Unmanaged Devices

Use Case
Third party users & non-employee identities

In the age of a highly digital connected economy, organisations are adapting to a more dispersed and remote workforce to stay competitive and continue growth. As technology advances, remote work is becoming more common in many industries. Providing secure remote access to enterprise resources has become an important requirement for the outsourced nature of modern work.

Defining the remote workforce

A remote worker is anyone an organisation employs but works outside of a traditional office environment. Typically, there are two types of remote workers: employees and third party/non-employee identities like a business partner, contractor, vendor or temp worker.

Employees can also come in many forms, those who work in the office and those who work remotely. Either way, both groups require access to corporate IT systems and data from anywhere, anytime.

The challenges and risks

Business productivity goes hand in hand with including external professionals in the work processes. It means giving access to critical business applications, which is risky but necessary.

The challenge is enabling secure remote access to an internal network or private clouds and balancing security and usability. To ensure attackers cannot gain access through external connections and keep malware off the network while providing a seamless user experience.

Remote access, specifically third-party access, is a proven weak link in network security. The typical problems are inadequate or default passwords, re-use and sharing passwords by contractors, poor or no network segmentation, not knowing which resources get accessed by who, when, and from which device. Devices might be unmanaged and might be compromised or infected.

Traditional remote access VPNs and even RDPs are used to establish the connection to the network but come with multiple security weaknesses, making VPN unsuitable for remote workers, specifically third party users who want to access the network and applications. They are insecure, slow, hard to deploy, and do not meet usability, security and compliance needs.

Software Defined Perimeter – Secure Resource Access

There is no question that traditional solutions, such as remote access VPNs and RDP, have too many security weaknesses to concur with the ever-evolving cyber threat landscape. Especially when these solutions are used to establish access to external workers, third party or non-employee identities.

Software-Defined Perimeter (SDP) solutions are proven to provide secure access for third parties and non-employee identities without introducing friction or complexity. SDP is a Zero Trust solution and provides granular network and application access and only permits access to specific applications on a need-to-know basis. Authorised users only gain access to the resources they need without connecting them to the network. This approach eliminates the need for remote access VPNs and RDPs and reduces the attack vector without interruption or increased burden for the user.

Common security vulnerabilities of VPNs:

Credential Theft

This is the most common security breach. It occurs when malicious actors steal account information (user credentials) to gain access to critical data and processes. User credentials are also hacked through brute force attacks, a trial-and-error method used by application programs to decode login information and encryption keys.

Unmanaged Devices

External users often use their own and thus untrusted devices to gain access to a company network.

VPN remote access has no security features detecting compromised devices or has any malware on the device allowing malicious software into the broader network.

Excessive Access

VPN often provides excessive access to network resources, including routers and switches, increasing the attack surface. Also, authenticated and trusted users can access resources that should be limited.

Exposed Servers

When a VPN connection is established, internal application servers are exposed to the external device, including whatever software and malware are running on it, making it an attractive attack vector for an attacker.

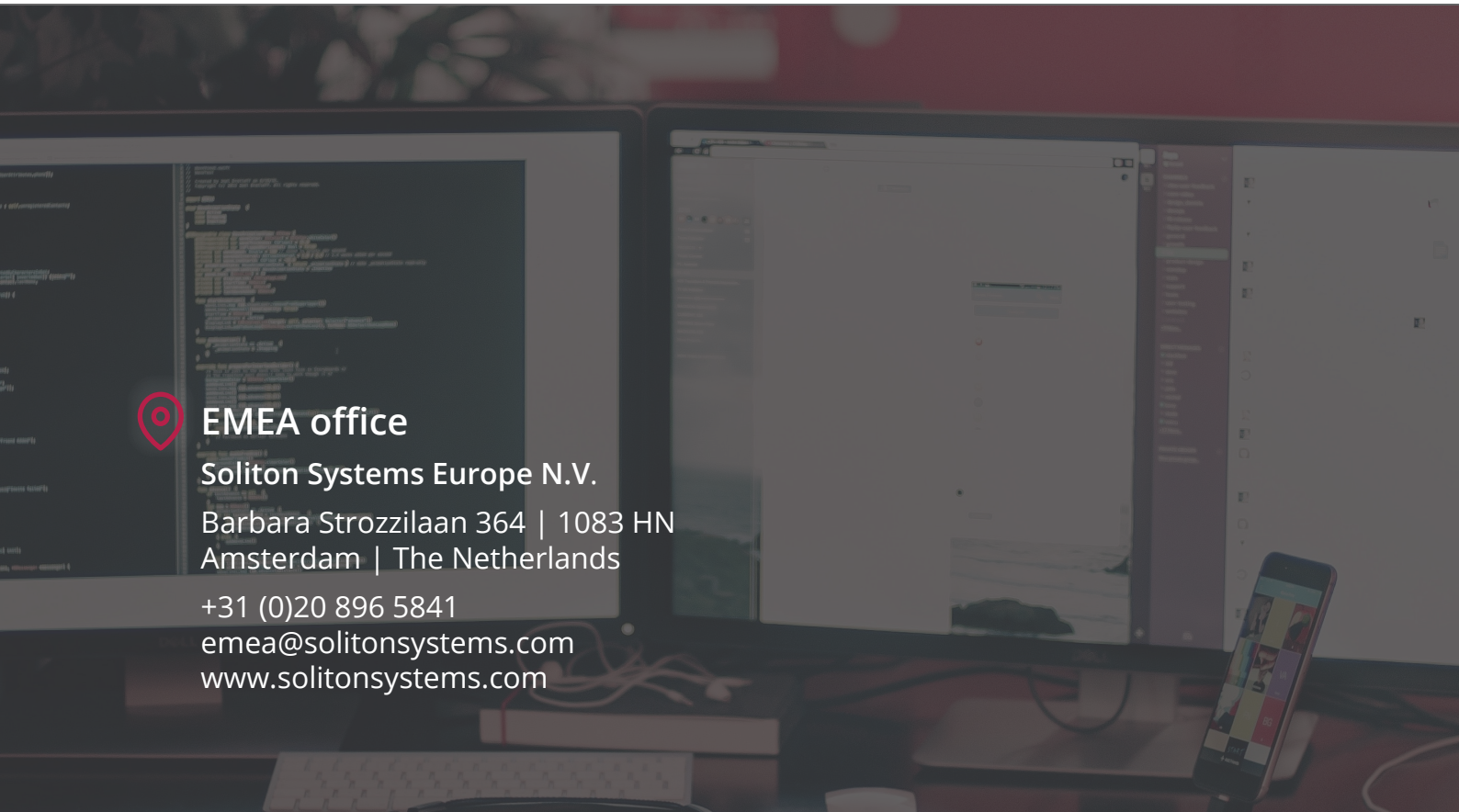
Expose Network

Vulnerabilities in VPN products can expose the entire network to cybercriminals.

SPD enabler for simple, trusted and secure application access

More and more organisations are opting for a hybrid infrastructure where on-premises data centres combine private and public clouds. A hybrid infrastructure contributes to optimised IT spending while lowering operational costs by using a secure public cloud for non-mission critical parts of the business. The downside, it also complicates access requirements when it's crucial to enable accessibility while preventing unauthorised access to applications and data.

To reduce risk, organisations are embracing the Zero Trust approach. Zero Trust security trusts nothing by default unless it can explicitly identify who it is each time it connects. Deployed as a component in a Zero Trust strategy, SDP verifies the identity of the requesting device and authorises the user, provides granular control and enhanced segmentation no matter where the applications and resources reside. All these elements will uplift the need for SDP security.



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