OPSWAT.

DATASHEET

METADEFENDER™

Network Access Control Cloud

Managing the increasing volume and diversity of devices accessing business-critical network resources is crucial for today's IT organizations. How can you restrict network access for unknown or risky devices while ensuring a seamless experience for authorized devices?

MetaDefender Network Access Control (NAC) Cloud automates device security compliance and network access assignment policies by gathering and presenting real-time and historical device information in a unified, cloud-managed platform. This enables granular and timely security decisions without the hassle of maintaining an on-premises setup.

Features

Cloud Service

A cloud-native SaaS RADIUS service that your networking equipment can integrate with directly via RadSec

Cloud and On-prem Hybrid

An easy-to-setup hybrid deployment with a headless RADIUS server, managed from the same cloud console as the SaaS service, performing core AAA functionality locally to maintain network operation even if Internet access is lost while retaining cloud SaaS convenience.

Device Remediation

A user-friendly captive portal guiding users back into compliance without help desk intervention.

Agentless Device Profiling

Provides visibility into all connected devices, including type, brand, OS.

Flexible Hybrid Deployment with NAC Edge

Choose between managing your own virtual appliance or leveraging a fully managed cloud SaaS solution. Enhance security posture with NAC Edge, which enforces device compliance and access control at the network perimeter, ideal for safeguarding hybrid environments.

Secure guest access

Offers 4 Guest Self-Registration modes for wired/wireless networks, with multiple profiles available simultaneously.

Regulatory Compliance

Enforces security compliance for NERC, CISA, PCI, HIPAA, SOC2, SOX, GLBA, and GDPR, and generates audit reports.

Unified Multi-Function Platform

Combines threat detection, compliance, incident response, featuring Vulnerability Detection of over 25,000 CVEs and OS security patch gaps; Patch Management automating about 10,000 third-party applications patching; Advanced Endpoint Protection utilizing over 20 antivirus engines.

Enhanced User Experience

A single-pane-of-glass management console that streamlines operations across multi-site deployments. Benefit from high-performance secure access with user-friendly captive portal and quick self-remediation.

IoT Device Registration

Associates user identities with browserless and non-802.1x devices, providing maximal context for device access decisions.

Visibility. Security. Control.

MetaDefender NAC Cloud automates device compliance and network access policies enforcement based on identity, device type, location, and security posture. It collects comprehensive real-time and historical context-aware device information, allowing for more timely and informed security decisions.

MetaDefender NAC Cloud also addresses the daunting task of correlating mobile and IoT device information to user identity over time and across network segments for regulatory compliance and security forensics. It also enables identity-based firewall rules and SIEM integration via API-based and Syslog-based Contextual Intelligence publishing options.

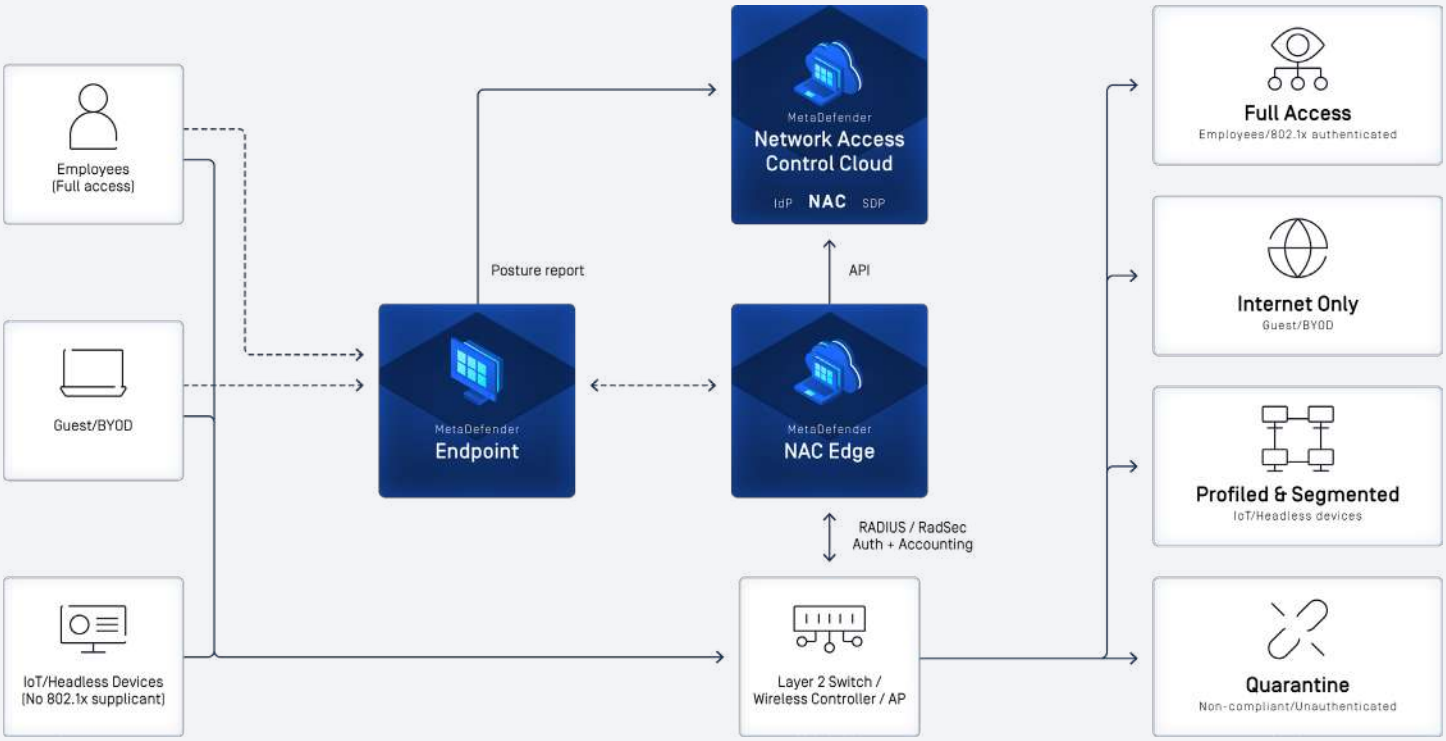
MetaDefender NAC Cloud delivers security, visibility, and control to every device accessing your network, all managed from a cloud-based console accessible from anywhere.

NAC 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

Supported Endpoints

- Windows 7 and above, Windows Server 2008 and above
- MacO SX 10.9 and above
- iOS 8.3 and above
- Android 5.1 and above
- Debian-based Linux v4 (15.4.x) Ubuntu 16/Mint 18/Debian 8
- Red Hat-based Linux v4 (15.6.x) CentOS 7.14/ Red Hat Enterprise 7/ OpenSuse 11.4/ Suse Enterprise 12.x/Fedora 27



OPSWAT.
Protecting the World's Critical Infrastructure