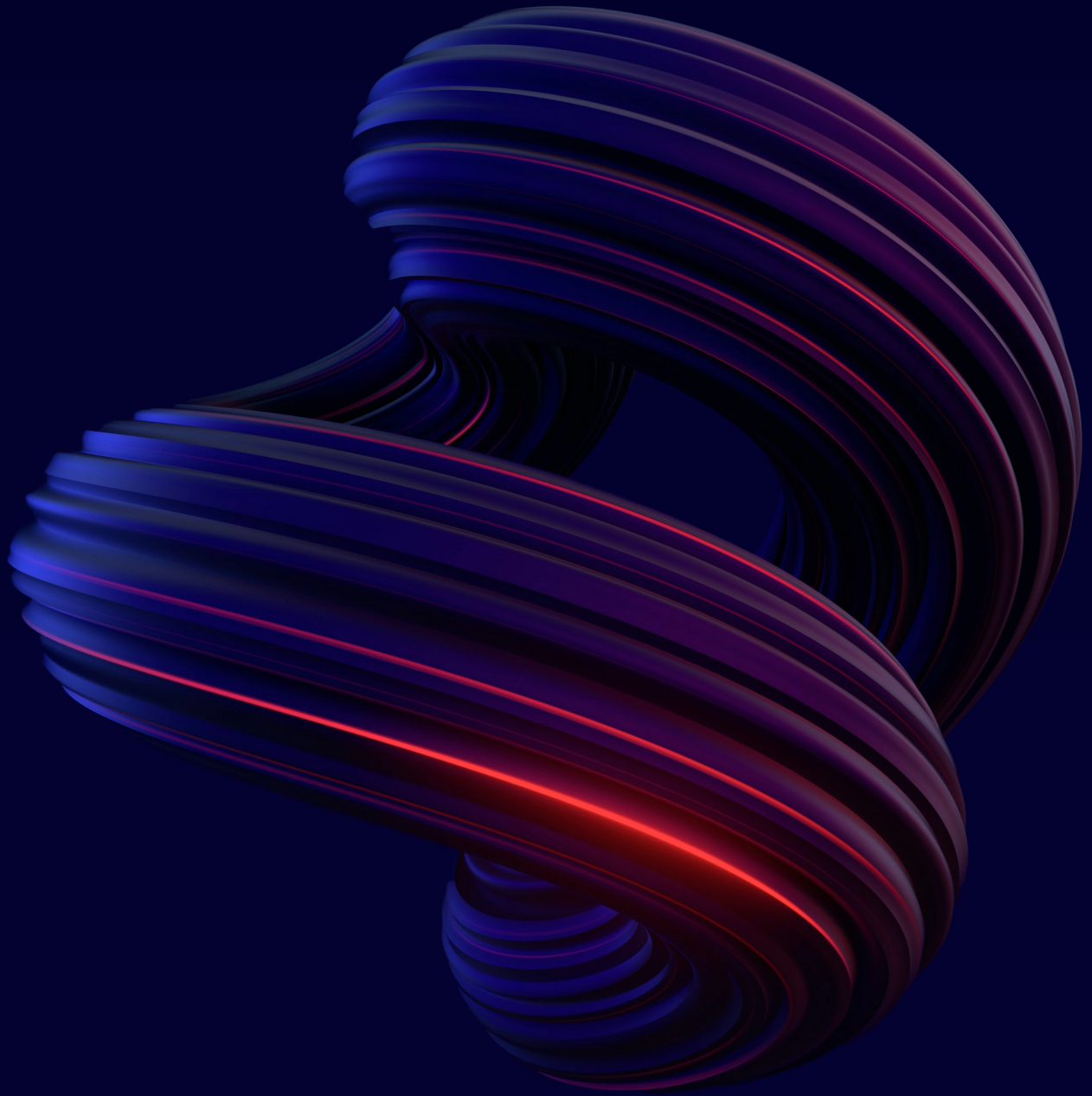
Soliton®



G/On

USE CASES

How G/On Makes the Difference

When you need to enable access to your applications or services, how do you make this happen?

Normally, companies connect all those systems to the internet, secure them one by one, and use two factor authentication to manage user access. But with every additional application you open up, it adds complexity - and increases your attack surface.

G/On combines everything you need to do in one package, making it easy to manage and scale.

It works with a gateway server or multiple gateway servers in front of your applications and services.

Direct access to these services is no longer possible; instead, they're hidden behind those gateway servers proxying information into those systems.

To ensure the right people access the G/On gateway server, the connections set up are encrypted and utilise strong authentication.

And to make it easy for users, the G/On client can automatically connect to those gateway servers, handling everything on their behalf.

USE CASE

Carry encryption all the way from the endpoint to the G/On gateway

Challenge

When you don't trust the local wireless hotspot, the carrier or the cloud provider, it's important to carry encryption from the endpoint to the entry point of your network.

Otherwise, you leave yourself open to man in the middle attacks, where someone intercepts your connection line, terminates your connection, sets up a new one to your destination and listens to the connections you've made.

Opportunity

When connecting over your infrastructure, you can argue that it's your protected infrastructure and it's safe. But in cases with unsecured WiFi, for example, it's impossible to defend it in the same way, so an alternative is required.

Solution

Carrying encryption from the application on the endpoint to the G/On gateway means you have absolute certainty that nobody is 'a man in the middle'.

It essentially ensures that the connection is authenticated, and you know that the person you expect to listen to is on the other end.

USE CASE

Opening access to applications and services to named collaborative ecosystem members

Challenge

Organisations need to open applications and services to named collaborative ecosystem members — such as distribution channels, suppliers, contractors or retail outlets. But using VPNs with these people is not sensible, because you don't know anything about them or the posture of their endpoint devices.

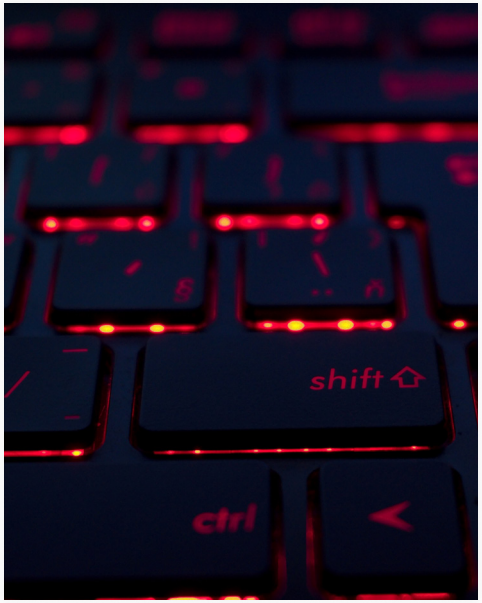
Opportunity

In the age of a highly digital connected economy, organisations are increasingly extending their workspace environment beyond their employees. From an IT Security perspective, facilitating this access in a safe, secure and user-friendly way enables business and protects important internal resources.

Solution

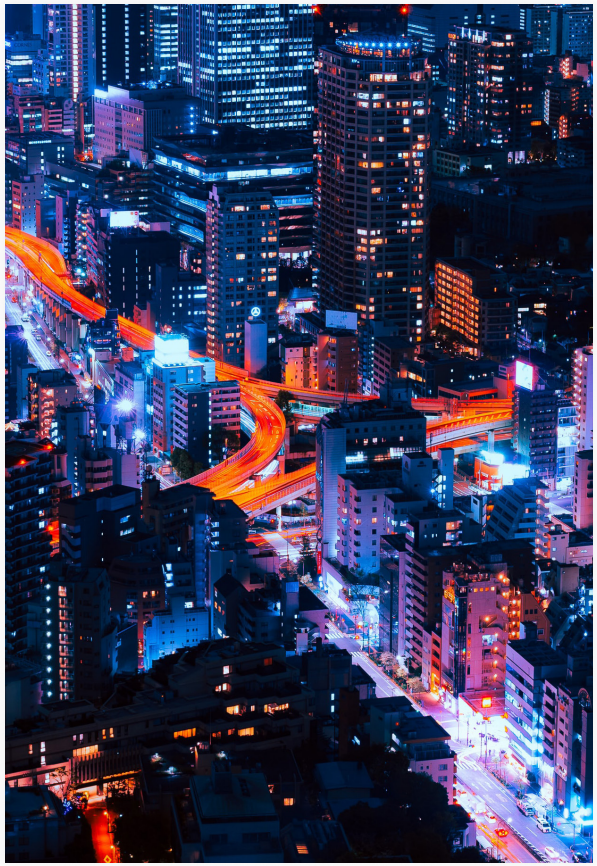
G/On replaces your VPN connections with a secure, software-defined perimeter. Operating on a zero-trust basis, G/On enables you to control access at an application or service level to people operating outside your organisation.

Instead of essentially opening up a unrestricted highway from an unknown device to your network, you open up specific applications to an individual user.



USE CASE

Providing application-specific access for remote or mobile employees



Challenge

Mobile and remote employees need access for their work. But, access provided using VPNs is typically too broad, especially for employees who often have more access than third parties or external contractors.

Opportunity

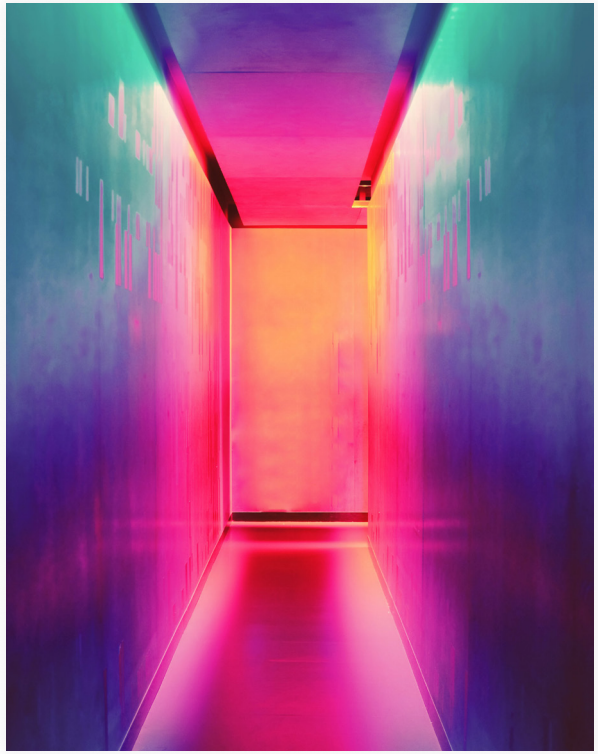
Controlling who, when, how, what, and for what time frame remote or mobile users can access is an absolute must to ensure secure business operations. It's critical to minimise the attack surface area and have complete control over every connection, tight credential management, and audit for all user activity.

Solution

Using application-specific access with a G/On solution ensures that employees have access appropriate to their requirements based on who they are, when they want to access, how they access and what they want to access. But it mitigates risks that come from overly broad VPN access capabilities.

USE CASE

Supporting Merger and Acquisition Activities, without having to combine networks



Challenge

During mergers and acquisitions, there's often a need for employees from one side to access systems from the other organisation.

However, it's highly likely that the two IT infrastructures are not well matched, and enabling access through is quite a complex thing to do with the VPN and firewall rules.

Opportunity

G/On provides high isolation, which means it's possible to run applications from the other company on your computer without having to really connect the networks together or to make connections, which would be difficult.

Solution

Using G/On opens up the possibility to start working together without requiring time-consuming and resource intensive deep integrations on day one. The end goal may be deep integration (though there are benefits to maintaining separation).
But, connecting together more quickly makes organisations more agile during the M&A process.

USE CASE

Isolating high-value enterprise applications

Challenge

When high-value enterprise applications are accessible on your network, they are vulnerable to insider threats and other security breaches.

Opportunity

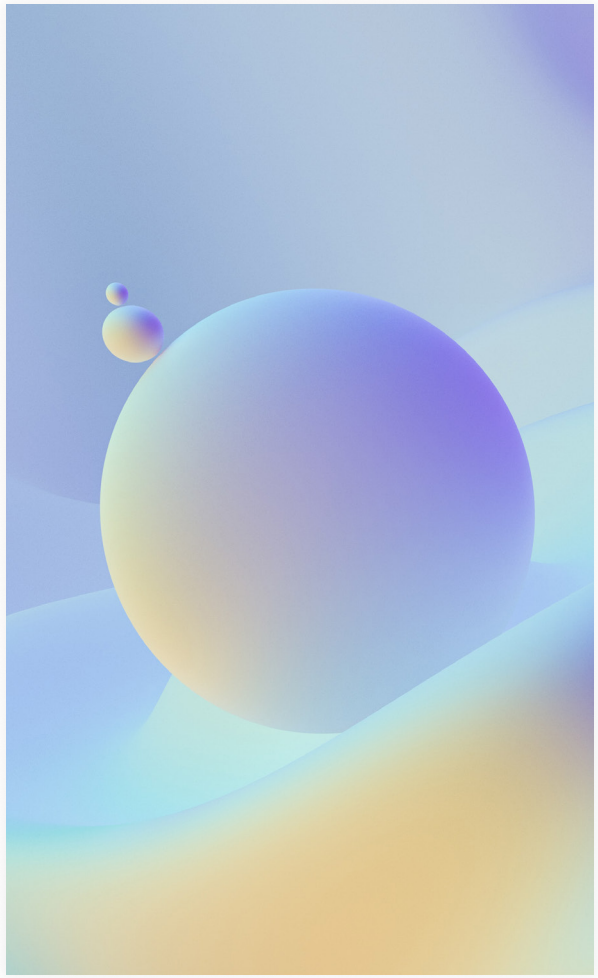
Isolating high value enterprise applications, reduces insider threats and affects separation of duties for administrative access, as it's not possible to access these applications without additional authentication.

Solution

Using a solution like G/On means it's possible to isolate high-value enterprise applications, and only enable access to authenticated people and devices.

USE CASE

Authenticating users on personal devices



Challenge

Managing security on unknown, personal devices remains a challenge for IT teams. When companies put device management software on personal devices, these change the configuration and are invasive on the device. And using personal devices for work risks leaving company data on the device.

Opportunity

G/On can improve security and simplify bring your own device (BYOD) programs by reducing full management requirements and enabling more-secure direct application access.

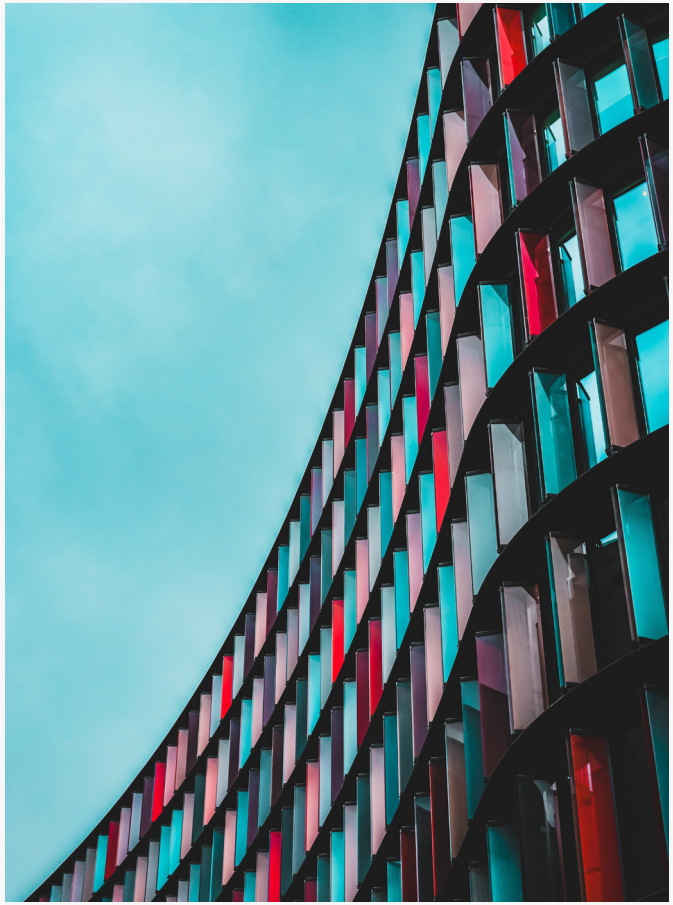
Solution

G/On brings all the tools that you need to connect with it to your laptop without having to install additional software or make any configuration changes.

It also enables full separation between company and personal data, improving both security and work-life balance.

USE CASE

Protecting internal systems from hostile networks



Challenge

Inbound access points to your internal systems create an attack surface from hostile networks including public internet. The more inbound access points that you have, the larger your attack surface and the harder it is to defend.

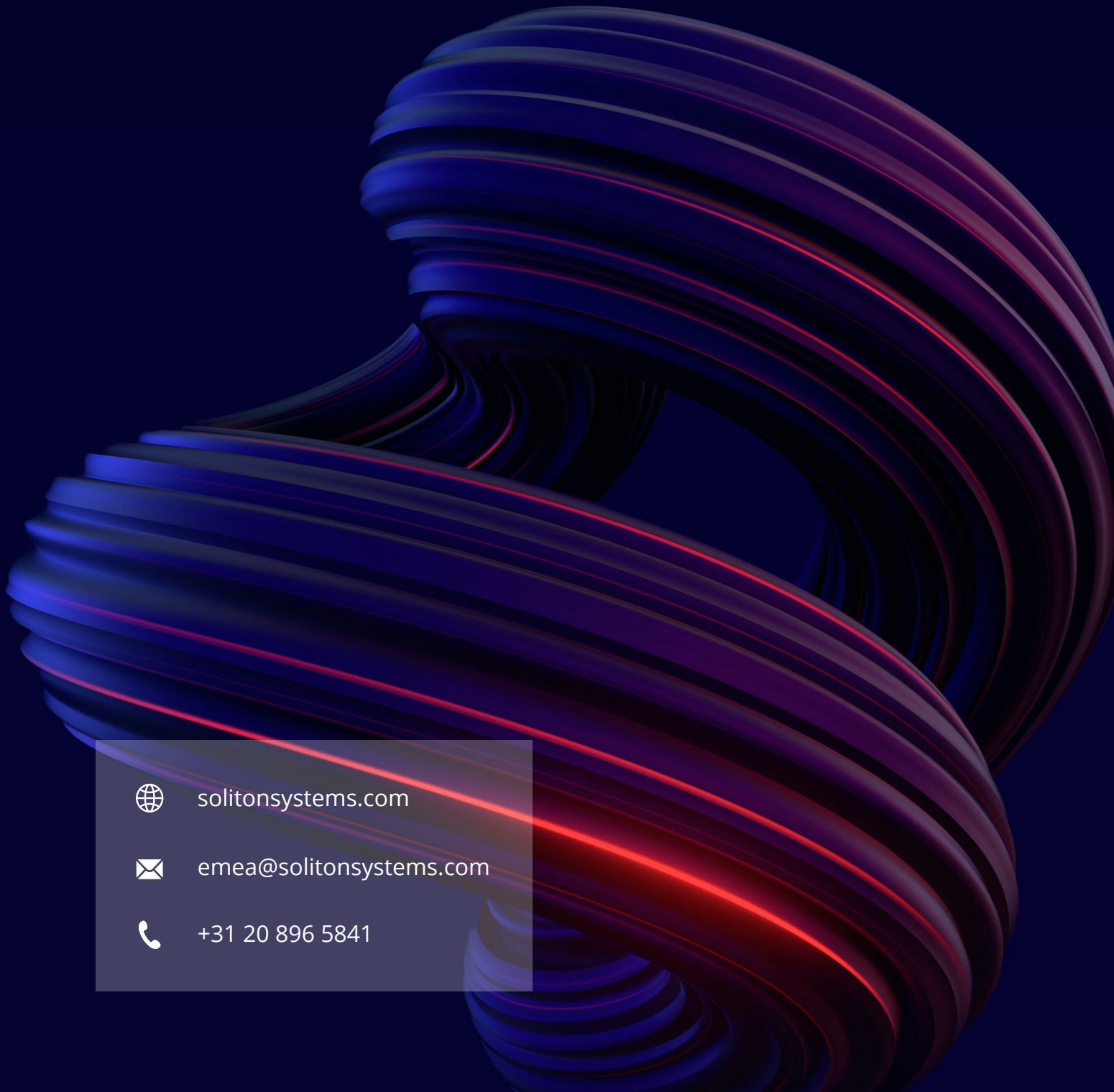
Opportunity

Reducing the attack surface means you get more control, more assurance around security of the systems behind your gateways. If there's a problem with them, or if there's a vulnerability in those systems, this is not necessarily leading to an immediate problem.

Solution

When you have multiple inbound routes to different systems, it's harder to protect those systems. Using G/On reduces this to one. Instead of waving to think about the security of A, B, C, and D all individually, now you can focus all your energy on just one system.

Soliton®



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.

solitonsystems.com

emea@solitonsystems.com

+31 20 896 5841