Case study

Enabling secure access to business critical banking networks

The banking industry is always investing in improving network performance. But the challenge for the industry is it handles very specific, confidential data. Often, these networks must be able to manage and process very high volumes of data and be very resilient, and outages cause high levels of disruption. Changes to these networks, therefore, need to be monitored and verified throughout. Therefore, its critical important business critical processes are not interrupted.

Understandably accessing these environments, for example, the SWIFT network, requires high levels of authentication, above and beyond the standard access rules. All the configuration that needs to be done on these networks is very secure and considered.

It is always a separate network; users must go through multiple security layers to make any changes and provide their credentials. Typically, you can only access this network via a separate dedicated remote desktop connection to systems in this network. But this brings complications, and the process of allowing users access and enabling them to perform changes is very specific. A lot of manual work is required before allowing access to those networks. First, users must ensure they've requested a particular account to perform those activities and specify the exact moment they will be doing them. Temporary passwords used in these cases will not be issued via emails. They'll be sent by an alternative means, and users need to receive a specific password to get access and make configuration changes. Many things need to be configured before granting access to those environments.
With G/On, it's much easier.

Enabling secure access to business critical networks

G/On enables secure access to these networks and ensures access to the networks is authorised in the way you need. For instance, users will be allowed to do the configuration changes at a specific time, which G/On can provide. It also provides more sophisticated, certificated-based authentication, rather than just relying on username and password, combined with multi-factor. It uses a specific certificate and can even verify the user's location - all factors that need accounting for before granting access to these environments.

Without a solution like G/On in place, banks need to have alternative ways to access those networks. Often this will be a remote desktop server with a specific dedicated network for these Windows machines. As a result, they have needed to set up a dedicated RDP server farm and apply separate authentication mechanisms besides the regular active directory.

G/On provides a certified way of your identity in a permanent sense. It's a physical token that you have, and it proves you say that you are who you are and allows temporary access to those environments to grant you a digital identity specifically for this network temporarily. For example, users could gain access and perform certain activities at specific times of the week. But they wouldn't be able to access the environment at any other time.

It means that administrators can allow specific users to have set access based on their identity instead of users having to receive a new verification method to prove their identity each time they need access. This use case applies to any highly secure environment in the banking networks, including customer databases and transaction processing.

Uncovering issued with existing VPN solution

In this case, the customer was a midsized financial responsible for a transaction processing network. The most critical element of this network is not the economic but the social impact of a possible outage. The transaction processing network was even divided into different security zones. There is a continuous focus and mentality to reduce the risk in the transaction processing network.

The current model is a dedicated endpoint VPN solution to enable the IT staff to perform necessary changes. Once a change is approved in the change process, the VPN connection is made, the changes are completed, and then verified afterwards by a reviewer - it's all part of their internal change process.

However, an Internal Pentest uncovered issues in the used VPN solution even though patches were applied to it. Another problem was that the VPN allowed communication between the endpoint and the transaction processing network.

Why did they choose the G/On solution?

The new solution needed to focus on application access, rather than network access to solve this challenge. And preferable to a high secure solution by design, meaning no cloud connection and certificate based identity verification.

The proposed G/On solution addressed both issues. And it proved to be scalable enough to enable a second administrator to approve the temporary access.

Since G/On is only application-based with included process inspection rules, the solution only allowed user-generated traffic instead of all traffic defined by the VPN firewall.

And the most appealing feature was not having to worry about vulnerabilities in the SSL VPN application. G/On ensure any application accessible remotely is invisible and inaccessible from the outside, reducing your attack surface to an absolute minimum.

The customer was also very happy the total deployment of the solution was finished only on a Saturday morning, making the solution up and running and ready for Monday morning changes. After the design for this specific situation and the easy of use, working with this solution they saw G/on as the ideal solution to eliminate all SSL VPN connections for remote users to internal applications. Therefor the customer decided to replace their VPN solution by G/On making all applications invisible and directly inaccessible from the internet.

The Results: Providing secure, continuous authentication

Typically people only require short-term access to the live environment when making network updates. But where more time is needed to complete the work, users would have to re-authenticate themselves and verify their identity. While this is a vital security feature, it is disruptive for the person working; every time the user is prompted to authenticate, they are presented with a question for multi-factor authentication.

G/On provides the continuous verification of your identity by using the certificate for encryption. Whereas the connection towards a network without G/On is authenticated once, you're authorised once that authentication is established. Then, there's a continuous flow of authorisation by default. On the application level this customer drastically reduced their attack surface, by making all application invisible and directly inaccessible from the internet they were no longer vulnerable for supply chain attacks such as Log4J, while their users never noticed the increase of security before gaining access.

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 40 years of IT security experience, its solutions are deployed by many of the world's leading companies.