Next-Generation Access Control: **Leveraging ZTNA and Flexible Authentication for Enhanced Security**

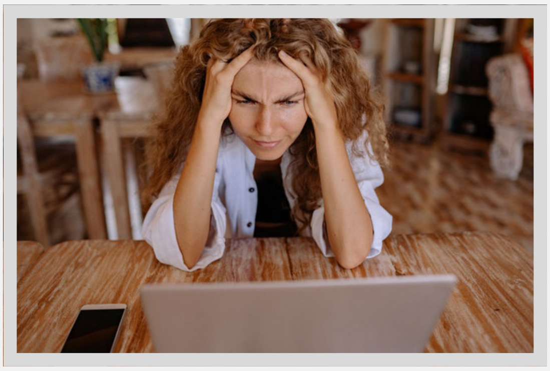
Soliton®

www.solitonsystems.com

Contents

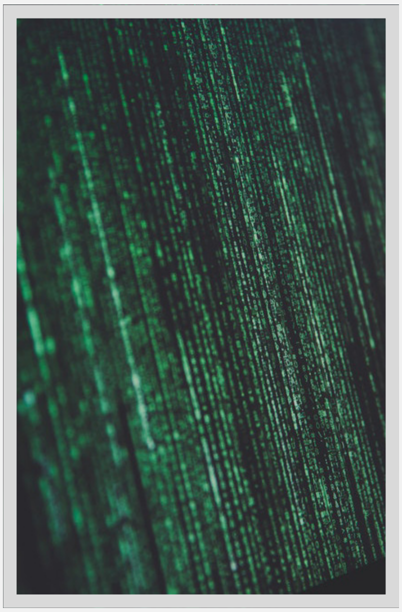
Next-Generation Access Control:
Leveraging ZTNA and Flexible Authentication for Enhanced Security

For many organisations, the process of adding new users or updating user access can be a complex and time-consuming process. With the rise of hybrid working and an increased need to control third-party access without granting overprivileged access, businesses need a solution that is both secure and easy to manage.



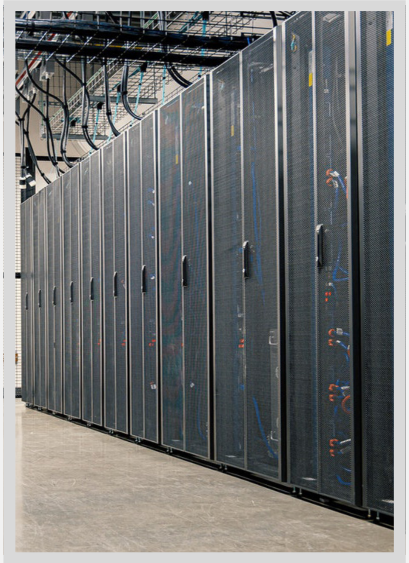
Traditional solutions like VPN connections and RDS infrastructures are costly, difficult to manage, and often extend company networks to unsecured locations. As cyberattacks become more prevalent, the risks of poorly implemented solutions increase as well.

The solution? Consider using a complementary solution to your VPN or existing solutions, such as Citrix Virtual Apps and Desktops or Microsoft Remote Desktop Services. A solution which provides a zero-trust access environment and with additional benefits, such as BYOD support, fast installation, scalability, affordable pricing, permission-based access, and a stable connection without bandwidth issues. It's important to note that this is not an all-or-nothing approach – there is no need to abandon your VPN entirely. Instead, you can minimise the risks associated with VPNs while supporting effective remote access and enabling your business to operate securely and efficiently.



Complexity is the enemy of scalability

Many companies today face significant challenges when it comes to scaling remote network access due to the evolving security landscape, particularly in the context of hybrid working and securing third-party access.



Overcoming complexity is one of the biggest hurdles to enable remote secure access to corporate networks. Setting up additional VPN connections or opening up RDP ports can take days or even weeks, and organisations often find it difficult to add separate two-factor authentication solutions to their existing remote access solutions.

As a result, IT teams are searching for ways to streamline their remote access solutions, making them easy to manage and scale, without compromising security or adding unnecessary complexity. It's crucial for organisations to have a secure and reliable remote access solution in place that can adapt to changing needs and threats.

A single all-in-one solution, like G/On, is not dependent on any external factor to develop autonomously. How exactly is it different? Quite simply, it's quick to install and provides everything users need to access company resources securely. G/On has built-in features for redundancy and load balancing. It means organisations can scale up remote working in minutes rather than weeks — scaling just comes down to licensing.

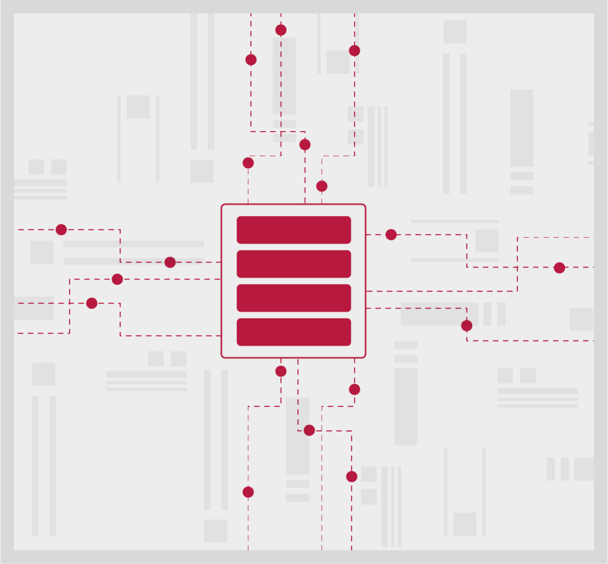
Installing gateways using a software component sets up an additional fully configured G/On-gateway server in a matter of minutes, not days. The G/On gateway installer supports the Just-In-Time (JIT) remote network access, providing secure access to corporate resources on an on-demand basis.

G/On can be used by any organisation or industry vertical. It’s a single place for you to control exactly who can see what on your networks and it works with both managed and unmanaged devices.

While the specific requirements for a law firm could be different to a manufacturer, G/On enables them both to solve the underlying challenge: Enabling full-time or temporary employees to securely access the applications required to get their jobs done, from an unmanaged location and/or device. Even if 'remotely' means being in the office, G/On can still help, as it supports consultants working from a customer location or and external contractors and freelancers working with your company data.

Why do we need an alternative approach?

From a security perspective, VPNs are problematic, particularly on devices you cannot manage. VPNs are typically used to control access in an all-or-nothing fashion. Authenticated users have overly-broad network access, increasing the attack surface area and enabling the types of wide-reaching breaches. They are also labour-intensive to install and manage, don't leverage user context to make access decisions and can't keep up with the pace of business.



Of course, IT wants to mitigate this risk. For a VPN, the available options are: Pinch down the VPN-connection or ask users to install a VPN-client, which prevents specific activity on the remote computer when the user connects to the company network. Neither of these is a good option. The first option means that IT staff now have to explicitly (and manually) set which connections are allowed and which should be blocked. As new applications are added, this strategy quickly becomes very complicated, which stands in the way of security and scalability. The second option gives IT more control (it could, for example, block simultaneous access to the internet on the remote device). But in practice, it means the user's PC also disconnects from the home network, causing other problems. So what is the alternative?

Why G/On is the new alternative

G/On is a remote access solution that is designed on the Software-Defined Perimeter (SDP) model, which is a security framework that micro-segments network access by creating one-to-one network connections between a user and the resources they wish to access.

Significantly, it does not facilitate direct access between the remote device and the network. The software-defined perimeter mediates the connection without ever placing the user on the network. And, according to Cloud Security Alliance, "The SDP security model has been shown to stop all forms of network attacks including DDoS, Man-in-the-Middle, Server Query (OWASP10) as well as Advanced Persistent Threat."

There are two core pillars to a software-defined perimeter: It's **identity-centric** and built on **zero-trust** principles. Identity-centric means it's based on the user's identity and authorisation levels, not the device. And zero-trust means it applies the principle of least privilege to the network (need-to-know), reducing the attack surface while also increasing IT's visibility into our user activity and applications.

With G/On, network resources are made inaccessible by default. An authenticated user can only access one or more specific services inside the network when explicitly authorised, rather than receiving the broad network access available when using a VPN. Therefore, G/On isolates the company services from the internet, stopping almost all forms of network attacks.

G/On also adds a crucial third pillar - **non-intrusive security measures.** This is particularly relevant in today's hybrid working environment where BYOD and third-party access are commonplace. With G/On's non-intrusive security measures, corporate data can be protected without invasive software installations or interference with personal data on employees' devices. This ensures that sensitive data is kept separate and secure, while also respecting the privacy of the device owner. The non-intrusive approach is especially important in the case of BYOD, where employees may be hesitant to allow the company access to their personal data. Additionally, third-party access can be safely granted without the risk of accessing personal data, providing secure access while maintaining data protection.

It’s OK; we have Citrix or use RDS

When you work with Citrix Virtual Apps and Desktops or Microsoft Remote Desktop Services, you may think you’ve got everything covered. However, these solutions are not originally built as remote working solutions, so these tools need a separate remote access layer for security. Additionally, both solutions need an access strategy and are often point solutions. You can equip Citrix or RDS with a security layer and an access strategy. However, it would be more efficient to use one tool to secure remote access f general PC working and cover Citrix or RDS with a single overall zero-trust strategy and more.

Solving for mobility

Users want the freedom to work on their preferred computer: this is mobility. But when employees use personal devices, organisations cannot:

- Rely on that computer’s security
- Install software components on the device (in fact, depending on the jurisdiction, this may not even be allowed)
- Manage it from a central location.

Using a security token is, of course, the highest level of authentication available. It functions as both an authentication factor and the storage of necessary software components. A G/On-token can carry the G/On-client for multiple platforms at the same time. It can also carry the application-clients for multiple operating systems at the same time. The G/On-client is self-contained, which means that it does not need anything from the underlying operating system, nor does it need elevated rights to run. If the USB-token is holding a micro-SD smart card, there is no need for driver support because that is already built-in.

Another part of mobility is the user’s situation: they might be in a locked-down network with only limited open ports open to the internet. Luckily, the G/On-client can be told to try different outgoing ports, use a proxy-server or even fallback to so-called HTTP-encapsulated traffic - without losing any feature or creating security loopholes. And a nice feature is configuration of the connection can be centrally changed by administrators and automatically pushed out to all clients without returning them to the office.

And finally, when G/On runs from a USB-token, it will automatically disconnect all user sessions when the USB-token is removed (smartcard-based token or soft token). It is crucial because users most likely will not forget their USB-token, but they will forget to log out. All factors above make G/On a genuinely mobile solution.

And if you don’t want the USB-token?

For organisations that don’t need or want the security tokens available in the mobility smartcard, G/On Desktop or its other flexible authentication options can still be a great choice for ensuring secure remote access. G/On Desktop essentially turns a user's remote computer into a token, which provides a high level of mobility when installed on a laptop.

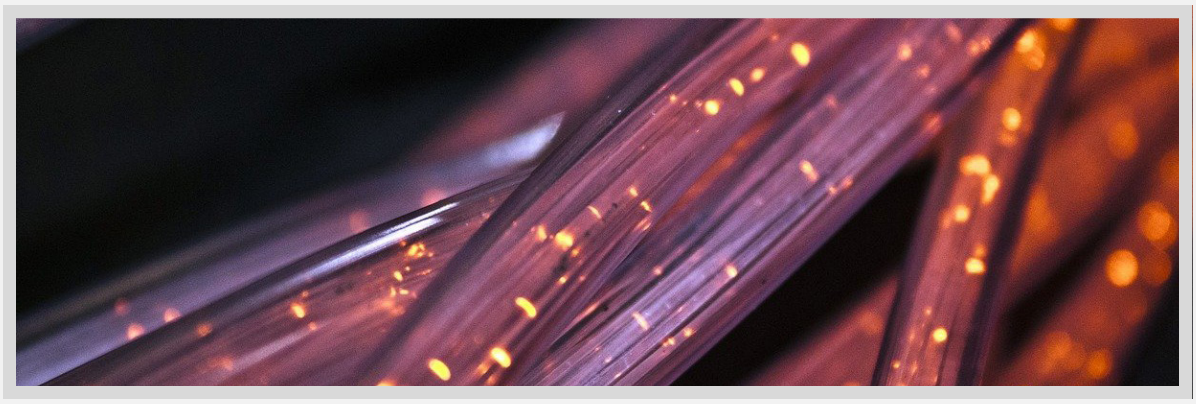
The G/On Desktop client installs itself and all client application components in the user profile, in such a way that is difficult to copy, making the remote computer quite a good second factor. Of course in this case, G/On Desktop needs to be ‘installed’, but it is not intrusive to the device (in exactly the same way the real ‘mobile’ G/On isn’t intrusive). It is available for virtually any Windows-based computer and doesn’t need rights to install and to run. It can be safely installed on a home computer or a personal laptop.

For even more flexibility, G/On also allows users to use external authentication services such as Google Authenticator or the Duo method. This creates a lot of possibilities to improve the service level to the user and ensures that the right people have access to the right tools at the right time.

With G/On, you can set rules for specific applications or data, requiring a certain level of assurance to ensure adaptive authorisation. And for other services or data that don't require the same high levels of authentication, alternative rules can be in place — for example, username and password on a business computer or username and password with authentication using a phone.

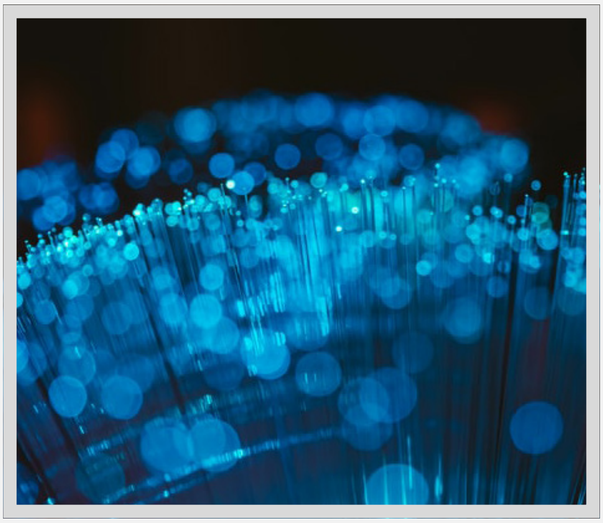
One of the key benefits of G/On is its ability to offer a standalone solution without the need for extensive IT resources or on-premise infrastructure. This means that even small IT departments can benefit from the authorisation capabilities of G/On.

Manage available bandwidth



Another often overlooked problem is the available bandwidth. Suppose there are multiple internet-lines available in the company. In that case, it is often quite hard to use them simultaneously because extra components in the form of network load balancers are needed. Network load balancers are costly, complicated, yet again introduce another scalability problem. However, with G/On, there is no need for load balancing. G/On clients can use numerous client connect addresses and connect to multiple client connect ports- in fact, many G/On-gateways. It's even possible to specify the order that these connect addresses and ports should be used. For instance, maybe connect to a specific location first and, only if that fails, connect to a second location - ideal for large organisations that have a backup data centre that is only used in cases where the primary data centre fails. Or G/On can be instructed to try all locations at the same time.

It means, in a single configuration, G/On-clients can be told to connect to connect addresses and connect ports at the same time and continue with the G/On-gateway server that completes the handshake first. For example, if G/On is told to connect to all data centres around the world at the same time, then, based on the location, the user would then most likely automatically connect to the nearest data centre.



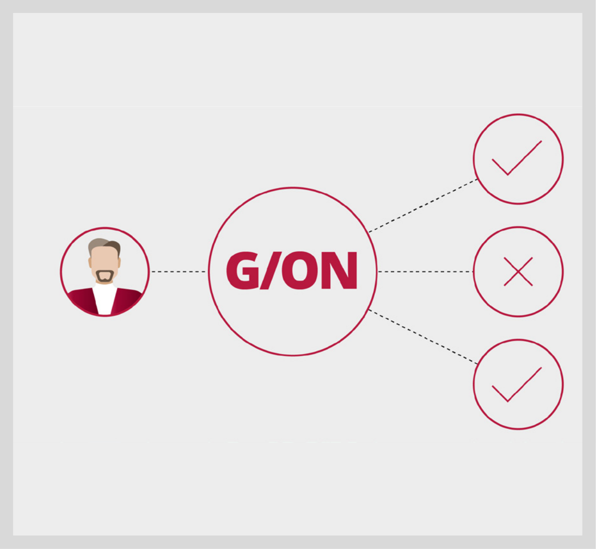
Easy to manage user access

A headache often facing IT teams is changing user access rights and adding (or removing) applications. So what if you could grant and revoke user access on the fly? G/On provides full control over settings, users and usage.

When asked about access challenges, over-privileged employee access is the top concern for 61% of organisations, followed by providing secure access to partners (53%), followed by cyberattacks (e.g. DOS, cross-site scripting, MiTM, phishing) (46%), and shadow IT (43%). But, with G/On, this doesn't need to be a concern: IT admins can control application access, prevent copy/paste/downloads and allow file downloads in a dedicated secure environment. And for users, there is no need for technical knowledge or any changes to the computer configuration. After logging in, users have immediate and secure access to their applications. Simple.

A safe, secure environment for all users

Of course, easy access and scalability don't mean much if a solution isn't secure. G/On is an integrated, secure Zero Trust solution, providing a safe environment for users. It features two-factor authentication, authorisation, data encryption, network protection and secure application access. G/On makes it simple to implement, manage and control access to company data and applications.



G/On is about securely enabling applications on unmanaged remote devices to access company internal applications and services. The G/On security model builds on the assumption: “The enemy knows the system” and assumes that the enemy will use targeted attacks. Most security elements in the G/On-gateway servers are under complete control of the administrators. The G/On client includes additional security elements, which by definition are under the control of the end-user and therefore cannot be protected and trusted to the same degree as the server-side. With G/On, the central services that must be protected are inside a security perimeter, and the only way to access the services is through one of the G/On-gateways.

User passwords can be stolen or accidentally disclosed. Therefore, it is an element of the G/On model that the G/On-gateway server checks for two authentication factors before trusting that the user is who they claim to be. In the G/On security model, the two aspects combine to strengthen each other. G/On supports authentication by the following two factors: a memorised username and password, combined with a physical token. There are several available options for the physical tokens: The mobility smartcard is the ‘strongest’ second factor, but other authentication methods are offered as well. Less strong, but allowing organisations flexibillity in the level of authentication they need for the different use cases.

It means that when a user starts a G/On-client, the client automatically connects to one (or more) G/On-gateway servers, proves its identity, and presents a login dialogue. The user types in a username and a password verified against a directory service, such as Active Directory, LDAP or the G/On internal user directory. Access requires the right combination of user identity and physical token (or physical second factor). In any other case, the G/On-client disconnects.

Assuming the user could log in, the G/On policy engine takes over and verifies if this user is allowed any connection to service inside the network, given the identity, location, time and other factors. If this is not the case, the G/On-client disconnects.

Assuming there is at least one connection available, the G/On-gateway computes a set of so-called menu-actions to which the user is authorised and sends control data to the G/On-client, which presents menu-actions in the G/On user's menu so that the user can make a selection. The selection can consist of many different types of connections, such as RDS, Citrix, Exchange, native client-server applications, administrator-tools and even the user's computer in the office. At this time, it makes no connection, and no traffic is allowed to travel from the endpoint to the network or vice versa. When the user launches a menu action, G/On will make sure that there is an end-to-end connection from that application to the service inside the company network — and only that connection, nothing else.

Ensuring secure application access

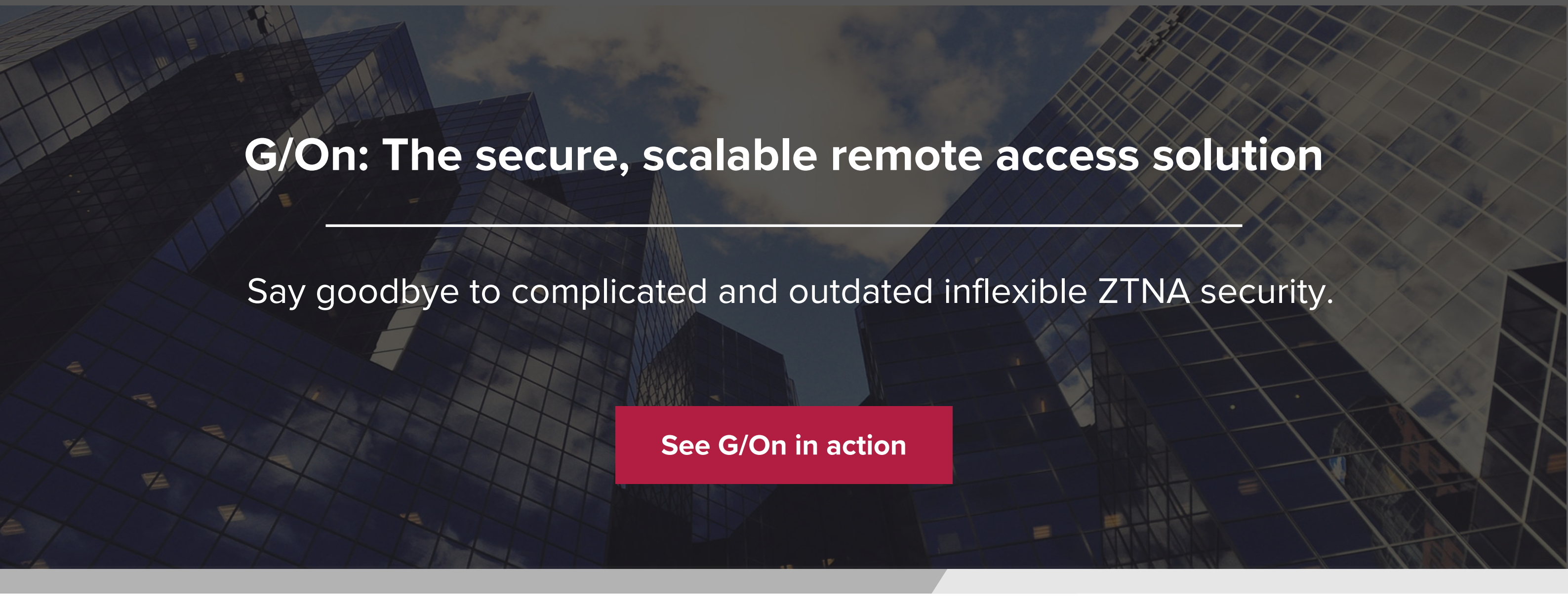
After receiving and validating the authentication factors, the server computes the authorised menu actions for that user, sending the control data to the client with the user's menu.

Once the user chooses a menu item, the client sends control data to the server, informing it of the user's choice. The server looks up the menu action definition and then directs the client to start the client side of the port forward, listening on a given port on the local loopback interface. The server may also instruct the G/On client to launch a given application client, with parameters that make the application client address the local loopback interface to reach the application server.

When the application client connects to the port, where the G/On Client is listening, the G/On Gateway Server connects to the application server, as defined in the menu action, and the G/On Client and Gateway Server collaborate on forwarding traffic.

Conclusion

At Soliton, we place the zero-trust approach at the centre of our solutions. Based on the user, we build a secure software-defined parameter around the company network, which stops unauthorised network access and protects data from being compromised within the company environment. Unlike with VPN, no information on the network is visible from the outside, meaning attackers cannot misuse information. Our products address the vulnerabilities of conventional solutions and prevent hacking and malware and protect personal and company data on unmanaged BYO devices from cross-contamination.



G/On: The secure, scalable remote access solution

Say goodbye to complicated and outdated inflexible ZTNA security.

See G/On in action

Get in touch

If you're concerned about remote access, cybercrime, or VPN user frustration, simply get in touch to find out more about G/On.

🌐 www.solitonsystems.com

✉ emea@solitonsystems.com

☎ +31 (0)20 896 5841