ARP-GUARD Endpoint Add-On

Kann die Sicherheit Ihres Unternehmensnetzwerkes den vielschichtigen Forderungen standhalten? Aus Unternehmenssicht stehen hohe Sicherheit und Verfügbarkeit sowie die Erfüllung von gesetzlichen Anforderungen im Fokus. Die Anwender hingegen wollen möglichst schnell und am besten ohne Einschränkungen ihrer Arbeit nachgehen.

ARP-GUARD bietet die Lösung, diese gegensätzlichen Anforderungen zu erfüllen, und unterstützt die IT-Administration, die für beide Seiten notwendigen Bedingungen zu schaffen. So können sich Nutzer flexibel auf die Kernkompetenz des Unternehmens fokussieren, ohne komplexe und verwaltungsintensive Hürden nehmen zu müssen.

Gleichzeitig setzt ARP-GUARD Ihre Unternehmensrichtlinien konsequent um und sichert Ihre Geschäftsprozesse. Aktuell nutzen immer mehr Unternehmen die ARP-GUARD Lösung, um ihre Infrastrukturen intern abzusichern und unbekannte Geräte aus dem Netzwerk auszuschließen.

Doch die mobile Arbeitswelt stellt die IT-Security vor weitere Herausforderungen: Was geschieht z.B. mit Notebooks von Mitarbeitern, die längere Zeit auf Geschäftsreise waren? Wie kann sichergestellt werden, dass die Notebooks erkannt werden und noch den erforderlichen Virenschutz und Updates haben?

Eine manuelle Überprüfung jedes Gerätes auf aktuellen Virenschutz oder Betriebssystemupdates ist aufgrund des immensen personellen Aufwandes kaum zu leisten.

Das ARP-GUARD Endpoint Add-On erfüllt diesen Sicherheitsanspruch automatisiert. Neben der eindeutigen Identifizierung eigener und unerwünschter Endgeräte im Netzwerk wird der Sicherheitszustand jedes einzelnen Gerätes geprüft. Ein bekanntes Endgerät, das nicht über einen aktuellen Virenschutz verfügt oder dessen Software nicht aktuell gewartet ist, wird zuerst in ein Quarantäne-VLAN geleitet. Nach erfolgreicher Aktualisierung und Prüfung verschiebt der ARP-GUARD das Endgerät automatisch in die gewohnte Arbeitsumgebung.

Das ARP-GUARD Endpoint Add-On nutzt unter anderem das WMI-Protokoll, um den aktuellen Sicherheitsstatus eines Windows Clients zu erfahren. Weitere Möglichkeiten sind die Auswertung von Traps.

In keinem Fall ist die Installation von Software auf dem Endgerät erforderlich. Die Aufwendungen zur manuellen Kontrolle des Sicherheitsstatus der einzelnen Geräte entfallen. ARP-GUARD liest alle sicherheitsrelevanten Informationen aus und agiert automatisch und gemäß dem von Ihnen hinterlegten Regelwerk.

Die Kennzeichnung in den Signalfarben grün, gelb und rot bringt eine schnelle Übersicht auf den allgemeinen Zustand aller Geräte. Die Nutzung des WMI-Protokolls macht den ARP-GUARD unabhängig vom Anti-Viren Hersteller. Zusätzlich können Sie weitere, selbst definierte Sicherheitsmerkmale über Ihre Endgeräte auslesen. Durch die intelligente Kombination aus Network Access Control und Endpoint Security steigert ARP-GUARD das Sicherheitsniveau Ihrer Infrastruktur. Die offene Systemarchitektur der ARP-GUARD Produkte bietet somit zusätzlichen Investitionsschutz.

ARP-GUARD Features:

Network Access Control

MAC-Adresse, 802.1X, RADIUS-Authentisierung

Inventarisierung

Zentrale standortübergreifende Administration

Switch-Hersteller unabhängig

VLAN-Management

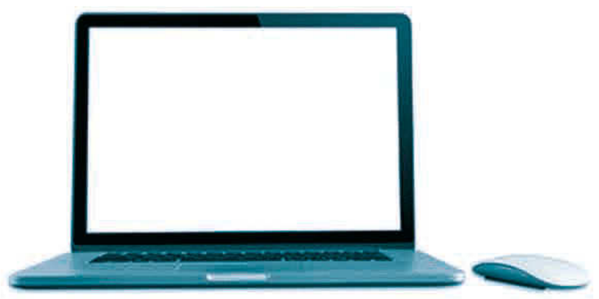
Ohne Client-Installation

IPv6 Support

RADIUS Server

Individuelles Reporting

Gästeticket-System mit Selbstregistrierung



Add-Ons/weitere Produkte

Captive Portal

Cluster

Erhältlich als

Appliance

Virtuelle Appliance

Software

- Linux
- Windows (nur Sensor)

Software Module