nile

Requirements for Next-Gen Enterprise Networks

Nile vs Legacy Products sold as NaaS
(Network as a Service)

nilesecure.com

Introduction

The following is designed to help IT leaders and their organizations understand the capabilities and differences between an AI-powered Nile Access Service versus competitive offerings.

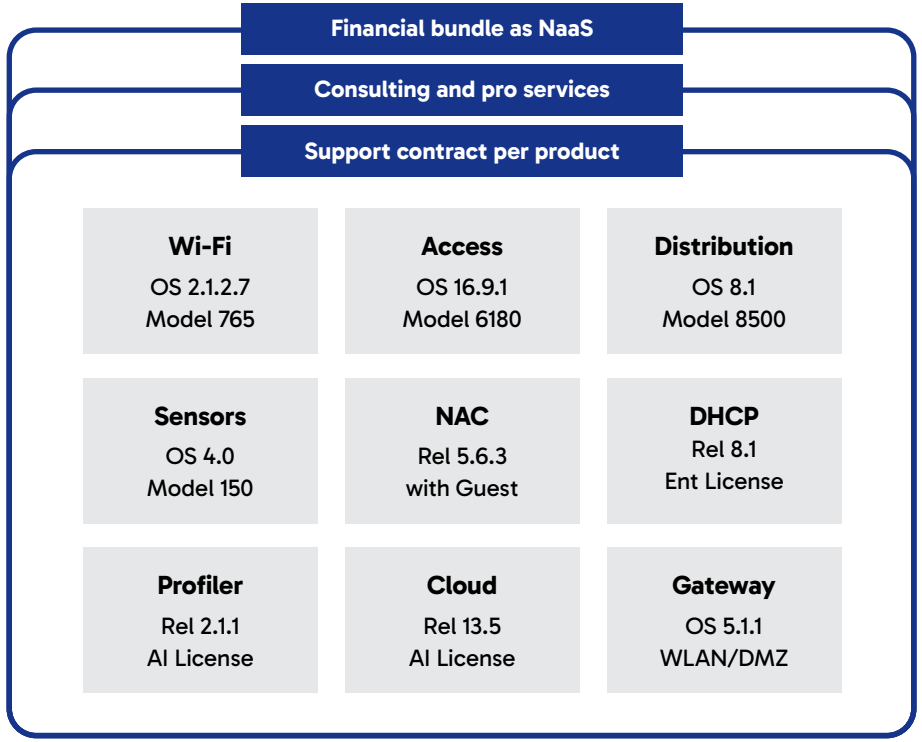
The Nile Access Service uses a revolutionary approach to wired and wireless access networks that redefines the requirements for next-generation deployments across an organization. It is designed from the ground up as a service, offering service level guarantees in overall system availability, wireless coverage, and total network capacity, and does not require upfront capital expenditure.

Nile's Access Service integrates a networking technology stack and lifecycle automation with AI in a single solution. It is not a collection of 10+ solutions or as-a-service SKUs that piece together wireless, wired, network access control and other functions of a network. Traditional licensing, management, and lifecycle headaches that are plaguing IT teams and organizations today are completely eliminated.

The following sections are broken out by design and installation, technology, operations/support, and consumption methods that target wired and wireless network requirements.

Note: The Nile Access Service or Legacy Products sold as NaaS can be delivered by their respective vendor or a managed service provider. The feature comparisons and associated costs apply in either consumption model.

Traditional model for enterprise networks with inherent complexity, stitching together 10+ products and services



Design and Installation

Typically an area where IT invests time working with vendors or managed service providers to assess what is needed, where APs and switches will be installed, with a detailed deployment plan that includes timelines and who does what. Nile Access Service enables closed loop automation for a deterministic design and install of a wired and wireless networks, radically reducing operational burden.

Important Considerations	Nile Access Service	Legacy Products sold as NaaS
Detailed site survey	✔ Full wired & Wi-Fi design including PoE budgets, cabling, rack space, power & cooling requirements	✘ Add-on option based on as-a-service bundle option
Full redundancy	✔ Redundant switch & AP coverage that delivers full-scale capacity	✘ Add-on option that adds to cost and scope
Standardized design	✔ Enterprise-class APs and switches for each site with deterministic system design across locations	✘ Trade-offs due to cost and CAPEX budget envelope
Auto-generated topology and BoM	✔ Complete and accurate material list for everything needed, including physical Wi-Fi sensors	✘ Manual generated and prone to missing components
Single AP model across deployment	✔ Highest performing Wi-Fi 6 certified access point for all sites, with only one firmware version across all customer deployments	✘ Requires IT to select AP per price point, features and performance expectation
Single switch platform across deployment	✔ High performing access & distribution switches for unified capabilities and performance	✘ Requires IT to choose switches per price point, features and performance
Sensors for proactive testing	✔ Physical and virtual sensors test against service level guarantees	✘ Requires add-on 3rd-party options and service
Load-balanced APs across switches	✔ Used to improve coverage in the event of an outage	✘ Requires written request, separate SKUs & add-on service
Automated deployment and activation	✔ Included as part of all customer deployments	✘ Optional per chosen NaaS vendor & service packs
Mobile-app for service activation	✔ All network elements activiated via secure bluetooth radio	⚠ Little to no AI automation for day 0 automation
Orchestrated firmware uploads - APs and switches	✔ Automatically manages software updates within maintenance windows, with pre- and post-validation of system status	✘ Level of orchestration depends on as-a-service bundle
Elimination of typical network element configuration errors	✔ Does not require network element configuration and provides IT staff full control to securely onboard user and IoT devices	✘ Operational burden in tackling configuration errors
Automated operational model	✔ Nile removes complexity at fundamental protocol, hardware and implementation points	✘ Requires manual management of separate components

Wired / Wireless Technology

This is where time is spent determining differences in the hardware and software of various vendors' offerings to see if desired features are supported for current and future use cases.

Important Considerations	Nile Access Service	Legacy Products sold as NaaS
Modern Layer 3 end-to-end architecture	✔ Included in base architecture design for reduced fault domains	✘ L3 to the edge supported but not typically implemented in base architecture
No use of legacy Layer 2 protocol	✔ No Spanning-Tree, 802.1q trunking, VLANs & broadcast domain issues	✘ Many vendor's now rely on L2 designs & VLANs for segmentation
Standard Guest Access	✔ Cloud-based service and onboarding portal included for traditional guest use cases	✔ Many vendors offers cloud-based guest but may require add-on NAC option
Closed loop automation with AI	✔ Offloading traditional network operations, going beyond generation of summarized task lists with AI	⚠ Depends on vendor, cloud or use of on-premise management. Extra cost for AI chatbot.
Microservices-based firmware	✔ Predictive & preventative issue resolution for Day -1 to N use cases with no add-on cost	⚠ Depends on vendor as most slowly migrating to microservices for cloud management
AI performance baselining	✔ Ground up implementation for design for true as-a-Service requirements	⚠ Depends on vendor with some requiring manual setup of SLEs & IT guesswork
AP radio for RF quality	✔ Per site baselining with no manual setup of thresholds or service level expectations (SLEs)	⚠ Depends on vendor with some arguing that dedicated monitoring is overkill
Cloud DHCP service	✔ Dedicated to automated testing of RF, wireless intrusion detection & location	✘ Requires using third party vendor options and associated setup
Universal Multi-Gig Support	✔ IT can choose built-in option or continue using 3rd-party legacy options	✘ Vendor specific switches may not support multi-gig on all ports
Dedicated HW sensors	✔ All Nile wired LAN ports support Multi-Gig	✘ Requires third party options, integration and extra monitoring dashboard

Network Security

Security is a paramount concern as in-building roaming, IoT, and working from everywhere are prevalent today. Today's networks must include features that fix legacy security design, simplify IT and end user workflows, as well as provide the ability to operate IoT devices securely.

Important Considerations	Nile Access Service	Legacy Products sold as NaaS
Layer 3 Campus Zero Trust design	✔ Complete host based isolation (user & IoT) for no unauthorized network connections	✘ Expensive add-on service with added configuration complexity & maintenance
End-to-end encryption	✔ Standard Nile Campus Zero Trust feature	✘ Depends on vendor as encryption is performance intensive & prohibitive
Secure Guest Access (optional)	✔ Replaces standard Nile Guest service for isolation of guest traffic & from internal network	✘ Requires a host of considerations like OWE supplicants & extra SSIDs
Simplified Secure Guest setup	✔ No anchor controllers, NAT setup or VLANs required	✘ Requires purchase of 3rd-party service & extra costs
Simple Secure Guest Login	✔ No added user inconvenience or IT management needed	✘ Require users to choose between secure & legacy supported guest SSIDs
TPM based hardware	✔ All Nile devices have built-in Trusted Platform modules	⚠ Depends on vendor as some transitioning from SMB to enterprise-class
Automatic MACsec encryption	✔ All Nile devices include dedicated HW & SW	✘ Depends on vendor as some include hardware but not software support
No access to APs / switches	✔ Nile devices do not have console ports for added security	✘ Other vendor devices open to possible threats and tampering
Built-in endpoint profiling	✔ Standard cloud-based Campus Zero Trust feature	⚠ Depends on vendor management or on-premise NAC solution chosen
Automated security patches	✔ Included in Nile service for no IT impact	✘ Vendor chosen determines the level of patch management

Important Considerations	Nile Access Service	Legacy Products sold as NaaS
SSO for IT admins	✔ Campus Zero Trust feature to eliminate need error prone RADIUS/TACACS rules	⚠ Depends on vendor solution and additional integration effort
Ful authenticated wired access	✔ Nile's switches and ports support 802.1X &/or MAB, SSO & Captive Portal (future) without typical config issues	⚠ Typically an expensive add-on service where 802.1X complexity stalls projects
Unique PSK Wireless Access per SSID	✔ Easy-to-use, secure user initiated keys & client/IoT onboarding (MyNile portal)	⚠ Some vendors charge extra and have key limits per network
Single Sign-On (SSO) Wi-Fi & wired access	✔ Built-in integration for a variety of user authentication use cases	⚠ Typically an add-on service with integration costs
Built-in host-based isolation	✔ Segmentation at host level to limit compromises to single endpoint	✘ Requires complex rules and an add-on integration service not required by Nile
Built-in WIPS/WIDS for wireless	✔ Full-time rogue detection & containment with AP impersonation detection & alerting (Honeypot AP, Evil Twin)	✘ Typically extra licensing (app and advanced management interface) for legacy vendors
Auto-detection of denial of service attacks	✔ Always-on, no configuration necessary (deauth flood, deauth broadcast, etc)	✘ A usable feature with extra licensing for most other vendors
Built-in BYOK (key) management	✔ Customer-owned / managed cloud encryption keys (add & revoke) & simplified PII controls	✘ Add-on service with third party solution that requires integration effort and cost
Built-in SIEM analytics	✔ Clickable buttons to capture per client security audit data for Splunk and Logicmonitor	✘ Add-on of third party service and additional dashboard integration via APIs
Palo Alto Networks integration	✔ Palo Alto's XML API on NGFW fully supported for user to IP mapping. No NAC/RADIUS server	✘ Add-on service that requires RADIUS/NAC server with added complexity and cost

Network Operations

The operation of your network is crucial for business continuity and user productivity. Today's networks must include AI, automation, and the ability to perform closed-loop operations. It is no longer prudent to rely on IT interaction at every step. The Nile Access Service is designed to proactively resolve deviations in service quality in software and/or via a "reliability/production engineering" team that keeps tabs on your network 24/7.

Important Considerations	Nile Access Service	Legacy Products sold as NaaS
Cloud-based customer operations portal	✔ Access to specific tools & visibility required to define characteristics of the network overlay, such as policies	✘ Access limited or overly broad based depending on chosen vendor solution
Automated software upgrades within pre-defined maintenance windows	✔ Essential part of Nile's cloud-native software architecture	✘ Requires add-on service option with coordinated outage planning
No repetitive configuration tasks	✔ Eliminates customer-led network configuration & associated tasks	✘ Add-on service option with often greater customer burden
Closed loop automation powered by AI vs. traditional troubleshooting	✔ Automated detection and remediation of performance issues against dynamic thresholds identified with AI	⚠ • Large focus on Day 2 issues with reactive troubleshooting • Very little optimization capabilities
Closed loop automation powered by AI vs. day -1 design/install	✔ Only solution that automates Day -1 planning & design, as well as Day 0 to Day N use cases	✘ Most solutions limited to minimal Day 0 and some Day N use cases
Proactive AP & switch reachability testing	✔ Proactive testing of network and services via built-in softbots and physical sensors	✘ Add-on service option - separate hardware sensors or endpoint software
Continuous testing of app availability	✔ Built-in checks of application availability & experience	✘ Requires separate devices, licensing and support
User-driven quality of service portal	✔ Useful visibility for troubleshooting & IT assistance	✘ No option exists that we are aware of
Auto RF tuning for no coverage holes	✔ Unique device level measurement (sensors) for 24/7/365 active site survey and software tuning	⚠ Additional cost for high-capacity design

Important Considerations	Nile Access Service	Legacy Products sold as NaaS
Automation of firmware upgrades on network elements	✔ Automated including pre and post validation checks	✘ Very time consuming depending on how many hardware models used for network elements
Elimination of alert and notification management	✔ Predictive maintenance against service quality baselines	⚠ Typical solutions still require alerts for common thresholds and only summarize task lists with AI
Closed loop automation powered by AI to enable problem resolution	✔ Known remedies automatically are applied and proactively eliminate potential future issues	⚠ Vendors have limited to no ability to automate troubleshooting or configuration changes
Simple ticketing with network provider	✔ Direct IT interaction with Nile via the cloud portal	⚠ Involves 3rd-party interaction before reaching the network vendor
End user self service Portal	✔ Available to all end users when on the Nile network	If possible, will require expensive ITSM integration

Consumption Models

With the speed of technology innovation and a volatile economy, more organizations are opting for an Opex vs Capex model to operate their wired and wireless networks.

Important Considerations	Nile Access Service	Legacy Products sold as NaaS
Per user pricing option	✔ Based on users per building / month	✘ Often based on per SKU / service pack or services chosen
Per square feet pricing option	✔ Based on size of building / month	✘ Often based on per SKU / service pack or services chosen
Flexible up/down billing	✔ Very simple adjustment per usage / growth	⚠ Depends on chosen vendor and scope of service pack / SKUs
Performance commitments	✔ Monitoring for 99.95% availability, coverage & capacity service level guarantees	⚠ Dependent on chosen vendor & serviceprovider. Will lack full-time sensor tests.
Service credits in case of violations	✔ Service Credit ($$) per month as outlined in the performance agreement	✘ No similar commitment that we're aware of
Monthly reporting	✔ Detailed metrics outlined in performance agreement with granular reports	✔ Often lack detailed metrics depending on depth of service
On-going hardware refreshes	✔ Designed to complement technology innovation &/or customer requirements & business needs	⚠ Depends on chosen vendor, as-a-service SKUs chosen & possible new CAPEX expense
Sustainability offload	✔ Customers no longer manage end-of-life / sale / support (EOL/EOS) cycles for hardware	⚠ Depends on chosen service packs or SKUs who is responsible

nile

3590 N First St, Suite 300
San Jose, CA 95134

(669) 369-6453

info@nilesecure.com | nilesecure.com