MACMON NAC
ANTIVIRUS CONNECTOR

Automatic isolation of infected endpoints

As a customer-focused developer of IT security technologies, we have seen the need to be able to respond quickly to critical situations, in many customer environments. Conficker and other Malware attacks have shown that in general, manual actions are often too late. Through centralized control of network accesses and its open architecture, macmon is in a powerful position to provide automated support.

Added value to commonly available antivirus systems

Virus scanners cannot always provide complete protection from the constant threats of new Malware and modified viruses. In addition to detecting them, they should also be cleaned. Regular patches, updated virus scanners and other technologies like desktop firewall, host intrusion prevention and application control, indeed provide excellent protection but the effort involved in managing these systems and in keeping them up-to-date is so much that, in general, not all of them are used or their maintenance is neglected.

Key facts

- ✓ **Quick isolation of sources of infection from your network.**
- ✓ **Prompt information about the measure and the threat situation.**
- ✓ **The live asset management of macmon provides information about the endpoint and its location.**
- ✓ **Based on the system information, the affected systems can be cleaned without any hurry and put back into operation.**

The macmon antivirus connector is hence the answer for a solution that responds automatically, if the virus scanner cannot deal with a threat. If the antivirus software on an endpoint reports that a Malware could not be cleaned and removed, then the affected system should be located and isolated as soon as possible in order to intervene manually. Different types of information is provided depending on the antivirus system that is used. Which are evaluated by the antivirus connector. The responses can be defined by oneself starting from a simple notification, over the assignment of a new VLAN to complete isolation of the system. Any virus protection event can be used as the trigger.

However, the macmon antivirus connector basically uses the following situations:

- ➡ an object could not be cleaned and could not be removed
- ➡ a Malware was removed a defined number of times within a specified period
- ➡ a specific Malware (definable) was detected

Different events can also be seen because of the different systems. Thus, the combination with McAfee for example, provides the additional option of responding to “attacks“. If a system (regardless of whether it is your own or external system) attempts to copy a Malware to one of your systems, then it is logged as an attack. Using this information macmon can appropriately deal with the “attacking“ system, even if it is a temporarily authorised guest. macmon antivirus connector is an add-on to the macmon Network Access Control solution and is part of the premium bundle. The licensing takes place through the macmon server or through the Antivirus management instance that is monitored.

The products manufactured by G-Data, F-Secure, Kaspersky, McAfee, Sophos, Symantec and Trend Mirco are supported at present. Other manufacturers are already in direct contact with the macmon development team and will also be integrated soon.

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