Secure Remote Working with the Zero-Trust Approach

-A SOLITON WHITE PAPER-

YOU CAN'T MANAGE WHAT YOU CAN'T CONTROL

Ever since COVID-19, remote working went into overdrive. As it turns out, most employees can do their jobs while being away from the office, even though their employers thought they couldn't. This shift has also increased the usage of privately owned devices that are not managed by the IT department. This, in turn, has increased the demand for security tools that protect company data. These tools are urgently needed, as company data is now being exchanged between private mobile phones and laptops that are on unsafe Wi-Fi, logging in from unknown places at an unknown time of day.

Unfortunately, it's also in this search for tools that the confusion starts.

After all, when you Google "managing unmanaged devices", you find a wealth of information from experts discussing best practices. These articles are mainly centered around VPN, encryption and removing default configurations and passwords, but once you drill down on their advice, none of these really solve the issues of remote access. Often, they're confusing "Remote Access" with "Remote Network Access", especially when it comes to personal devices owned and used by remote workers. These devices shouldn't be the responsibility of the IT department, as you can't manage what you can't control.

To avoid risks that come with BYOD (Bring Your Own Device) policies, some companies choose to issue their workers with laptops for remote working – managed devices that the company controls. The remote network connection between these laptops and the company is often secured with a VPN. This may seem like a solid solution, but handing out managed devices to all employees is resource intensive, potentially quite expensive and still not necessarily safe. There's no virus scanner in the world that can fend off all sorts of viruses and malware, and the VPN, although widely used, can still be compromised.

It's time for a new approach

Clearly, we need a new approach to remote working, so that we can secure all possible ways of communication with the company network. In this approach, it should't matter where people are, which device they use and if they're Apple or Android fans. It should make remote working easy and secure, and help employees do their jobs without burdening IT managers with extra work. The good news is that this approach already exists. It's called the zero-trust model and can be implemented through different tools depending on your situation. Below, you'll learn how the zero-trust model works and which tools work best for you.

But first... what's wrong with VPN?

There's nothing wrong with VPN if you use it to connect two trusted environments, such as two branches of the same organisation. VPNs become a problem when you don't know what's going on at the other end of the line, which is the case with unmanaged devices. In this situation, think of your company network as your house. Then, think of VPNs as tunnels that connect the outside world to this house. Some tunnels lead to houses of co-workers, others lead to cafes where your manager likes to catch up on paperwork, and others lead to places you've never heard of. Now, wouldn't your house be safer if all your visitors came in through the front door where you could see and manage them? Probably yes. The same principle goes for your company network. Unmanaged devices can connect from anywhere by anyone, which makes it hard to verify who's entering your company network- no matter how you secure your VPN connection.

A VPN doesn't have embedded 2-factor authentication, neither does it manage the applications or data transfer. It also doesn't prevent malware or viruses coming onto the network. This makes VPN an entry point for hackers and susceptible to man-in-the-middle attacks. Apart from all that, VPN doesn't load balance without additional infrastructure, it's not easy to scale and takes time and resource to roll-out. It's a remote network connection that's made to gain continuous access to devices, which is a problem when this device isn't

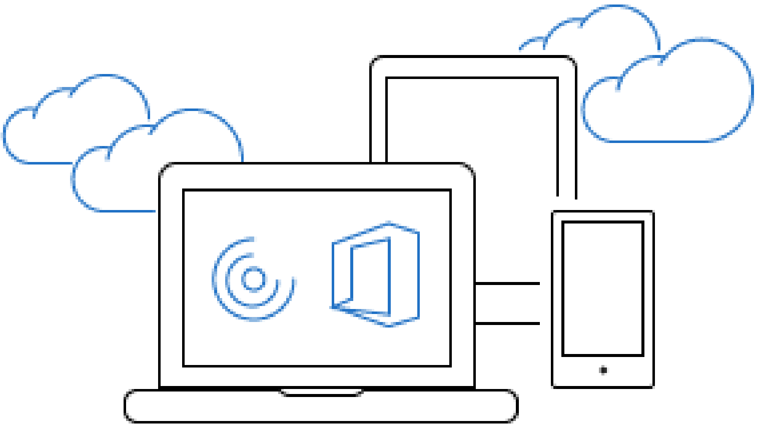
managed by the IT department. And last but not least: VPN can be replicated across many devices and is therefore vulnerable to fraud.

...Okay, you get it: when it comes to remote working, VPN simply isn't the best tool for the job.

An alternative to VPN is a secure gateway principle that's the opposite of a VPN and follows the strategy of "zero trust". In this zero-trust approach, nothing is allowed to connect, unless it can explicitly identify itself each time it does. Explicit identification means a stringent 2-way authentication procedure for both the remote device and for the network device to communicate back.

It's OK, we have Citrix or use RDP, we don't need VPN anyway

When you work with Citrix or Remote Desktop Protocols (RDP), you may think you've got everything covered. However, Citrix and RPD were never designed for remote working, which is why 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 and RPD with a security layer and an access strategy, however, it would be more efficient if one tool could be deployed to both secure remote access for general PC working and covered Citrix and RDP in a single overall zero-trust strategy.



What is “Zero-trust”?

Soliton uses a zero-trust approach for connectivity between remote devices and the company network, and vice versa. Unlike a VPN, which provides continuous network connectivity and then has rules put in place which explicitly denies things that aren’t allowed access, zero-trust conversely denies everything by default. It’s up to the users to prove they’re authorised to access specific resources, every time they log in. This makes a zero-trust approach user-orientated instead of device-oriented, as is the case with VPN. Because of this user-oriented approach, zero-trust tools are almost impossible to replicate. The user authentication is a very strong 2-factor authentication to strenuously prove the identity of the user. It will also not rely on third party trust to authenticate a user, making it extremely safe.

ZERO-TRUST SECURITY ACCESS SOLUTIONS FOR REMOTE WORKERS

At Soliton, we always put the zero-trust approach at the center of our solutions. Based on the user, we build a secure “Software Defined Parameter” around the company network, that not only stops unauthorised network access, but also protects data from being compromised within the company environment. Unlike with VPN, no information on the network is visible from the outside, so there’s no information out there that can be misused.

The foundations of our products address the vulnerabilities of conventional solutions and not only prevent hacking and malware, but also protect both personal and company data on unmanaged BYO personal devices from cross contamination. Below, we’ll introduce our three main security solutions.

G/On- for secured PCs and Macs

The G/On solution can be used on remote PCs and Macs. It allows encrypted communications between a remote application and an internal service without the need of creating a physical network connection, making it much safer than a VPN connection.

G/On supports 2-factor authentication and prevents man-in-the middle attacks. It communicates through the local host of the remote device, meaning the remote PC has no knowledge of the company network. This way, the company network is effectively out of reach, which eliminates risks altogether. With the additional option of using the G/ On Operating System through a USB stick, it's possible for data and applications to be "containerised" and separated from the PC operating system. As a result, viruses and malware cannot travel from the remote device to the company network.

G/On can be used for Windows and Mac, but also for Citrix and RDP environments. Individual point solutions are no longer required.

MailZen- for unmanaged mobile phones

Soliton's MailZen solution has a similar secure approach as G/On, but can be installed on smartphones and remote tablets. MailZen combines a broad set of business functions, provided in one single application. Company data, such as telephone numbers, contacts, calendars, files and photos, are securely stored inside that application, called the secure container. This makes it safe for remote workers to use these assets, no matter how well (or poorly) their device is secured. For example, Microsoft Exchange was never built to be used by remote workers. Security and protection were never an original part of its DNA, which makes it hugely vulnerable when connected to the internet. Also, information from the Exchange server is synchronised with the endpoint, making the application even more vulnerable. In contrast, MailZen uses a secure gateway to access Exchange to handle requests, so that Exchange is not directly connected to the internet. At the same time, MailZen encrypts and protects the information as it resides on the endpoint device. But Mailzen does more than simply protecting company assets- it can also be used to isolate company data from personal data. As a result, company assets are never "contaminated" with private assets, which avoids problems in the field of GDPR.

MailZen works for Microsoft Exchange, but also in the cloud with Office 365. Using MailZen for O365 gives you all the flexibility of O365 services, plus the peace of mind of a safe working environment.

3 SecureBrowser- for safe browsing

Speaking of the cloud: when you and your co-workers work with many cloud applications such as intranet, SharePoint, and other online tools, we recommend you look into our SecureBrowser solution. This solution prevents plug ins from getting installed, keeps cookies from following your co-workers and deletes all data when they go offline. Moreover, SecureBrowser creates one spot where all portals and log ins are assembled, giving you control over your browser instead of the other way around. SecureBrowser works for company PCs, but also for unmanaged devices such as privately owned phones, tablets and low-cost Chrome devices (if enabled for Android apps). Like G/On and MailZen, SecureBrowser doesn't work with VPN and doesn't have any other vulnerability that could possibly effect the company network or compromise data.

4 SecureDesktop- for remote access to office PCs and Macs

Soliton SecureDesktop is a desktop solution, providing employees with remote access to their internal office desktop. It securely connects an internal office PC or Mac to a remote device, without having to open up the firewall or make complex infrastructure changes. Both the remote device and the internal office device connect outbound to the SecureDesktop service, and the service connects the two together. Users and devices are strongly authenticated on both ends, using digital certificates to provide an added security layer.

The outbound connections mean it's unlikely that changes to the firewall are necessary, saving the IT department time and reducing implementation costs. As well, the office desktop computers can take any route to the internet that is available, which prevents a single point of congestion and improves performance.

The IT department can immediately upscale (or downscale) users, without having to modify the IT infrastructure, and users can simply download the application to their home device to access an office PC.

The streaming technology used in SecureDesktop compresses and transfers the information on the PC screen for remote operation and ensures a stable connection — even with low bandwidth internet lines.

DON'T LOOK FOR THE ULTIMATE SOLUTION- DO THE MATH!

As you can see, there's no one-size-fits all that will make all your security problems go away. This is because, in IT security, there's no such thing. The ultimate solution is the combination of the zero-trust mindset and a set of tools that match your budget, scope and technology you already have in place. So, if you ever come across a company that claims they can solve all your problems with one single tool: run! Instead, ask yourself to which risks you're exposed by doing the math:

Your risk = the chance of anything happening to your network x the damage it will cost you.

Based on your answer and your budget, you can decide which tools you need to optimally secure your company assets, your data and your people. Need some help figuring it out? Contact us through the Soliton website and have a local representative get in touch!

ABOUT SOLITON

Soliton Systems specialises in IT Security and Ultra-Low Latency Video Streaming, and is headquartered in Tokyo, Japan. Our current CEO and founder, Nobuo Kamata, PhD has been a technology-oriented leader and pioneer since 1979. Soliton has a strong vision to innovate solutions to logically satisfy the needs of our customers, without adding complexity. Soliton Systems has continuously set new standards in performance, quality and reliability in our areas of expertise: Cyber Security, Mobile Live Broadcasting and Public Safety. For more info, visit www.solitonsystems.com.

Secure Remote Working with the Zero-Trust Approach

Disclaimer: All information herein was carefully gathered and examined, however, Soliton Systems cannot be held responsible for mistakes or incompleteness of content. Soliton Systems may change or modify parts at any time without notification and accepts no liability for the consequences of activities undertaken based on the contents.

Soliton®

EMEA office

Soliton Systems Europe N.V.
Barbara Strozzilaan 364, 1083 HN Amsterdam, The Netherlands
+31 (0)20 896 5841 | emea@solitonsystems.com | www.solitonsystems.com