Network Access Control

Use Case
Shortage of Cybersecurity Professionals

Confronting the lack of cybersecurity professionals

Organisations face an unprecedented challenge: finding enough skilled cyber security professionals to answer the growing needs of businesses, which are 24/7 facing an ever-growing threat of increasingly sophisticated cyberattacks. Even when companies can find potential workers, they may not bring the appropriate experience or skills.

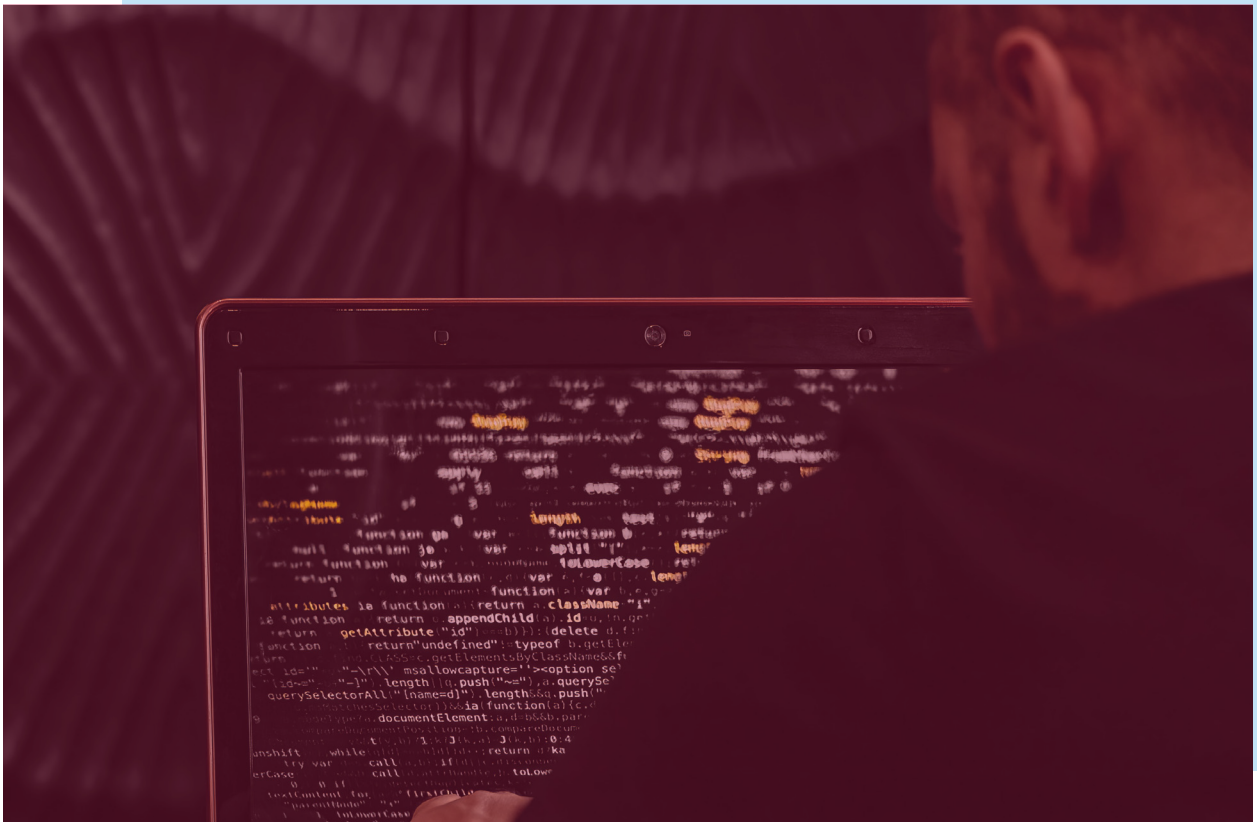
Now that cybercrime has become more prominent, authorities respond by creating cybersecurity regulations and standards. The challenge is that rules may differ per region, plus specific industries may even have particular regulations. This uneven regulatory landscape can make it difficult to understand the requirements and adapt.

Why organisations need cyber security specialists

Employees store vast data on computers and other internet-connected devices, including critical information like passwords or financial data. Cyber security is the practice of securing data, applications, systems, networks and devices from digital attacks or data leakage.

The role of a cyber security professional is not easy. They need to stay up to date on new trends, understand the data protection and privacy regulations and cope with increased workloads.

As businesses adopt more connected technologies, network attack surfaces grow. Growing IoT adoption has made organisations more agile and transparent. But it also creates more cybersecurity vulnerabilities. Cybersecurity professionals now need to manage more entry points, which can be challenging, particularly as it involves unknown (unmanaged) devices.



How NAC unburdens IT

Increasing reliance on an interconnected ecosystem of online devices in today's business environment greatly increases the dependence on network security to prevent cyber attacks. Suddenly every user became an endpoint requiring access to a company network.

NAC unburdens IT, increases productivity and maintains secure network environments with easy control and management for IT:

Network segmentation

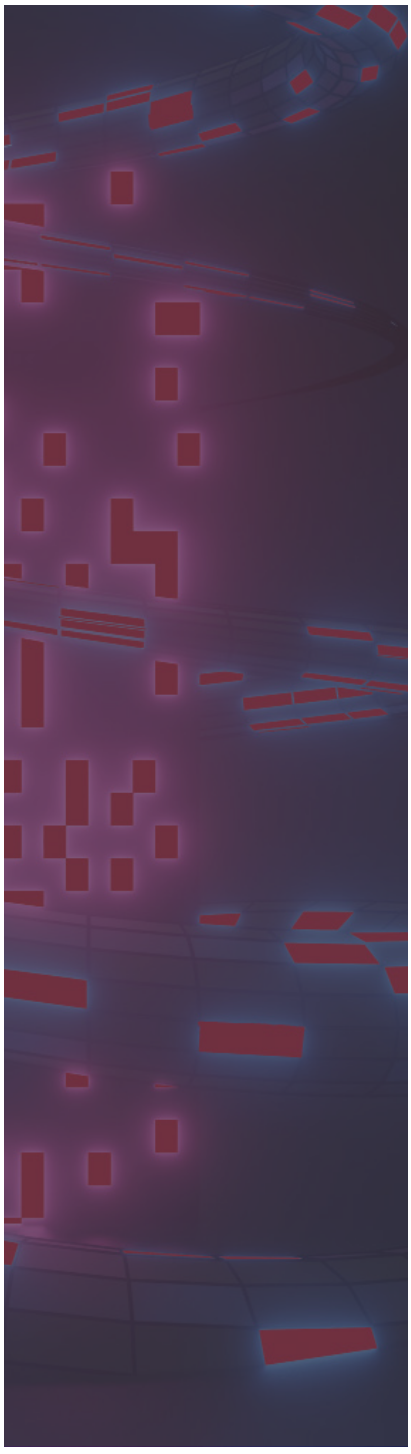
One of the best ways to secure entry points is network segmentation. A device or user should only have access to the parts of the network it needs to function. Today, the most common approach for performing network segmentation is done through NAC. Network segmentation is an architectural approach that divides a network into smaller segments, each acting as an independent network.

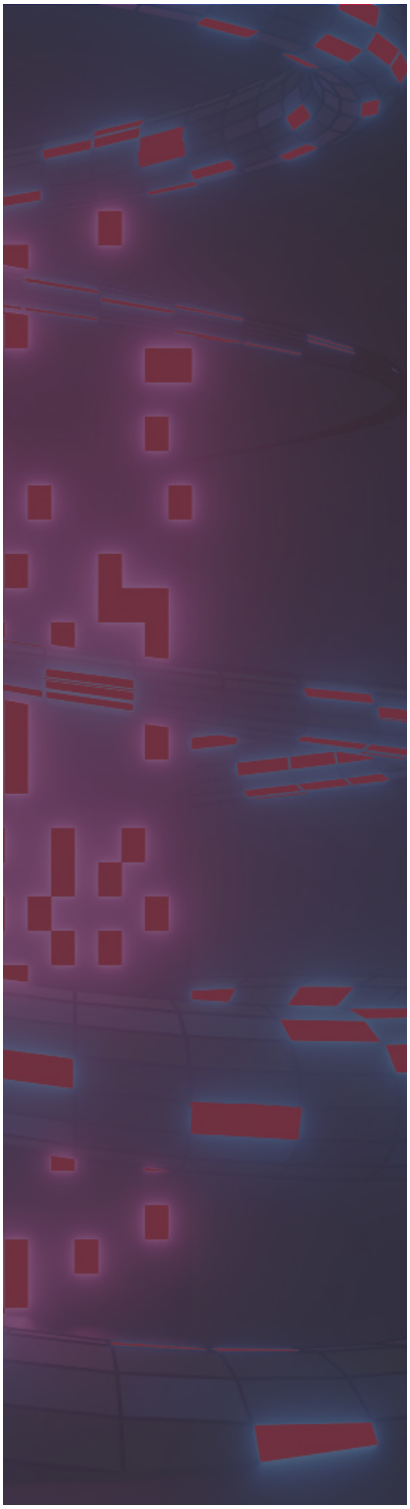
Zero Trust

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.

Automation

NAC support IT admins to automatically assess and verify devices and users' security policies requirements. NAC can handle numerous endpoint devices trying to connect to the network, allowing for faster processing times. NAC allows for enforcing policies to regulate the areas of the network users can access while continuously monitoring and logging their activity.





Self-registration

NAC often supports user-self onboarding, allowing users self-registration for each of their devices to perform their task.

Centralised Control Access

There is no longer a need to monitor and authenticate endpoint users and device types from multiple points of contact. NAC provides a single and centralised security management system that supports IT in monitoring and granting network access to individual and guest users (i.e. temps, third-party users, vendors).

Ease of control

NAC gives an organisation an edge to determine what device or user can access their network. By regulating devices and users access to the parts of the network it needs to function, network resources are effectively protected from infiltration by unauthorised persons.

Comply with regulatory requirements

NAC helps businesses comply with government and industry-specific regulations about information security.

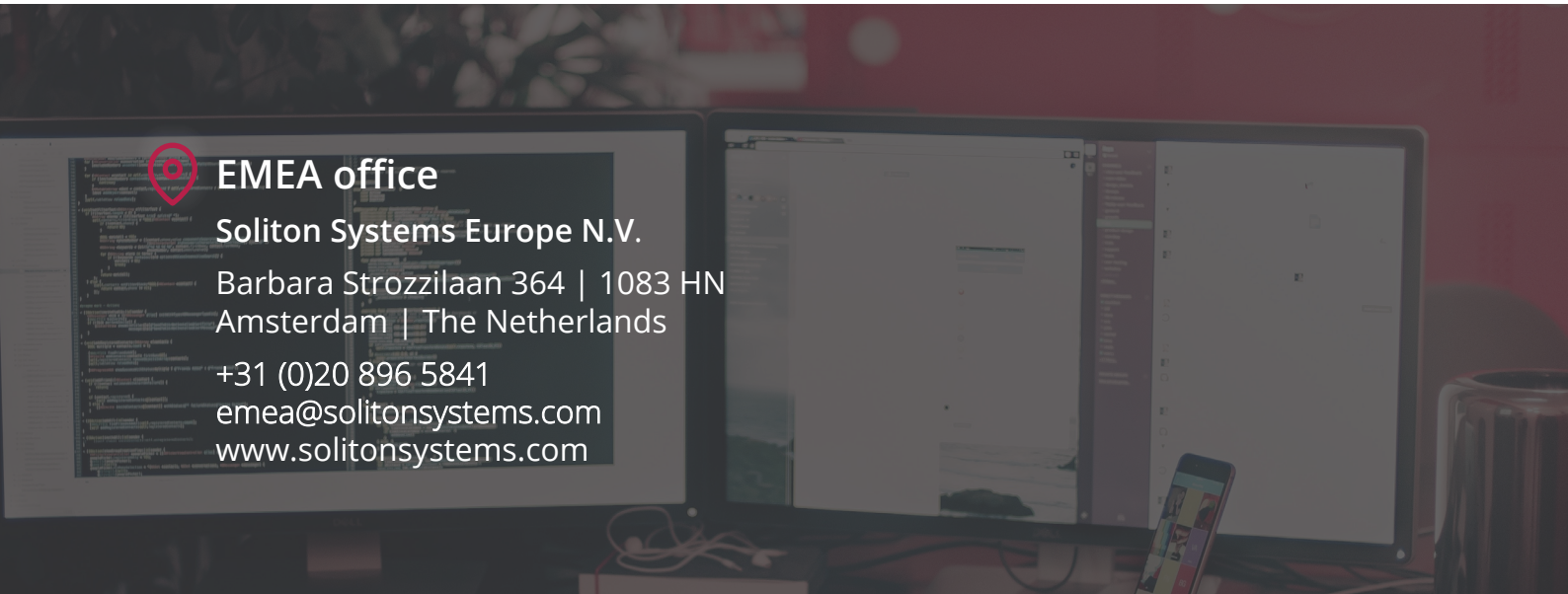
NAC continuously supports IT

Cybersecurity is dynamic. New challenges always emerge, and professionals need to stay on top of these changes to stay secure. And as organisations grow, more endpoints will get on the network, naturally creating greater exposure to security breaches. NAC hinders any negative effect this might pose on an organisation.

NAC supports regulatory certifications and security best practices and provides a clear view of network assets and activity. NAC offloads IT professionals with automated processes with pre-set rules for device policy, user access, and more to establish and maintain secure network infrastructure.

Unfortunately, NAC is still perceived as difficult and expensive. Arguments for not considering NAC include the lack of standards and concerns about vendor lock-in. There are also misconceptions about NAC implementations taking months; and concerns that it requires software agents to be loaded on client devices, which takes staff time and introduce high indirect costs due to downtime.

NAC is not a complete security solution, but it is important for network security. Soliton developed its NAC solution that it does not require long implementation. It isn't expensive or burdensome to manage, making NAC available and affordable for all businesses. Soliton's NAC solution follows a standard, eliminating vendor lock-in. It also doesn't use agents, which unburdens IT with simplified installation and improved security as agents are vulnerable to hacking. Simplifying implementation and management also result in fewer highly skilled IT personnel requirements.



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