ARP GUARD by ISL

mehr als nur

NETWORK ACCESS CONTROL

ÜBERSICHT
KONTROLLE
SICHERHEIT

- CAPTIVE PORTAL
- CLUSTER
- ENDPOINT
- FINGERPRINTING
- GERÄTEERKENNUNG
- SENSOR-MANAGEMENTSYSTEM
- VLAN-MANAGER
- ZUGANGSSCHUTZ

ARP-GUARD ist unsere etablierte Network Access Control (NAC) Lösung, welche sich im Gegensatz zu aufwendigen, komplexen sowie teuren Netzwerkanwendungen auch in heterogenen und großen Netzwerken unkompliziert realisieren lässt. Der Zugangsschutz identifiziert unabhängig von Herstellern oder Technologien bekannte sowie unbekannte Geräte schnell und eindeutig, bevor diese Zugang zum Netzwerk erhalten. Über den Standard eines reinen Zugangsschutzes hinaus, bündelt die Lösung zudem als zentrale Instanz sicherheitsrelevante Informationen, erkennt und meldet Anomalien im Netzwerk und korrigiert sie umgehend.

SecurITy made in Germany

Trust Seal
www.teletrust.de/itsmig

DIE ARP-GUARD LÖSUNG IM DETAIL

GERÄTEERKENNUNG & INVENTARISIERUNG

ARP-GUARD kommuniziert mit der gesamten Netzwerkinfrastruktur und erfasst innerhalb kürzester Zeit alle im Netzwerk befindlichen Systeme. Jedes Endgerät wird sichtbar und Störquellen lassen sich schnell lokalisieren sowie beseitigen. Zudem stellt die Lösung die gesamte Architektur in einer grafischen Topologie dar. Das erleichtert nicht nur die Netzwerkplanung. Es ermöglicht insbesondere die von Audits und Revision geforderte Transparenz.

ZUGANGSSCHUTZ

Die zentrale Steuerung und Regulierung aller Netzwerkzugänge bietet eine umfassende Kontrolle. Unbekannte Geräte werden in Echtzeit erkannt und gemeldet. Nach der eindeutigen Identifizierung erfolgt das weitere Vorgehen. Von der sofortigen Portabschaltung bis zur Verlegung in ein spezielles Virtual Local Area Network (VLAN) kann jede gewünschte Aktion im Regelwerk für das gesamte Netzwerk festgelegt und verwaltet werden.

NETZWERKSEGMENTIERUNG MIT VLAN-MANAGER

Mit dem VLAN-Management lässt sich die Segmentierung in VLANs einfach umsetzen und komfortabel verwalten. Sensible Bereiche werden dadurch zusätzlich geschützt, öffentliche Bereiche klar von internen abgegrenzt und Gästen sowie Dienstleistern nur spezieller Zugang gewährt. Statt manueller Einrichtung auf den einzelnen Switch-Ports erfolgt die Zuweisung in das zugehörige VLAN automatisiert nach Regelwerk. Mitarbeiter, die umziehen, reisen oder an anderen Standorten arbeiten, nehmen immer ihre Umgebung mit.

FINGERPRINTING

Die Kombination verschiedener Authentifizierungsmethoden, wie MAC-based RADIUS und 802.1X, bietet Sicherheit und Flexibilität. Wir ergänzen diese Methoden zusätzlich durch das ARP-GUARD Fingerprinting. Es erfasst verschiedene Eigenschaften, z. B. kryptografische Zertifikate und Schlüssel, um ein Gerät wirklich eindeutig zu identifizieren.

SENSOR-MANAGEMENT-ARCHITEKTUR

Durch die besondere Sensor-Management-Architektur ist ARP-GUARD mandantenfähig und enorm skalierbar. Der Einsatz von Sensoren ermöglicht die effektive Einbindung beliebig vieler Standorte. Das Umbrella-Management ermöglicht hierbei die Verwaltung dezentraler, großer Netzwerkumgebungen. Dabei ist ein zentrales Regelwerk wie ein Schirm über das gesamte Netzwerk ausgebreitet, simpel und automatisiert. Benutzer, Rollen, Rechte und Policies werden synchronisiert. Sensoren können jedoch auch dezentral eingesetzt werden.

ARP-GUARD ADD-ONS

CAPTIVE PORTAL - GASTZUGÄNGE & BOYD

Das Captive Portal Add-on regelt den Netzwerkzugang von Gast- und Fremdkomponenten, z. B. Smartphones oder Notebooks. In jeder Umgebung können für Fremdgeräte gezielte Netzwerkzugänge definiert werden, jederzeit kontrolliert durch ein dynamisches Firewall-Regelwerk, dank der Sensor-Management-Architektur auch standortübergreifend. Somit ist Bring Your Own Device (BYOD) einfach zu verwirklichen und die privaten Devices erhalten nur per Regelwerk explizit freigegebene Zugriffe.

NETZWERKINTEGRITÄT AN ALLEN ENDGERÄTEN

Die ARP-GUARD Endpoint-Funktion liefert eine wertvolle Unterstützung für die Umsetzung von Compliance-Anforderungen. Während der Authentifizierung wird geprüft, ob Endgeräte den Sicherheitsrichtlinien entsprechen und bezüglich sicherheitsrelevanter Details, z. B. Status, Antivirus oder Patch-Level des Betriebssystems compliant sind. Werden die Richtlinien nicht erfüllt, wird das Gerät isoliert und beispielsweise in einem Quarantäne-VLAN aktualisiert. Erst nach der Prüfung bzw. Anpassung erhalten die Devices einen Zugang zu den Netzwerkbereichen.

CLUSTER-HOCHVERFÜGBARKEIT FÜR SENSIBLE IT-BEREICHE

Das Cluster Add-on ermöglicht mit einfachen Soft- und Hardwaremitteln eine Server-Replikation zur erhöhten Ausfallsicherheit sowie Skalierbarkeit für kritische IT-Systeme.

ARP-GUARD AUF EINEN BLICK

- Geräteerkennung und -inventarisierung
- Grafische Darstellung der Netzwerkinfrastruktur
- Zentralisierte Kontrolle und Überwachung der Netzwerkzugänge
- Zentrale Definition und Durchsetzung von Richtlinien in Echtzeit
- Netzwerksegmentierung
- LAN/WLAN Netzwerkintegrität bis zu den Endgeräten
- Einzigartiges Fingerprinting zur eindeutigen Device-Identifizierung
- Compliance-Prüfung der Endgeräte
- Regulierung von Gastzugängen und BYOD
- Reduzierung von IT-Verwaltungsaufwand durch Automatisierung
- Hersteller- und technologieunabhängig
- Unterstützung von ISO/IEC 27001, DIN EN 80001-1, PCI/DDS
- Deutschsprachiger Support

IHRE MEHRWERTE

EINFACHE IMPLEMENTIERUNG

Bereits mit der erfolgreichen Basisinstallation wird ein deutlich höheres Sicherheitsniveau erreicht, welches Schritt für Schritt weiter ausgebaut werden kann. Die Integration in die bestehende Infrastruktur erfolgt nahtlos und störungsfrei, ohne dass Änderungen oder weitere Investitionen notwendig sind.

BEREITSTELLUNG

Das ARP-GUARD Management wird als virtuelle und physische Appliance zur Verfügung gestellt. Bei einer Clusterinstallation besteht zudem die zusätzliche Möglichkeit eines Mischbetriebs. Außerdem können Sensoren auch direkt auf den unternehmenseigenen Servern installiert werden

BRANCHENÜBERGREIFENDE STÄRKEN

ARP-GUARD kommt in allen Bereichen zum Einsatz. Neben Industrie, Handel, Gesundheitswesen, Behörden, Bildung und Forschung, ist die Lösung vor allem im Finanzsektor, als einer der sicherheitssensibelsten Branchen überhaupt, nicht wegzudenken. Die Flexibilität, Architektur und Funktionsweise von ARP-GUARD eignen sich hervorragend für kritische Infrastrukturen (KRITIS). Die Erfüllung der Sicherheitsanforderungen nach ISO 27001 und DIN EN 80001-1, PCI/DSS sowie die Zertifizierung auf der Basis des IT-Grundschutzes sind für uns selbstverständlich.

METHODENMIX FÜR MEHR SICHERHEIT & FLEXIBILITÄT

ARP-GUARD deckt die gesamte Bandbreite der Authentifizierungsmöglichkeiten ab. Mit der 4.0 Version ist das Zusammenspiel zu einer perfekten Symbiose auf aktuellstem Entwicklungsstand gereift. Die Lizenz ermöglicht den Mischbetrieb von SNMP, MAC based RADIUS und 802.1X mit dem gleichen Feature-Set. Auch eine spätere Migration von SNMP zu 802.1X ist einfach zu verwirklichen.

SERVICE & SUPPORT

Unsere qualifizierten und erfahrenen ARP-GUARD Partner unterstützen Sie als 1. Instanz gern bei sämtlichen Problemstellungen und Support-Angelegenheiten.
www.arp-guard.com/kontakt/vertriebspartner

Darüber hinaus profitieren Sie auch von unseren umfassenden Serviceangeboten: Software-Subscription (Zugriff auf alle Minor- und Major Releases, Updates sowie neue Versionen), Third-Level-Support (Herstellerunterstützung zur kundenspezifischen Optimierung und Anpassung), technisches Training.

SPEZIFIKATIONEN

Virtualisierungsplattformen

Virtuelle Appliances werden unterstützt auf

- VMware
- Microsoft Hyper-V
- KVM

Unterstützte Betriebssysteme

- Linux, Red Hat
- DOMOS
- CentOS
- Microsoft (Sensoren)

Authentifizierungsmethoden

- MAC-based RADIUS
- EAP
- SNMP
- 802.1X

Protokolle

- RADIUS
- SNMP
- SSH
- Telnet
- DHCP
- LDAP
- HTTPS
- Kerberos
- WMI

Browserunterstützung

- Google Chrome
- Mozilla Firefox
- Safari
- Microsoft Internet Explorer
- Microsoft Edge