MACMON COMPLIANCE

Automated enforcement of the central company and IT security guidelines

In addition to the Network Access Control, detailed monitoring of the authorized systems with respect to compliance with the security guidelines is increasingly important. In many situations, small "security breaches" are adequate to provide easily accessible points of attack. Permanent monitoring of the "compliance status" and automated enforcement of guidelines is thus indispensable. As a specialist for Network Access Control, macmon secure is aware of this requirement. With macmon compliance, macmon is the first manufacturer to offer the option to use multiple, connectable components in order to effectively enforce the company guidelines.

Use of any manufacturer independent sources for ascertaining compliance status

The decisive factor here is that 99% of companies already use systems that is capable of ascertaining the compliance status of the endpoints and informing the administrators about any discrepancies. However, almost all of them commonly require manual enforcement of the guidelines or the enforcement is reactive at best.

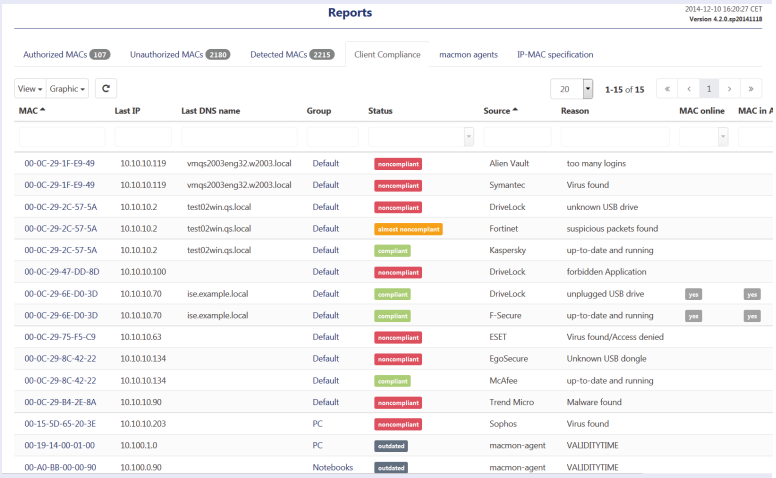
Key facts

- ✓ Comprehensive illustration of compliance statuses through any, vendor independent data providers and optionally through macmon agents
- ✓ Proactive reaction to sources of infection
- ✓ Quick and automated isolation of insecure systems in the network
- ✓ Simple and quick implementtation as no changes are required to the infrastructure
- ✓ Immediate increase of the ROI with the use of all existing systems and investments

Here, macmon Network Access Control solution offers the required, decisive support: The macmon compliance add on module includes four different components: Depending on the requirements, the compliance status can be received from external sources, actively solicited through connection to external databases or actively determined by macmon agents. Additionally, macmon can use events from the integrated IF-MAP technology. The key function therefore takes over the open interface of macmon, that can smartly use any manufacturer independent source to transfer the compliance status of an endpoint to macmon. Connection of multiple and different sources is also easily possible at the same time.

The compliance status for every endpoint is displayed within the macmon GUI. If the status is changed by another system, such as Endpoint Security, Intrusion Prevention, Security Incident and Event Management, Patch Management or Vulnerability Management, the change including information about the source and the reason for the change are displayed. The flexible macmon policy enables configuration of the reaction to the change in status in the usual, simple way. Endpoints that are not compliant any more are then, for example, moved to quarantine and moved back to their original network area after healing and corresponding change to the new status. The options for combination are therefore free from limitations and allows you to use macmon as the central force in the network. Complete vendor independence at this stage adds again value to the investments that have been made by you. Existing systems with the task of monitoring the guidelines obtain an automatically enforcement instance from macmon. A key advantage of the combination of different

solutions is that the responsibilities of the individual IT departments are not altered. The administrator of the respective system decides on how and when a violation of the guidelines will be reacted to. With macmon, the network department offers automation for isolation tasks. They do not have to interfere in any way as isolation and restoration take place automatically as per the policy.



Added value to commonly available antivirus systems: Automatic isolation of infected endpoints

The second component of macmon compliance consists of macmon's own antivirus connector. This active component enables you to connect to diverse antivirus systems such as F-Secure®, G-Data®, Kaspersky®, McAfee®, Sophos®, Symantec®, or TrendMicro® in order to be able to automatically react to critical events without necessitating configurations in the antivirus management tool itself. Virus scanners cannot always provide complete protection from the constant threats of new MalWare and modified viruses. While in addition to detecting them, they also should be cleaned/removed. Regular patches, up-to-date virus scanners and additional technologies such as desktop firewall, host intrusion prevention or application control, offer distinguished protection. However, there are situations in which the virus scanners cannot react appropriately to 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.
macmon antivirus connector identifies these situations and directly isolates the concerned endpoint or changes its status to "Non-Compliant". The macmon policy thereby takes effect, through which the endpoint is isolated or the concerned group of people is informed to avoid further distribution.

Active status change through macmon agents

The third component of macmon compliance consists of Compliance Agents of macmon that are managed centrally using the macmon GUI. If a solution has only been partially implemented for monitoring the compliance of the endpoints with the guidelines or if no solution has been found for the same, the macmon agent is used. Distributed over the company's Windows endpoints, it cyclically determines the status of the antivirus, the firewall, the patch levels and other configurable properties. If the endpoint does not correspond to the specifications, the status is changed and the endpoint is isolated according to the policy - as with the antivirus connector or through another existing compliance system. Regardless of which of the three components are used: Endpoints classified as unsafe are automatically moved to a quarantine VLAN or even a remediation VLAN to update their security statuses in this protected environment. After updating successfully, the systems are immediately reassigned to their original environment in the network.

With the help of the report and statistic functions, macmon compliance offers an extensive overview of the level of security, of the sources transmitting compliance statuses and information on discrepancies in security of the endpoints being managed. The futuristic IF-MAP technology, that was developed in collaboration with Trusted Computing Group, macmon secure and other partners in research projects, has been integrated for the fourth component.

Using this, participating products can publish their status on the network, while macmon can also respond to corresponding messages and in turn isolate threat generating systems from the network. You can find detailed information at www.esukom.de.

Contact

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