ARP GUARD by ISL

SERVIZIO

CLIENT-GUARD

Network Access Control

SecurITy made in Germany

Trust Seal www.teletrust.de/itsmig

LA RIVOLUZIONE DEL NETWORK ACCESS CONTROL

LE SFIDE PER I DISPOSITIVI FINALI CON ACCESSO DA REMOTO

La gestione degli accessi alla rete rappresenta una sfida fondamentale, soprattutto nell'ambito della crescente tendenza al lavoro da remoto. Fino ad oggi, l'integrazione di dispositivi esterni nell'infrastruttura di rete, ad esempio in smartworking tramite VPN, rappresentava una sfida particolare in termini di rispetto delle policy di sicurezza.

CLIENT-GUARD: UNA NUOVA SOLUZIONE PER UNA COMPLIANCE A 360°

Per rafforzare la resilienza della rete aziendale, soprattutto in situazioni in cui i dispositivi finali vengono utilizzati da remoto, è necessario un maggiore livello di sicurezza per ridurre al minimo il rischio per l'intera infrastruttura IT. CLIENT-GUARD stabilisce un nuovo standard per le policy di sicurezza che riguardano i dispositivi finali utilizzati da remoto, mantenendo tutte le funzionalità di ARP-GUARD per la gestione e l'applicazione dei criteri di conformità e garantendo così il massimo livello di sicurezza.

DEVICE INFORMATION & ACCESS CONTROL

CLIENT-GUARD si occupa della gestione delle informazioni relative ai dispositivi e del controllo degli accessi. In primo luogo, determina l'identità dei dispositivi connessi e raccoglie informazioni complete. Ciò include anche la raccolta di dati al fine di garantire lo stato di conformità e l'adempimento delle policy di sicurezza dei dispositivi finali. Sulla base di queste informazioni, CLIENT-GUARD può eseguire diverse azioni, ad esempio ha la possibilità di concedere o negare l'accesso alla rete ai dispositivi in base alle policy e ai requisiti di sicurezza definiti. Il sistema di gestione centralizzato consente di configurare set di regole personalizzate per i dispositivi finali. In questo modo è possibile definire requisiti specifici e policy di sicurezza per ogni dispositivo della rete.

COMPLETA TRASPARENZA

Un controllo di sicurezza di base assicura che le applicazioni necessarie e rilevanti per la sicurezza siano installate e aggiornate correttamente. Ciò include programmi anti-malware, firewall, software di crittografia, browser web, strumenti di comunicazione e VPN. Inoltre, vengono fornite informazioni come quelle relative all'utente, al sistema operativo e un elenco delle applicazioni installate, compreso lo stato dei certificati. Queste informazioni consentono di ottenere una panoramica completa degli aspetti di sicurezza e di configurazione di tutti i dispositivi esterni e di garantire la loro conformità agli standard di sicurezza applicabili.

IL PERCORSO VERSO L'APPROCCIO ZERO TRUST

Con ARP-GUARD Network Access Control, CLIENT-GUARD e la soluzione IDENTITY, vi prepariamo al meglio all'approccio Zero Trust. Con ARP-GUARD NAC, vengono verificate tutte le identità utilizzando la nostra tecnologia di Fingerprinting e ogni tentativo di accesso viene registrato in tempo reale. CLIENT-GUARD tiene conto dello stato e della conformità dei dispositivi, fornendo importanti informazioni contestuali. IDENTITY consente di autorizzare l'accesso in base al principio del „Least Privilege" e utilizza metodi di autenticazione a più fattori per aumentare ulteriormente la sicurezza dell'accesso e prevenire gli accessi non autorizzati.

VANTAGGI DEL CLIENT-GUARD IN SINTESI

- Client „as a Service" che ti permette di risparmiare risorse, ospitato in data centre tedeschi e certificati
- Trasparenza e controllo completi di tutti i dispositivi finali all'interno e all'esterno della rete aziendale
- Set di regole configurabili individualmente per policy di sicurezza e requisiti di conformità dedicati
- In combinazione con ARP-GUARD NAC e IDENTITY, il percorso ideale verso l'approccio Zero Trust