CASE STUDY
SOMERSET PARTNERSHIP

macmon
nac smartly simple

macmon - continuing to assist NHS trusts in the UK

Somerset Partnership NHS Foundation Trust provides a wide range of integrated services, including community health, mental health and learning disability to people of all ages. It employs 4,000 staff and has a turnover of £169 million. The trust's services cover 13 community hospitals across the county and provide mental health in-patient services on 9 mental health wards. More than 1.1 million patients' records are dealt with every year.

Challenge

Network visibility is key in order to take control of a network. Many organisations have no idea who or what is on their network let alone what sensitive resources are available to complete strangers within the corporate infrastructure.

A network infrastructure with a variety of vendor devices and models is nearly impossible to manage, such as the one at Somerset Partnership NHS Foundation Trust. The administrator faces the task of manually configuring, monitoring and actively controlling the configuration of each network device. This is an unfeasible scenario with limited resources.

In addition to managing the network, keeping track of changes and incidents on the network is undoubtedly something that cannot be done manually in a complex environment.

Minehead Hospital

Solution

Somerset Partnership NHS Foundation Trust transitioned to macmon as the primary management platform on their network. Lawrence Heard - Somerset NHS - can now see his network brought from the darkness into the light.

macmon makes the entire network visible and presents Lawrence with a clear picture of all network activity. His existing environment integrates seamlessly with macmon. The support of Active Directory and MobileIron ensures the management of his corporate accounts and mobile devices is effortless. These identity stores merge with gathered network information and track user activity in tune with the endpoints.

MobileIron in particular aides in overseeing all mobile devices and even reports to macmon on the compliance status of a device. Proprietary labels are being mapped to macmon groups and make for a comprehensive sync between both platforms. Lawrence allows MobileIron to take the lead in enforcing network access control through macmon for all mobile devices in his infrastructure.

The fail-over cluster gives peace of mind that at any point in time, users will be allowed onto the network via 802.1X.

Lawrence segments his network by applying group specific VLANs and allows macmon to take care of the execution in the background. There is also the ability to activate macmon's pre-defined policies and enforce them on the network with just a click of a button.

Any form of unauthorised access outside the rules that have been set will trigger an alarm – typically in the form of an SMS or email. These threats can then be isolated immediately and investigated.

Lawrence Heard,
IT Systems Administrator

"The authentication procedure is entirely handled by macmon. It tracks, analyses and reports on each endpoint device."

A Transforming Process

Installing and applying macmon to his environment gave Lawrence the time and freedom to re-think and restructure his network. He was able to add new network segments by simply adding another dedicated endpoint group.

With macmon in place Lawrence is in a position to handle his entire network with ease. He reviews his reports once or twice a week and can quickly troubleshoot network failures he might have by using graphical topology. macmon also allows him to be prepared for upcoming GDPR audits by pulling ISO compliant reports within seconds.

Lawrence Heard,
IT Systems Administrator

"Before macmon I was not able to manage my network let alone protect it."

Minehead Hospital Entrance

Infrastructure

- 10,000 endpoint devices
- Microsoft Active Directory (AD)
- 802.1X authentication against AD
- MobileIron MDM platform

Solutions

- macmon Network Bundle & Cluster

Key Benefits

- The network devices are being polled every minute, enabling complete network visibility.
- The network is being segmented by automated policy enforcement, acting on threats swiftly and closing major vulnerability gaps appropriately.
- Network administrators can manage their network from one central platform resulting in no need to amend a device's configuration again (Ensuring a huge reduction to an administrator's workload).
- The RADIUS authentication server is backed up by the fail-over cluster, resulting in zero down time.
- The tracking and monitoring of any network incident, providing an overall picture not only of the static configuration but also of the network activity in real time.

Conclusion

Somerset Partnership NHS Foundation Trust has the protection and comprehensive tracking it needs to remain secure in today's world of being interconnected. Unauthorised devices do not stand a chance against macmon's automated policy enforcement. The ease of managing the network means that it can be re-structured and controlled in a whole new way and can be easily tailored to your requirements.

Contact

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