SCUDOS Platform

An adaptive Infrastructure Security Management solution

Know, visualize and control which devices
are connected to your network, and respond
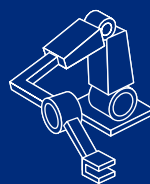potential risks with minimal operational effort

Delivers Total Network Visibility

Sees every device in your network, what it is, who it belongs to and where it is connected

Proactively Protects Your Core Network

Prevents unauthorized access to your network and detects potential threats
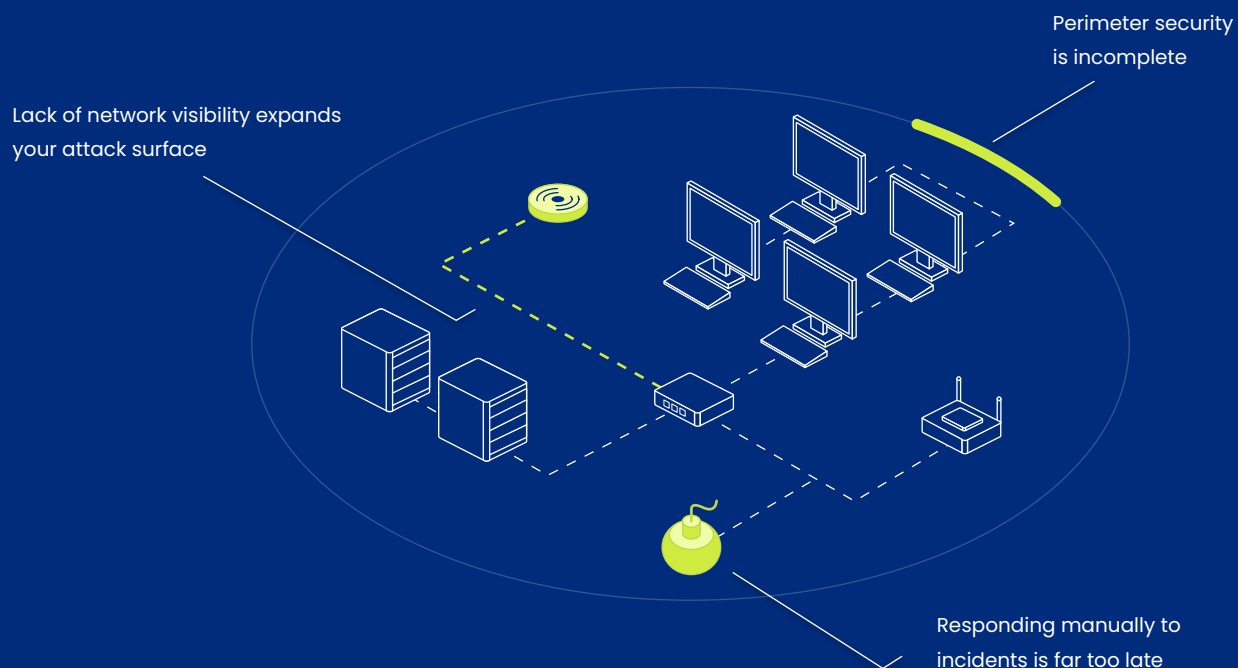
Automates Threat Mitigation & Response

Transforms your existing security tools from alarms-generators into real preventive measures

Minimizes IT Administration Efforts

Immediate setup of a single console to manage both your infrastructure security and IT inventory

Your Network Infrastructure is Vulnerable Can You Keep it Safe?

Perimeter security is incomplete

Lack of network visibility expands your attack surface

Responding manually to incidents is far too late

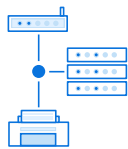# Immediately See and Control Every Device Connected to Your Network

SCUDOS is providing a holistic approach to network infrastructure security to protect organizations against internal threats and minimize network attack surface.

The SCUDOS platform incorporates agentless mapping and fingerprinting techniques with access control policies and network segmentation mechanisms, allowing organizations to implement a zero-trust security model.

In case of an incident, the SCUDOS orchestration module can automatically contain compromised devices before a human becomes involved in the process.

How It Works

Transparency

Agentless scanning for a complete mapping of the network topology

Fingerprinting of all connected devices, creating a central inventory

Continuous remote scanning of devices for existing vulnerabilities

Protection

Prevention of unauthorized access using whitelisting techniques

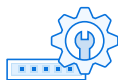**Network segmentation** using VLANs that ensures need-only access permissions

Prevention of layer-2 security threats, such as spoofing and flooding attacks

Orchestration

APIs to automatically quarantine a device in case of a 3rd party security alert

Regularly checks the network for irregularities and networking issues

Integration into monitoring and management platforms such as SIEM
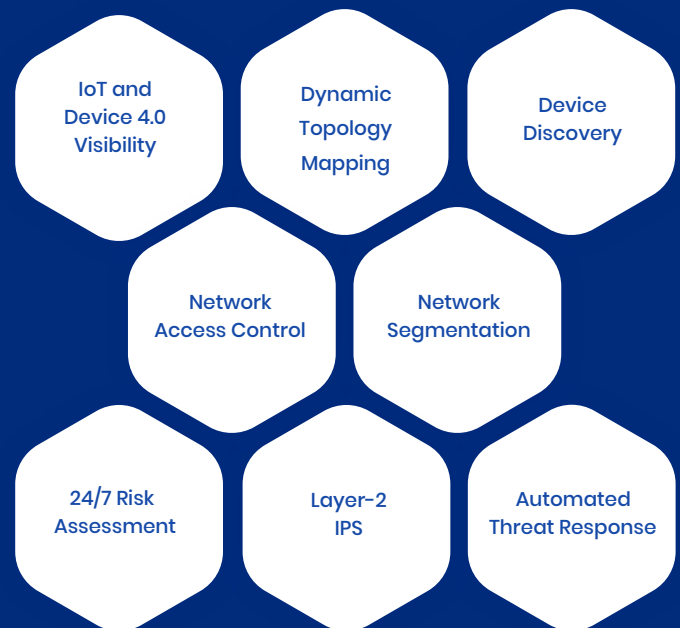
All of that in just one tool

A holistic approach to network infrastructure security

Single Day Deployment to Solve Your Critical Security Needs

- Consolidated solution, combining NAC with device inventory, risk assessment and incident response orchestration

- Supports the increasing demand for IoT visibility and control

- Lightweight, agentless deployment with easy setup, delivering immediate results

- Agnostic to existing HW; freedom from vendors lock-in

- Made in Germany

IoT and Device 4.0 Visibility

Dynamic Topology Mapping

Device Discovery

Network Access Control

Network Segmentation

24/7 Risk Assessment

Layer-2 IPS

Automated Threat Response

SCUDOS is a registered product by IFASEC GmbH

IFASEC GmbH is a software manufacturer and penetration testing company based in Dortmund, Germany. The company was founded in 2013 by Udo Kalinna, an IT security expert with over 20 years of experience working in collaboration with the forefront of IT research institutions worldwide. Over the years, IFASEC has helped hundreds of companies to evaluate the security state of their networks and has provided security teams with end-to-end solutions to tackle today's modern threats.
IFASEC holds several IT innovation awards for contributing to and pioneering in the network security landscape, and is a member in the TeleTrusT and Bitkom (Information Technology Security Working Group) associations.

IFASEC

SecurITy
made in Germany
Trust Seal
www.teletrust.de/itsmig

SCUDOS
SECURE YOUR BASE

Lissaboner Allee 7
44269 Dortmund, Germany
+49 231 5869020
info@scudos.eu
www.scudos.eu