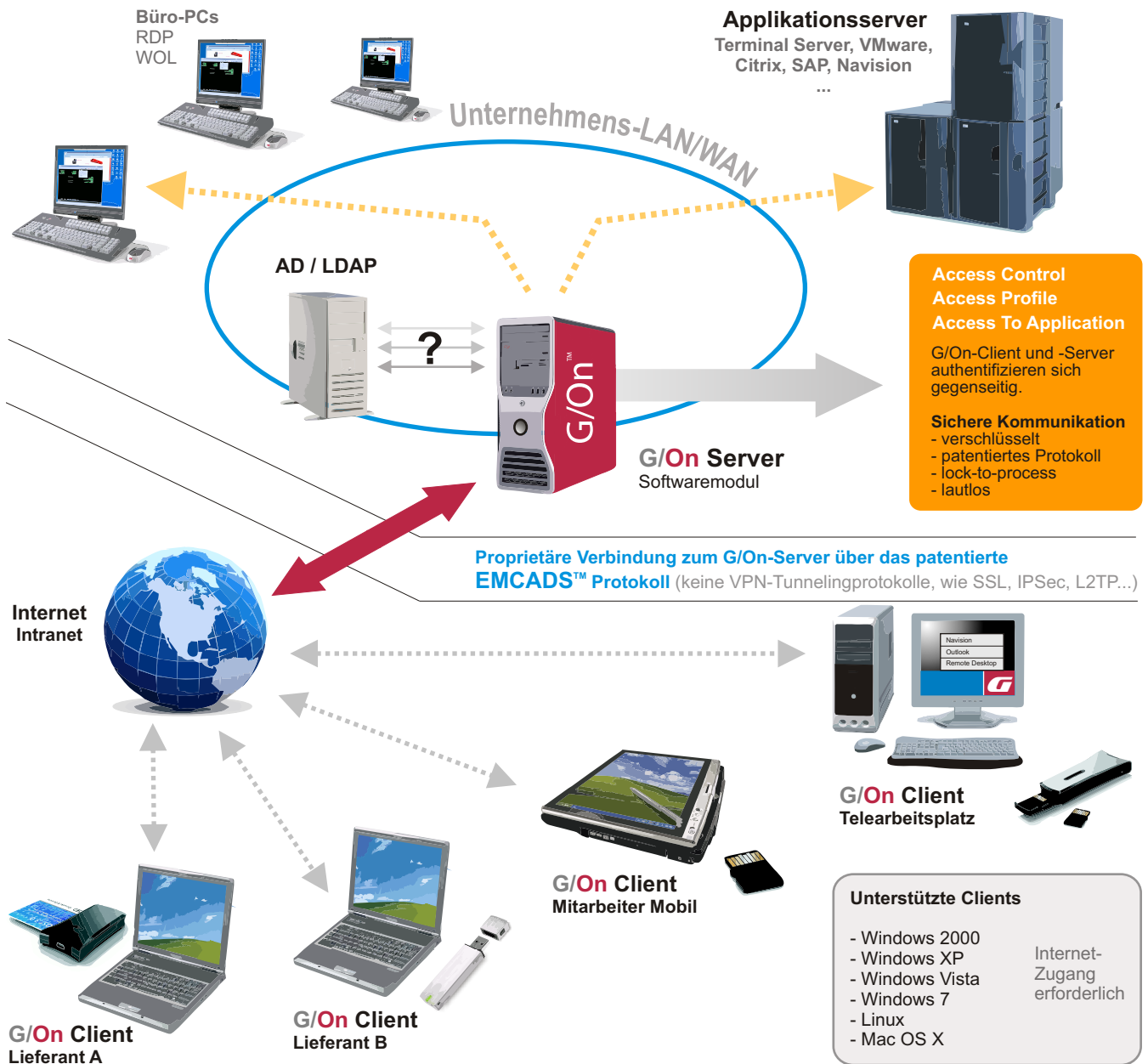


# G/On™ Funktionsschema & Sicherheit



## Grundsätzliches

- alle Anwendungen werden innerhalb des Netzwerks sicher betrieben
- der externe Client ist **nie Mitglied im LAN** - er erstellt nur eine virtuelle, auf den Prozess gelockte Verbindung (nodeless client)
- auf dem Client werden **keine Entscheidungen** bezüglich des Zugriffs (Rechte, Anwendungen) getroffen
- es sind **keinerlei** VPN-Konfigurationen erforderlich
- die externen Zugänge setzen **keine zu installierende Software** auf den jeweiligen PCs voraus
- Nutzer wählt aus dem vom Server angebotenen Applikations-Menü

**Access Control**  
**Access Profile**  
**Access To Application**

- ist der Zugang für diesen Token-Gerät am G/On Server eindeutig freigeschaltet?
- ist Benutzer vereinbart (aus AD- / LDAP- oder G/On-Benutzerdatenbank) und das Passwort gültig?
- ist der Zugriff durch freigeschaltete G/On-Lizenzen abgedeckt?
- sind weitere, optionale (Zugriffs)Parameter eingehalten?

## Der G/On Server

Der G/On Server ist die Schaltzentrale für alle Funktionen. Er implementiert die Funktionalität, die für den sicheren Zugriff von Nutzern auf alle Anwendungen notwendig ist. Komplexe Strukturen aus mehrstufigen Firewalls, Authentifizierungssystemen, Zertifikat- und Tokenservern, DMZ usw., die die man üblicherweise in VPN basierten IT-Umgebungen antrifft, können entfallen. Folglich lässt sich durch den Einsatz des G/On Servers die Infrastruktur deutlich vereinfachen und mit drastisch reduzierten Kosten betreiben.

### Firewall auf Applikationsebene

Der G/On Gateway Server und der G/On Client inspizieren den gesamten Datenverkehr und entscheiden, was erlaubt ist und was abgelehnt wird. Gegenüber herkömmlichen, applikationsbasierten Firewalls geht G/On deutlich weiter: Die Lösung kontrolliert die gesamte end-to-end Kommunikation und erlaubt nur Traffic von authentifizierten Nutzern auf autorisierte Anwendungen. G/On kennt den User, den Applikationsclient und die Anwendungsserver für jedes einzelne Datenpaket, das transportiert wird. Diese Informationen werden ausgewertet, um zu entscheiden, was weitergeleitet und was abgelehnt wird.

### Proxy Funktionalität

Der G/On Gateway Server implementiert die G/On Proxy-Funktionalität, um externe Applikationsclientverbindungen von den internen Applikationsserververbindungen zu separieren. Der Gateway Server ist der Schlüssel zum Aufbau von virtuellen end-to-end Verbindungen, einem wesentlichen Merkmal der G/On Technologie.

### Application Access Control

Im Gegensatz zur herkömmlichen Network Admission Control (NAC), stellt G/On keinen Zugriff auf das Netzwerk zur Verfügung. Die G/On Architektur ist vielmehr so aufgebaut, dass detaillierte Informationen über die Geräte der Anwender gesammelt und als Teil einer vollständigen Autorisierungsentscheidung verwendet werden (device authentication).

Nur Verbindungen von authentifizierten Nutzern und zugelassenen Anwendergeräten werden für den Zugriff auf definierte Anwendungen über spezifische Applikationsclients autorisiert. Wo also klassische NAC-Systeme entscheiden, welche Geräte auf das gesamte Netzwerk zugreifen dürfen (und in welchem Zustand diese Maschinen sein müssen), richtet G/On den Fokus auf den Nutzer und die Applikation - und genau diese Information entscheidet, ob das Gerät, das der Anwender gerade benutzt, am G/On

Server bekannt ist oder nicht. Dies ist eine weitaus einfachere Autorisierungsentscheidung, da sie darauf basiert, welche Aktion der Nutzer auszuführen versucht, anstatt nur das Gerät zu untersuchen und außer Acht zu lassen, was der Anwender tut, nachdem er einen Zugriff erhalten hat.

### Authentifizierung der Nutzer

Wenn Sicherheitsrichtlinien wirklich sinnvoll sein sollen, dann ist die Überprüfung der Identität des Remoteanwenders durch Multi-Faktor-Authentifizierungslösungen zwingend erforderlich. Komplex werden solche Verfahren, sobald das Unternehmen verschiedene Technologien und Richtlinien für eine starke Authentifizierung kombiniert. G/On erlaubt deshalb die Zusammenführung verschiedener Authentifizierungstechnologien und Richtlinien in einer einfach zu verwaltenden "Single-Point-Of-Management"-Plattform.

### Implementierung und Durchsetzung von Sicherheitsrichtlinien

Am G/On Management Server erfolgt die zentrale Administration (Single Point of Management) zur Implementierung, Dokumentierung und Durchsetzung von Zugriffssicherheitsrichtlinien. Protokolle des Traffics im XML-Format ermöglichen ereignisbasierte Alarmmeldungen sowie Auswertungsoptionen für interne sowie externe Audits (Ausführungsbestimmungen, Compliance usw.).

## Der G/On Client

Der G/On Client sorgt dafür, dass alle Entscheidungen des Servers auf der

Clientseite implementiert und durchgesetzt werden. Zusätzlich steuert er den Anwenderdialog, adaptiert Hinweise, Warnmeldungen und Aktivitätsanzeigen auf das Endgerät (z. B. das genutzte Betriebssystem). Er zeigt das Ergebnis der Autorisierungsentscheidungen in Form von nutzerspezifischen Menüs an und akzeptiert Menüauswahlen bzw. handelt aufgrund dieser entsprechend.

### Authentifizierung und Autorisierung

kontrolliert durch den G/On Server, abhängig von den verfügbaren Authentifizierungsoptionen

### Launch and Traffic

starten des autorisierten Applikationsclients und Transportieren des Datenverkehrs zwischen Applikationsclient und G/On Server im Netzwerk

### Anwenderdialog

für die Anmeldung (Login) sowie die Darstellung des für den Nutzer gültigen Autorisierungsergebnisses (wie und in welcher Form darf er auf Applikationen zugreifen)

### Deployment

der lokalen Software auf das Anwendergerät, basierend auf der Anforderung des Nutzers oder des G/On Servers.

Sämtliche clientseitigen Funktionen inkl. Konfiguration und Einrichtung der Anwenderdialoge sind vollständig über den G/On Server kontrolliert.

## G/On Virtual Access - Technologie und Sicherheit

### • Virtuelle Verbindung

Im Gegensatz zur üblichen VPN-Praxis, macht G/On den Remote-PC nicht zum Teil des Unternehmensnetzwerks. Nutzer greifen über eine virtuelle Client/Server-Verbindung auf Applikationen zu (Distributed Port Forwarding Proxy). G/On nutzt keine Tunnelingprotokolle wie IPSec, SSL, L2TP oder PPTP.

### • Starke Verschlüsselung

Wechselnde 256-bit AES Schlüssel, getrennt für Up-/Downstream. 163-bit ECC für das zeichnende Schlüsselpaar (Client/Server) und den Schlüsselaustausch. Prüfsummen (SHA-1 Hashing) verhindern Man-in-the-Middle-, Relay- und Spoofing-Angriffe.

### • n-Faktor Authentifizierung / Token und Hardware-ID

G/On integriert eine gegenseitige 2- bis n-Faktor-Authentifizierung. Akzeptierte Token-Hardware, Username mit Passwort, Regeln und mehr sichern das System.

### • Umfassender Schutz vor Malware / lock to process

Eine Kompromittierung durch, Viren, Trojaner, Spyware oder Hacking ist aufgrund der fehlenden IP-Verbindung sowie "lock-to-process" ausgeschlossen.

### • Zentrale Autorisierung & Benutzerverwaltung

Der G/On Server steuert, wer Zugriff auf welche Applikationen erhält (Single Point of Administration). Anbindung an das ActiveDirectory und LDAP-Anbindung optional.

### • Lautloser G/On Server

Über die Single-Port-Verbindung antwortet der Server nur auf Anfragen von auf Echtheit geprüften G/On Clients.

### • Isolierung der Endgeräte / Geräteunabhängigkeit

G/On isoliert Clients vom Netzwerk. Die Verbindung kann so konfiguriert werden, dass auch nicht-vertrauenswürdige PCs sicher nutzbar sind.