OPSWAT.

MetaDefender NAC

Network Access Control

The volume and diversity of devices accessing business- critical network resources represent an increasing challenge for today's IT organizations. How can you easily block unknown devices from the network, while maintaining a positive experience for devices that belong? And how do you know which devices meet your security standards?

MetaDefender NAC, formerly SafeConnect, automates device security compliance and network access assignment policies by gathering a wealth of real-time and historical device information. This allows for granular and more timely security decisions when it counts.

Visibility. Security. Control.

MetaDefender NAC automates device security compliance and network access assignment policies based on identity role, device type, location, and ownership and gathers a wealth of real-time and historical context-aware device information that allows for more timely and informed security decisions.

MetaDefender NAC also addresses the daunting task of correlating mobile and IOT device information and user identity over time and across network segments for regulatory compliance, security forensics; and enabling identity-based firewall, web content, SIEM, and bandwidth management policies.

MetaDefender NAC delivers security, visibility, and control to every device accessing your network and cloud applications.
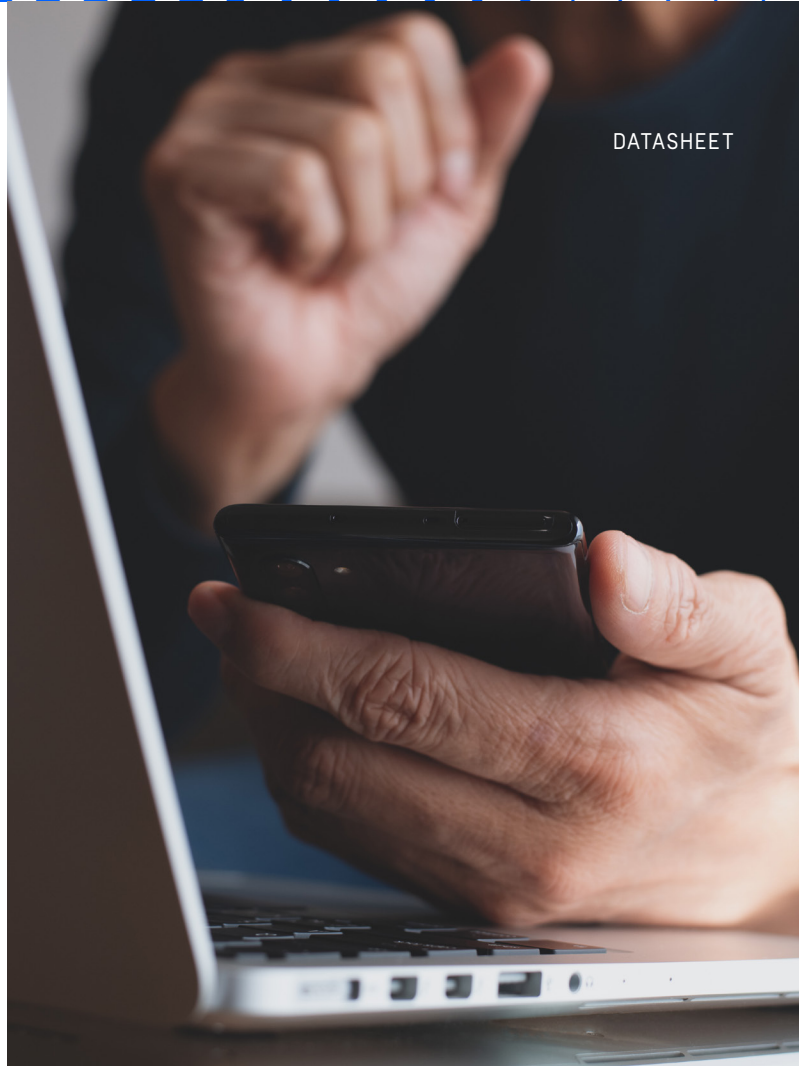
Benefits

Real-Time Visibility and Security
Complete visibility to all devices on both wired and wireless networks with authentication or blocking. Security assessment and enforcement for Windows, macOS and mobile devices.

Flexible Enforcement Options
The only solution on the market that offers either RADIUS-based enforcement that requires no VLAN changes or a unique Level 3 option that negates 802.1X requirements.

Streamlined User Authentication
Intuitive user access for guests, vendors and employees with a fully customizable self-registration portal.

Contextual Intelligence
Gain greater visibility into device types in context with the network, and publish that information to other security utilities to automate enforcement and remediation.

Remote Installation, Training, and Deployment
Remote deploy and install; includes 24x7 proactive monitoring & support, nightly backups and pushes of new devices, OS & Antivirus, automated updates.

OPSWAT.

MetaDefender NAC

Features

MetaDefender NAC has an integrated **RADIUS server** which can stand alone or proxy to an existing RADIUS solution.

Simplify **Device Remediation** with an intuitive captive portal that guides the user back onto the network without intervention

Gain visibility into all connected device types, brands, OS and other characteristics with **Agentless Device Profiling**

IoT Device Registration associates an identity to browserless devices, allowing for granular access policies to mitigate security vulnerabilities

Provide secure guest access to wired or wireless networks with a selection of three **Guest User Self-Registration** models

Remote 24x7 Proactive Monitoring Support is remotely managed for you, and includes daily remote backups, software upgrades, problem determination/resolution ownership

Capabilities

- Port Level Control
- Role-Based Access Control
- Agentless Device Profiling
- Acceptable User Policy [AUP] Enforcement
- Custom Policy Builder
- Guest and IOT Self-Registration
- Flexible Network Integration Options
- Contextual Intelligence Publishing
- Application Usage Policies

MetaDefender NAC specifications for standard VM

- **Appliance Specifications**
  SafeConnect VMWare Enforcer

- **VMWare Version***
  ESXi 5.1 or newer

- **Virtual Hardware Version**
  Minimum version 8

- **CPU**
  2 quad-core CPUs [2-3Ghz]

- **Memory**
  16 GB minimum

- **Hard Drive Storage**
  300 GB minimum

- **Appliance Scalability**
  Up to 25,000 devices

- **Network Interface**
  Gigabit NIC

*Hyper-V and Azure also supported
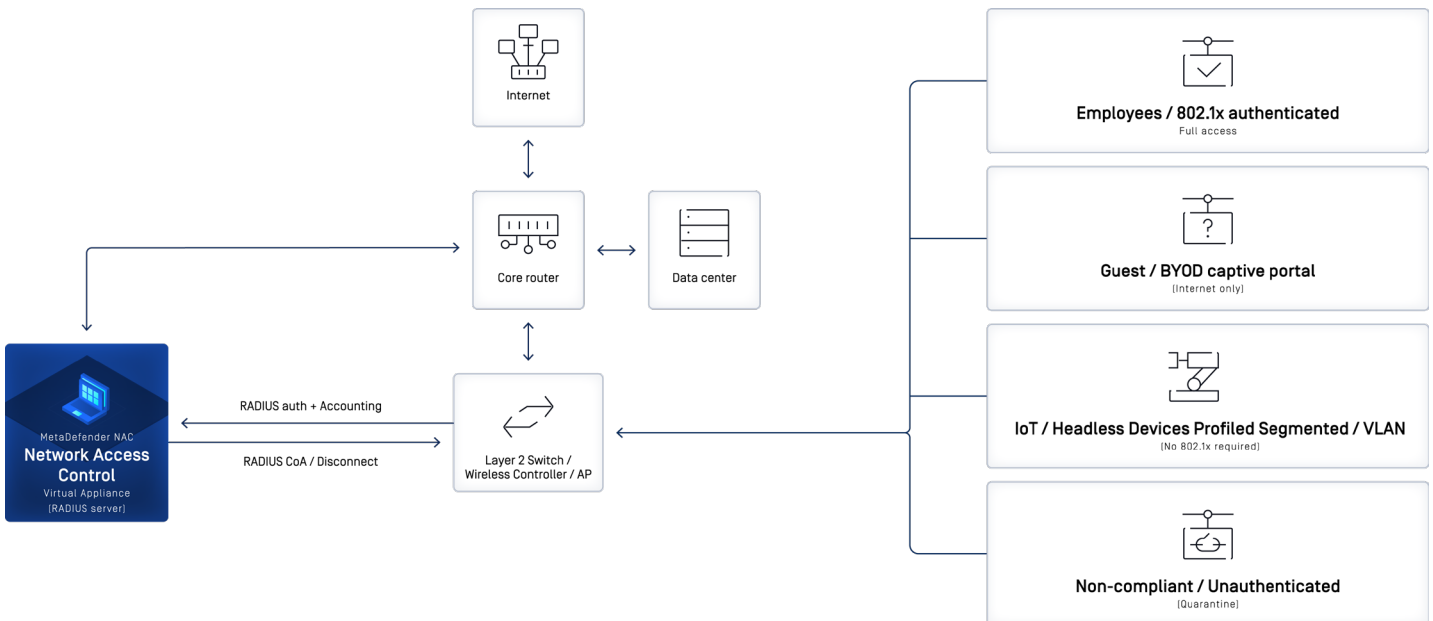
OPSWAT.

Protecting the World's Critical Infrastructure

OPSWAT.com/contact