ISL Internet Sicherheits-lösungen GmbH

ARP GUARD by ISL

ZERO TRUST NETWORK ACCESS

ARP-GUARD unterstützt Sie bei der Umsetzung eines netzwerkbasierten Zero Trust-Modells, das jedem Zugriff misstraut und jede Verbindung eineindeutig authentifiziert.

Unsere Fingerprint-Technologie identifiziert Geräte zweifelsfrei und lässt Netzwerkzugriff nur für autorisierte Geräte zu. Jeder Netzwerkzugriff wird in Echtzeit erfasst, bewertet und bei Anomalien sofort gemeldet, für maximale Transparenz, Kontrolle und Sicherheit.

Durch zentrale Orchestrierung, dynamische Regelwerke und VLAN-Segmentierung schützen Sie sensible Bereiche zuverlässig. Dank der skalierbaren Sensor-Architektur und Enterprise Management sichern Sie Ihr Unternehmen standortübergreifend, mandantengetrennt und georedundant ab.

Unabhängig von Hersteller oder Technologie profitieren Sie von unserer Multi-Vendor-Strategie und integrieren ARP-GUARD nahtlos in Ihre bestehende IT-Infrastruktur.

NEXT-GEN NETWORK ACCESS CONTROL

BASIS-FUNKTIONEN

NETZWERKZUGANGSKONTROLLE

Erkennt Geräte in Echtzeit, verhindert unautorisierte Zugriffe und schützt durch Mechanismen wie Fingerprinting, VLAN-Management vor schwererkennbaren Angriffen wie etwa MAC-Spoofing. Über flexible Regeln, Schnittstellen und Integrationen in SIEM- oder Monitoring-Systeme lassen sich Sicherheitsmaßnahmen automatisieren und Netzwerke herstellerunabhängig absichern.

FINGERPRINTING

Diese Technologie erstellt für jedes Endgerät einen eineindeutigen digitalen Fingerabdruck auf Basis charakteristischer Merkmale und verhindert so zuverlässig MAC-Spoofing sowie unautorisierte Zugriffe. Multi-Fingerprinting, umfassende Protokollunterstützung und automatisierte Regeln gewährleisten ein hohes Maß an Sicherheit, das mit 802.1X vergleichbar ist, jedoch eine deutlich größere Flexibilität bietet. Auch für Geräte, welche keine zertifikatsbasierte Authentifizierung unterstützen.

GERÄTEERKENNUNG

ARP-GUARD verschafft vollständige Transparenz über alle im Netzwerk befindlichen Geräte, erfasst deren Verbindungen in Echtzeit und stellt die Informationen in einer grafischen Topologie dar. Die Integration von SNMP, automatisierten Abfragen und Reporting ermöglicht effizientes Netzwerkmonitoring, schnelle Störungsbehebung und die Einhaltung von Audit- und Revisionsanforderungen.

NETZWERKSEGMENTIERUNG

Hiermit lassen sich Netzwerke zentral, herstellerunabhängig und automatisiert segmentieren, wodurch sensible und öffentliche Bereiche klar abgegrenzt und geschützt werden. Geräte erhalten standortübergreifend automatisch das passende VLAN, während Captive Portals, flexible Regelwerke und zentrale Verwaltung eine einfache und sichere Handhabung ermöglichen.

SENSOR-MANAGEMENT

Ermöglicht die zentrale, hochskalierbare Verwaltung verteilter Netzwerke mit unbegrenzt vielen Sensoren und eignet sich dadurch besonders für Unternehmen mit mehreren Standorten. Mit dem Enterprise Management wird diese Flexibilität auf global agierende Organisationen mit typischerweise über 100.000 Endgeräten in mandantenfähigen Umgebungen ausgeweitet.

MODULARE ERWEITERUNGEN

CAPTIVE PORTAL

Ermöglicht die sichere und kontrollierte Vergabe von Netzwerkzugängen für Gäste und BYOD-Geräte, die individuell per Regelwerk eingeschränkt werden können. Es ist standortübergreifend einsetzbar, vollständig anpassbar an das Corporate Design und unterstützt komfortable Verfahren wie Selbstregistrierung oder Sponsoring.

ENDPOINT

Überprüft Endgeräte agentenlos, innerhalb des Netzwerks, während der Authentifizierung auf Compliance- und Sicherheitsrichtlinien wie Antivirus-Status oder Patch-Level. Nicht konforme Geräte werden automatisch isoliert, bis sie die Vorgaben erfüllen, wodurch die Netzwerkintegrität bis zum Endgerät sichergestellt wird.

LAYER 2 IPS

Überwacht den Netzwerkverkehr in Echtzeit, erkennt Man-in-the-Middle-Angriffe wie ARP-Poisoning oder MAC-Spoofing und wehrt Angriffe automatisch nach definierten Regeln ab. So wird ein hoher Schutz vor internen Bedrohungen und maximale Transparenz über Angriffsquellen gewährleistet.

CLUSTER MANAGEMENT

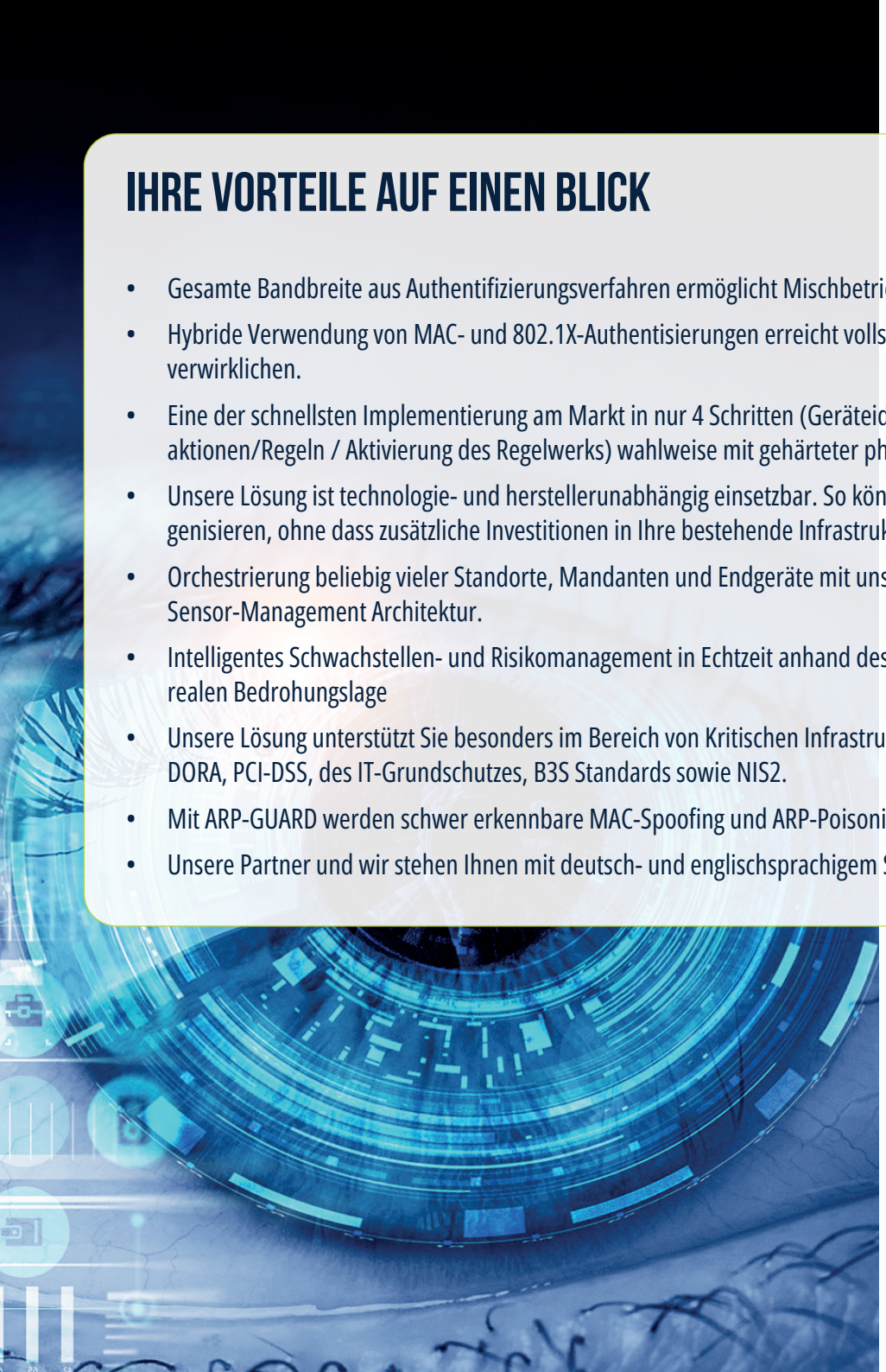
Sorgt durch automatische Server-Replikation und georedundante Ausfallsicherheit für einen hochverfügbaren, unterbrechungsfreien Betrieb kritischer IT-Systeme. Im Störfall übernimmt ein Ersatzsystem nahtlos alle Funktionen, wodurch maximale Systemsicherheit und Verfügbarkeit gewährleistet werden.

ENTERPRISE-MANAGEMENT

Zentrale Steuerung mehrerer unabhängiger Instanzen, wodurch Konfigurationen, Richtlinien und Protokolldaten standortübergreifend synchronisiert und verwaltet werden können. Dabei bleiben die lokalen Systeme autark funktionsfähig, während Mandantenfähigkeit, Single Sign-On und zentrale Sicherheitsüberwachung den Betrieb in großen, komplexen Netzwerkumgebungen unterstützen.

CLIENT-GUARD

Zur Durchsetzung von Compliance-Richtlinien auch für Endgeräte, die außerhalb des Firmennetzwerks genutzt werden. Es sammelt Geräteinformationen, bewertet Sicherheitszustände wie installierte Software und Versionsstände und gesteuert über zentrale Regelwerke entscheidet er über Zugriff oder Sperrung des remote Zugangs, sodass ein hoher Schutz auch bei remote genutzten Clients gewährleistet ist.



IHRE VORTEILE AUF EINEN BLICK

- Gesamte Bandbreite aus Authentifizierungsverfahren ermöglicht Mischbetrieb aus SNMP, MAC based RADIUS und 802.1X mit dem gleichen Feature-Set.
- Hybride Verwendung von MAC- und 802.1X-Authentisierungen erreicht vollständige NAC-Abdeckung, eine spätere Migration von SNMP auf 802.1X ist bei Bedarf einfach zu verwirklichen.
- Eine der schnellsten Implementierung am Markt in nur 4 Schritten (Geräteidentifizierung und -lokalisierung / Klassifizierung der Endgeräte / Definition individueller Reaktionen/Regeln / Aktivierung des Regelwerks) wahlweise mit gehärteter physikalischer und/oder virtueller Appliance.
- Unsere Lösung ist technologie- und herstellerunabhängig einsetzbar. So können Sie Ihr Netzwerk unter Network Security und Management Aspekten durchgängig homogenisieren, ohne dass zusätzliche Investitionen in Ihre bestehende Infrastruktur notwendig werden.
- Orchestrierung beliebig vieler Standorte, Mandanten und Endgeräte mit unserem Enterprise Management unter dem Einsatz der revolutionären und hochskalierbaren Sensor-Management Architektur.
- Intelligentes Schwachstellen- und Risikomanagement in Echtzeit anhand des Industriestandards Common Vulnerability Scoring System (CVSS) unter Berücksichtigung der realen Bedrohungslage
- Unsere Lösung unterstützt Sie besonders im Bereich von Kritischen Infrastrukturen bei wichtigen Zertifizierungen wie ISO/IEC 27001, TISAX, ISO 27799, DIN EN 80001-1, DORA, PCI-DSS, des IT-Grundschutzes, B3S Standards sowie NIS2.
- Mit ARP-GUARD werden schwer erkennbare MAC-Spoofing und ARP-Poisoning-Angriffe effektiv verhindert und das Sicherheitsniveau Ihres Netzwerks signifikant erhöht.
- Unsere Partner und wir stehen Ihnen mit deutsch- und englischsprachigem Support zur Verfügung.

SecurITy made in Germany

Trust Seal
www.teletrust.de/itsmig

Mit ARP-GUARD, einer der weltweit ersten Lösungen für Network Access Control, behalten Unternehmen die volle Kontrolle über ihre Netzwerkzugriffe und Daten – und sichern sich ihre digitale Souveränität, unabhängig von Drittstaaten und anderen Vorschriften außerhalb der EU. Unsere Lösung ist „Made in Germany" und steht für ein Höchstmaß an IT-Sicherheit und Datenschutzkonformität, wodurch die Einhaltung lokaler gesetzlicher Anforderungen zuverlässig unterstützt wird. Zusammen mit über 50 Vertriebspartnern und fünf Technologiepartnern aus Deutschland, Frankreich und Italien bilden wir einen europäischen Standard für resiliente Netzwerksicherheit.

SPEZIFIKATIONEN

VIRTUALISIERUNGSPLATTFORMEN

Virtuelle Appliances werden unterstützt auf:

- VMware
- Microsoft Hyper-V
- KVM

UNTERSTÜTZTE BETRIEBSSYSTEME

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

AUTHENTIFIZIERUNGSMETHODEN

- MAC-based RADIUS
- EAP-PEAP TLS
- SNMP V3
- 802.1X
- LDAP(S)
- TACACS+

PROTOKOLLE

- RADIUS
- SNMP
- SSH
- Telnet
- DHCP
- LDAP
- HTTPS
- Kerberos
- WMI
- PowerShell
- TACACS+

BROWSERUNTERSTÜTZUNG

- Google Chrome
- Mozilla Firefox
- Apple Safari
- Microsoft Edge