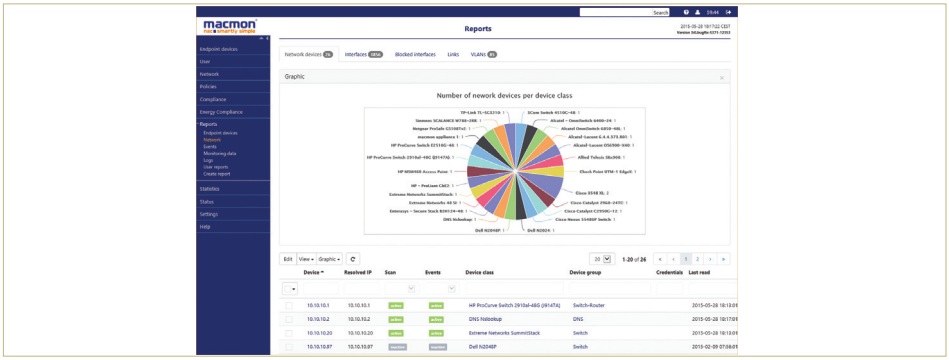
macmon NAC



PRODUCT REVIEW PRODUCT REVIEW PRODUCT R

Network access control has traditionally had a mixed reception in enterprises, as all too many solutions are notoriously difficult to install, complex to manage and expensive. NAC from German company macmon neatly avoids these pitfalls, as its minimal system requirements and agentless architecture means it can be installed and protecting your network within 24 hours.

NAC is deployed as a physical or virtual appliance and, for the latter, supports VMware and Hyper-V. It doesn't need agents or sensors, as it queries all your manageable switches and uses SNMP, Telnet/SSH and 802.1X to find out what devices are on the network.

Key to NAC operations is each device's unique MAC address, which it can glean from the switches, and by reading information sources such as ARP caches and DNS servers. This simple approach has major benefits in the fight to control mobile workforces, as NAC can see a device, regardless of whether it's a desktop, laptop or a BYOD user.

NAC can also see mobile users, no matter which switch or WLAN they access, and it uses white lists to determine what devices are allowed on the network. Another advantage is NAC is vendor-agnostic and so works with any switch - and can scale easily as the network grows and new infrastructure devices are added.

For authentication, the NAC appliance has its own embedded RADIUS server. It also integrates seamlessly with Active Directory, and can use both computer and user accounts for authentication.

It's capable of working with other managed security solutions, such as those from Sophos, Kaspersky, Symantec and McAfee. With Kasperksy, for example, it just requires the management server to send anti-malware alerts to the NAC appliance, which can then block the infected system from the network.

Connectors are also available for a wide range of other AV solutions. These allow NAC to remotely connect to the product's database, search for events such as detected malware, flag the system up as compromised and block further access.

Deployment is swift, and we found the freshly designed web console easy to use. Our first task was to create a list of credentials for monitored switches where it defaults to SNMP and requires write permissions.

NAC gathers information from scanned devices for all detected MAC addresses and these can be added to the list of 'known' addresses in the console. Usefully, you can sort devices into categories such as corporate, guests, BYOD, laptops and even printers.

From this point on, any new MAC addresses it discovers are deemed as unauthorised and policies are used to determine what access level, if any, they should have. Policy rules for unauthorised devices could be used to send an email alert, but they go much further, as actions can be applied such as blocking the device or switch port it is connecting to.

Rules are very versatile and can be used to dynamically manage VLAN membership. This is ideal for businesses operating guest networks and meeting rooms, as they can ensure visitors are placed in the correct VLAN with appropriate access privileges and even presented with custom web portals.

The intuitive NAC web console opens with a dashboard showing details such as detected and unauthorised MAC addresses, blocked switch ports and much more. The animated topology map is very slick, providing a total overview of the network, and NAC can run full compliance scans on devices, as well as providing extensive reporting facilities which can be customised to suit.

Macmon proves that network access control doesn't have to be complicated or expensive. NAC is easy to manage and its agentless operation means it can be protecting your network in no time at all. NC

Product: NAC
Supplier: macmon secure GmbH
Tel: +44 (0) 845 860 5121
Web site: www.macmon.eu
Price: 500 licence network bundle, £7,000 excluding VAT