Network Access Control

Use Case
Bring Your Own Device

The rise of BYOD and unmanaged devices is a critical focus for IT today for one reason: Security

67% of employees already use personal devices at work, and hybrid working means this number will only increase. BYOD refers to companies allowing employees to use their personal devices, such as smartphones, tablets, and laptops, to connect to the corporate networks and access the resources and critical data for work purposes.

BYOD provides many benefits: employees are more productive, workplaces are more flexible, and organisations gain substantial cost reductions per employee. However, it also introduces unique security risks and challenges to the organisation.

Organisations need to re-evaluate their existing policies to cater for this trend and keep up with an ever-evolving digital environment.

The new challenges and risk that come with BYOD

BYOD adoption carry certain risks and while corporate-owned devices can be closely monitored, a lack of insight into the health of BYOD creates a significant risk.

Mixing Personal and Business Use

Employees will inevitably perform both work and personal tasks on their personal devices.

Your organisation can't control the websites visited by employees or their access to sensitive data on public wireless or unsecured home networks — the list of potential threats is endless.

Device Infection

Smartphones are commonly infected by malware, and in most cases, smart-phone users are not aware their phone is infected. Another threat is that users often install questionable applications.

Unprotected (public) Wi-Fi networks

Wi-Fi is an excellent tool enabling users to access networks as guests or BYOD users with their personal devices. However, failure to properly secure that network can breach your defences, and data can be compromised.

Compliance and certifications

Privacy and data sovereignty laws introduced common frameworks to manage and monitor compliance for a range of IT regulations and standards.

Data Leakage and Loss

When employees use personal devices at work, any access to the corporate network poses a risk. Attackers can access a device via phishing or malware to:

- Steal data stored locally on the device
- Use credentials stored on the device to access the corporate network
- Destroy data on the device

What to look for in a NAC solution today and for the future?

IT security professionals are already stretched thin in most organisations today. NAC should off-load tasks from IT and Help-Desk to increase their productivity while maintaining secure network environments with easy control and management for IT.

The optimum NAC solution supports:

Stand-alone all-in-one solution

Includes everything you need in a NAC solution, including the necessary Public Key Infrastructure and Certificate Authority for creating certificates and a RADIUS server for enforcing access policies.

Agentless

Secure NAC for any device, employee, contractor or guest, across any multi-vendor wired, wireless and VPN infrastructure. Avoid complex life cycle management due to software updates and agents with security holes.

Automated Features

Wizard guided and automated features for easy control and management for IT, including task-driven menu builder for optimised operation dashboard.

Flexible

Suitable for businesses of all sizes, flexible deployment with high availability. 100% vendor agnostic and easily integrates with 3rd party products.

Unified deployment

Unified deployment process to distribute and install digital certificates on any device regardless of device or operating systems.

Cost-effective

Low implementation cost and low operating costs.

How NAC enables secure BYOD

Organisations have embraced BYOD initiatives like never before. Remote working and the proliferation of different personal device types, including IoT, have instigated widespread change.

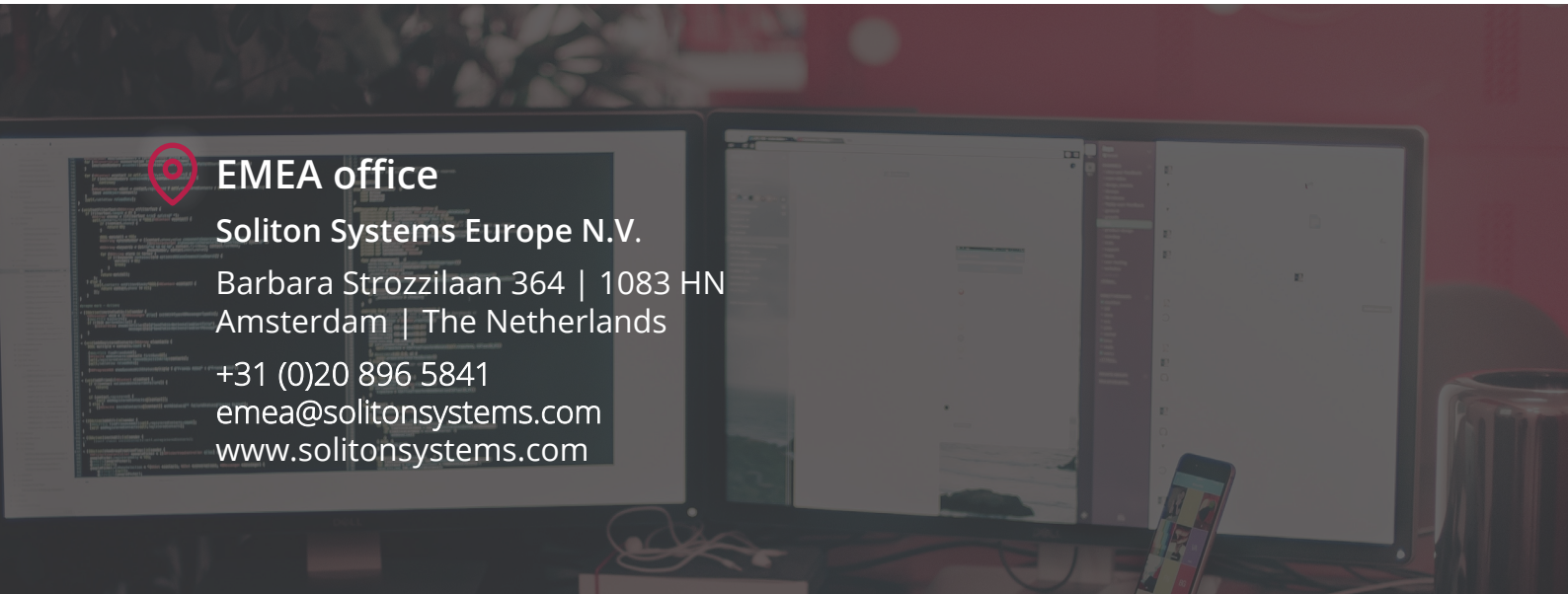
Network Access Control (NAC) provides control to the IT department, ensuring only authenticated users/devices can access the private company network. NAC enforces policies to regulate the network users can access areas while continuously monitoring and logging their activity.

NAC solutions automatically detect devices as they connect from inside or outside to the network and verify they are not compromising the security in place. As an important part of a Zero Trust, NAC enables IT admins to control network onboarding, access to network resources, and the devices connected to it - even those we don't know.

BYOD is here to stay

Employees will use their own devices - it's unavoidable. Organisations only have one option: be stringent in securing critical data and networks, without hampering the ease of access.

BYOD forces organisations to reconsider the existing security policies while creating flexibility for employees to be productive and engaged. As long as there are strong policies and strict implementation, organisations can reap great benefits from BYOD.



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