Soliton®

# G/On

**G/On is an integrated, scalable and secure remote access solution built on Zero-Trust principles — everything is on a need-to-know basis. It decreases your attack surface, increases visibility into user activity and reduces complexity. Plus, it delivers additional business benefits like BYOD, fast installation, scalability, affordability, permission access and a stable connection with no bandwidth issues.**

It's a single place where IT Teams can control individual access to applications and services — from both managed and unmanaged devices. Access is identity-based, checking the user and the device. It also includes strong mutual two-factor authentication, authorisation, data encryption, network protection and secure application access as standard.

G/On is simple for IT to implement, manage and control. It enables business and supports effective remote working.

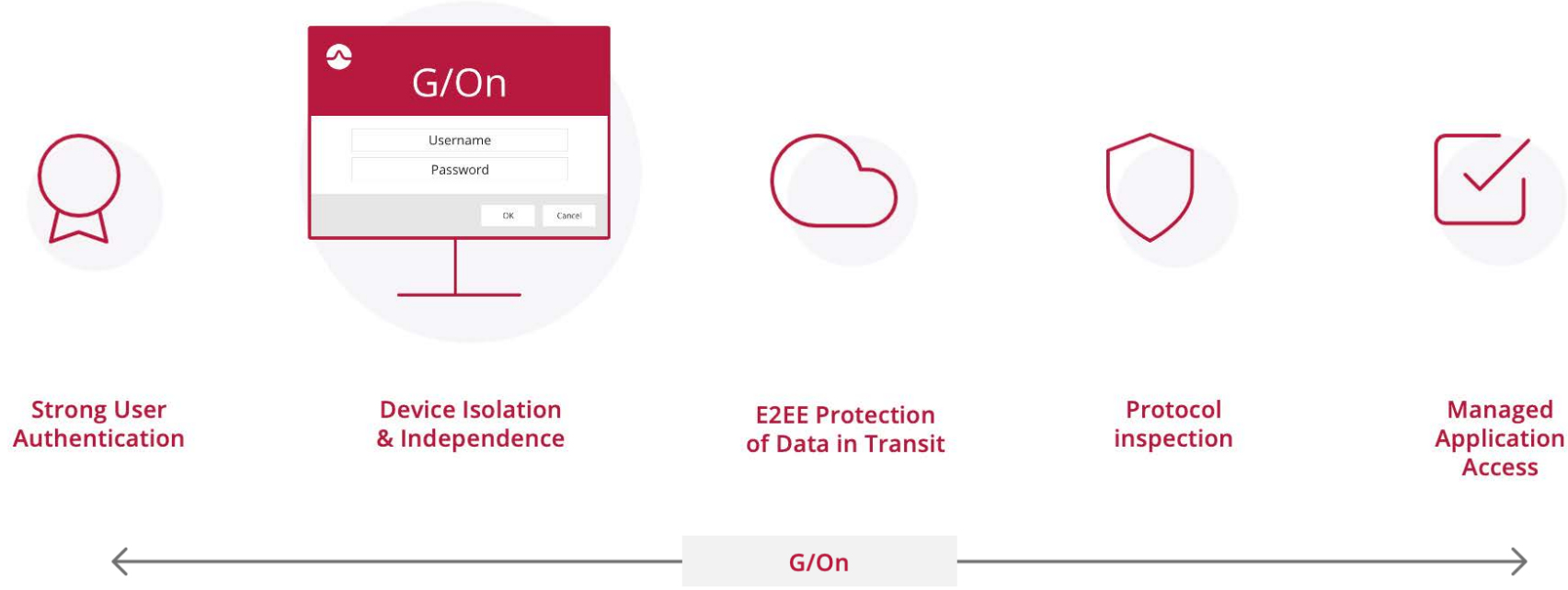
## How does it work?

G/On establishes connections between applications on 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 no longer have to be Internet-facing while still 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 directory group memberships.

They are presented with a dynamically generated menu and do not need to remember URLs or create bookmarks to access their application. G/On includes application clients for RDP, Citrix, VNC, SSH, Browsers, File Access and much more.

On the server side, administrators use the central management console to control the complete G/On-environment. Even with many secure gateway servers, administrators can manage it all from a single dashboard. Access Management of applications is done in real time. Due to the dynamic menu creation, access to the applications is instantly presented to the user.



## Two-factor mutual user and device authentication.

Based on this verified authentication, a connection is established. It doesn't use VPN, and the client is never part of the corporate network. The authentication is performed by mutual verification of the user certificate and the gateway certificate. Once this is verified, the trust relationship is set, and the connection is established.

## Flexibility

G/On does not restrict the user's daily activities. For example, users can still use other applications to connect to Internet resources, such as a browser. Also, a user can set up an unlimited number of G/On connections simultaneously without the risk of interactions between sessions.

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

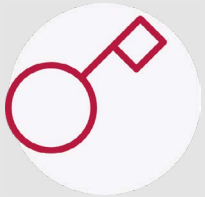
## Our Approach

Soliton's Zero Trust Security delivers cutting-edge technology that helps companies solve their IT security challenges with a unique set of high-quality, cost-effective products and solutions.

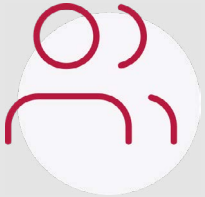
It achieves this through:

- Mutual authentication between client and gateway creating a secure connection.
- Gateway protects the servers and the network from cyber-attacks and unauthorised 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.
- End-users can run and install remote access client - no special rights required for PCs or Macs.
- User access is based on permission rules or Directory group membership; users are presented with a menu of applications based on their access rights.

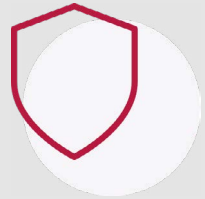
**At its core,
G/On allows organisations to:**



Provide secure access to valuable company resources.



Authenticate users and secure devices without sacrificing user convenience.



Keep out attackers and manage different threat complexities.

## G/On Components

**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 dynamic menu to the client. This menu contains the specific applications available to the user, based on the device, authentication level, location, time and more.

Other features include:

- The G/On client does not need to be installed.
- No elevated rights are needed to run the application.
- Users do not need to remember any URLs or other information to access applications.
- Access rights are enforced in the gateway, preventing the user from starting not allowed applications or elevating access rights. Unavailable applications are not visible.
- User menus can be adjusted in real time, even during active user sessions.
- Automatic application launch and Single-Sign-On (SSO).
- Ability to encapsulate all traffic in HTTP and traverse proxies without sacrificing security.
- Includes application clients for RDP, Citrix, VNC, Browsers, File Access and much more.

**G/On Management:**

Is the central web-based management console that controls one or more G/On Gateways and the behaviour of the clients:

- Full control on users, applications, authentication levels and access authorization policies.
- Granular application access based on individual permission rules or group membership.
- Ability to control the behaviour of client applications– IT administrators can control the settings of client applications, e.g. to prevent copy/paste/download of files or allow the download of files in a dedicated secure environment.
- Usage log – The SecureGateway logs all access attempts including details about which user, when and what resources are accessed by that user.

**G/On Gateway:**

G/On Gateway hides the internal network and its resources from the Internet

- Data in transit between the gateway and the remote client is encrypted using FIPS 140.2 certified AES 256-bit encryption.
- Full application functionality at the client is created by using Proxy and DNS services from the internal network.
- Built-in load-balancing and fail-over functionality, also works with third-party load-balancing products.
- Additional gateways are easily created in seconds.

**G/On Authentication Factors:**

The level of authentication needed to provide access to certain information depends on the degree of sensitivity or confidentiality of that information. G/On offers authorization based on the level of authentication that a user provides at logon time:

- No authentication: the user just connects to G/On
- Single-factor authentication (SFA): This is the simplest form of authentication because it prompts the user to provide just a single factor or credential to verify their identity. In the case of G/On, the user presents a password, a G/On token or one of the supported external authentication factors (OTP, SMS-authentication and push-authentication to a supported app)
- Multi-factor authentication (2FA): This is the case where the user must provide an one or more additional credentials after entering their username and password, e.g. one of the G/On tokens and/or one of the supported external authentication factors (OTP, SMS-authentication and push-authentication to a supported app)

In addition, USB-based G/On can be combined with a Fedora Linux bootable OS called G/On OS.

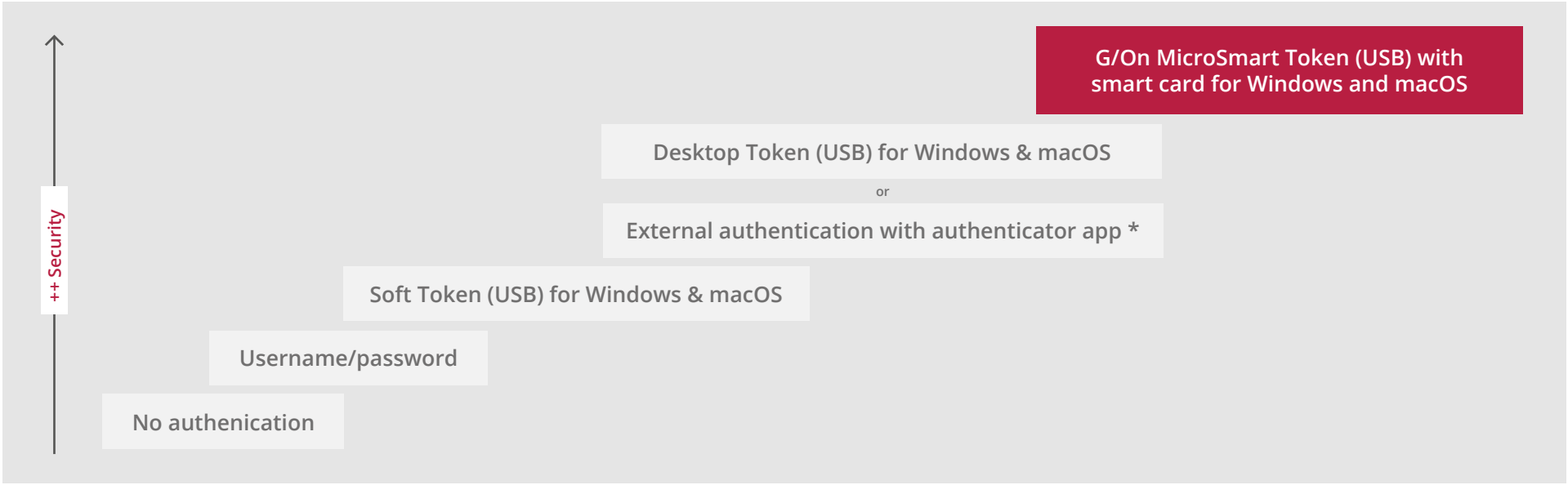
### Authentication level based Application Access

Different authentication factors, including G/On OS, can be combined, leading to different authorisation levels. For instance, a user on holiday logging in with only a username/password will be allowed access to e-mail only. When the same user presents an OTP from an allowed authenticator app, access to additional applications is provided. If the user uses a smart card based mobile token, the authorisation level is further extended. Finally, the maximum authorisation is granted when the computer is started with G/On OS.

### Challenge/Response authentication protocol

The built-in G/On authentication is based on industry standard public/private key cryptography, like certificates, but without the complexity of X.509 and without the need for Public Key Infrastructure (PKI). G/On uses challenge/response authentication, bypassing the limitations of time-synchronisation or a mathematical algorithms to generate new codes based on time or previous authentication codes. The challenge/response mechanism does not involve any user interaction

G/On MicroSmart tokens contain a Java Card smart card that allows a Java-based applet to be run security on the smart card itself. During enrolment, G/On MicroSmart tokens autonomously create a public/private keypair and hand the public key to the G/On Management Server. The private key never leaves the smart card.



# Key Features

### No Need for VPN

G/On can replace or work alongside your VPN infrastructure. It creates one access route to the internal applications and uses internal DNS servers. Operating on a Zero-Trust basis, G/On only allows verified users to access their authorised applications. The network is completely disconnected from the outside world.

### User-friendly

G/On does not have complex start-up or login procedures. No need for technical knowledge or any changes to the computer configuration. No elevated rights are required. Users only need to insert the G/On USB Token, launch the G/On Client, and log in with their AD credentials. The user menu is generated and presented to the user. Single-Sign-On is included, and the most used applications can automatically be started after authentication.

### Field Enrolment

No elevated rights are required. G/On is a single app deployment with easy client certificate self-enrolment. There is no need for users to take devices into the office or get IT to set up. Organisations can scale up remote working in minutes rather than weeks — scaling comes down to licensing.

### Usage Log

The G/On Gateway logs all access attempts, including which user, when and what resources are accessed by that user.

### No Need for Load Balancing

G/On clients can use numerous client connect addresses and connect to multiple client connect ports. It's even possible to specify the order that these connect addresses and ports should be used.

### Suitable for Any Device Policy

G/On separates corporate applications from private applications at the end-user computer. The connection is secured, and the end-user computer is never connected to the internal network.

### Central Management Console

G/On provides complete control over settings, users and usage. IT admins can control application access, prevent copy/paste/downloads and allow file downloads in a dedicated secure environment.

### Built-in proxies for Citrix, RDP and Web-Applications

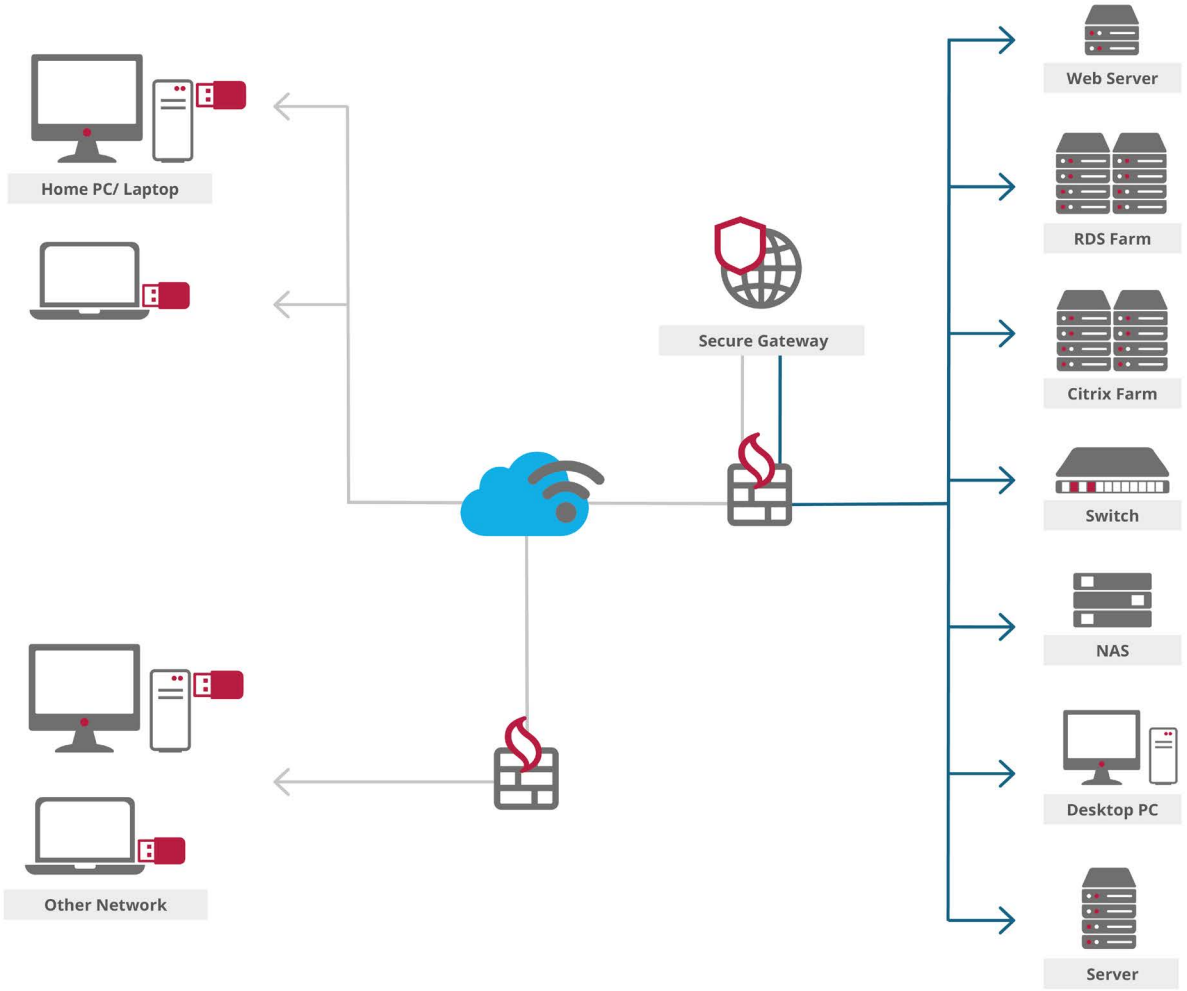
G/On communicates directly with the broker services on both Citrix and RDP. There is no need for any front-end components, like NetScaler and RDP Gateway. The G/On-client can also include the Citrix- and RDP-clients, no need to install these on the remote computer.

# G/On OS

G/On OS is a secured OS with the G/On client, enabling total lockdown on the client-side. Other features include:

A hardened, minimal Fedora Linux image booted directly into memory from the G/On Security Token. It does not include drivers to access hard disks; it's impossible to leave data behind or transmit data from the computer used.

Application clients for Citrix, RDP, VNC, SSH, Browsers and more.



## G/On Gateway Server

| | |
|---|---|
| Platform | Windows |
| Operating systems version | Windows Server 2022, Windows Server 2019 or Windows Server 2016 |
| Number of users | Up to 2,000 per gateway, depending on application load |
| Supported authentication server | Active Directory, LDAP and local accounts |

* Even though the G/On Server will install and run on Windows Server 2008, Windows Server 2008R2, Windows Server 2012, Windows Server 2012R2 these platforms are not anymore supported from G-On version 7.0 or above

## G/On Client

| | |
|---|---|
| Platform | Windows, MacOS and Linux |
| Operating systems version | • Windows 11 64-bit only<br>• Windows 10 64-bit only*<br>• macOS 10.15 Catalina, macOS 11 Big Sur or macOS 12 Monterey, both Intel and Apple silicon |

* The G/On client also works on Windows 7 and Windows 8.1, however, these platforms are not supported anymore

## G/On Database (optional)

| | |
|---|---|
| Platform | Microsoft SQL Server |
| Operating systems version | • Microsoft SQL Server 2012, 2014, 2016, 2017 and 2019<br>• Microsoft SQL Server Express 2012, 2014, 2016, 2017 and 2019 |

## G/On Security Token

| | |
|---|---|
| Platform | Windows, MacOS and Linux |
| Token types | • G/On MicroSmart token: USB Token with Smartcard for strong two-factor mutual authentication<br>• G/On Desktop token (ComputerUser token): stored in the user profile in Windows or macOS<br>• Soft token: stored on any USB-key of 2 GB and larger |

## External authentication factors

| | |
|---|---|
| External authentication with authenticator app* | • Google Authenticator (OTP authentication)<br>• DUO Authenticator (OTP, SMS and push authentication) |

* G/On can be integrated with any other external authentication system using the RADIUS-protocol and if necessary by changing the plug-in based authentication architecture

## EMEA office

**Soliton Systems Europe N.V.**

Barbara Strozzilaan 364
1083 HN, Amsterdam,
The Netherlands

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


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.