Soliton®

G/On

Soliton G/On is a remote access solution which establishes connections between a remote device and application servers inside an organisations' network. A secure gateway is used to separate the remote device from the network, secure the connection and provide all necessary connectivity. The internal applications servers do not have to be Internet-facing, while at the same time offering full functionality.

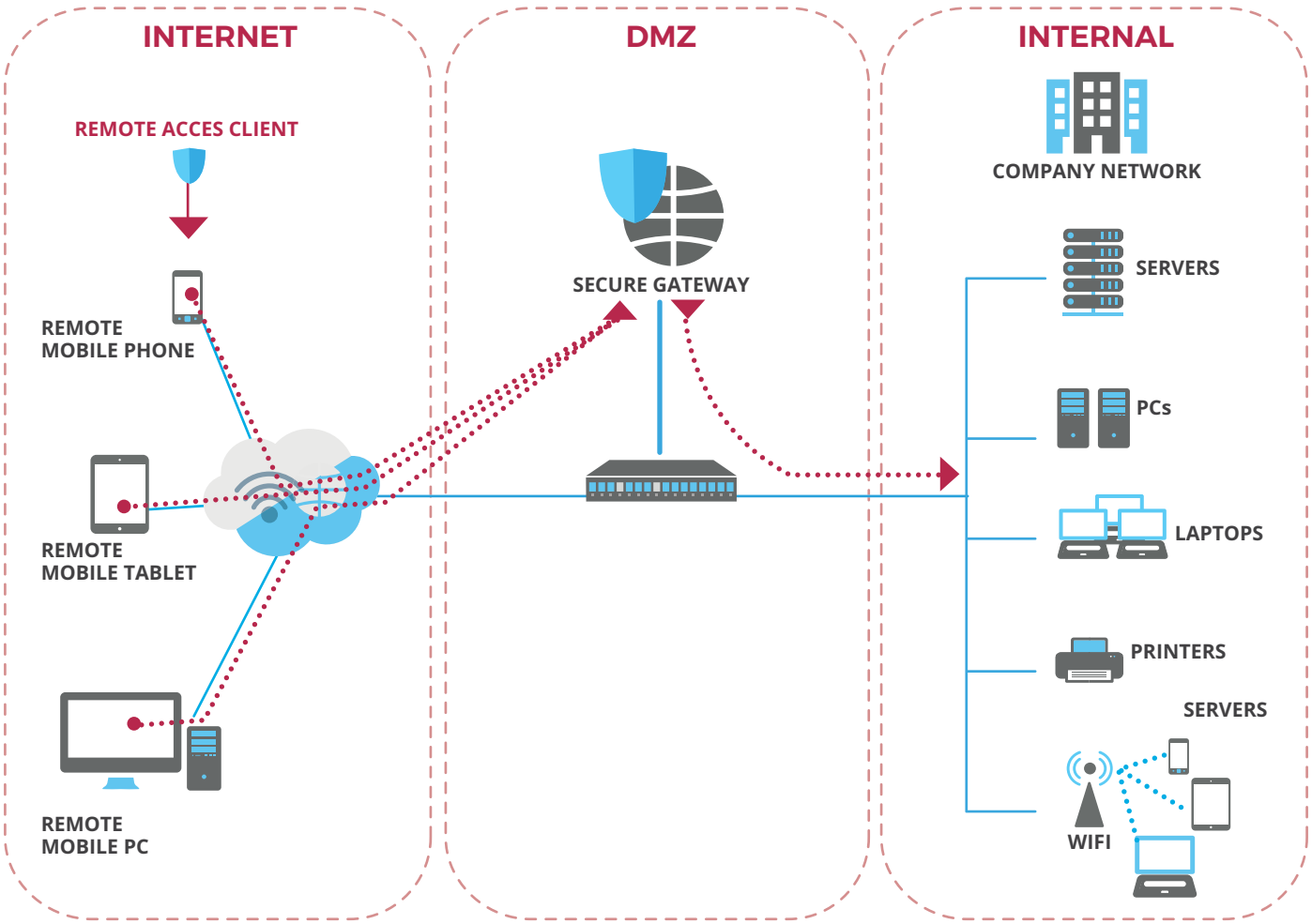
On the client-side, users use a dedicated G/On Client that is only used to connect to the gateway server. Users get application access based on permission rules or Active Directory group membership and do not need to remember any URL's or other information to access applications. G/On includes application clients for RDP, Citrix, VNC, Browsers, File Access and much more.

On the server-side, administrators use the central management console to control the complete G/On-environment, which may consist of many secure gateway servers, from one view.

G/On provides two-factor mutual user and device authentication. If required, it can connect a user identity to a device. The fact there is no VPN created and the client is never part of the corporate network, there is no need for the configuration of a TCP/IP-address on the client. The user can still use other applications, such as a browser on the client to connect to Internet-resources. In addition, a user is able set up an unlimited number of G/On connections at the same time.

G/On is available for Windows, MacOS and Linux (selected distributions).

OUR GENERAL APPROACH IN REMOTE ACCESS SECURITY



All Soliton's remote access security solutions are developed based on the same principles:

- Mutual authentication between client and gateway creating a secure connection.
- Gateway protects the servers and the network from cyber-attacks and from unauthorized access.
- Gateway separates the client from the network, the remote device is never part of the network.
- Gateway exchanges information with the network and enables secure access to the network resources.
- Remote access client can be installed by end-user, no special rights required for PCs or Macs.
- User access is based on permission rules or Active Directory group membership; users do not need to remember any URLs.

G/ON COMPONENTS

SecureGateway: Prevents the corporate application servers from having to be Internet-facing.

- Data in transit between the gateway and the remote client is always encrypted using FIPS 140.2 certified AES 256-bit encryption.
- Provides proxy services and DNS name resolving on the internal network to offer full functionality to the applications on the client.
- Offers automatic load-balancing and fail-over functionality and works with third-party load-balancing products.
- Additional gateways are easily created in seconds using a Gateway installer.

G/On Client: Connects applications on the client to resources inside the corporate network, without a VPN. After mutual two-factor authentication, the gateway server sends a menu-object to the client that contains the start-up configuration for each application the user can use at that device, location and/or time.
Other features include:

- Unavailable applications are not visible and access rights are enforced in the gateway, preventing the user from starting not allowed applications or elevating access rights.
- The G/On-client also provides the automatic launch of applications and single-sign-on (SSO).
- The client can encapsulate all traffic in HTTP and traverse proxies, without sacrificing on security.
- G/On clients are easily created using a G/On Client Installer, either by the admin or an end user and are available for Windows, MacOS and selected Linux-distributions.

G/On USB Token: A small USB form factor token with a mobile smart card integrated in the MicroSD-card. End users receive a fully functional G/On client which is either pre-enrolled, or the end user goes through a simple enrolment process to activate the G/On client. During enrolment, the smart card generates a private/public keypair. The public key is used for smart card authentication, the private key is protected by the smart card and can never leave it. The G/On USB-token can therefore be uniquely identified based on the smart card private/public keypair during authentication time.

G/On Desktop Client: Runs from a computer instead of a G/On USB-token and uses the computer as a second authentication factor instead of a smart card. Only available on Windows.

G/ON SUPPORTS A NUMBER OF KEY FEATURES, INCLUDING:

- **No need for VPN:** G/On creates one access route to the internal applications and uses internal DNS servers. The SecureGateway isolates the remote computer from the internal network. Users can still use their personal applications.

- **Usage log:** the SecureGateway logs all access attempts including details about which user, when and what resources are accessed by that user.

- **Central management console:** provides IT full control on settings, users and usage. IT administrators can control the access to other applications, prevent copy/paste/download of files or allow the download of files in a dedicated secure environment.

- **Built-in proxies for Citrix and RDP:** G/On communicates directly with the broker services on both Citrix and RDP, so there is no need for any of the front-end components, such as NetScaler and RD Gateway. The G/On-client can also include the Citrix- and RDP-clients, in which case there is no need to install these on the remote computer.

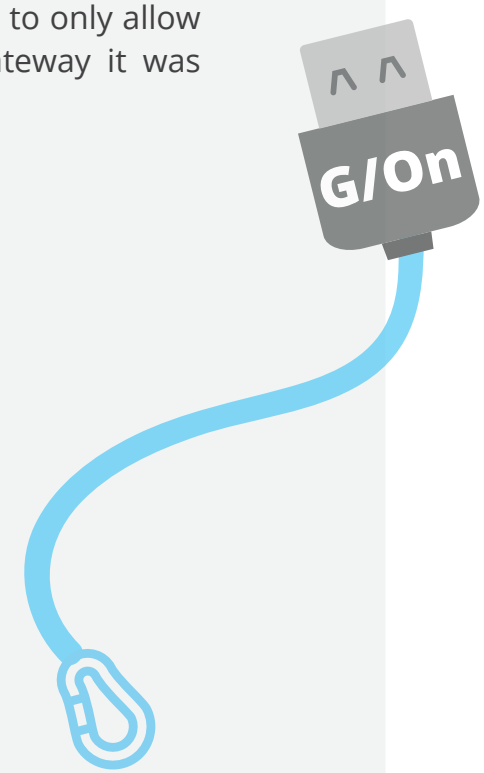
- **User-friendly:** No complex start-up and login procedures. Insert the G/On USB Token, launch the G/On Client, log in with AD credentials and select the apps needed. Single-sign-on is include and the most used apps can automatically be started after authentication.

- **No need for managed devices:** G/On separates corporate applications from local applications on the end-user computer. The connection is secured, and the end-user computer is never given any access to the internal network, as all connections are proxied through the SecureGateway.

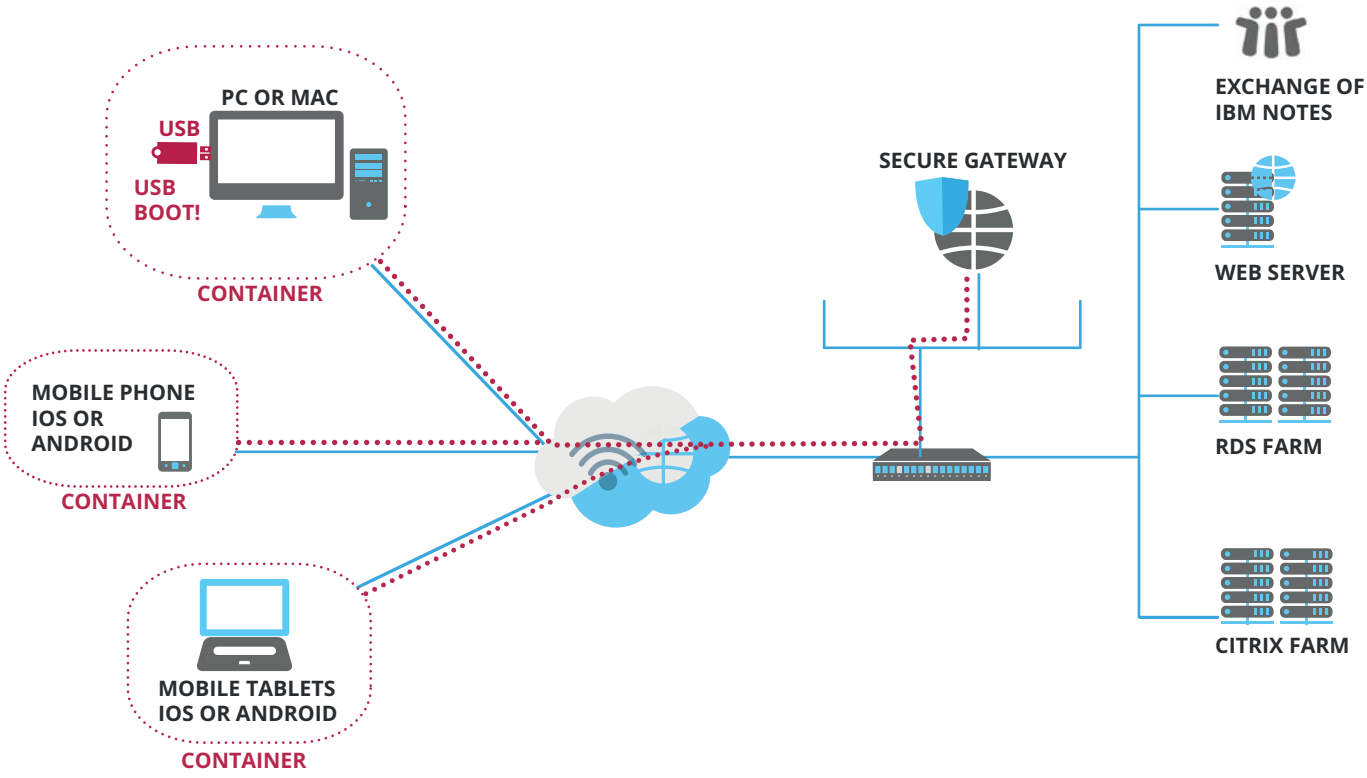
OPTIONS G/ON OS

G/On OS is a secure container added to G/On to have a full lock-down in the client side. Other features include:

- G/On OS is a hardened, minimal Fedora Linux image, which is booted directly into memory from the G/On USB Token. It does not include drivers to access hard disks, so there is no way to leave data behind, or transmit data from the computer used.
- G/On OS comes full features with application clients for Citrix, RDP, VNC, Browsers and much more.
- G/On OS is locked down to only allow access to the SecureGateway it was originally enrolled on.



G/ON INFRASTRUCTURE



SPECIFICATIONS

SECUREGATEWAY	
Platform	Windows
Operating systems version	Windows Server 2008, 2008 R2, 2012, 2012 R2* and 2016
Number of users	Up to ~ 2,000 per gateway
Supported authentication server	Active Directory, LDAP and local accounts
Log output destination	Local file

**requires G/On Server 5.7 or later*

DATABASE (OPTIONAL)	
Platform	Windows
Operating systems version	Microsoft SQL server 2008, 2012, 2014, 2016 and 2017 (2012 and later requires G/On server 5.7 or later)

G/ON CLIENT	
Platform	Windows, Mac OS and Linux
Operating systems version	**Windows** 7, 8, 8.1 and 10 **Apple Mac OS** X 10.6 (Snow Leopard) through OS X 10.13 (High Sierra) **Linux** Fedora 21 through 27 with GTK+ GUI (64 bit)

G/ON TOKEN	
Platform	USB and Windows
Token types	**G/On USB Token** including built-in Smartcard for two-factor mutual authentication **SoftToken** on any USB, 2 GB or larger **Computer User Token** installed on Windows platform

ABOUT SOLITON

Soliton Systems has a strong vision to innovate solutions to logically fulfil the needs of our customers without adding complexity. Soliton support companies with their security management challenges, including network security and remote access to the internal and cloud applications. Soliton's solutions protect the company's resources from unauthorized access and accidental data leakage.

EMEA office

Soliton Systems Europe N.V.

Gustav Mahlerplein 2, 1082 MA Amsterdam, The Netherlands

+31 20 301 2166 | emea@solitonsystems.com | www.solitonsystems.com

SOL18042901v1