Customer Case Study

GOVERNMENT MINISTRIES SHARED SERVICES CENTRE DEPLOYS G/ON TO ENABLE ZERO TRUST SECURITY AT SCALE

Having an easy-to-use, cost-effective zero trust solution that maintains security is critical for safe remote working. For a government ministry shared service centre, zero trust solutions helps to connected users with internal systems, even when the team cannot work from the office. But in a complex environment, implementing a reliable solution isn't easy.

When a shared services centre for national government ministries needed to support more users working outside the office they turned to Soliton Systems for a solution that meets all their needs.

How zero trust security supports remote working in a safe environment?

A shared services centre for a national government needed to enable remote working outside the office in a safe environment. They were not happy with the existing setup: it simply wasn't secure. The complex configuration, which includes Citrix, Remote Desktop, and Web Servers deployed across the service, makes it incredibly difficult to implement a safe and easy solution for users to access services.

The IT team explored multiple point solutions. But it became apparent that they would need multiple, different technologies to solve their challenges. When these solutions grew, it increased complexity in the internal structure, becoming exponentially more complicated - especially with user information stored in multiple locations.

Users also needed to authenticate via 2FA - a considerable problem for a shared service centre given the number of users involved. The solution also had to be user friendly: simple to use and solve for mobility.

G/On: Solving many use cases in one solution

Working with Soliton, the shared services centre turned to G/On. It's a scalable solution, built on zero-trust principles. It works by decreasing the attack surface, increases visibility into user activity and reduces complexity.

For the shared service centre, it provides a single alternative to all the multiple point solutions and meets the additional requirements: 2FA authentication and user friendly.

Compared to the total operational costs, combined with investment in point solutions, G/On proved highly cost-effective.

Balancing the load

Many point solutions need additional load balancers to add more users, which can take many weeks to scale up. Network load balancers are also costly and complicated.

G/On negates the need for load balancing. G/On clients can use numerous client connect addresses and connect to multiple client connect ports — and, in fact, use many G/On-gateways. It's even possible to specify the order that G/On used these connect addresses and ports. For instance, maybe connect to a specific location first. If that fails, then use a second location - ideal for large organisations, like the government shared services centre, with a backup data centre for cases where the primary data centre fails. G/On is programmed to access a specific location first and then go to the backup locations if the main one is down.

Using G/On OS for highly confidential applications

Unsurprisingly for a government shared services centre, some applications are so confidential that they cannot be accessed by unmanaged devices using Windows or macOS. The organisation also deployed G/On OS. It's Linux-based (but hardened) and is booted directly into memory from the G/On USB Token. It does not include drivers to access hard disks, so it's impossible to leave data behind or transmit data from the computer used.

The only operation available with the G/On is to make G/On connections, which solves the problem of accessing the particular applications outside of the office.

Authenticating users with the G/On USB Token

To support the high-level security required, all users at the shared services centre have a G/On USB token; it functions as both an authentication factor and the storage of necessary software components.

It is a USB form factor token with a mobile smart card integrated into the MicroSD card. On it, end-users receive a fully functional G/On client. It can be pre-enrolled, or end-users can go through a simple field enrolment process to enrol the G/On client. During enrolment, the smart card autonomously generates a private/ public keypair. The private key is protected by the smart card and can never leave it, and the public key is sent to the G/On Management Server to be used for future user authentication.

And, when users unplug the key, the connection is gone.

Secure, easy-to-use and scalable. G/On ticks all the boxes

G/On meant the shared services centre could deploy a zero trust solution at scale, keep even sensitive data secure and provide a solution that made life easy for users. It offered a much faster implementation, as it didn't require the same infrastructure changes needed to scale using point solutions. It also provided users with a more stable and faster connection when working remote.

Have unknown devices that are operating in unfamiliar environments across multiple locations? It's all manageable with G/On.

The nature of this customer's work means we can't divulge their name. We've worked on similar use cases across multiple countries - helping organisations enable secure remote working at scale.

About Soliton Systems

Soliton Systems helps companies solve IT security challenges with a unique set of high quality, cost-effective products and solutions. As a global company with over 30 years of IT security experience, its solutions are already deployed by many of the world's leading companies.