# CASE STUDY APS SPA

macmon
nac smartly simple

## APS – Company Profile

**APS SpA is a leading Engineering and Power Plant Construction Company. It operates in the areas of Energy (Oil & Gas) and Petrochemical, offering a wide range of services, including feasibility study and EPC contracts (Engineering Procurement Construction).**

The company has more than 400 employees working at four different European sites (Rome, Moscow, Budapest and Warsaw), ensuring high performance and flexibility. The mission of APS SpA is to find the most suitable solution for all involved stakeholders, promoting the best work environment and respect everyone's wishes and needs, as stated in their statement of purpose: *"Generate prosperity in full safety and reliability"*. Mr. Antonio Quadrato, Chief Executive Officer at APS SpA, sees any technological challenge as an opportunity to grow: *"Challenges are our inspiration for action and actions inspire others to dream more."*

APS

Designing Energy

## The issue: Network Access Control

A large organization like APS SpA needs to rely on a stable and secure network. A complex high tech infrastructure connects the four international branches, both offices, construction site and other production sites. Plenty of people access these networks every day. Not only employees but also consultants, independent contractors and guests. Managing every single user is not an easy task. It is even harder to control this large group of "occasional users", because they tend to ignore corporate security policies.

Thus, there is need to protect the network, both wired and wireless, from unauthorized access.
APS SpA did a market research to find a solution to safeguard all their headquarters (critical to their mission), avoiding unauthorized access and at the same time tracking authorized consultants, contractors and all corporate devices. This latter feature has proven itself to be essential to generate the security reports required by ISO-IEC 27001 standards.

It was crucial to the company to find an easy and fast-to-implement solution that ensures the lowest number of failures, and does not require changing the existing infrastructure. A solution that could meet their needs without disrupting everyday work routines.

## The solution: macmon

macmon, a leading NAC-solution enriched with a range of features, fulfils all the aforementioned requirements. Both ICT and IT Security Teams welcomed the solution, as it was easy to install in the virtual VMware environment and easy to setup. macmon was immediately able to talk to every access switch through the SNMv3 protocol.
Once all mac-addresses were detected, a comprehensive inventory of all corporate devices was automatically generated by macmon through the WMI component. Each device was assigned to a specific endpoint group that contains certain VLAN access privileges.

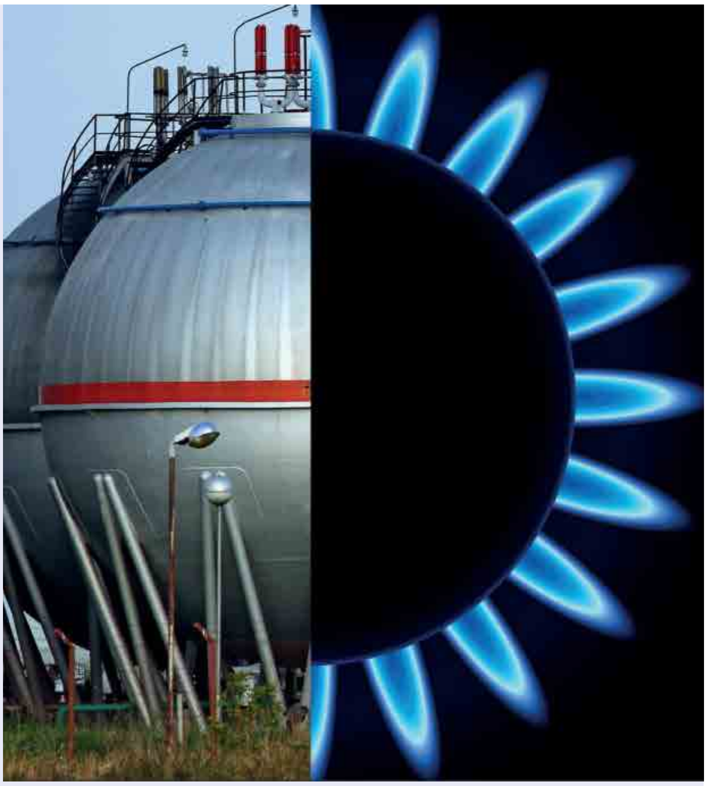
Thanks to the "VLAN Manager" macmon ensures secure and reliable access to the network on every corporate device in sync with the privileges set up by the administrator, regardless of the gateway being used (this feature is called "VLAN dynamic management").

Afterwards, rules were activated to detect unauthorized access, both for wired and wireless connections. The VLAN is being switched individually on each subnet, redirecting all traffic to a special VLAN called "Guest" that only allows access to the Internet. This implementation automatically isolates foreign devices and forbids access to resources on the corporate network. Meanwhile the "Guest Portal" that operates on the guest network, allows users to register with their own devices and get online.

Guests will get access after being handed a voucher print-out. The guests can access the network on their own (within the predefined time period). Time-limited access policies and the possibility to easily access security and audit guidelines when signing in, guarantees high protection of all corporate activities.

## The result

Thanks to macmon, Asset Management has become much easier for ICT Teams, as all corporate devices are continuously monitored (PCs, laptops, printers etc.).
Also, Security Management got easier, as Network Logging & Monitoring takes place on one central platform. When devices come onto the Guest VLAN, users have to sign in to browse the Internet without exception. Control and protection of the network is maximized.
Another very helpful feature is the "Man in the Middle" attack-detector (e.g. ARP Poisoning and MAC spoofing), that also allows administrators to have full visibility of the network topology and to manage all gateways remotely on the web-based GUI, along with other controlling functionalities.



## Future Development

macmon can easily integrate with third-party security solutions such as Antivirus, Firewalls, System Management software, SIEM, etc. through the "Compliance Module" that isolates non-compliant devices and quarantines them on a separate VLAN.

First macmon integrates with an Endpoint Antivirus software and then with a System Management software. This combination automatically shuts out critical devices, for instance those currently infected by malware or that show a high number of unsuccessful patch attempts. This guarantees total protection of all machines. Those quarantined devices will be put back on the regular VLAN only after the Antivirus or Management software tells macmon that the issue has been resolved.

### Contact

macmon secure GmbH
Alte Jakobstrasse 79-80 | 10179 Berlin | Germany
Phone: +49 30 2325777-0 | nac@macmon.eu | www.macmon.eu