

METADEFENDER™

Network Access Control

Global organizations need to allow a wide range of users (from employees and customers to contractors, and suppliers) to connect via unknown or unmanaged devices. But each connection is a potential threat that must be controlled without disrupting workflows.

MetaDefender Network Access Control (NAC) automatically verifies every device trying to access your network and enforces access policies in real time. Trusted devices connect instantly, while unknown or non-compliant ones are restricted, without manual intervention.

With full visibility, flexible deployment options, continuous compliance monitoring, and centralized control, IT teams can secure access, stay audit-ready, and keep operations running without friction.

Features



Device Remediation

A user-friendly captive portal guides users back into compliance without help desk intervention (available in hybrid and on-prem deployments).



Agentless Device Profiling

Provides visibility into all connected devices, including type, and OS (available in hybrid and on-prem deployments).



Endpoint Posture Enforcement

Restrict or block network access based on device compliance across every deployment model.



Secure Guest Access

Highly-customizable Guest Self-Registration flow for both wired/wireless networks, including ability to restrict allowed email domains (available in hybrid and on-prem deployments)



Flexible Deployment Options

Choose the model that fits your environment — a cloud-native SaaS RADIUS service integrated via RadSec for EAP-TLS authentication and endpoint-agent posture enforcement; a hybrid deployment (our recommended model) that pairs the cloud console with an on-prem virtual appliance to unlock the full feature set and keep AAA running locally even if Internet access is lost; or a fully on-premises install for air-gapped and sovereignty-sensitive networks.



Unified Multi-Function Platform

Combines threat detection, compliance, and incident response, featuring Vulnerability Detection of over 25,000 CVEs and OS security patch gaps; Patch Management automating about 10,000 third-party applications; and Advanced Endpoint Protection utilizing over 20 anti-malwares 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 a user-friendly captive portal and quick self-remediation.

Visibility. Security. Control.

MetaDefender NAC automates device compliance and network access policy 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 also simplifies correlating mobile and IoT device data to user identity over time and across network segments for regulatory compliance and security forensics. It enables identity-based firewall rules and SIEM integration via API-based and Syslog-based Contextual Intelligence publishing options.

Managed from a unified console, MetaDefender NAC can be deployed as a cloud-native SaaS, a hybrid model combining cloud and on-prem deployment, or full on-prem for air-gapped environments.

NAC Capabilities

- Port Level Control
- Role-Based Access Control
- Agentless Device Profiling
- Custom Policy Builder
- Guest Self-Registration
- Flexible Network Integration Options
- Contextual Intelligence Publishing
- Application Usage Policies

Supported Endpoints

- Windows 7 and above, Windows Server 2008 and above
- Mac OS X 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

*The diagram illustrates the hybrid deployment model only.

