Soliton®

G/On

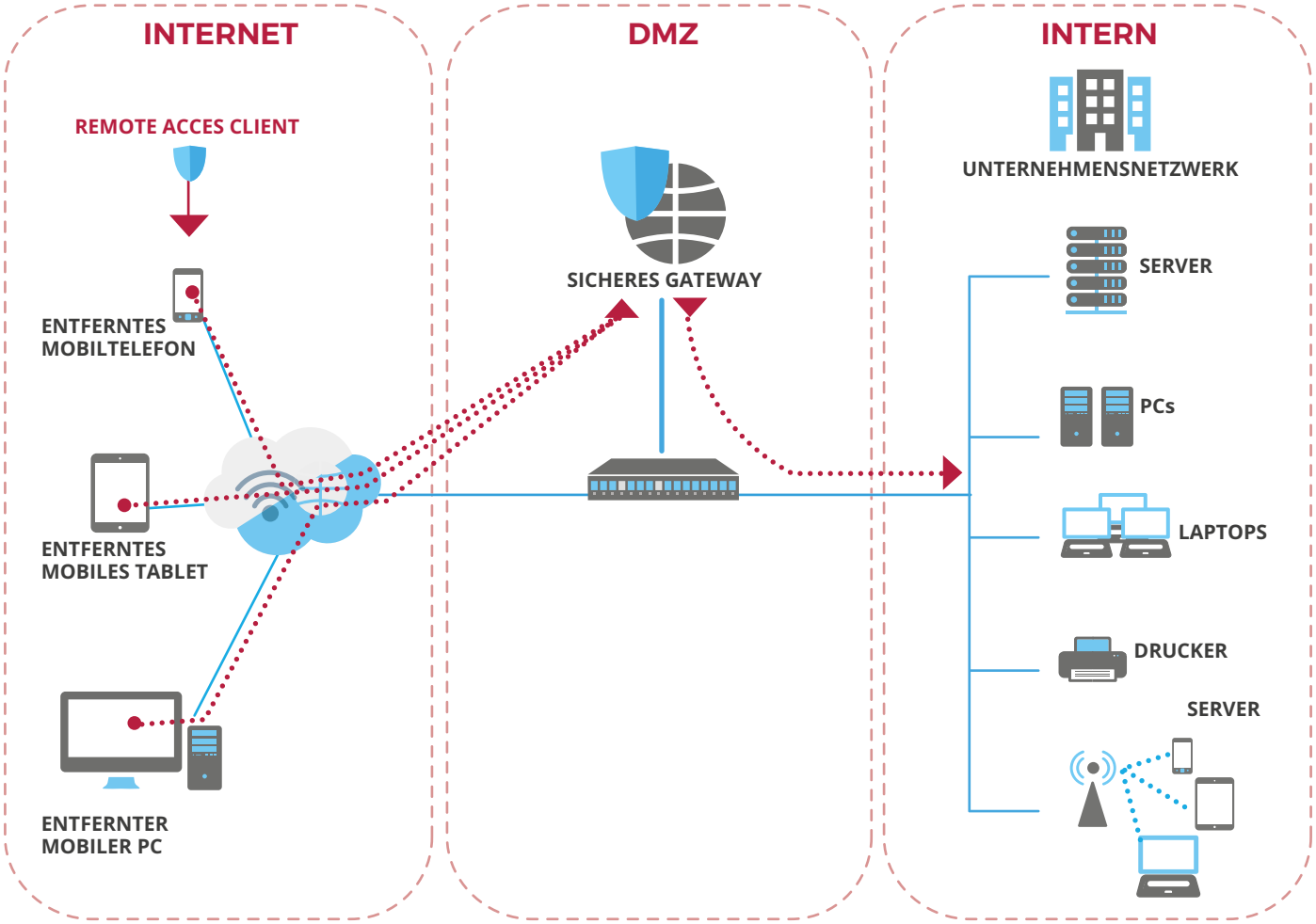
Soliton G/On ist eine Fernzugriffslösung, die eine Verbindung zwischen einem Remote-Gerät und Anwendungsservern in einem Unternehmensnetzwerk herstellt. Ein sicheres Gateway trennt das Remote-Gerät vom Netzwerk, sichert die Verbindung und gewährleistet die erforderliche Konnektivität. Die internen Anwendungsserver müssen nicht mit dem Internet verbunden sein und bieten dennoch volle Funktionalität.

Client-seitig verwenden die Benutzer einen speziellen G/On-Client, der ausschließlich für die Verbindung mit dem Gateway-Server genutzt wird. Die Benutzer bekommen Anwendungszugriff anhand von Berechtigungsregeln oder einer Active Directory-Gruppenzugehörigkeit und müssen sich keine URLs oder andere Zugriffsinformationen mehr merken. G/On beinhaltet Anwendungsclients für RDP, Citrix, VNC, Browser, Dateizugriff und vieles mehr.
Server-seitig kontrollieren die Administratoren anhand der zentralen Managementkonsole die komplette G/On-Umgebung, die aus vielen sicheren Gateway-Servern bestehen kann, auf einen Blick.

G/On bietet gegenseitige Zwei-Faktor-Benutzer- und Geräteauthentifizierung. Falls erforderlich, kann es eine Benutzeridentität mit einem Gerät verbinden. Da kein VPN erstellt wird und der Client zu keinem Zeitpunkt Teil des Unternehmensnetzwerks ist, besteht keine Notwendigkeit für die Konfiguration einer TCP/IP-Adresse auf dem Client. Der Benutzer kann weiterhin andere Anwendungen wie z. B. einen Browser auf dem Client nutzen, um sich mit Internet-Ressourcen zu verbinden. Zusätzlich ist ein Benutzer in der Lage, eine unbegrenzte Anzahl von G/On-Verbindungen gleichzeitig einzurichten.

G/On ist für Windows, MacOS und Linux (ausgewählte Distributionen) verfügbar.

UNSER ALLGEMEINER LÖSUNGSANSATZ ZUR SICHERUNG DES FERNZUGRIFFS



Alle Fernzugriff-Sicherheitslösungen von Soliton wurden auf der Grundlage der gleichen Prinzipien entwickelt:

- Gegenseitige Authentifizierung zwischen Client und Gateway zum Aufbau einer sicheren Verbindung.
- Das Gateway schützt die Server und das Netzwerk vor Cyber-Angriffen und unbefugtem Zugriff.
- Das Gateway trennt den Client vom Netzwerk, das Remote-Gerät ist zu keinem Zeitpunkt Teil des Netzwerkes.
- Das Gateway tauscht Informationen mit dem Netzwerk aus und ermöglicht einen sicheren Zugriff auf die Netzwerkressourcen.
- Der Remote Access Client kann vom Endanwender installiert werden, es sind keine zusätzlichen Rechte für PCs oder Macs erforderlich.
- Der Benutzerzugriff wird anhand von Berechtigungsregeln oder einer Active Directory-Gruppenzugehörigkeit geregelt; Benutzer müssen sich keine URLs mehr merken.

G/ON-KOMPONENTEN

SecureGateway: Sorgt dafür, dass die Unternehmensanwendungsserver nicht mit dem Internet verbunden sein müssen.

- Zwischen dem Gateway und dem Remote-Client übertragene Daten sind immer mit FIPS 140.2-zertifizierter AES 256-Bit-Verschlüsselung verschlüsselt.
- Ermöglicht Proxy-Services und DNS-Namensauflösung im internen Netzwerk, um den Anwendungen auf dem Client volle Funktionsfähigkeit zu bieten.
- Bietet automatischen Lastenausgleich und Failover-Funktionalität und funktioniert mit Drittanbieter-Lastenausgleichsprodukten.
- Zusätzliche Gateways können leicht innerhalb von Sekunden mit einem Gateway-Installationsprogramm erstellt werden.

G/On-Client: Verbindet Anwendungen auf dem Client mit Ressourcen im Unternehmensnetzwerk ohne VPN. Nach gegenseitiger Zwei-Faktor-Authentifizierung sendet der Gateway-Server ein Menüobjekt an den Client, das die Start-up-Konfiguration für jede Anwendung, die der Benutzer auf diesem Gerät, Standort und/oder zu dieser Uhrzeit benutzen kann, enthält.

Weitere Funktionen:

- Nicht verfügbare Anwendungen sind nicht sichtbar, und Zugriffsrechte werden im Gateway durchgesetzt, sodass der Benutzer keine unerlaubten Anwendungen starten oder die Zugriffsrechte erhöhen kann.
- Der G/On-Client bietet auch das automatische Starten von Anwendungen und einmaliges Anmelden (Single-Sign-On – SSO).
- Der Client kann den gesamten Datenverkehr in HTTP einkapseln und Proxies durchqueren, ohne Abstriche bei der Sicherheit zu machen.
- G/On-Clients können leicht entweder durch den Administrator oder einen Endanwender mit einem G/On-Client Installationsprogramm erstellt werden, und sind für Windows, MacOS und ausgewählte Linux-Distributionen erhältlich.

G/On-USB-Token: Ein USB-Token mit kleinem Formfaktor mit einer in der MicroSD-Karte integrierten mobilen Smartcard. Endanwender erhalten einen voll funktionsfähigen G/On-Client, der entweder bereits vorangemeldet ist, oder der Endanwender durchläuft einen einfachen Anmeldeprozess zum Aktivieren des G/On-Clients. Bei der Anmeldung generiert die Smartcard ein Privat/Öffentlich-Schlüsselpaar. Der öffentliche Schlüssel wird für die Smartcard-Authentifizierung verwendet; der private Schlüssel wird von der Smartcard geschützt und kann sie niemals verlassen. Der G/On-USB-Token kann daher auf der Grundlage des Privat/Öffentlich-Schlüsselpaars der Smartcard während der Authentifizierung eindeutig identifiziert werden.

G/On-Desktop Client: Läuft auf einem Computer anstatt auf dem G/On-USB-Token und verwendet den Computer als zweiten Authentifizierungsfaktor anstelle einer Smartcard. Nur unter Windows verfügbar.

G/ON UNTERSTÜTZT EINE REIHE WICHTIGER FUNKTIONEN, UNTER ANDEREM:

- **Kein VPN erforderlich:** G/On erstellt einen Zugangspfad zu den internen Anwendungen und nutzt interne DNS-Server. Das SecureGateway isoliert den Remotecomputer vom internen Netzwerk. Die Benutzer können weiterhin ihre persönlichen Anwendungen verwenden.

- **Nutzungsprotokoll:** Das SecureGateway protokolliert alle Zugriffsversuche, einschließlich Angaben über den Benutzer sowie wann und auf welche Ressourcen von diesem Benutzer zugegriffen wurde.

- **Zentrale Managementkonsole:** Bietet der IT volle Kontrolle über die Einstellungen, Benutzer und Nutzung. IT-Administratoren können den Zugriff auf andere Anwendungen steuern, das Kopieren/Einfügen/Downloaden von Dateien verhindern bzw. das Herunterladen von Dateien in einer eigens dafür vorgesehenen sicheren Umgebung gestatten.

- **Integrierte Proxies für Citrix und RDP:** G/On kommuniziert direkt mit den Broker-Services sowohl auf Citrix als auch auf RDP, daher besteht kein Bedarf für Frontend-Komponenten wie NetScaler und RD Gateway. Der G/On-Client kann auch die Citrix- und RDP-Clients enthalten. In diesem Fall müssen diese nicht auf dem Remotecomputer installiert werden.

- **Benutzerfreundlich:** Keine komplexen Start-up- und Anmeldeverfahren. Stecken Sie den G/On-USB-Token ein, starten Sie den G/On-Client, melden Sie sich mit AD-Anmeldedaten an und wählen Sie die benötigten Anwendungen aus. Single-Sign-On ist verfügbar und die am häufigsten verwendeten Anwendungen können automatisch nach der Authentifizierung gestartet werden.

- **Keine Notwendigkeit für verwaltete Geräte:** G/On trennt Unternehmensanwendungen von lokalen Anwendungen auf dem Computer des Endanwenders. Die Verbindung ist gesichert und der Endanwender-Computer erhält niemals Zugriff auf das interne Netzwerk, da alle Verbindungen durch das SecureGateway geleitet werden.

OPTIONEN G/ON OS

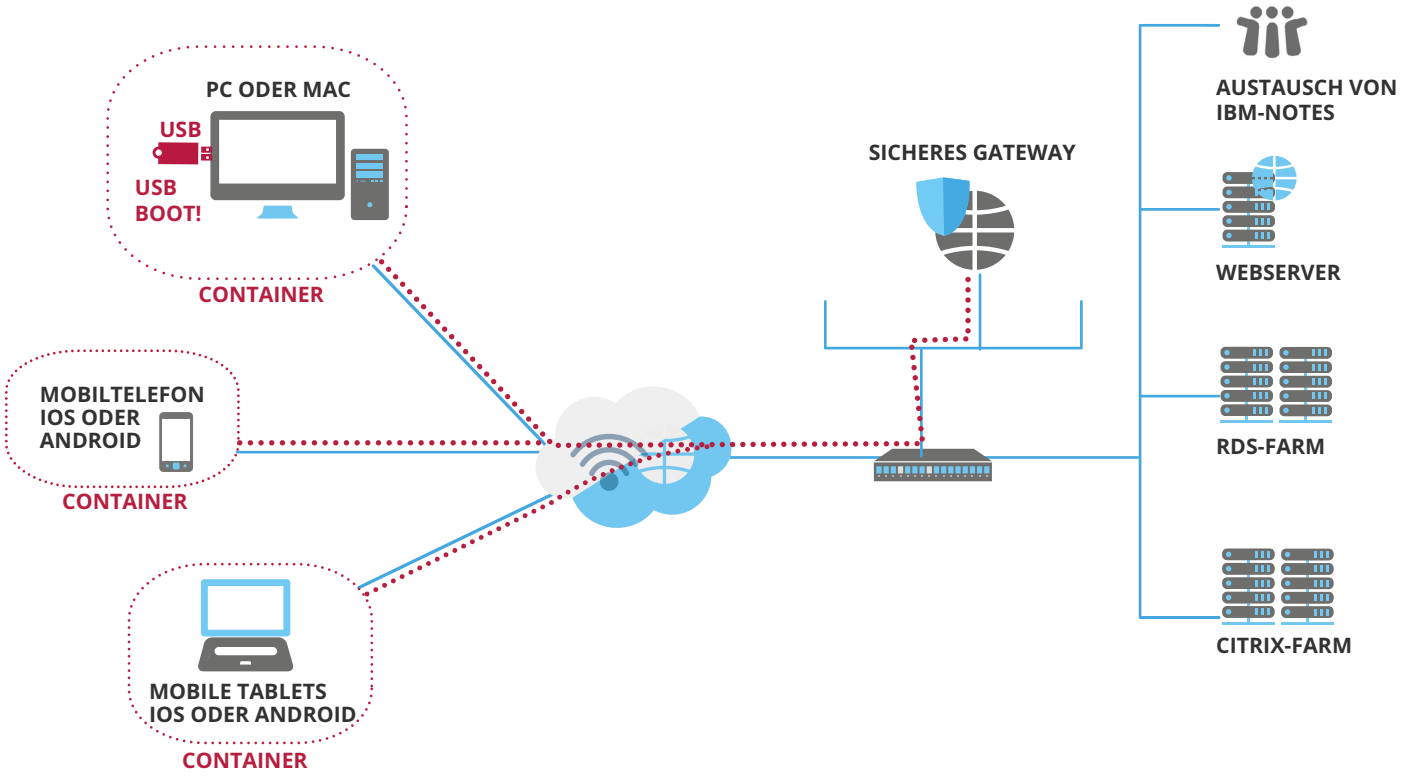
G/On OS ist ein sicherer Container, der G/On hinzugefügt wird, um eine vollständige Sperre auf der Client-Seite zu erhalten. Weitere Funktionen:

- G/On OS ist ein gehärtetes und auf das Minimum reduziertes Linux-Betriebssystem, das direkt von dem USB-Token in den Speicher gebootet wird. Es enthält keine Treiber für den Zugriff auf Festplatten, sodass keine Daten zurückgelassen oder vom benutzten Computer übertragen werden können.

- G/On OS ist vollständig mit Anwendungsclients für Citrix, RDP, VNC, Browser und vielem mehr ausgestattet.

- G/On OS ist gesperrt, um nur den Zugriff auf das SecureGateway zu erlauben, an dem es ursprünglich angemeldet wurde.

G/ON INFRASTRUKTUR



TECHNISCHE DATEN

SecureGateway

Plattform	Windows
Betriebssystemversion	Windows Server 2008, 2008 R2, 2012, 2012 R2* und 2016
Benutzeranzahl	Bis zu ~ 2.000 pro Gateway
Unterstützter Authentifizierungsserver	Active Directory, LDAP und lokale Konten
Protokollausgabeziel	Lokale Datei

**erfordert G/On Server 5.7 oder höher*

Datenbank (optional)

Plattform	Windows
Betriebssystemversion	Microsoft SQL Server 2008, 2012, 2014, 2016 und 2017 (2012 und höher erfordert G/On Server 5.7 oder höher)

G/On-Client

Plattform	Windows, Mac OS und Linux
Betriebssystemversion	**Windows** 7, 8, 8.1 und 10 **Apple Mac OS** X 10.6 (Snow Leopard) bis OS X 10.13 (High Sierra) **Linux** Fedora 21 bis 27 mit GTK+ GUI (64-Bit)

G/On-Token

Plattform	USB und Windows
Tokentypen	**G/On USB-Token** einschließlich integrierter Smartcard für gegenseitige Zwei-Faktor-Authentifizierung **SoftToken** auf einem beliebigen USB, 2 GB oder größer **Computer User Token** auf Windows-Plattform installiert

ÜBER SOLITON

Soliton Systems hat ein klares Ziel vor Augen: Die Entwicklung innovativer Lösungen, um die Bedürfnisse unserer Kunden konsequent und unkompliziert zu erfüllen. Soliton unterstützt Unternehmen bei der Umsetzung ihrer Sicherheitsmanagementanforderungen, unter anderem in Hinblick auf die Netzwerksicherheit und den mobilen Zugriff auf interne Ressourcen und Cloud-Anwendungen. Lösungen von Soliton schützen die Unternehmensressourcen vor unbefugtem Zugriff und unbeabsichtigtem Datenverlust.

Soliton®

EMEA office

Soliton Systems Europe N.V.

Jachthavenweg 109-A, 1081 KM Amsterdam, The Netherlands

+31 (0)20 280 6060 | emea@solitonsystems.com | www.solitonsystems.com

SOL200107