Unmanaged Devices

Use Case Remote Employees

How it all changed: From telework to remote work

Employees connecting remotely to a corporate network is not new; we just used to call it 'Telework'. Before the pandemic, telework was often an optional benefit, mostly in ICT- and knowledge-intensive sectors. The trend emerged to move non-critical business applications to different cloud infrastructures - for instance: O365, HubSpot, Salesforce, and likes are no longer office-based applications.

As a result, organisations started working on security protocols that included both on-premises and remote work.

The pandemic outbreak caused an abrupt closure of many offices and workplaces, bringing a new era of remote work for millions of employees. It requires IT leaders to rethink their security perimeters protecting the corporate IT systems and data while considering a distributed office and workforce are here to stay.

The pandemic placed the bulk of the workforce at home

Organisations had to move abruptly to remote work at the start of the COVID-19 pandemic, forcing them to tackle sudden, potentially significant operational and organisational challenges overnight rapidly. Many organisations transitioned to remote work quickly without compromising security.

However, others had no choice but to emphasise “connectivity first” in their initial response, taking shortcuts to expand remote connectivity. Not surprisingly, that abrupt turnaround had some negative consequences for organisations, too. There is a possibility that many employees’ access is still unknown to IT departments and could present a huge data security risk.

Now is the time to assess security and control gaps to stop cybercriminals eager to take advantage.

Ask yourself a basic question: ‘Which assets do my remote user need to access?

Providing remote access requires organisations to expose service from their premises and allow internet access. Telling critical services on the internet makes them vulnerable and much-wanted targets for cybercriminals.

Traditional VPN-based remote access solutions, on the other hand, are inadequate and have a large security risk. They are insecure, slow, hard to deploy and do not meet the usability, security, and compliance needs.

The right approach to secure remote access is based on a framework of user and device trust with a security posture to authorise access continuously - a software-defined perimeter (SDP). Users only gain access to the network resources mandatory to perform their daily task prevents broad network access but ensures users are not placed on the network unless required.

SDP is the new security protocol for remote workers

SDP is a security framework designed to micro-segment network access. In other words: SDP mediates the connection between users and internal applications without placing the users on the network.

SDP is completely designed around three pillars, the user's identity and its authorisation level, Zero Trust and non-intrusive. Zero trust applies the principle of least privilege to the network (need-to-know), reducing the attack surface and 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.

With a Software Defined Perimeter, network resources are made inaccessible by default. An authenticated user can only access one or more specific services inside the network when explicitly authorised, rather than receiving broad network access when using a VPN. Therefore, a software-defined Perimeter isolates the company services from the internet, stopping almost all forms of network attacks.

SDP is a vast component in a Zero Trust strategy

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. SDP can connect users to applications but block access to specific features in real-time, enabling business flow while still protecting companies from potential data breaches.

SDP provides each user, whether a remote worker, 3rd party user or an internal employee, secure and personalised private access to internal apps while preventing intruders from spreading inside the network and unknown threats from gaining entry into the network from remote devices.

SDP removes the complexity and associated costs of traditional remote access solutions such as VPN and RDP. It has proven the best defence for security professionals as it 'blacks out' the network, making it impossible for malicious attackers to enter the network.

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