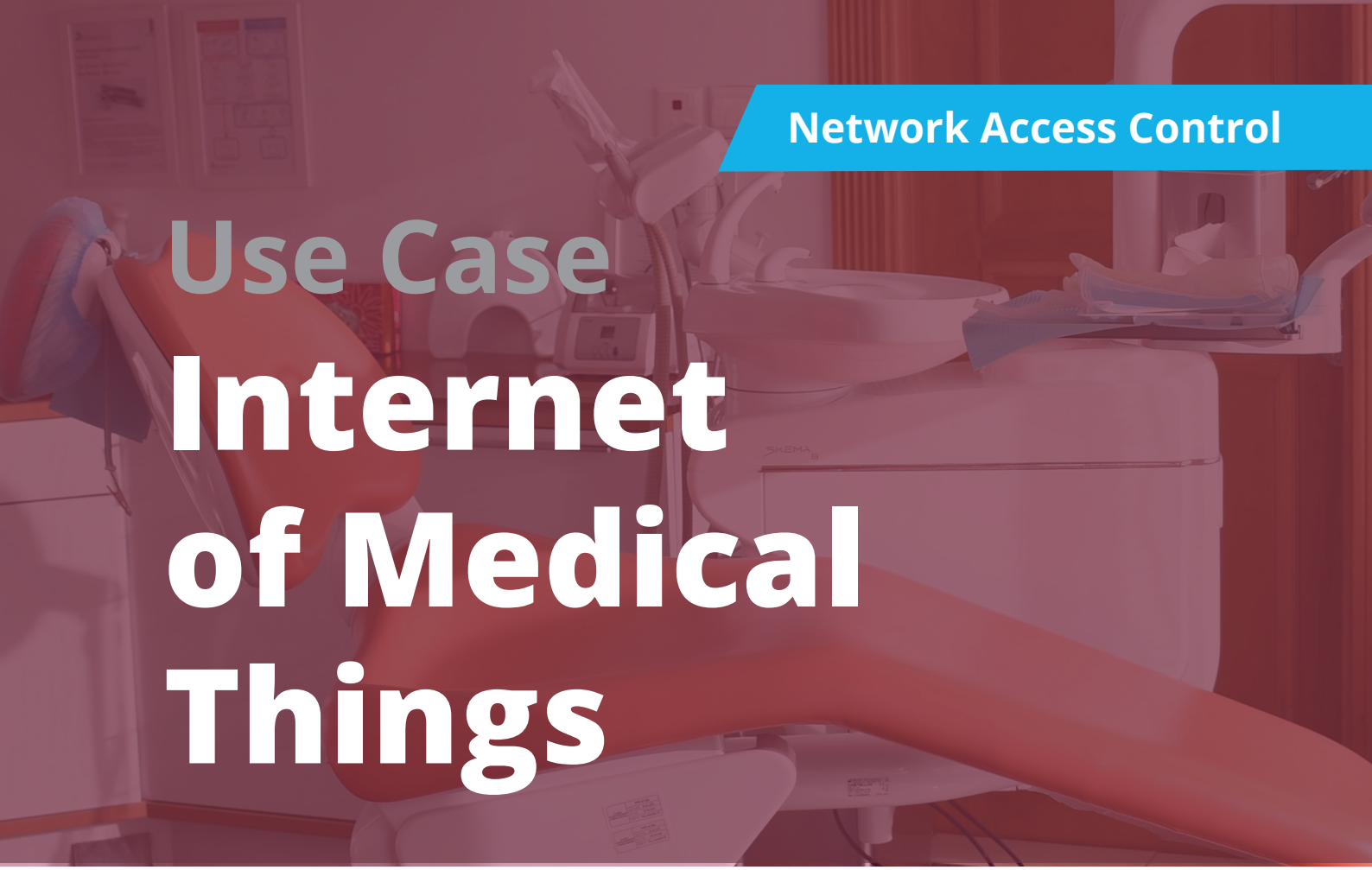


Network Access Control

Use Case
Internet of Medical Things

The proliferation of IoMT devices also creates potential privacy and security threats

What is the Internet of Medical Things (IoMT)?

The Internet of Medical Things (IoMT) is essentially the integration of IoT in the medical field. The Internet of Medical Things is an architecture of connected healthcare software and hardware devices that connect healthcare IT platforms via online computer systems. It can be defined as a set of devices that use the Internet of Things for medical purposes.

IoMT is not only an investment for healthcare institutions; it helps them respond effectively and efficiently to patient needs, reduce healthcare costs, provide timely attendance of medical responses, and increase the quality of medical treatment. Unfortunately, the proliferation of IoMT devices also creates potential privacy and security threats. Studies have shown that IoMT is not immune to privacy and security because of the myriad IoMT vendors and devices in the market. Many healthcare organisations are experiencing potential cyber-attacks on IoMT devices, leading to fatal outcomes for patients and severe implications for healthcare providers.

Security Challenges

Cyber attacks often take place when these devices are placed into service

According to a Netscout report, an attack takes place within five minutes of connecting to the internet. These devices are often being controlled outside of the IT department's scope or the medical device manufacturer. Other issues are hardcoded or default passwords, and when communication takes place between the different devices or between a specific workstation and machine, the communication lacks encryption.

(Un)patchable devices

Unpatchable medical devices are devices their manufacturers no longer support because they were phased out and no longer part of the manufacturer's product portfolio. These devices are not easily replaced for healthcare institutions because they represent a large capital investment. Still, these - both patchable and unpatchable - medical devices have become a major security concern as they have become vulnerable to attacks. A recent KLAS report shows that about 33% of all managed connected medical devices are listed as "unpatchable."

Vulnerability in IoMT Devices

An average hospital room has 15 to 20 connected medical devices such as patient monitors, IV pumps, ventilators, etc. Many of these devices are still running on unsupported operating systems (OSs)—such as Windows 95, 98, 2000—and can no longer be patched against vulnerabilities.

The common attacks in IoMTs

IoMT deals with the communication and control of smart medical devices. With the different variations of IoT malware constantly emerging, these emerging malware can also affect the communication of IoMT and used to control medical devices.
Some examples of common attacks include Eavesdropping, Man in the Middle, Packet capture, Flooding, Dictionary, Brute Force Attack & Birthday attacks.

How NAC helps IoMT

A key feature of NAC is inventory and tag every (unknown) device inside the network. The devices can be categorised into groups and enforce different security policies. Understanding the full inventory of medical or any other device in the network will provide adequate insight for segmenting the network.

Network segmentation is a proven strategy to increase security and control large-scale network environments and is ideal for securing medical devices connected to a network. Network segmentation divides a network into smaller segments and allows network traffic to be isolated to prevent access between network areas, VLANs and switch ports. When a network is segmented wisely, most traffic stays between devices and applications within each segment, with much less traffic crossing segment boundaries.

This approach reduces the risk of breach or spreading malware attacks because it is impossible to move from one network. Only certain users will be allowed to access the network resources. If attackers compromise accounts in a specific network segment, their ability to escalate privileges or perform lateral movement across the network will be contained to that segment.

NAC solutions provide granular control of endpoint access policies and permissions, allowing healthcare institutions to protect critical data by providing employees and contractors role-based access. Role-based access control restricts system access to authorised users.

Digital certificates play a key role in the healthcare industry

Healthcare organisations need to be assured that their ecosystems of all connected devices, including IoMT, are trusted and secured. This requires authentication and data encryption for these medical devices, among other capabilities. Digital certificates provide the mechanisms for controlling access to devices and prohibiting fraudulent data or communication origination. Using digital certificates validates that a device is authentic and assures that its messages are genuine. This approach ensures that critical healthcare information is sent from and received by only the intended recipients. The potential impact of a compromised device is minimised because it carries a unique identity, encrypts its data, and is programmed with a cryptographic key associated with that identity.

IoMT requires NAC

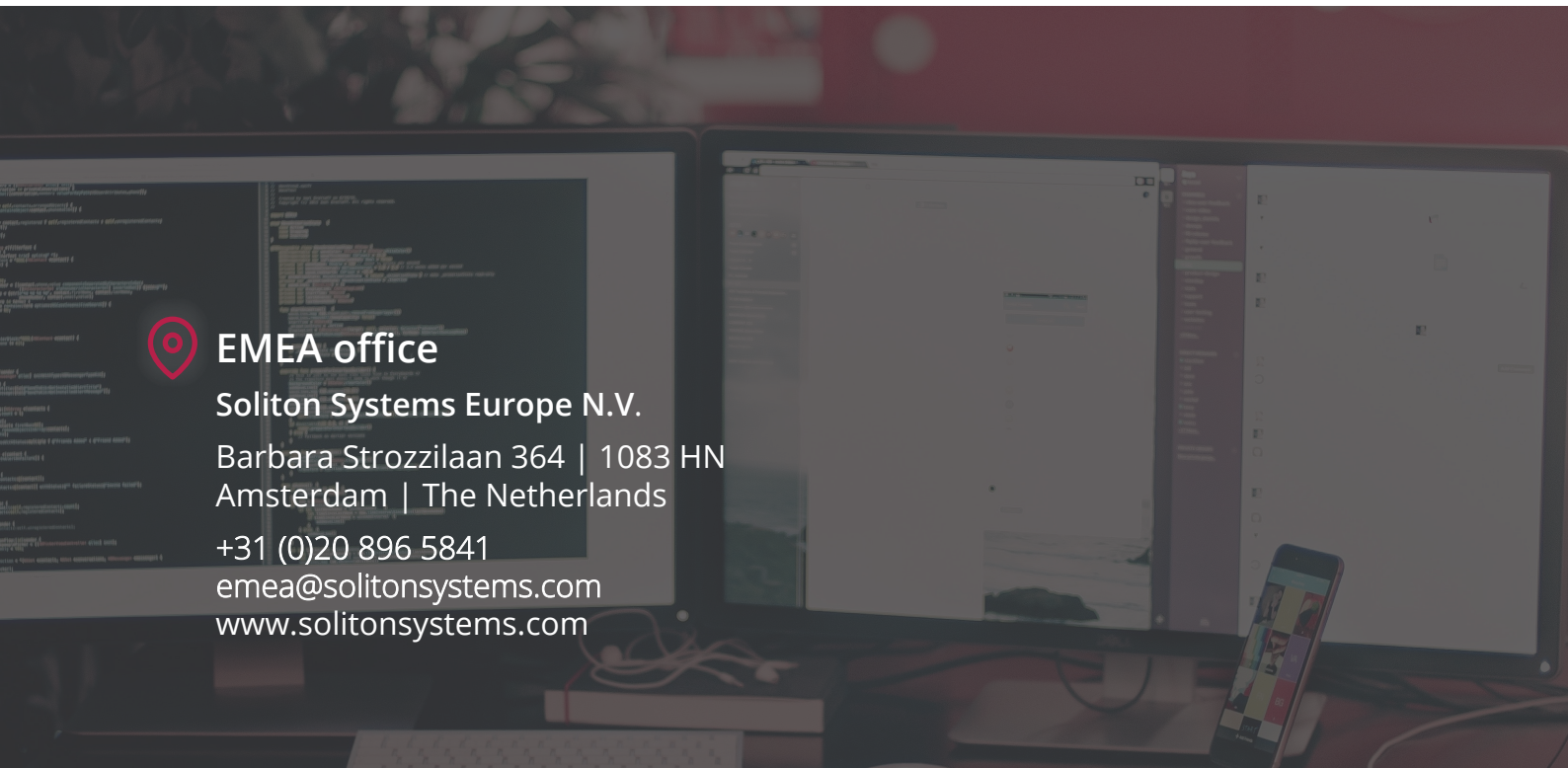
NAC solutions are an extremely valuable tool for any network infrastructure. NAC increases the overall security of any internal infrastructure by enforcing policies across all users and devices and provides improved visibility and monitoring of each device inside the network.

Health institutions must protect against the risks posed by connecting medical devices.

While IoMT has undoubtedly improved patient care, it has also led to increased vulnerabilities. A NAC solution supports regulatory certifications and security best practices and provides a clear view into network assets and network activity. It can automate processes with pre-set rules for device policy, user access and more to establish and maintain secure network infrastructure.

Digital certificates will be increasingly important for ensuring that healthcare devices meet industry and regulatory bodies. Digital certificates play a central role in delivering this confidence in traditional healthcare applications and IoT use cases for connected medical devices.

It's important to remember that NAC is only part of a security plan, not a complete security measure. NAC is a critical component of a multi-layered security policy because it monitors the inside of a company's 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