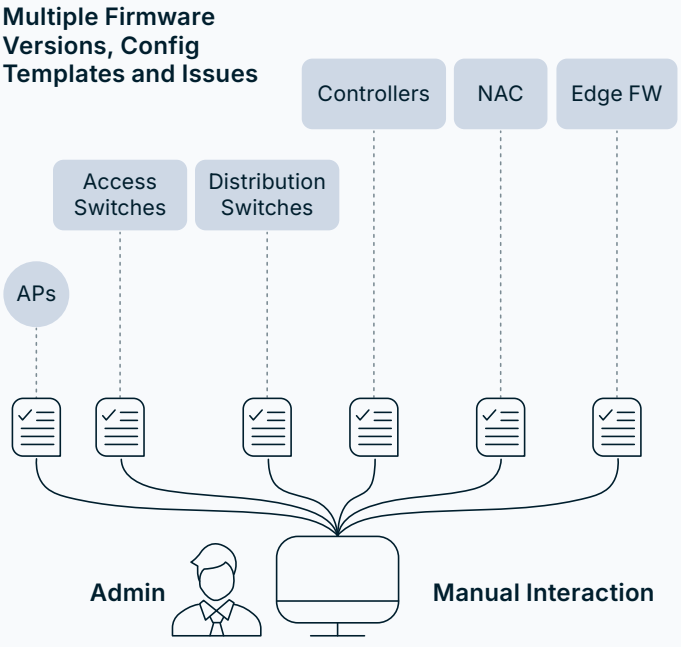
USE CASE

Network Operations Complexity

Software Lifecycle Management Remains A Concerning IT Burden

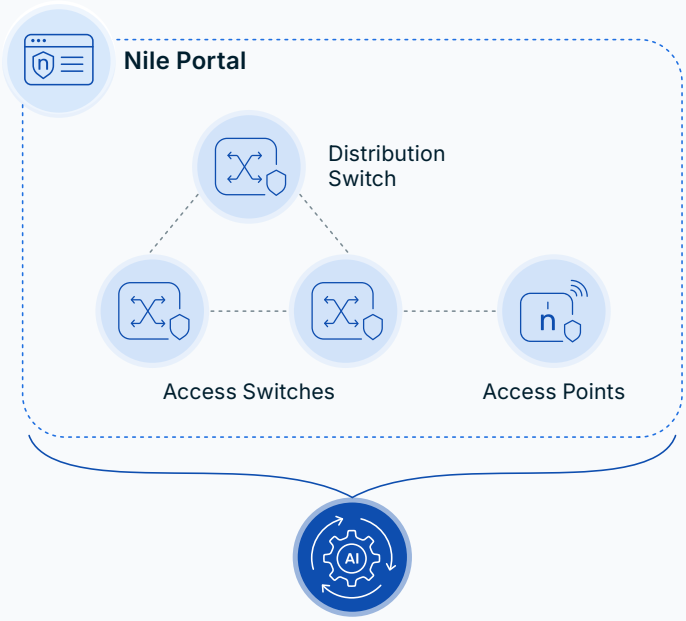
Upgrading legacy access points, controllers, and switches triggers firmware conflicts, reboots, and outages, requiring risky manual change windows. An automated update model eliminates uncertainty and boosts IT and business productivity.

Fragmented Legacy Network Upgrades



- Time-consuming per device upgrades
- Disparate deices introduces high risk

Unified Zero Trust Fabric Upgrade



- Synchronized upgrade of all Nile elements
- Integrated architecture delivers low risk

Nile's Leading-Edge Differentiation

Nile's automation simultaneously upgrades firmware across the entire Zero Trust Fabric, eliminating version drift, reducing operational risk, and ensuring validated, consistent access without manual coordination or service disruption.

Automated orchestration upgrades entire Zero Trust Fabric software simultaneously as needed across all locations.

Predictability eliminates version inconsistencies, rollbacks, and security exposure.

Standardization improves uptime and ability to use new features, while improving IT efficiency and user experiences.

1. Automation Negates Traditional Planning And Manual Intervention
2. Timely upgrades Eliminate Traditional Network 12-18 Month Feature Gaps
3. Exploit Vectors And Risk Tied To ~20% of Breaches Quickly Closed

Nile Makes Network Operations Easy

Automated execution and rollback assurance for enhanced uptime.

Digital twin validation that tests 3rd-party ecosystem solution operability.

Operations overhead improved by up to 30 to 35%.

Escaping Software Upgrade Chaos

For a large company with distributed locations and multi-vendor LAN infrastructure, every firmware upgrade felt like roulette—different versions, independencies, and late-night outages. Each independent release risked broken network device/NAC/firewall integrations, and unpredictable behavior.

Nile's Zero Trust Fabric and standardized software eliminated guesswork and IT saw delay vanish into the background.

From Time Consuming Manual Operations to Autonomous Assurance

Legacy Upgrade Approach	Nile Secure NaaS Approach
IT involved in all aspects of every upgrade	Nile owns and delivers all firmware upgrades as-a-service
Mixed firmware versions for every deployment	Uniform, standardized software image across the Zero Trust Fabric
Unpredictable windows, manual rollback, real outage risk	Customer-approved windows, automated pre/post digital twin validation and rollback
Limited testing with issues often discovered "live"	Engineered rollouts across Nile locations and install base
Uptick in war room meetings, tickets, and firefighting.	No IT dependencies, tickets, and long-term burden

Ready to Get Started?

Let's Talk ↗