Network Access Control

Use Case

Third-Party Access

Organisations often forget about third-party user access security control

Organisations want to protect their networks, but they often forget about third-party user access security controls. These security measures can protect third-party user access to privileged credentials and strengthen security aspects that malicious attackers typically exploit to gain access to corporate networks.

Privileged access demands more protection than employee access

Third-party accounts provide an easy avenue for unrestricted access into corporate networks. These third parties often service multiple customers, and their ability to access these resources poses an additional risk. Instead of going after one large company's data, attackers prefer to go after an organisation that works with third-party users to access more critical data. This method has proven very effective for hackers; research shows that approximately 50% of organisations have experienced a data breach caused by a 3rd party.

Controlling who, when, how, what, and for what time-frame third-party users can access is an absolute must to ensure secure business operations. It's critical to minimise the attack surface area and have complete control over every connection, tight credential management, and audit for all user activity.

Who are these Third-Party users?

Many organisations work with third parties providing specialised and often more cost-effective services. These third-party users can be a diverse population, including outsourced IT, temp workers, interns, contractors, suppliers, resellers, etc. Most of the time, third-party users work offsite and require remote access to internally hosted resources such as applications, data, and services to deliver what they are hired to do.

Third-party access challenges security

Providing access to external and internal accounts can be very challenging, and too much access can lead to an increased risk for data leakage or attack. Too little access could result in 3rd-party users being unable to complete their job, as it requires access to specific internal assets.

Even the duration a third-party user account is granted access is usually not properly defined, resulting in forgotten and even privileged accounts being available in the security perimeter of authentication.

Many organisations still rely on dominating legacy solutions such as VPNs to secure third-party access, which are not designed to manage privileged access requirements like role-based access. On the visibility front, organisations have limited visibility over what third parties do on their network once they authenticate.

NAC: extend control to third-party devices through digital certificates

While NAC is thought of as a security technology that either allows or denies access to the network, it has major advantages in securing networks.

The most important feature is that NAC can provide certificate-based network authentication using digital certificates through its PKI (Public Key Infrastructure).

There is no stronger authentication than the digital identity provided by PKI to control and secure access to companies' networks. PKI certificates safeguard confidential data from the eyes of unauthorised parties and against vulnerabilities that put businesses at risk. NAC validates a user or device's certificate when it attempts to join the network. If the certificate is invalid, the device can be handled appropriately, such as by a remote or limited VLAN with no access to corporate resources. With certificate-based authentication, a business can verify that all devices connected to its network are authorised.

NAC solutions can deliver network access on a granular basis providing access only to areas of the network required for the owner of a device to perform their job even for a specific period. It can centrally adopt Active Directory (AD) group membership and network share permissions in (large) networks allowing greater control and flexibility for delivering access to shared folders. NAC supports logically defined network segments by grouping resources and limiting access to a specific group of users and/or devices while blocking non-authorised access. If a device is compromised, its ability to travel in the network and attack other resources will be limited.

Securing third party user access quickly rising in the ranks to become a top priority

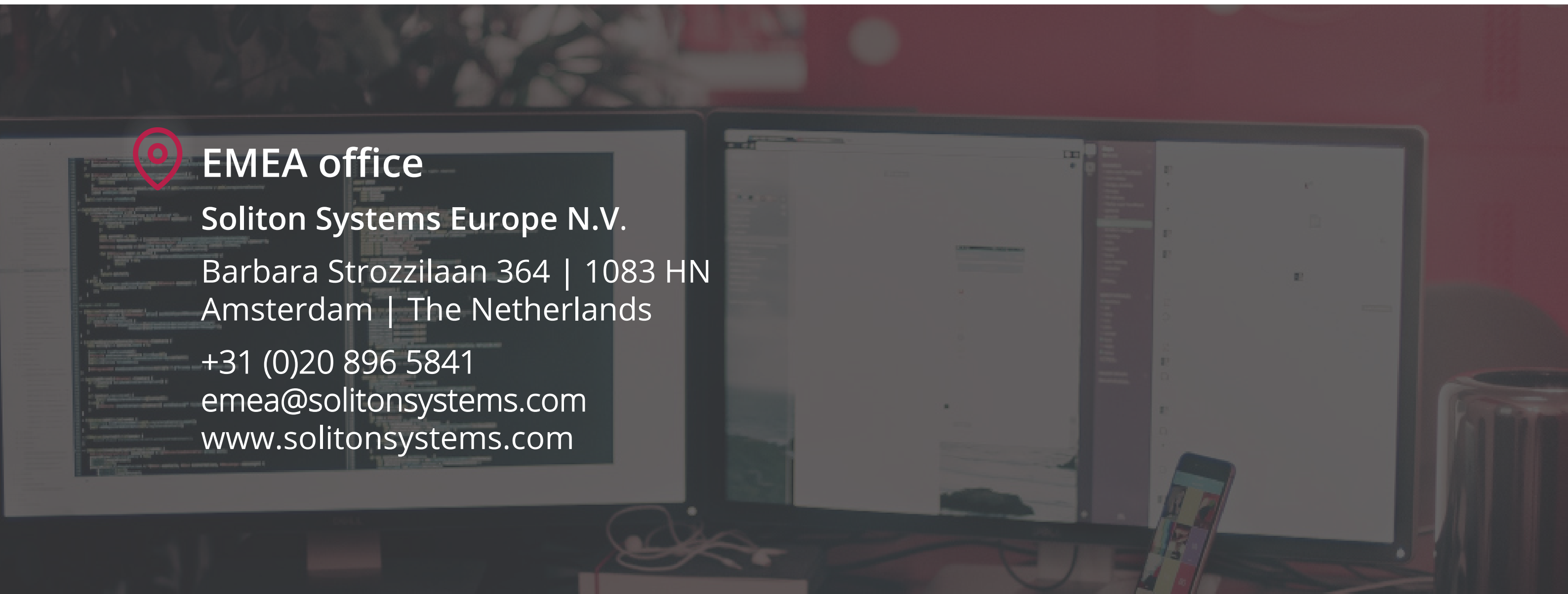
Businesses are increasingly outsourcing internal functions and operations and external services. Third-party users access needs to be managed separately and without clients. Managing their access to sensitive data at scale is a nearly impossible task, exposing companies to potential security risks.

Whether they are obtained maliciously or leveraged inappropriately by a valid user, exploited third-party user accounts are a common thread in many data breaches. These attacks and resulting data breaches can be incredibly costly for organizations, both in terms of reputation and financial losses.

NAC can drastically improve an organization's network security posture by allowing for greater control over what devices are accessing the network, and what they are granted access to.

NAC supports in defining what resources are available to a user and enforce these policies, limiting an individual to just those systems. Once third-party users (or any other user) are granted access to the network, NAC regulates the areas of the network users can access while monitoring and logging their activity.

The use of digital certificates with a NAC solution reduces the risk of an intentional or accidental breach drastically. The wonderful thing about using digital certificates for authentication (as opposed to usernames and passwords) is that you can issue them to devices that your company does not manage. Solutions like NetAttest EPS use digital certificates to make this process faster, simpler, and most secure.



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