How G/On provides a giant leap into the Zero Trust era

Soliton®

The IT security landscape has changed dramatically in recent years. As more organisations undergo digital transformations, the traditional approach to security gets less effective.

Legacy networks, a shortage of security professionals, and a growing number of cyber threats are some of the complications that IT teams face when securing their organisations. Ransomware attacks have increased by 57% since the disclosure of the vulnerabilities experienced by Microsoft Exchange, and a UK government survey found that 41% of businesses experienced a cyber security breach or attack in the last 12 months.

The Zero Trust Security model shifts the focus from device-oriented security to user-centric security. It requires users to prove their identity and authorisation each time they access a resource, regardless of whether they are inside or outside the organisation's network perimeter. This way, organisations can reduce the risk of unauthorised access and prevent data breaches.

Furthermore, the Zero Trust Security model is gaining momentum. A 2022 survey by Cybersecurity Insiders found that 72% of organisations have implemented or plan to implement a Zero Trust Security strategy. This is not surprising given that organisations with a formal Zero Trust strategy experience fewer breaches than those without one.

In summary, the changing IT security landscape, coupled with the growing popularity and effectiveness of the Zero Trust Security model, are driving companies to embrace this approach to better secure their organisations.

Contents

01.

Why Companies are Turning to Zero Trust: **Understanding the Changing Landscape**

Organisations across the globe are increasingly turning to Zero Trust Security as a way to mitigate the risk of future incidents. The drivers behind this trend revolve around the need to protect sensitive data and ensure that critical systems remain secure.

Cyberattacks have become increasingly sophisticated and frequent in recent years, making it more difficult for traditional security measures to keep up. In 2020, for instance, the SolarWinds attack compromised multiple US government agencies and major corporations, highlighting the need for more robust security measures. And estimates suggest that the global cost of cybercrime could reach $10.5 trillion annually by 2025.

According to a 2022 survey by IDG, 63% of organisations stated that improving IT security is a top priority for the coming year. In addition, a 2022 UK government survey found that 41% of businesses had experienced a cyber security breach or attack in the last 12 months, with 67% of larger businesses being targeted. These attacks have far-reaching consequences, with 26% of businesses experiencing negative impacts on their operations, 19% experiencing financial costs and 18% experiencing reputational damage.

As a result, it is not surprising that more organisations are embracing Zero Trust Security, with a 2022 survey by Cybersecurity Insiders finding that 72% of organisations have implemented or plan to implement a Zero Trust Security strategy.

Adopting Zero Trust Security can help to mitigate these risks by shifting the focus from device-oriented security to user-centric security. This user-centric approach means users must prove their identity and authorisation each time they access a resource – rather than assuming that all devices on a network can be trusted. Zero Trust helps to prevent unauthorised access and reduce the risk of data breaches.

#01

Mitigating account breaches due to phishing or account leakage

Cybercriminals often steal user credentials to sell it on, resulting in anything from SPAM in your mailbox, targeted phishing attacks on select groups of users, right through to an attack on company systems because the user used the same password on different platforms.

Combining these credentials with 2 Factor Authentication (2FA) improves the security level, but it doesn't yet give a 100% guarantee. For example, allekabels.nl experienced an attack where millions of captured encrypted passwords were not properly hashed/encrypted, resulting in plaintext passwords.

How Zero Trust Security helps:

With this in mind, Soliton Systems focused (many years ago) on using safely stored certificates that can be used with traditional credentials to gain access to company data. This approach enables direct control over certificates, both fully automated and manually, and allows secure (and even temporary) user access.

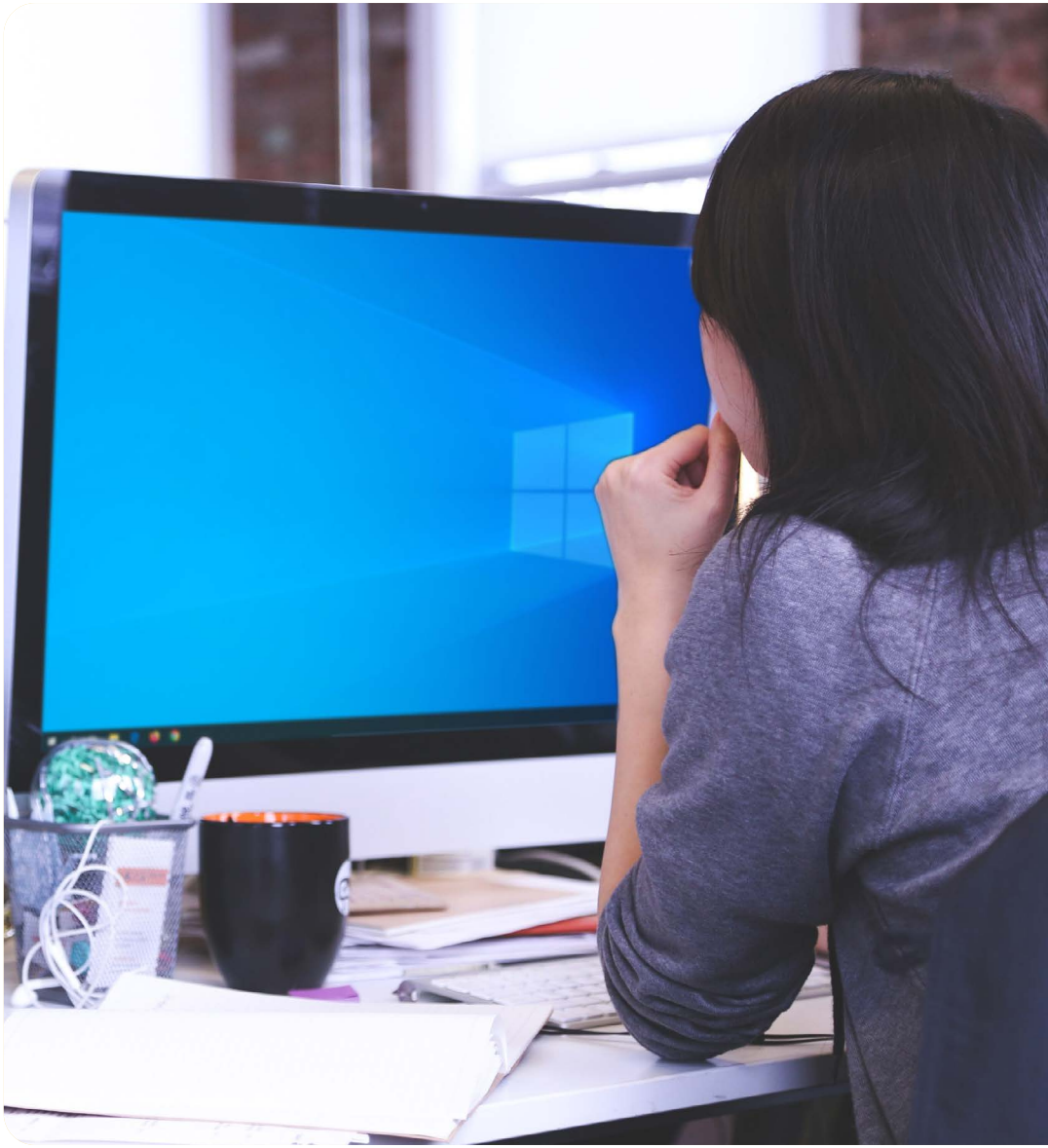
#02

Reduce network breaches through infrastructure vulnerabilities

Recent months have seen a significant increase in network vulnerabilities, including Pulse Secure, Sonicwall, Netscaler and Cisco. The number of Common Vulnerabilities and Exposures (CVEs) alone isn't the only concern; it's also the related risk score. Increasingly, the risk score per vulnerability found is more than 8 (max. 10).

How Zero Trust Security helps:

It reduces network breaches through infrastructure vulnerabilities. As a result, these weaknesses cannot directly lead to unauthorised access to internal company systems - which in most cases leads to ransomware attacks or a data breach. It's certainly not the case that Zero Trust security will prevent data breaches. But the risk of a data breach through exploiting vulnerabilities in VPN portals etc. is drastically reduced.



#03

Prevent vulnerabilities in internet-facing applications from being exposed

We've all heard news stories about companies brought down by ransomware attacks - these attacks impact all of us, not only people working in IT security. Recent cheese shortages at Dutch supermarket firm Albert Heijn are a case in point.

The truth is, vulnerabilities will always exist. Tackling them comes down to investing in a good vulnerability management platform. Then weaknesses, even in network configurations, can be quickly spotted and remedied. In addition, a good security infrastructure design will always take into account a breach and limit the impact of any vulnerability.

How Zero Trust Security helps:

It focuses on limiting the visibility of these applications — and, therefore, the unavoidable associated vulnerabilities. Applications are only visible to the legitimate user and certainly not exposed to the internet. Direct access to the applications is controlled using the Zero Trust model.

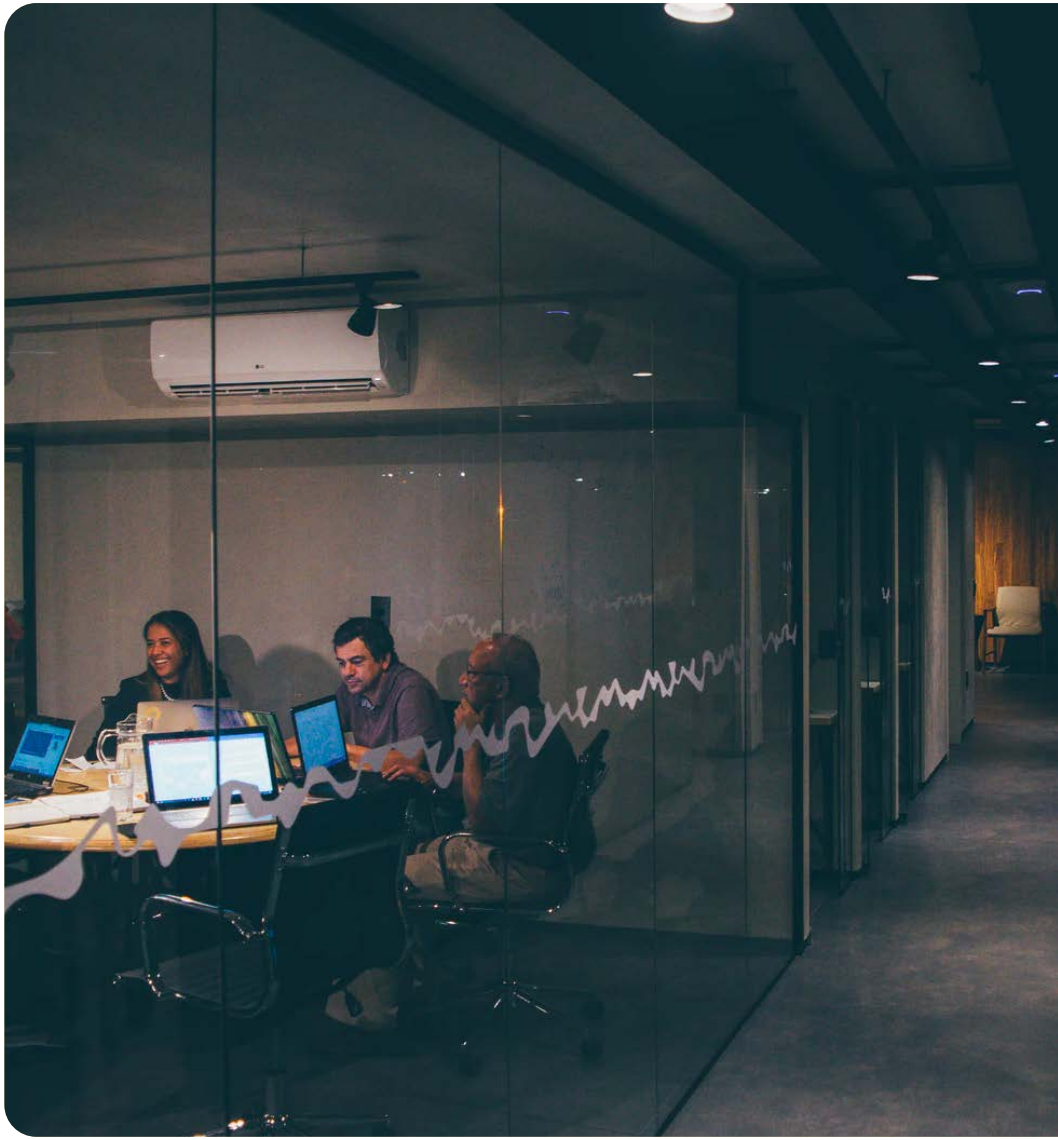
#04

Stop “Man-in-the-Middle” Attacks

Man in the Middle (MiTM) attacks are not a new cybercrime, but they still result in costly data loss. The number of MiTM attacks has increased in recent years. Scenarios like employees accessing company data on devices via unsecured or public Wi-Fi networks combined with relatively easy-to-access tools have made it a popular and relatively easy form of criminal activity.

How Zero Trust Security helps:

If the solution uses an encryption protocol with mutual authentication based on certificates, endpoints are never different from what they declare - it means a technique like MITM is not possible.



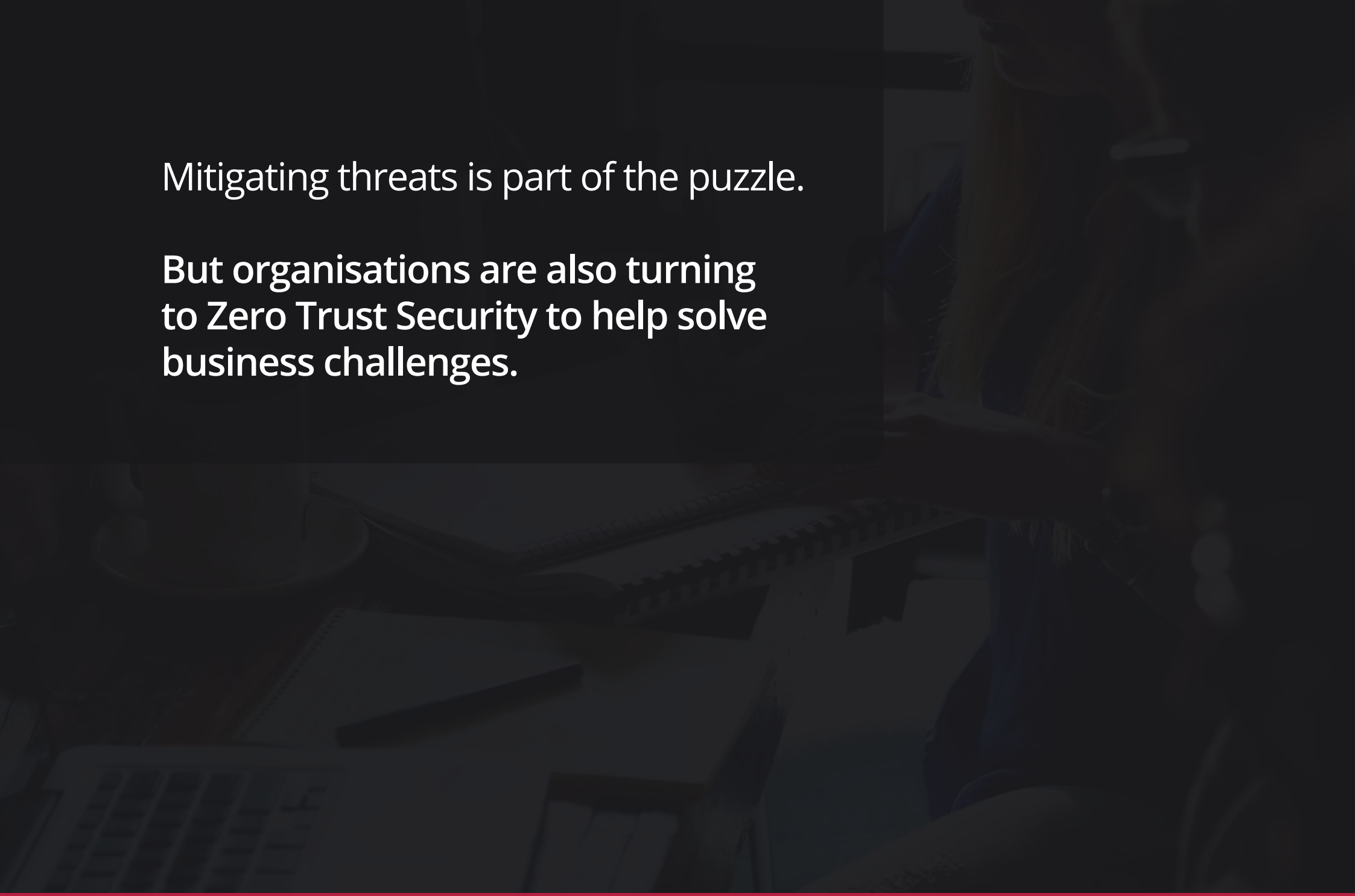
#05

Unsynchronised identity store

When user access is controlled in multiple stores, it's easy for them to get out of sync. Over time, when people leave and join the organisation, changes roles or move departments, changes in their access permissions, things get missed, and changes aren't universally made. Essentially it means some users can end up with the wrong access privileges.

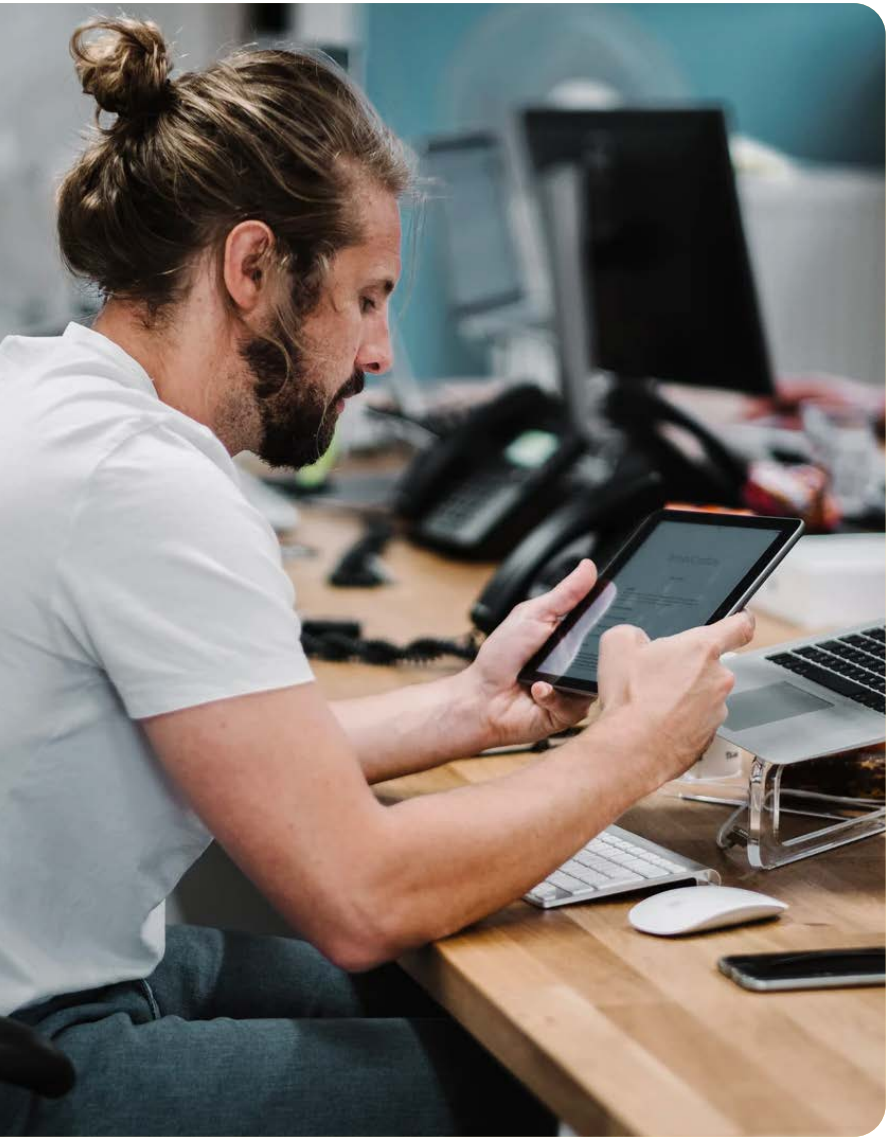
How Zero Trust Security helps:

It provides a single central point, organising application authorisation. However, solutions can use multiple Identity Providers (IdPs) for this: Access to applications can be managed per user. Revoking rights and changing access times can also be managed there, so there's no longer a risk that the user can access the platforms through another application.



Mitigating threats is part of the puzzle.

But organisations are also turning to Zero Trust Security to help solve business challenges.



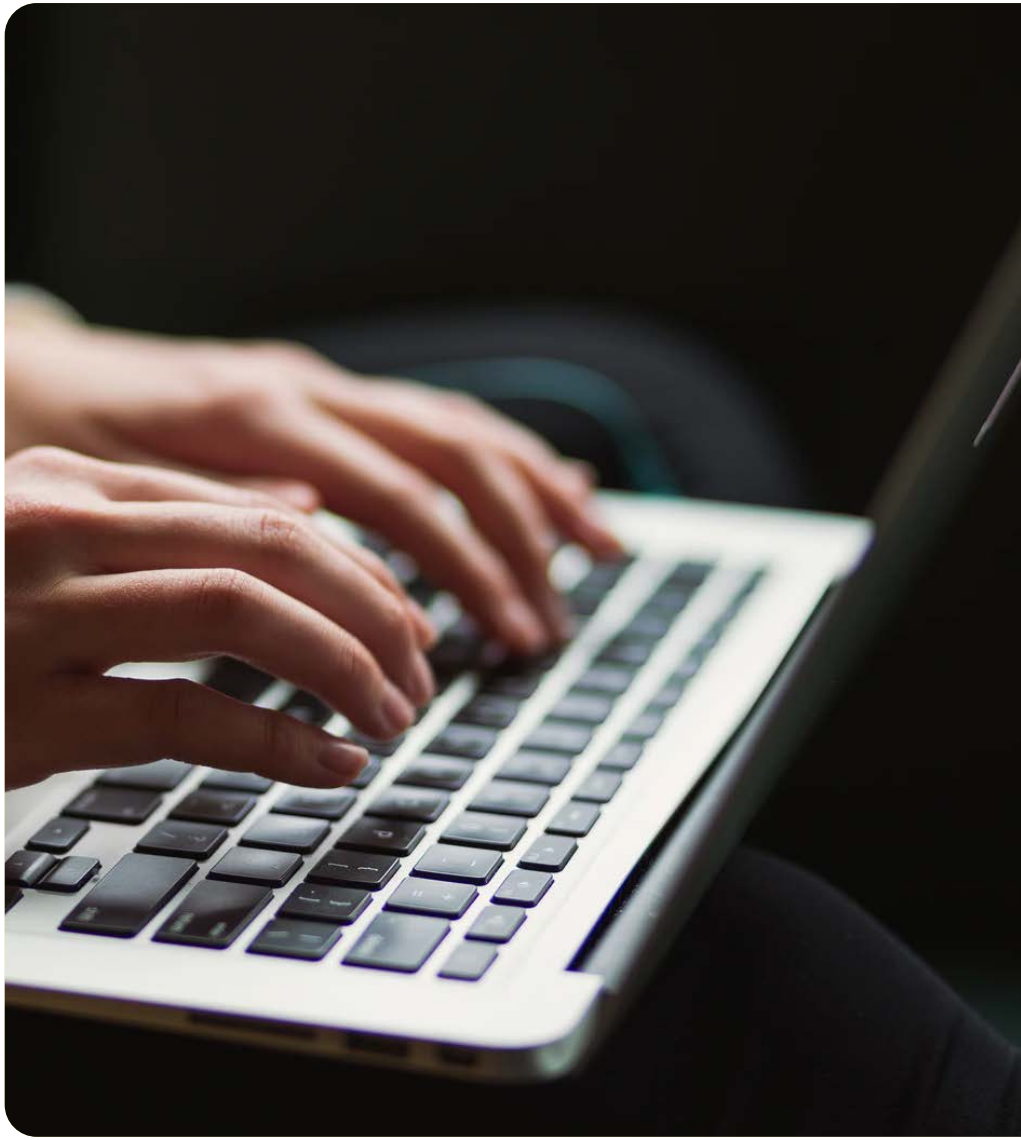
Supporting access for unmanaged devices

The current security debate often focuses on whether to use VPN or Zero Trust. However, another option is to combine both technologies. This is most helpful in the short term while moving to a Zero Trust approach, which can be lengthy due to how complex the shift can be. Because VPN provides access to remote users, while Zero Trust is a holistic authentication approach, VPN can be used as an access method as part of Zero Trust. However, once the Zero Trust framework is rolled out, it's much less time consuming to scale and grow the framework.

From a security perspective, VPNs are also problematic when used on unmanaged devices. VPNs are typically used to control access in an all-or-nothing fashion. Due to the nature of VPN-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 (requires a higher administrative level) and manage (updates and vulnerabilities), don't leverage user context to make access decisions and can't keep up with the pace of business. Unlike VPN, Zero Trust should allow for unmanaged devices, and remove the need for embedded policies and endpoint management.

Scalable, grow with your needs

Complexity is the enemy of scalability. When a remote working solution consists of multiple components, it isn't easy to scale up because, at different moments, the various solutions need to grow. A single all-in-one solution for Zero Trust Security, 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. It means organisations can scale up remote working in minutes rather than weeks — scaling just comes down to licencing.



Easy to manage user access

A headache often facing IT teams is managing user access rights and adding (or removing) applications. It's particularly challenging because of the shortage of specialist cyber security professionals.

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. cross-site scripting, MiTM, phishing) (46%), and shadow IT (43%). But, with a robust Zero Trust solution, 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 — there's no need for specialist knowledge, making it easier to manage

And for users, there is no need for technical knowledge or any changes to the computer configuration. So, no required walks to the companies "Knowledge Bar" for assistance. After logging in, users have immediate and secure access to their applications. Simple.

02.

The Time is Now for Zero Trust Security

Whether you work in manufacturing, local government, healthcare or a completely different industry, it's clear the IT security landscape is changing. Evolving and growing cyber security threats, combined with new, hybrid working patterns, mean you have an opportunity to explore a new approach to enable business and securely connect remote users to internal systems and applications.

Zero Trust isn't an easy concept to understand. Moving from a traditional security architecture that assumes trust based on certain devices, individuals and locations toward a model that instead trusts nothing until it is verified, requires new tools, methodologies and most importantly a different way of thinking.

To help bring it to life, here are five easy to understand example use cases where Zero Trust Security helps:

#01

Secure third party/non-employee identities working inside the corporate network

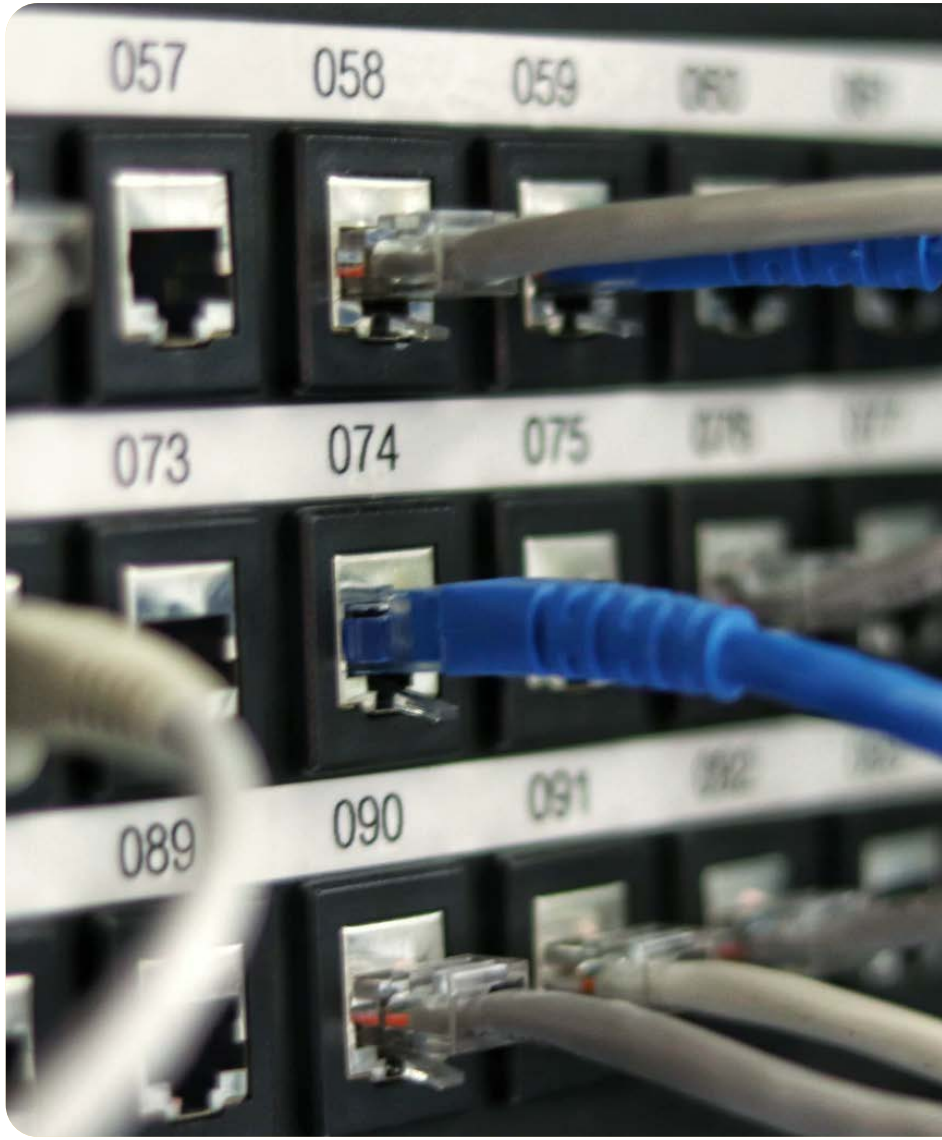
Most enterprises support employees on the corporate network. However, inevitably, other users, such as third-party business partners, contractors, and temps, will also work from within your corporate network. These situations highlight why location-based security metrics are woefully overrated and why security should be uniform across the board.

When bringing non-employees or third parties into a corporate network, utilise the Zero Trust philosophy of “trust no-one outside or inside the network”. If the only security you have is at the physical layer, granting third party access creates a significant security risk. However, if “identity is the new firewall”, making sure any identity (user) inside or outside the network only has the access they need and is governed correctly will ensure that access to company resources remains secure.

#02

Protect remote workers accessing public and private (cloud) resources

Managing the security of remote employees became a significant concern in 2020 in the wake of the COVID-19 pandemic. Security administrators find their edge security products provide no benefit to remote workers who use the internet to connect directly to public and private (cloud) resources. While it is possible to force remote workers to use VPN or virtual desktop infrastructure technologies through the corporate network, these options often prove inefficient and burdensome. Another often overlooked problem is the available bandwidth and latency: Zero Trust becomes a great alternative because it does not require users to connect to the corporate network before accessing services.



#03

Support globally distributed teams

Within an organisation, there are often multiple satellite offices and remote employees that connect to a central headquarters. And because the teams and employees are remote, many organisations use cloud resources and applications to connect teams. Since these resources are outside the traditional network, traditional security tools and processes are not very effective. Some companies force remote workers and locations to reach resources using a VPN or virtual desktop infrastructure.

However, these options often prove inefficient and burdensome. Again Zero Trust does not require users to connect to the corporate network before accessing resources. Understanding the identity of the user is needed to make sure any access is secure and appropriate.

#04

Accessing OT management or control stations from the IT environment

Operational Technology (OT) environments operate management stations controlling multiple industrial devices, Programmable Logic Controllers (PLCs) etc. These OT environments have a high demand for real-time operation, which can stand in the way of a decent security design. Therefore an almost physical split between OT and IT networks was the common practice. Resulting from this design the challenges include:

- Lack of security awareness among OT staff.
- Lack of visibility into all of the OT systems.
- Shared network infrastructure within the manufacturing floor between systems.
- Inability to address security issues by patching the OT systems.
- Increased attack surface with the increase in OT/IT convergence.

The resulting structure is primarily a strict separation between OT and the IT environment. Port-based bridges (firewalls) are introduced to enable access to this environment, with all the additional monitoring required for this approach.

Zero Trust will enable you to allow the securely verified user to set up a connection to these OT management stations. All other connections are no longer needed or allowed, resulting in far less time spent monitoring these sessions.

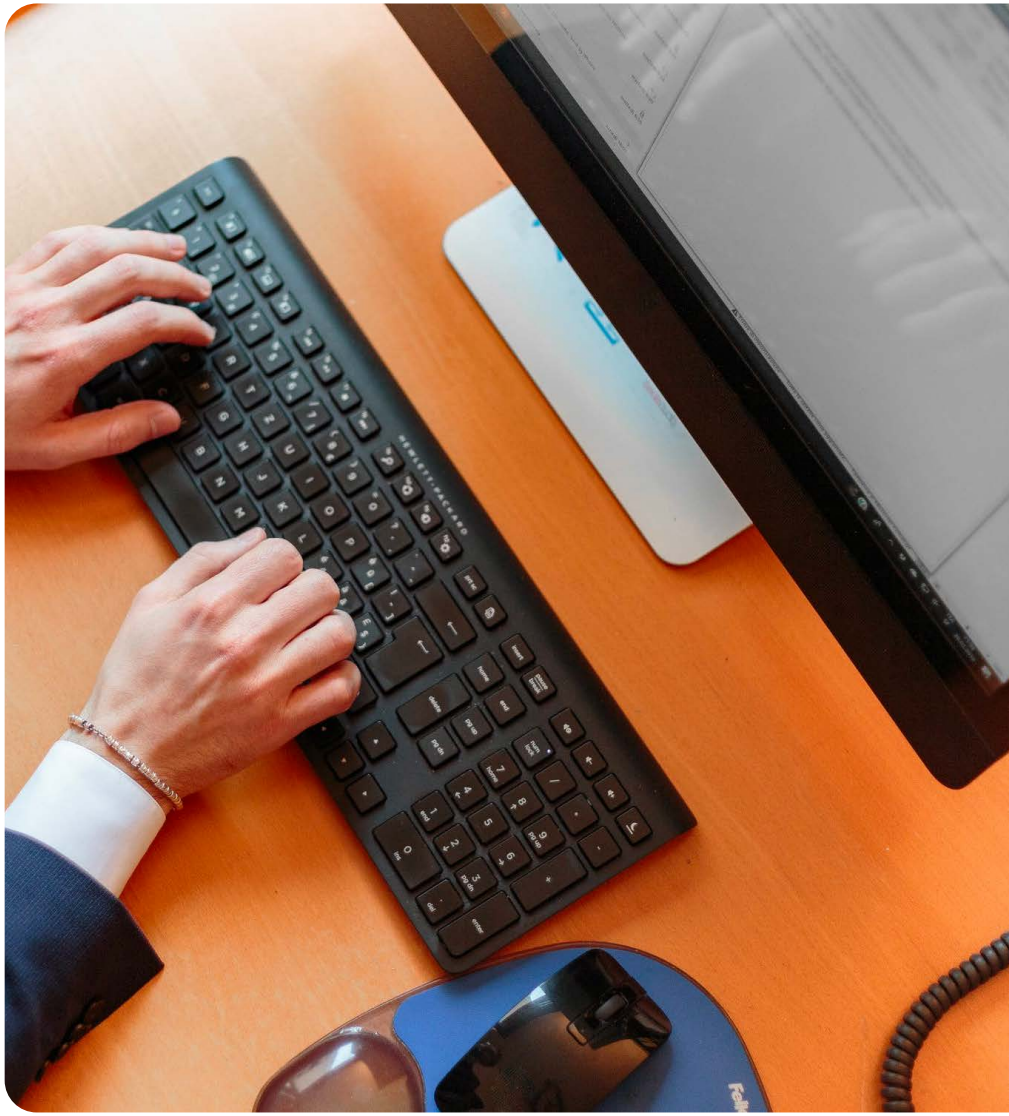
#05

Secure Traditional Windows Applications

Traditional applications may not be designed for external access. Such an application typically:

- Relies heavily on Microsoft Active Directory
- Might use proprietary communication methods
- Often requires a Windows machine to run the end-user-facing client software

These traditional applications are often business-critical, and there is no upgrade path to modern architecture. Using Zero Trust offers a path to access, without compromising security.



Introducing G/On:

A Non-Intrusive Approach to Zero Trust Adoption

G/On is a scalable, Zero Trust solution that connects all your users to internal and on-premise resources — regardless of device or location. Decrease your attack surface, enhance security and reduce complexity. Stop managing devices and empower IT to focus on business process innovation, not threat mitigation. It's simplicity without compromise.

There are three core pillars to G/On: software-defined perimeter (SDP), identity centric and non-intrusive. SDP network resources are made inaccessible by default and makes the application infrastructure invisible from the internet. Identity centric is based on the principle of least privilege access (need-to-know), reducing the attack surface while also increasing IT's visibility into user activity and applications. And non-intrusive ensures it promotes data protection and prevents access to personal data on devices.

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. 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. Whereas the G/On gateway will only present the allowed applications to the verified user with a per user dynamically generated menu.

03.

Zero Trust Security: **The Roadmap to Success**

Implementing Zero Trust Security can feel like it's going to be a large, challenging process — but it doesn't need to be. The answer lies in our roadmap to success, which outlines everything to look for when researching your options.

#01

Connect users to internal systems

What to Look for in a Solution

Bridge the gap between your IT resources and your human resources.

Empower remote workers and contractors to be more productive by safely freeing them from the complexities of VPNs and providing the same work environment everywhere. Experience improved user satisfaction, with no bandwidth or latency issues.

How Zero Trust Helps

With its Zero Trust access-centric approach, G/On protects all your access methods in one place, with more robust security policies and evaluation of user credentials and their context of access. You will know who is requesting access, from where and when – along with many other factors you can incorporate that reveal the user's proper current disposition.

G/On also provides critical segmentation of your most valuable assets. Instead of getting access to the entire network like many agencies allow today, users are only given access to the explicit resources they are authenticated to need to do their jobs, such as applications. They are effectively captive within those named resources, so even if in some cases hackers could compromise a user's credentials, they would also be captive inside only that application. This neutralises their ability to attack other resources within your environment.

#02

Enable business in a hybrid world

What to Look for in a Solution

Futureproof your infrastructure, as you transition to a hybrid world

Zero Trust Security can help your organisation rapidly drive digital transformation – for example, organisations used G/On to enable secure mobility during the pandemic with the mass global exodus of workers from offices to work from home.

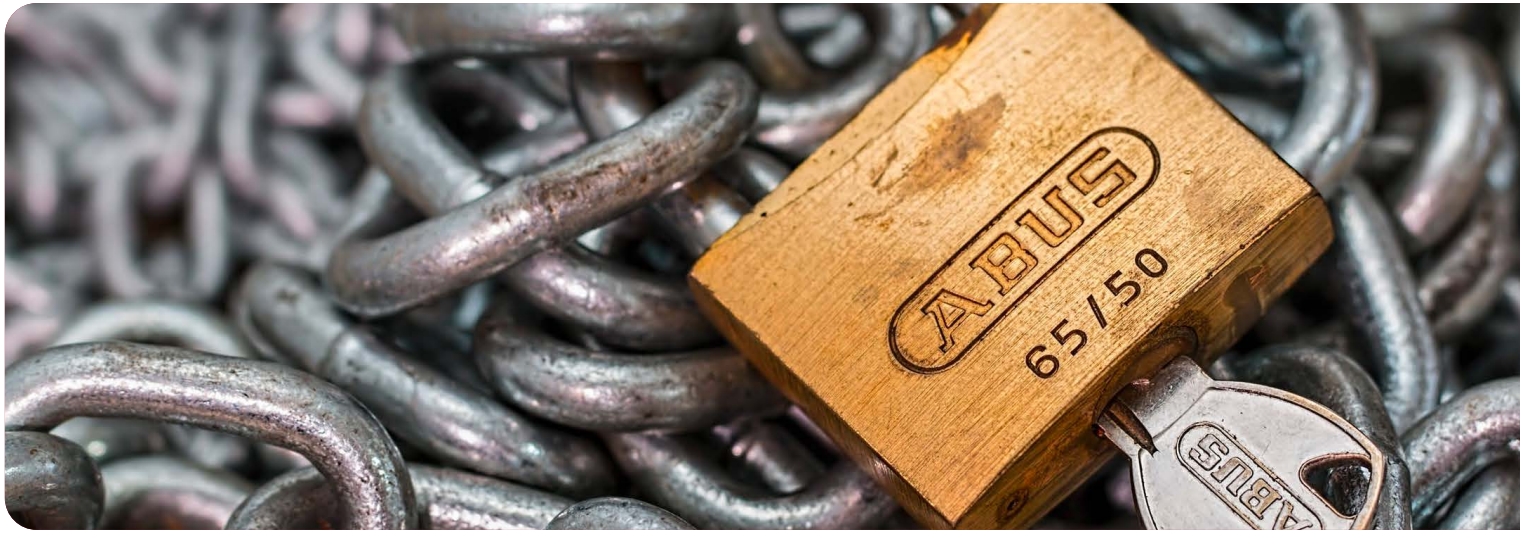
How Zero Trust Helps

Mitigate risk with Zero Trust secure remote access. Deliver continuous verification of user identity and trust to eliminate user credentials from the attack surface:

- Enable remote work productivity, by empowering employees with streamlined access, increased security and upgraded performance compared to traditional VPN technology.
- Enjoy scalability: The G/On architecture is designed upon high-performance load-balanced gateways, which can be deployed to share the load of multiple sessions. This will provide the flexibility to scale from 10 users to far beyond 10.000 users in a single setup.
- Utilise true mobility: Users carry everything they need on a single G/On USB key with a mobility smartcard inside. The client does not have to be installed, and the client can automatically find its way to the company network

#03

Proactive prevention



What to Look for in a Solution

Stop attacks from happening in the first place

Implement your Zero Trust strategy at your own pace without the need to rip-and-replace your current infrastructure.

How Zero Trust Helps

Data-focused Zero Trust solutions usually require a complex, hard-to-deploy, rip-and-replace approach. It can take years to implement — critical time lost, accompanied by escalating costs, while new threats continue to evolve and attack.

However, with an access-based approach, you rapidly accelerate your speed to Zero Trust, and transition from threat mitigation to innovation

That's because you don't have to re-architect your entire network and all your applications, and you don't have to install an entirely new layer of infrastructure to protect access to your data.

An access-based approach is designed to speed up the process – for instance, G/On, our Zero Trust solution, is implemented quickly without changing your existing infrastructure.

#04

Focus on innovation, not threat mitigation

What to Look for in a Solution

Empower IT to work for the company again

An access-based approach to Zero Trust propels innovation at great speeds across your enterprise, allowing you, your IT team and your employees to be more creative.

How Zero Trust Helps

An access-focused approach to Zero Trust can drive forward innovation across your enterprise, enabling you to work more securely, more effectively and more efficiently than ever before.

G/On, for example, enables you to close all the open ports that tempt hackers so much by removing them entirely from your firewalls. Remote access solutions – like VPNs, RDP, Citrix and others – no longer require open ports with potential vulnerabilities to the outside of your infrastructure when using G/On. That's a critical security consideration with the rapid rise in remote workers in today's work-from-home world and releases IT to focus on innovation.

#05

Enjoy simplicity without compromise

What to Look for in a Solution

Bring IT to users, without intrusion on your network or for your users

End users and administrators find this access-based approach to Zero Trust makes their lives easier as well.

How Zero Trust Helps

In today's hybrid world, G/On, for instance, unifies access control over all your corporate data, resources and applications, wherever they may be – local or cloud. It also allows you to define your robust security policies for each resource and provides a centralised view of overall access across your organisation.

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

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.

#06

Maintain privacy at all times

What to Look for in a Solution

Keep private and business data separate

As more privacy and data sovereignty laws are introduced, immediately meet those needs - No client installation, no intrusion on private devices and leaves no traces

How Zero Trust Helps

International businesses have to consider the local laws and regulations of the countries where they operate. Zero Trust solutions, where no data is stored on the device are less intrusive for users. There is a clear separation between what the company owns and what the individual owns and controls.

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.

Conclusion

Zero Trust Security protects the enterprise by enforcing granular controls over user access permissions, allowing only access to applications defined and within defined security policies.

Whether a user is trying to view, copy/paste, upload, or download, the company will have direct control, independent of the device the employee is using. Zero Trust policies control access permissions on a very granular level based on verified user context. This ability to connect users to applications but block access to specific features in real-time enables the flow of business while still protecting companies from potential data breaches.

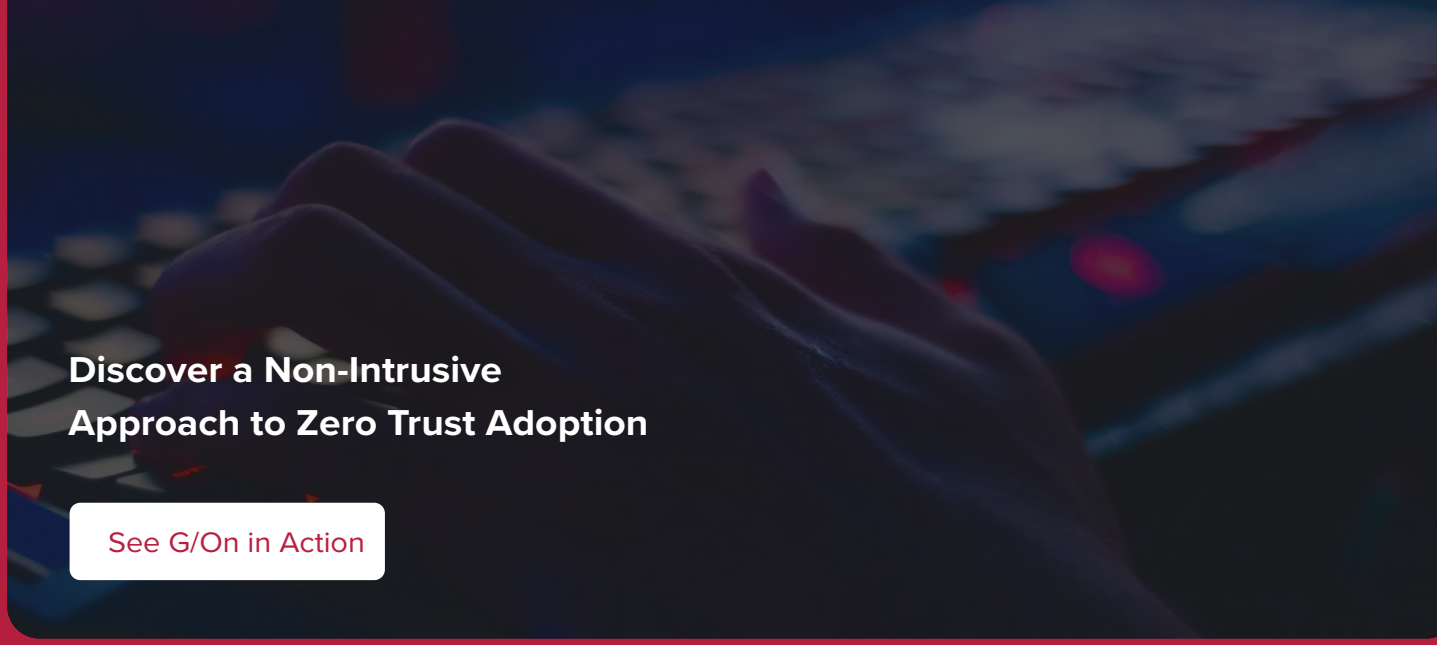
Unlike VPNs or network-centric Zero Trust access approaches, G/On can operate without agents on the endpoints, easily scales as traffic increases, and doesn't require reconfiguring your network. This is what enables fast deployment and simplicity to manage; and removes all barriers for BYOD/CYOD/COPE device strategy.

Implement Zero Trust Security with one solution, including:

- Certificate-based recognised users and apply the relevant policy.
- Segmented access — define which resources are accessible to which users, cloud or on-prem.
- Agentless user access, who instead connect to the application through G/On.

Give each user secure private access to internal apps while preventing intruders from spreading inside your network. Stop unknown threats from gaining access into your network from remote devices. Personalise access so each user can only get to the apps they need and connect your user to IT resources with Zero Trust Security.

G/On enables fast deployment of a Zero Trust Security framework in any type of infrastructure.



Discover a Non-Intrusive Approach to Zero Trust Adoption

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.

solitonsystems.com

emea@solitonsystems.com

+31 20 896 5841