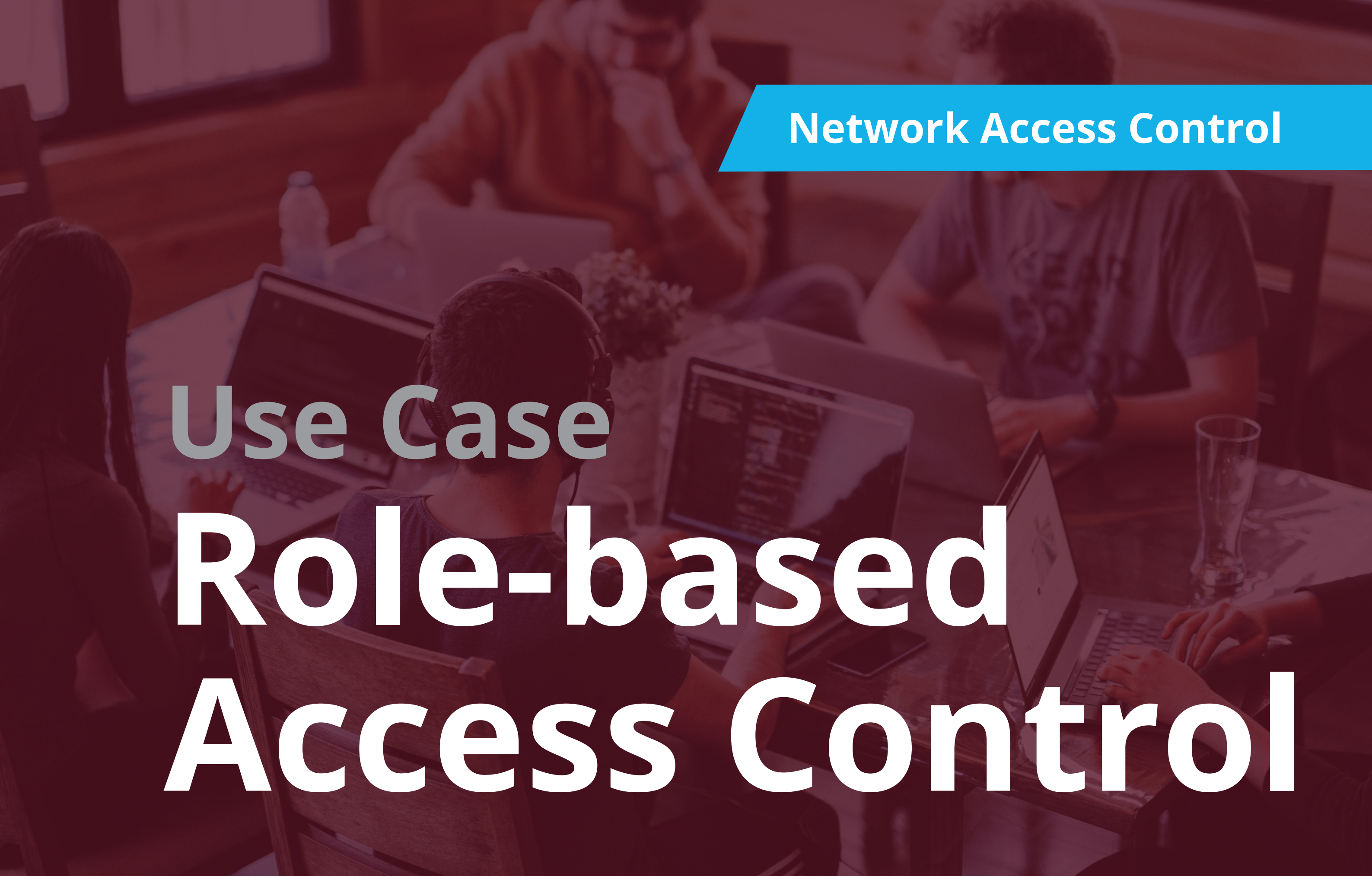


Network Access Control

Use Case

Role-based Access Control

Use job functions (roles) performed by individual users to determine their appropriate access levels

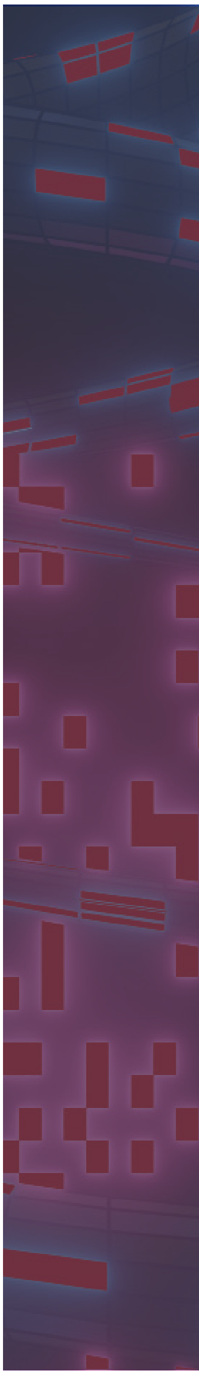
One of the biggest challenges IT managers face today is enabling and managing secure access. The growing number of devices interacting with company networks and users accessing this network from inside and outside makes it increasingly difficult to control what’s happening.

Many organisations - often larger organisations - use job functions (roles) performed by individual users to determine their appropriate access levels. A role can be seen as a collection of permissions, and users receive approvals through their assigned roles.

Role-based access control (RABC)

This approach or security method is known as role-based access control or role-based security. Role-based access control assigns specific rules or policies to individual users or groups of users connecting to a company network. It is a strategy of limiting access to networks aligned to the roles of individual users.

There are many benefits to role-based access controls, including:



Minimise data breach risk

Following the principle of least privilege, users are provided with only enough access for that individual to perform his job. It helps reduce the risk of cyber threats and abuse by malicious insiders and limits the damage from an attacker who has compromised user credentials. It reduces third-party risk by giving external users such as vendors and business partners strictly defined roles and permissions for fulfilling their responsibilities.

Demonstrate and enforce compliance

It helps organisations meet compliance regulations enforced by regional and local government and industry bodies and provides reporting capabilities.

Improved operational productivity and efficiency

It accelerates the onboarding, by automatically assigning access to new employees based on HR attributes. It also reduces the workload for IT support personnel, as they no longer need to manually manage the access permissions.

The value of NAC

The (personal) devices of employees, contractors and visitors connecting to a company network need to be securely enabled to perform their tasks. These tasks are related to their role within the organisation.

Network Access Control (NAC) controls who and what is accessing the network. Instead of setting up guidelines for every user - a very burdensome task - users are grouped based on their job roles and build access policies that way. Another important aspect of NAC is the possibility to apply the Principle of Least Privilege, instructing IT admin teams only to provide users access with the access levels required to fulfil their tasks.

NAC also enables network segmentation - one of the best ways to secure entry points. A device or user should only have access to the parts of the network it needs to function. Today, the most common approach for performing network segmentation is through NAC. Network segmentation is an architectural approach that divides a network into smaller segments, each acting as an independent network. As an important part of a Zero Trust, NAC solutions can identify and categorise every device accessing the network and enable IT admins to control network onboarding and access to network resources and the devices connected to it, even unknown devices.

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