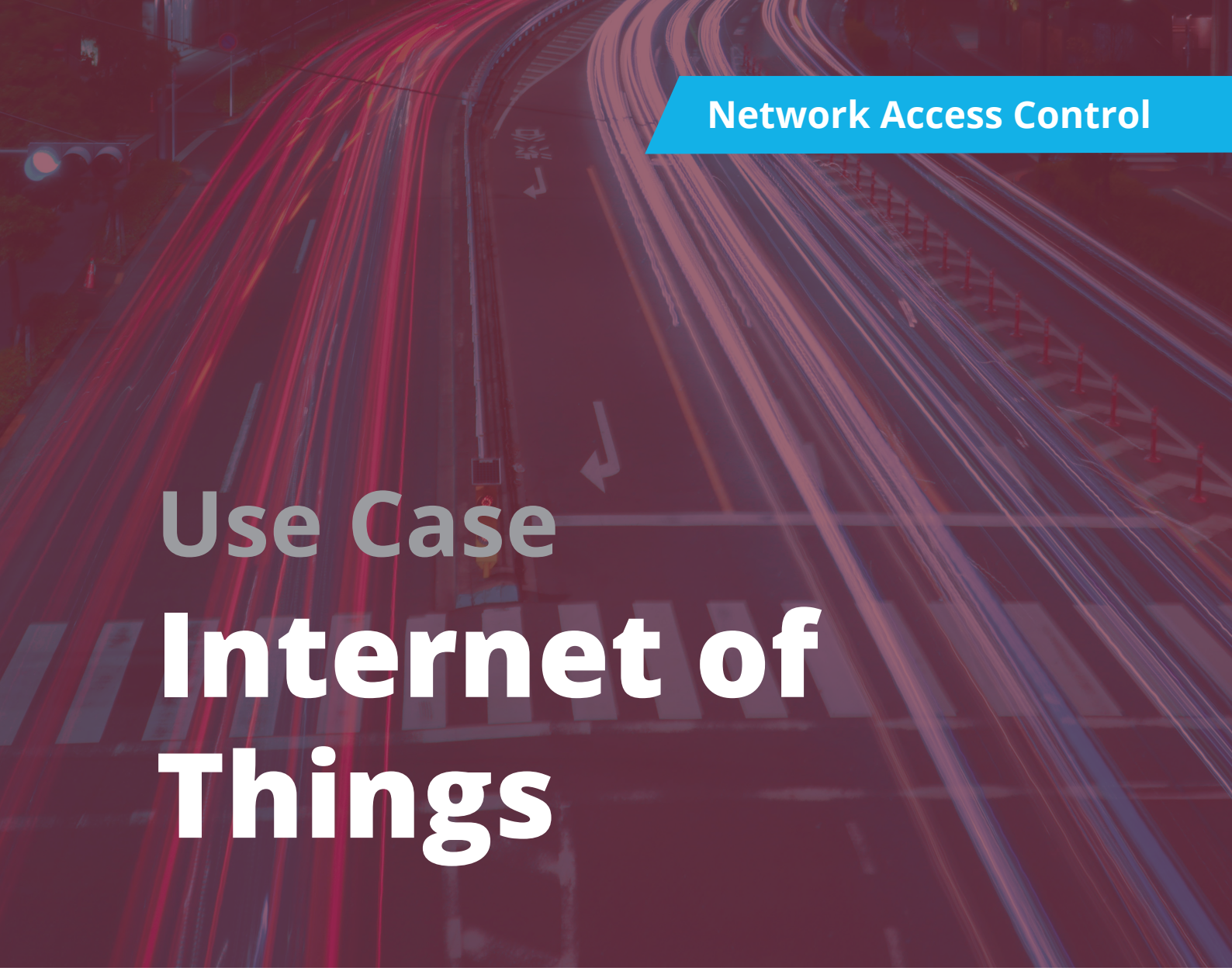


Network Access Control

Use Case
Internet of Things

IoT devices have become the prime target for cybercriminals

What is IoT exactly?

The broadest definition of the Internet of Things (IoT) encompasses multiple devices connected to a cellular network connection such as the internet to exchange data. Sensors are connected to these devices for collecting data, monitoring objects, and managing processes, from thermostats and factory machines to printers, TVs, and even refrigerators. The connected devices are considered part of an IoT network when they communicate back and forth with a central hub.

IoT Security issues

IoT security focuses on securing connected devices and networks in IoT.

The security methods to protect internet-connected or network-based devices from becoming compromised. The Open Web Application Security Project (OWASP) has published a detailed draft list of IoT attack surface areas, which can be broadly categorised into three areas:

Devices

Attackers use device vulnerabilities such as firmware, physical interface, web interface, and network services, and also take advantage of insecure default settings or outdated components and create backdoors to bypass normal authentication, amongst many others.

Communication channels

Attacks can originate from channels that connect and communicate IoT devices with one another. Protocols used in IoT systems can have security issues, making it simple for attackers to impact the entire system. IoT systems are also susceptible to network attacks such as man-in-the-middle, replay attacks, denial of service (DoS) and spoofing.

Applications and software

Applications and software are essential to IoT. Vulnerabilities in the administrative interface, web applications and related software for IoT devices can lead to compromised systems. A few examples include user credentials being compromised through the web and attackers infiltrating into a company's network through vulnerable routers.

NAC and IoT

IoT devices can be a challenge due to the ubiquity of devices. Before connecting an IoT device to an IP network, it should be configured with security built on the assumption of compromise.

NAC systems detect devices trying to connect to a network via a wireless, wired or VPN connection, authenticate the trusted device, and dynamically send the right policy to the network switch.

NAC helps identify and manage inventory so that organisations have continuous visibility into which IoT devices exist and when they connect to a network - providing a baseline for tracking and monitoring devices.

NAC solutions allow IT departments to lock down IoT devices by enforcing a policy of least privilege or blocking devices from the internal network until they meet the organisation's security policy criteria.

NAC offers network segmentation which can minimise the risk of IoT-related attacks by creating an own separate unique network for IoT devices and with restricted access to the enterprise network.

Network segmentation also helps prevent the spread of attacks and isolate possibly problematic devices that cannot be immediately taken offline.

PKI and digital certificates

A full-blown NAC solution, such as Soliton's NetAttest EPS, is equipped with a Public Key Infrastructure (PKI). A PKI is an excellent method to secure the client-server connections between multiple network-connected devices.

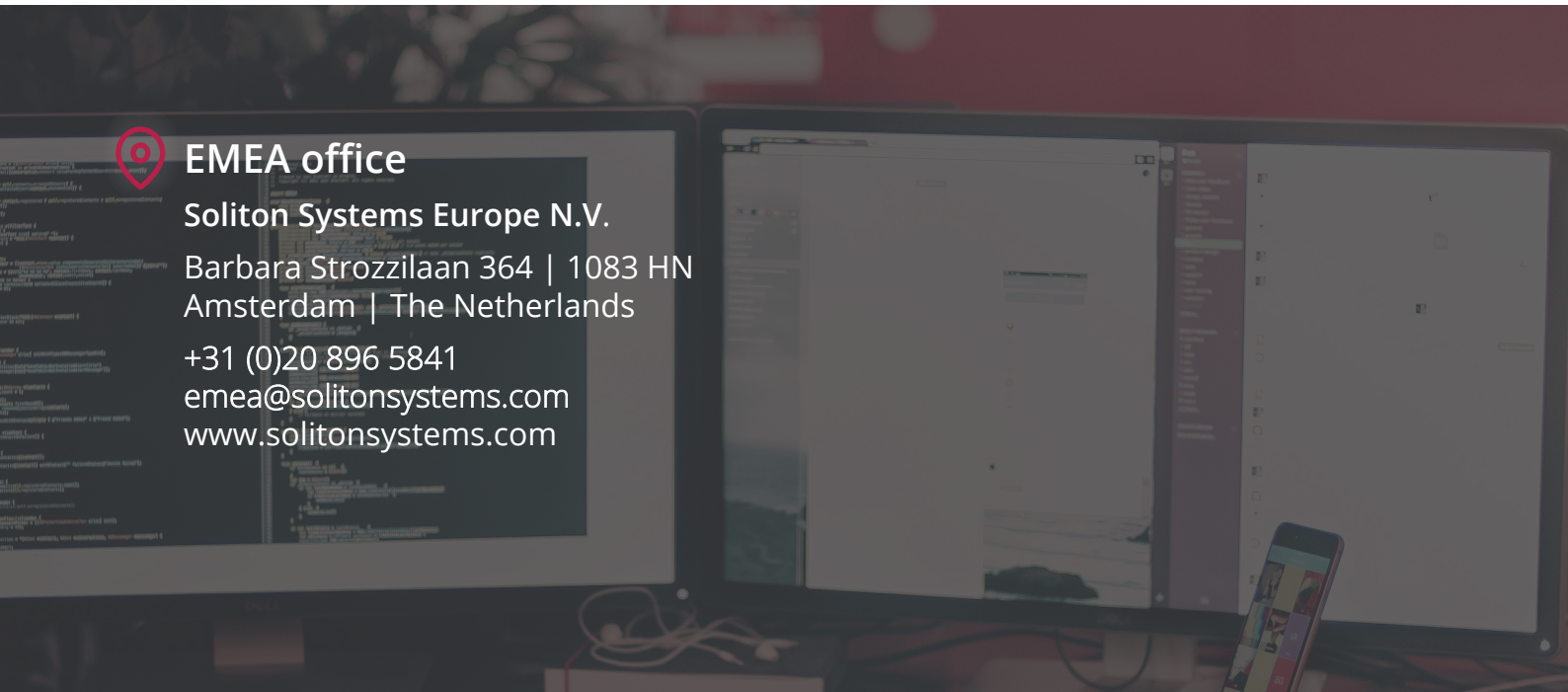
Using a two-key asymmetric cryptosystem, PKI can facilitate the encryption and decryption of data flows and interactions using digital certificates.

The Inevitable Future of IoT

IoT has emerged as a leading technology worldwide and is here to stay because of the convenience and benefits that it affords to many people and businesses. Increased network mobility, advanced artificial intelligence (AI), and the ability to deploy, automate, orchestrate, and defend complex use cases at hyper-scale will drive further advancements in IoT.

The future of IoT is virtually limitless, and significant work will be carried out around security and regulations to make it as safe as possible. Yet, the security vulnerabilities in millions of IoT devices grant attackers many opportunities to control devices remotely, act as a gateway to the rest of the network, or even take IoT devices offline.

NAC solutions can help secure all networked resources and prevent the proliferation of malware or ransomware attacks on an organisation's infrastructure through IoT 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