ARP GUARD by ISL

SERVICE

CLIENT-GUARD

Network Access Control

SecurITy made in Germany

Trust Seal www.teletrust.de/itsmig

DIE REVOLUTION VON NETWORK ACCESS CONTROL

HERAUSFORDERUNGEN VON STANDORTUNABHÄNGIGEN ENDGERÄTEN

Die Verwaltung von Netzwerkzugriffen stellt eine zentrale Herausforderung dar, insbesondere im Kontext des zunehmenden Trends zum standortunabhängigen Arbeiten. Bisher war die Einbindung externer Geräte, beispielsweise aus dem Homeoffice über VPN, in die Netzwerkinfrastruktur eine besondere Herausforderung hinsichtlich der Einhaltung von Compliance-Richtlinien.

CLIENT-GUARD ALS NEUER STANDARD FÜR UMFASSENDE COMPLIANCE

Um die Resilienz des Unternehmensnetzwerks zu stärken, vornehmlich in Situationen, in denen Endgeräte außerhalb des Firmennetzwerks genutzt werden, ist ein erhöhtes Maß an Sicherheit erforderlich, um das Risiko für die gesamte IT-Infrastruktur zu minimieren. Der Client setzt einen neuen Standard für die Einhaltung von Compliance-Richtlinien für standortunabhängig genutzte Endgeräte.

Dabei bleibt der volle Funktionsumfang von ARP-GUARD für die Orchestrierung und Durchsetzung von Compliance-Richtlinien erhalten, um ein Höchstmaß an Sicherheit zu gewährleisten.

DEVICE INFORMATION & ACCESS CONTROL

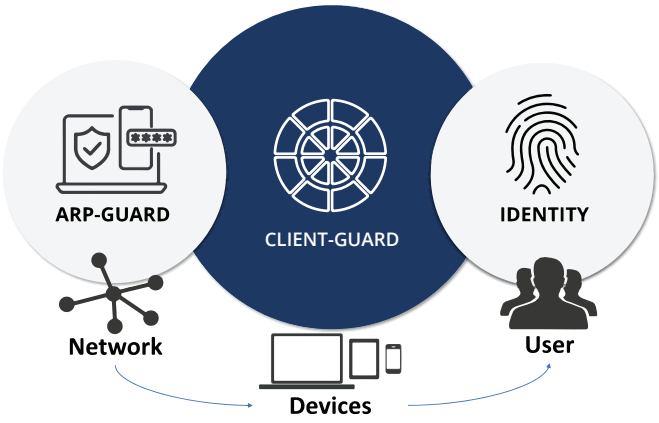
Der CLIENT-GUARD übernimmt wichtige Funktionen im Bereich der Geräteinformationen und des Zugriffskontrollmanagements. Zunächst ermittelt er die Identität der angeschlossenen Geräte und sammelt umfassende Informationen. Hierzu gehört auch die Erfassung von Daten, um die Einhaltung der Endpunktrichtlinien und den Compliance-Zustand sicherzustellen. Basierend auf diesen Informationen kann der Client verschiedene Aktionen ausführen. Er hat die Fähigkeit, den Netzwerkzugang für Geräte zu gewähren oder zu verweigern, je nach den definierten Richtlinien und Sicherheitsanforderungen. Das zentrale Management ermöglicht es, universale Regelwerke für Endpunkte zu hinterlegen. Dadurch können spezifische Anforderungen und Sicherheitsrichtlinien für jedes Gerät im Netzwerk definiert werden.

UMFASSENDE TRANSPARENZ

Durch eine grundlegende Sicherheitsüberprüfung wird sichergestellt, dass sicherheitsrelevante und erforderliche Anwendungen ordnungsgemäß installiert und versioniert sind. Dies umfasst unter anderem Anti-Malware-Programme, Firewalls, Verschlüsselungssoftware, Webbrowser, Kommunikationstools und VPNs. Zusätzlich werden Informationen, wie Benutzerinformationen, Betriebssysteminformationen, eine Liste der installierten Anwendung inkl. Zertifikatsstatus ausgegeben. Diese Informationen ermöglichen es, einen umfassenden Überblick über die Sicherheits- und Konfigurationsaspekte aller externen Geräte zu erhalten und sicherzustellen, dass sie den geltenden Sicherheitsstandards entsprechen.

DER WEG ZUM ZERO-TRUST-ANSATZ

Mit unserem ARP-GUARD Network Access Control, unserem CLIENT-GUARD und unserer IDENTITY Lösung machen wir Sie bereit für Zero Trust. Mit ARP-GUARD NAC erfolgt die Identitätsprüfung durch eine eigene Fingerprint-Technologie; jeder Zugriffsversuch wird in Echtzeit erfasst. Der Client berücksichtigt den Zustand und die Compliance der Geräte, indem er wichtige Kontextinformationen bereitstellt. IDENTITY ermöglicht eine Zugriffsberechtigung basierend auf dem „Least Privilege“ Prinzip und setzt starke Multi-Faktor-Authentifizierungsmethoden ein, um die Sicherheit der Zugriffe weiter zu erhöhen und unautorisierte Zugriffe zu verhindern.



DIE VORTEILE VOM CLIENT-GUARD AUF EINEN BLICK

- Ressourcenschonender Client „as a Service“ aus deutschen und zertifizierten Rechenzentren
- Umfassende Transparenz und Kontrolle für alle Endgeräte inner- und außerhalb des Firmennetzwerkes
- Universale Richtlinien für alle angebundenen Clients können festgelegt werden
- Common Vulnerability or Exposures (CVE) in CLIENT-GUARD hinterlegt und in einem Scoring zusammengefasst
- In Kombination mit ARP-GUARD NAC und IDENTITY der ideale Weg zum Zero-Trust-Konzept