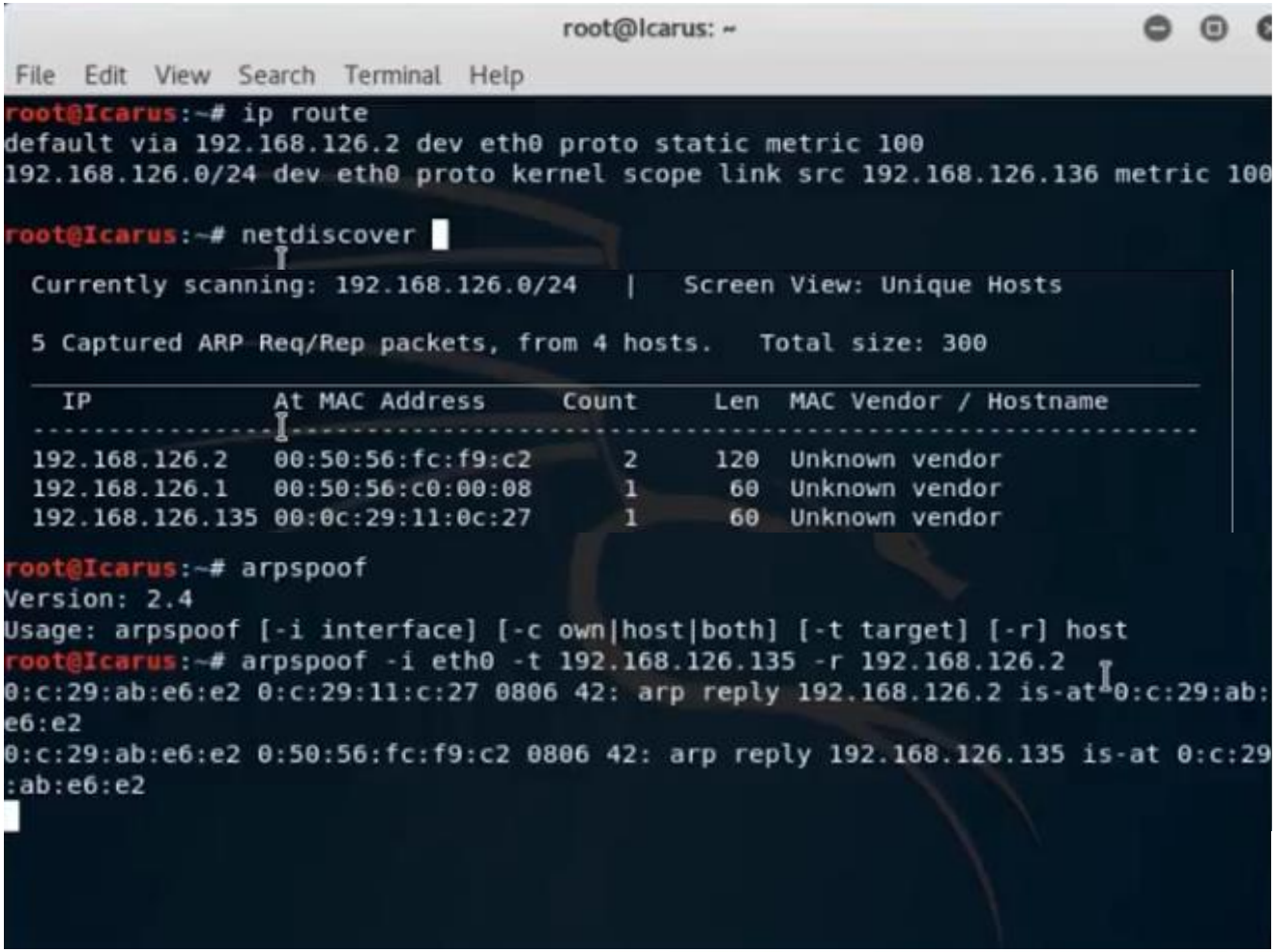
Controllo e gestione permessi di accesso



- **Mac authentication**
- **User and password**
- **Certificato**

IL NAC nel lavoro quotidiano

Protezione da attacchi di livello 2



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

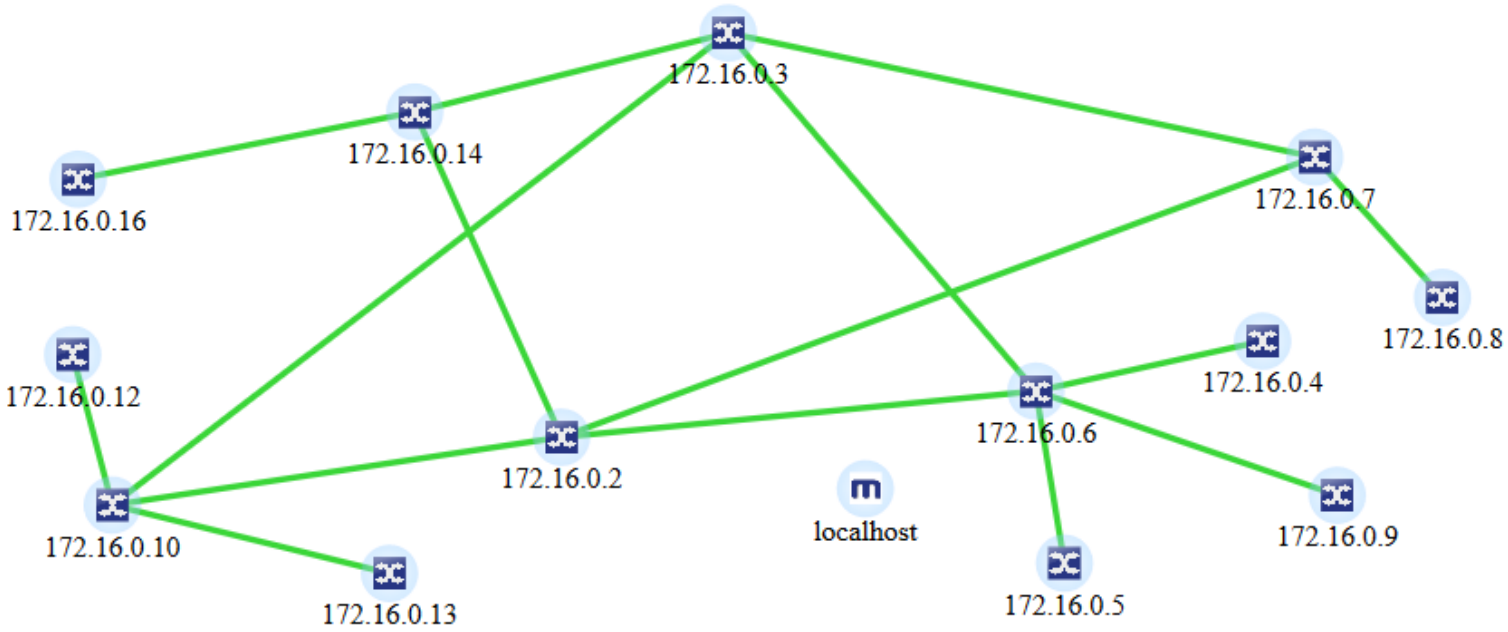
Gestione degli accessi degli ospiti e dei dispositivi personali

IL NAC nel lavoro quotidiano

Integrazione con sistemi di sicurezza di terze parti

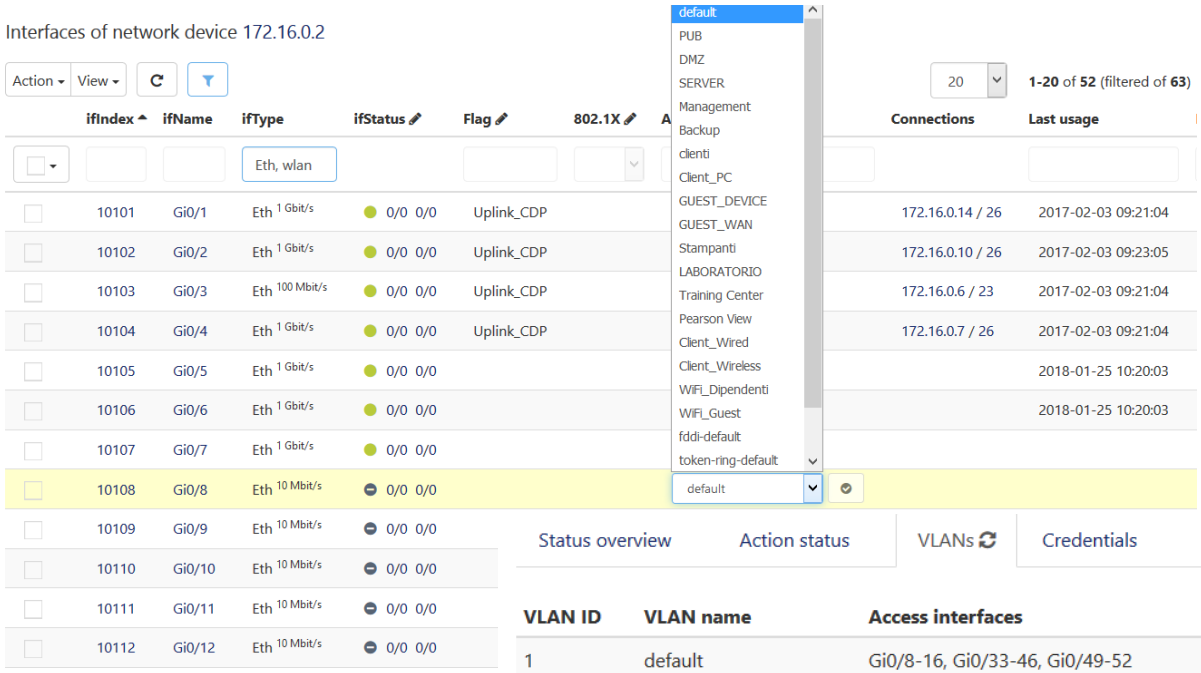
IL NAC nel lavoro quotidiano

Topologia interattiva della rete



IL NAC nel lavoro quotidiano

Modifica delle vlan da GUI o VLAN Dinamiche



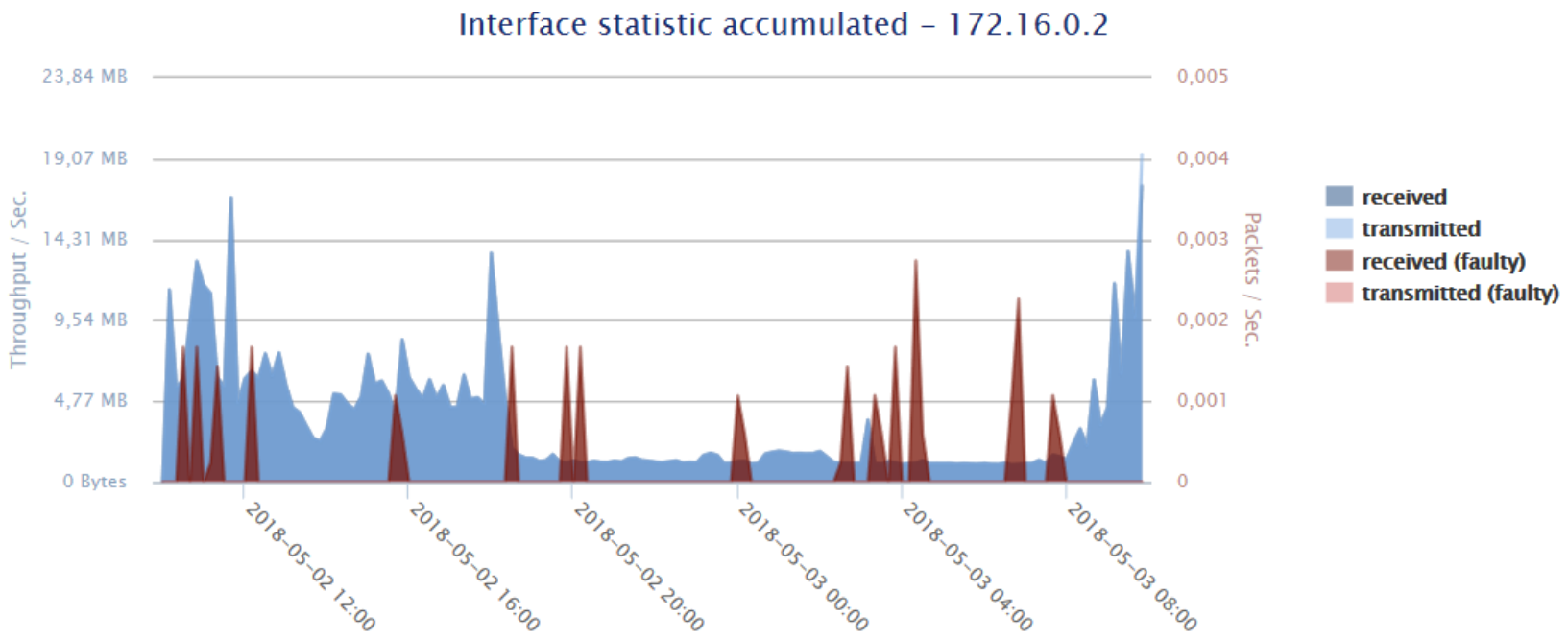
Status overview | Action status | VLANs | Credentials | SNMP | Statistics | MIB probe

VLAN ID	VLAN name	Access interfaces	Tagged interfaces	Voice interfaces
1	default	Gi0/8-16, Gi0/33-46, Gi0/49-52	Gi0/1-6, Gi0/47-48, Po1	
2	PUB	Gi0/17-19, Gi0/21-24	Gi0/1-6, Gi0/47-48, Po1	
3	DMZ	Gi0/25-32	Gi0/1-6, Gi0/47-48, Po1	
4	SERVER		Gi0/5-6, Gi0/47-48, Po1	
10	Management		Gi0/3, Gi0/5-6, Gi0/47-48, Po1	
11	Backup		Gi0/5-6, Gi0/47-48	
17	clienti	Gi0/20	Gi0/1-6, Gi0/47-48, Po1	

IL NAC nel lavoro quotidiano

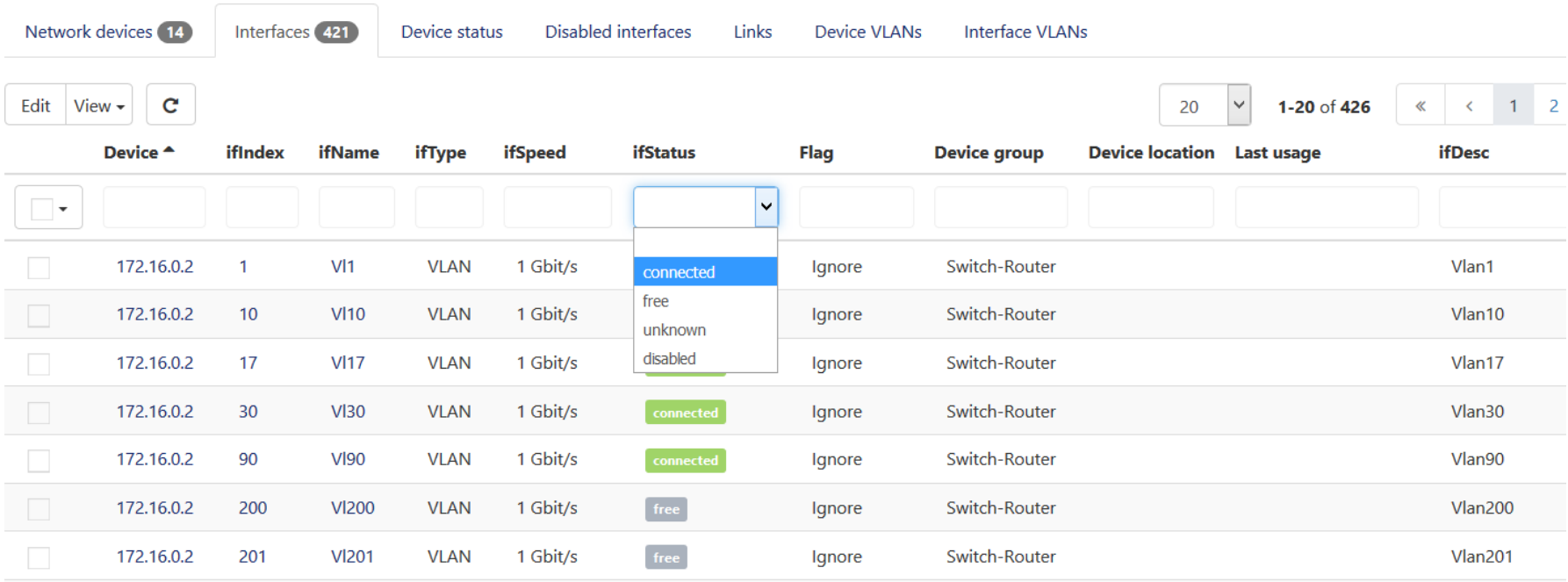
Statistiche del traffico

Status overview | Action status | VLANs | Credentials | SNMP | Statistics | MIB probe



IL NAC nel lavoro quotidiano

Controllo stato delle porte



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

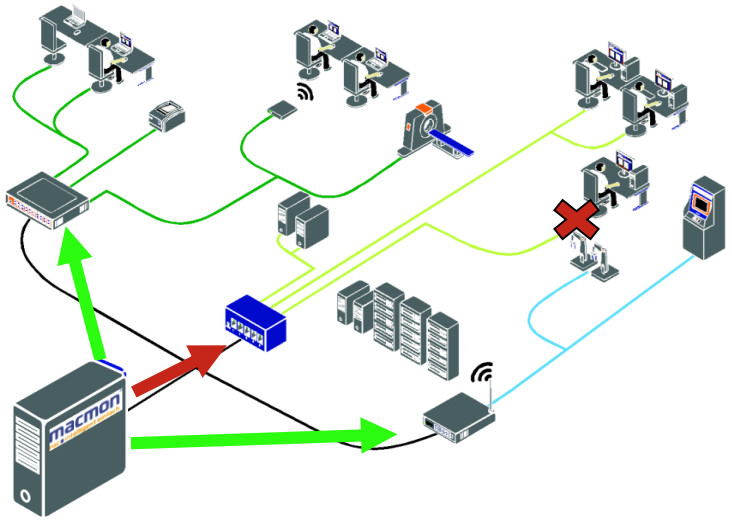

macmon
nac smartly simple

Macmon NAC

- HQ a Berlino
- 100% di ingegneria tedesca
- Sviluppatori di teconologie 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 TRUSTED COMPUTING GROUP

Macmon NAC

VISIBILITA' E SICUREZZA DELLA RETE



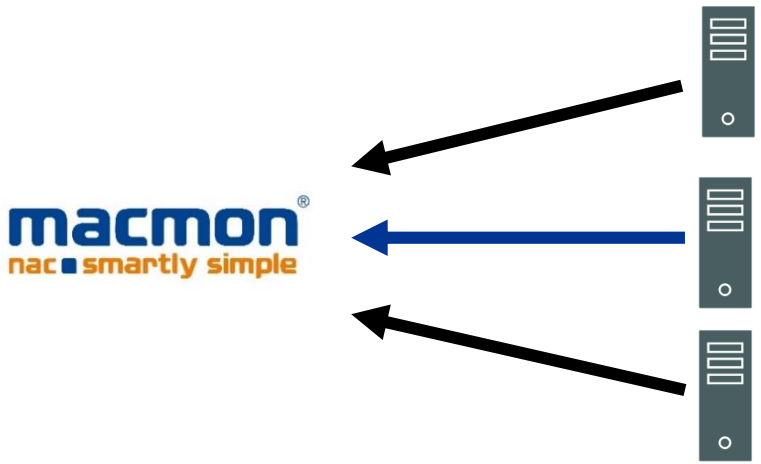
- Nessun Agent
- Nessuna modifica alla rete
- Semplice da implementare e gestire
- Vendor agnostic
- Mixed operation con e senza 802.1X

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 parzi
- antivirus connector : Con i principali sistemi anti-virus
- macmon compliance agent : controllo basilare dei dispositivi



Endpoint security systems e.g. F-Secure, G DATA, Kaspersky, McAfee, Sophos, Symantec, Trend Micro, DriveLock, EGOSECURE

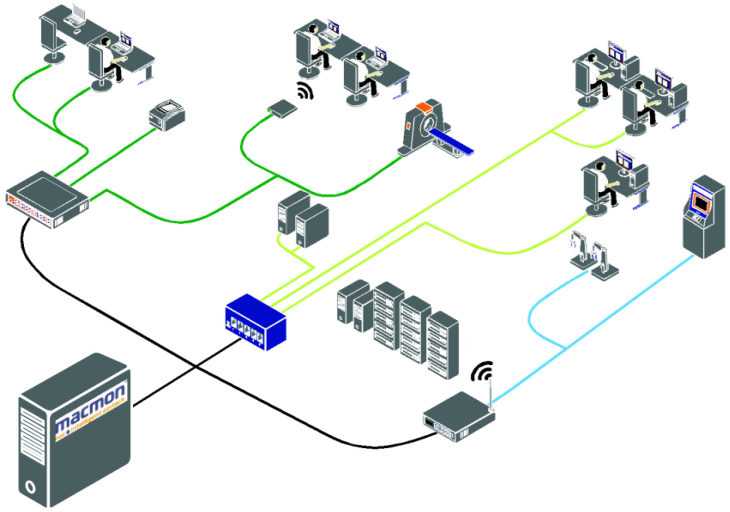
IDS/IPS, Firewall Systems
Vulnerability-, SIEM Systems

Everything else, which „knows" a compliance status

e.g. WSUS or SCCM

Macmon NAC

VLAN MANAGER



Guest-VLAN *Office-VLAN* *Production-VLAN*

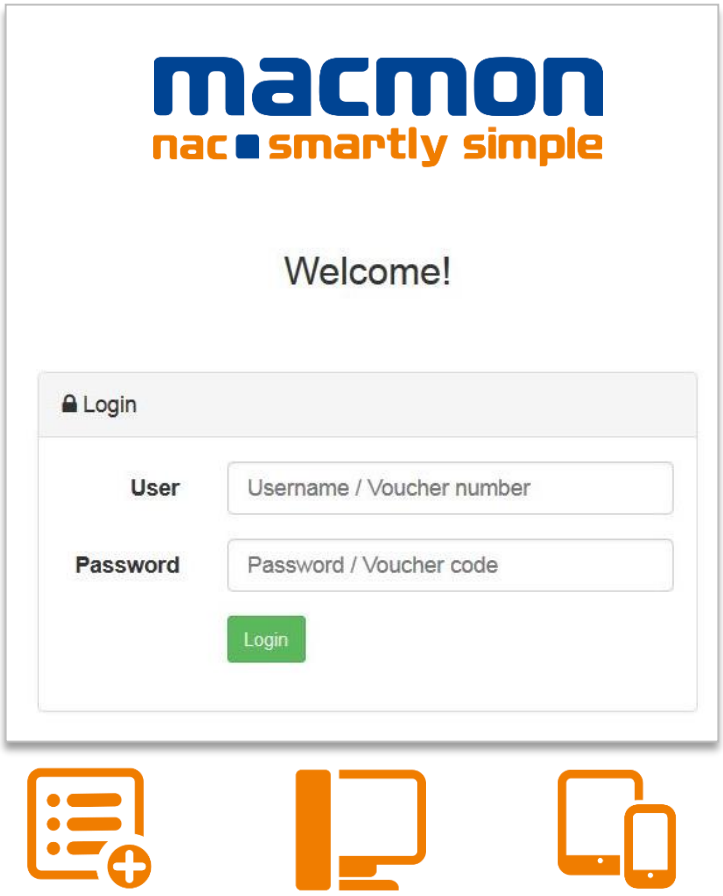
La VLAN è definita tramite l'associazione (MAC address VLAN-ID).

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

Macmon NAC

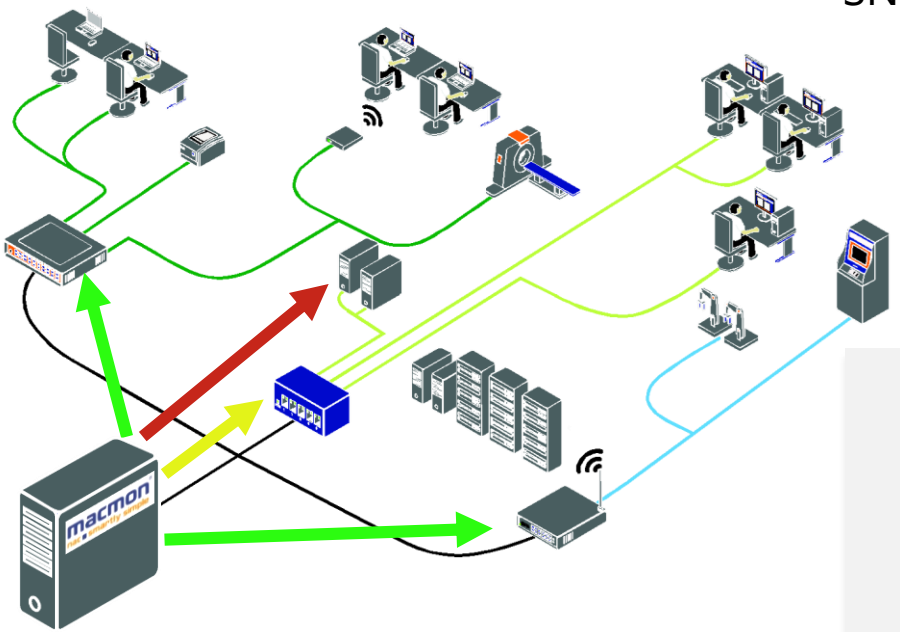
GUEST e BYOD Management



- ✓ Captive portal completamente personalizzabile
- ✓ Dieversi livelli di permessi per l'accesso alla rete
- ✓ Indipendente dal vendor dell'infrastruttua 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

Macmon NAC

Advanced Security



SNMP

IP-address-identification by ARP

Network-services DNS and DHCP

Identificazione avanzata dei dispositivi

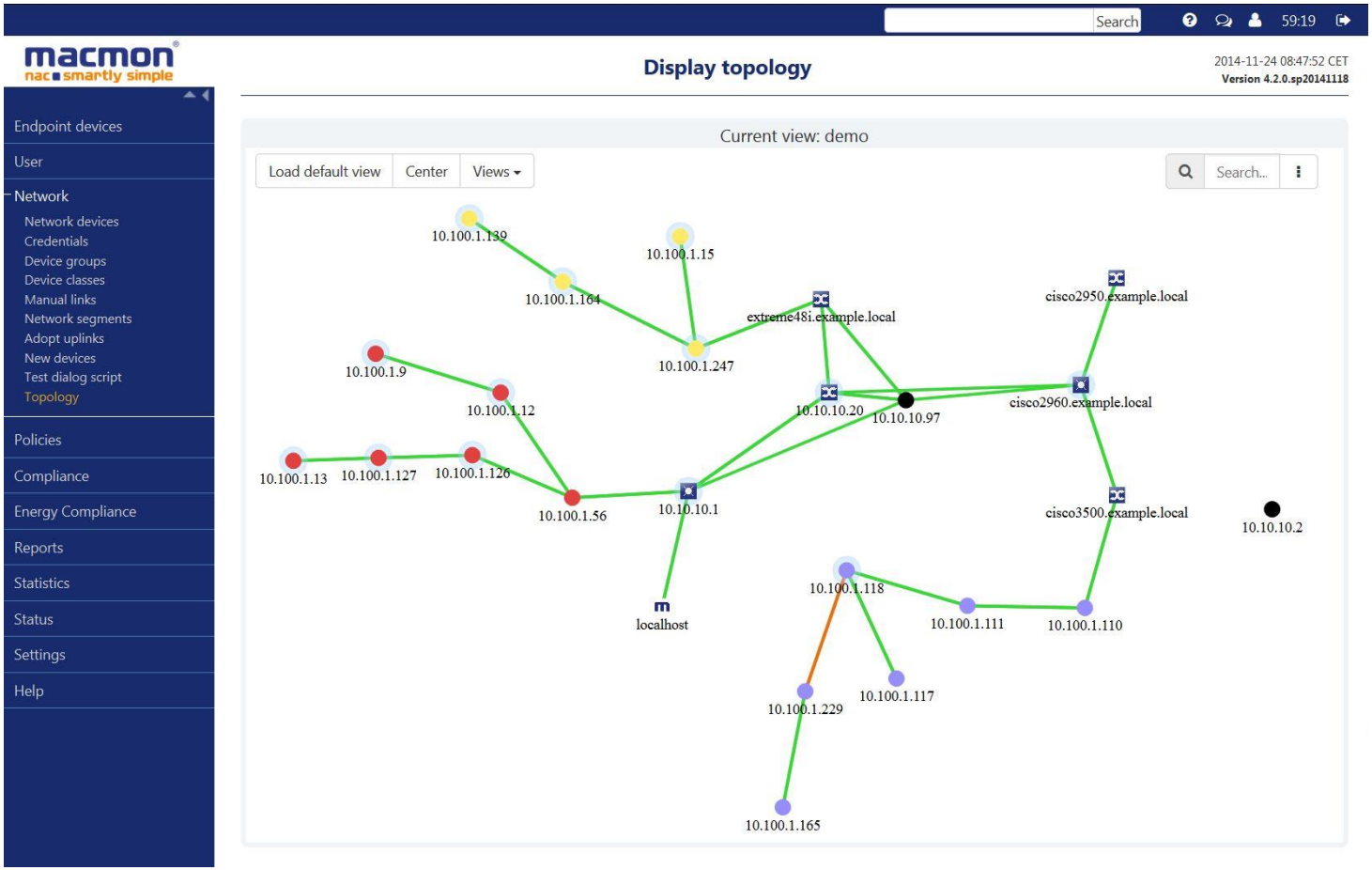
- Footprinting

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