

Nile’s AI-driven NaaS solves SDI CTO’s aging infrastructure and poor performance challenges

25%

Reduction in cybersecurity insurance premium after Nile

>2 days

Time it took Nile to deploy the network

3

Debates with Finance over capital expenditure, unpredictable costs

The Challenge

When Neil Clover started at SDI as its new CTO, he quickly realized he’d inherited a network that was long on problems and short on reliable connectivity. User frustration with the Wi-Fi network was the most obvious problem, but upon digging deeper, Clover’s background led him to believe there were bigger issues than just unreliable Wi-Fi infrastructure. This was a network in need of an entire overhaul.

Before embarking on a project of that scope, he needed to prioritize an already-growing, list of things that his team was responsible for. With a very lean IT team, they needed a new approach to deploying and operating a network that wouldn’t be all consuming in order to solve the following challenges.

- Quickly complete refresh of failing infrastructure without burdening internal IT staff
- Fix inconsistent connectivity that was hampering employee productivity
- Remedy complex security policies that were causing vulnerabilities
- Gain control over unpredictable, costly and complex network refresh cycles

The Solution

By looking at a network vendor as a potential partner and as-a-service provider, Nile's simpler, more secure network-as-a-Service (NaaS) offering made sense to Clover. With Nile, the SDI team would gain a network that would solve planning, installation and operations challenges, while also providing the security and future-proofing needed to satisfy fast-paced business objectives.

While the IT team could oversee that refresh, they time could be better spent as built-in AI-driven automation and autonomous operations eliminated tedious, time-consuming, and complex optimization and troubleshooting tasks.

- Nile secure NaaS now provides a stable foundation that just works
- Built-in Zero Trust immediately filled well-known security gaps
- Deterministic fabric allows Nile AI and autonomous operations to seamlessly optimize the entire network
- IT-centric Nile Customer Portal provides granular visibility into connectivity and network performance metrics

The Results

Full-site coverage and high-performance Nile infrastructure enabled SDI to offer an uninterrupted user experience regardless of employee, device type, or application being using. Nile's built-in Zero Trust Fabric and deterministic architecture also allowed Clover to overcome intimidating security challenges with confidence.

Nile's OpEx model also eliminated the age-old question regarding the real cost of operating a network. Gone was the high cost of purchasing infrastructure, solely being responsible for customization of software, performing upgrades and being on the hook again when aging equipment starts to impact users and the business.

- Holistic, pay-per-user subscription model with ultimate cost predictability
- Zero Trust network that immediately delivered a cybersecurity premium reduction
- Finance and IT organizations that now align on how best to spend on LAN technology
- IT staff adds value by prioritizing business-critical projects that help drive revenue

Network Simplicity Outweighs Complexity

"I never thought I'd outsource my network, but that was before I started looking into Nile," Clover explains. "When I saw what Nile was doing, I was immediately very interested. The relentless simplicity of the Nile model just made sense."

The beauty of the Nile experience started with eliminating the complex nature of planning, designing and monitoring a network. Nile AI and sensors then continuously conduct monitoring to analyze and autonomously optimize the network to guarantee performance. The automation significantly changed where the SDI IT staff spends its time and effort.

"Network problems were always in the back of our minds, and that stress distracted us from diving deeper into other issues," says Clover. "Nile eliminated that worry, making us more effective as an IT team. Nile's elimination of manually performing configuration changes vastly reduce the real risk of waiting for changes to happen and potential human errors."

The level of insight enabled by the Nile Customer Portal helps the IT team troubleshoot issues outside of the network for faster resolution time.

“When you’re having performance issues and you don’t know why, it’s frustrating and a huge time sink,” says Clover. “But Nile takes the network out of the equation and the slotting of different views in the portal lets us troubleshoot outside the network.”

Connecting to the wireless network now a "Wow" experience

The prior Wi-Fi network was unreliable and unevenly distributed: some wireless access points were oversubscribed while others were underutilized. The resulting congestion created latency and performance issues, leaving employees with a poor experience that ultimately increased trouble-tickets and the IT burden.

“People never hesitate to complain when the Wi-Fi is bad and never say anything when it improves,” says Clover. “But with Nile, we have users proactively commenting on how great the performance is. It’s been a fantastic change that people noticed.”

In a major departure from his long-held belief that video conferencing must be hardwired for high-quality performance, Clover embraced the Nile Service Guarantee. He left his cables behind and hasn’t looked backed. High-definition video carts are now wirelessly connected and more reliable than ever.

A security solution that actually locks down threats and cost

“Emerging threats are a reality, there’s no getting around the ever present that your user devices and network are a target in today’s world,” says Clover.

Nile built-in Zero Trust per-device isolation only allows for traffic to flow north and south and through a defined enforcement point, eliminating legacy VLAN-based network issues, like malware proliferation. There’s no need for complex and expensive NAC or segmentation add-on projects that are rarely completed.

The standard use of TPM-certificate authentication for each Nile element also prevents unauthorized devices from gaining access to the network. This security model eliminates man-in-the-middle and rogue device threats that are in a traditional network. End-to-end MACSec encryption then protects network data, abolishing snooping and sniffing.

To further bolster security, Nile natively supports IEEE 802.1X authentication across wired and wireless, assuring Clover and his IT team that weak passwords are no longer an issue. IoT devices leverage MAC Auth and again are placed in a segment-of-one, creating a very limited blast radius in the event of a breach.

Added bonus: security reduces costs. Many companies, including SDI, are required to protect themselves and their data with security insurance. After the Nile network went live and an insurance policy review was performed, the carrier was so impressed with the quality of the Nile Zero Trust Fabric, that SDI’s premium was lowered.

The CFO and CTO Align

It can be a difficult balancing act when it comes to sourcing infrastructure equipment as there’s a fine line between keeping networking equipment for a little bit longer and risking performance issues. Prior to the refresh, Clover was looking to upgrade a legacy switch that was severely impacting network performance, but the finance team showed that the equipment was passable by meeting the bare minimum.

Nile’s as-a-service model includes the delivery of access points and switches as they are designed to work together as a deterministic fabric. This and the fact that Nile offers an OpEx model vs a limiting CapEx model, shifted the conversations as SDI would receive the high-performance needed without

penalizing the budget.

This subscription encompasses the entire network, eliminating all capital expenditures and the unexpected costs and complexities that come with an old-fashioned CapEx model.

“Thanks to Nile, we don’t have to worry about aging infrastructure impacting our network or procuring expensive replacements. We only pay for what we use and need – not a dollar more,” says Chris Moore, SDI CEO. “Conversations with my team have now shifted from hard, inflexible CapEx costs to predictable OpEx costs that we can rely on.”