nile

Solutions Brief

Extending Zero Trust Security to the Campus and Branch

nilesecure.com

Introduction

IT organizations are being asked to build a state of security for their wired and wireless campus and branch networks where all users, devices, and applications are seamlessly protected, regardless of evolving threats, location, or role. Achieving this has been challenging as networking vendors do not traditionally build consistent security features and services into the foundation of their solutions.

As a result, networks are often brought online with security gaps where additional features and solutions are bolted-on to mitigate the risk of cyberattacks and internal compliance issues. This commonly includes RADIUS and NAC services for device authorization, VLANs for traffic segmentation, ACLs for access control, firewalls for perimeter protection, and more recently Secure Access Service Edge (SASE) and zero trust network access for remote use cases.

However, this approach adds complexity, is time-consuming, and has led to misconfigurations that resulted in an organization's security posture being compromised. With the growing use of cloud and IoT, hybrid work demands, and resource constraints, there's a pressing desire for security to be woven into the network.

Enter Nile.

Zero trust networking principles and features have been natively integrated into every element of the Nile Access Service, applying policy and security controls for every connection method, endpoint type, role, and authorization privileges. The result is a wired and wireless architecture designed to protect against any risk factors traditionally associated with legacy enterprise network infrastructure, from the tampering of an access point or IoT device to the isolation of guest traffic without complex IT or end user requirements.

The service also includes unique integration capabilities that allow network and security teams to leverage best-in-class third-party vendor solutions such as Palo Alto Networks, Okta, Zscaler, and others. This ensures that each endpoint connection and its subsequent traffic are secure within the Nile next-generation wired and wireless network, as well as when traffic is destined for the WAN and Internet.

With Nile, campus zero trust goes beyond just a set of principles – it's a practical approach that can be implemented without compromise for today's modern enterprises where every aspect of their business is in the middle of digital transformation.

Infrastructure that forms a trusted foundation

Physical protection for networks includes securing equipment under lock and key where possible, but unfortunately wireless access points are left vulnerable as they must be visible. As an industry first, Nile's campus zero trust approach starts with enterprise-grade security built into the Nile access points and switches.

- Each contains a Trusted Platform Module (TPM) with integrated cryptographic keys to prevent unauthorized access.
- Access points contain a dedicated radio to protect against rogues and to detect and prevent against wireless intrusion.
- Console ports from the Nile hardware elements so that SSH, Telnet, or other remote services cannot be used to attack the network.

For additional security, configuration of infrastructure devices is fully automated, removing the potential for human errors that can potentially create a security hole. Each device also leverages Nile's custom-hardened OS and automatic security patch updates to ensure cyber insurance, network security audit, and corporate compliance mandates are met.

Secure connectivity that delivers peace of mind

Within an enterprise or educational environment where multiple generations of digital applications are traversing the wired and wireless network, traditional VLANs, ACLs, and simple password protection are no longer adequate to meet network security requirements.

Organizations must move beyond the limitations of legacy approaches that were originally created to solve different use cases. For example, VLANs were designed to segment a network into separate broadcast domains, and then were creatively used for security use cases. Overtime, this turned out to be a significant management burden to maintain.

Instead, Nile's Access Service utilizes a per host (or endpoint) approach where all communication is limited to Layer 3 only, and eliminates the use of Layer 2 VLANs and associated use of static ACLs. All traffic is routed through an existing firewall within the enterprise IT infrastructure to prevent unauthorized access to sensitive information and protect against eaves-dropping attacks. This form of micro-segmentation offers greater protection, prevents any risk of malware proliferation, and is considerably simpler to manage across a distributed environment.

Other Nile advantages include:

- Existing third-party NAC solutions for authentication and authorization allow for certificates and multi-factor solutions in addition to passwords for added security.
- IoT devices are completely isolated as many lack strong security compared to today's computers and cellular devices.
- Optional Secure Guest Service isolates endpoints, sending traffic directly to a Nile cloud instance, eliminating the guest network from reaching internal data and resources.

Nile's campus zero trust model also ensures that every connection can be analyzed and all policies appropriately enforced, to satisfy the needs of the network and security organizations if separate.

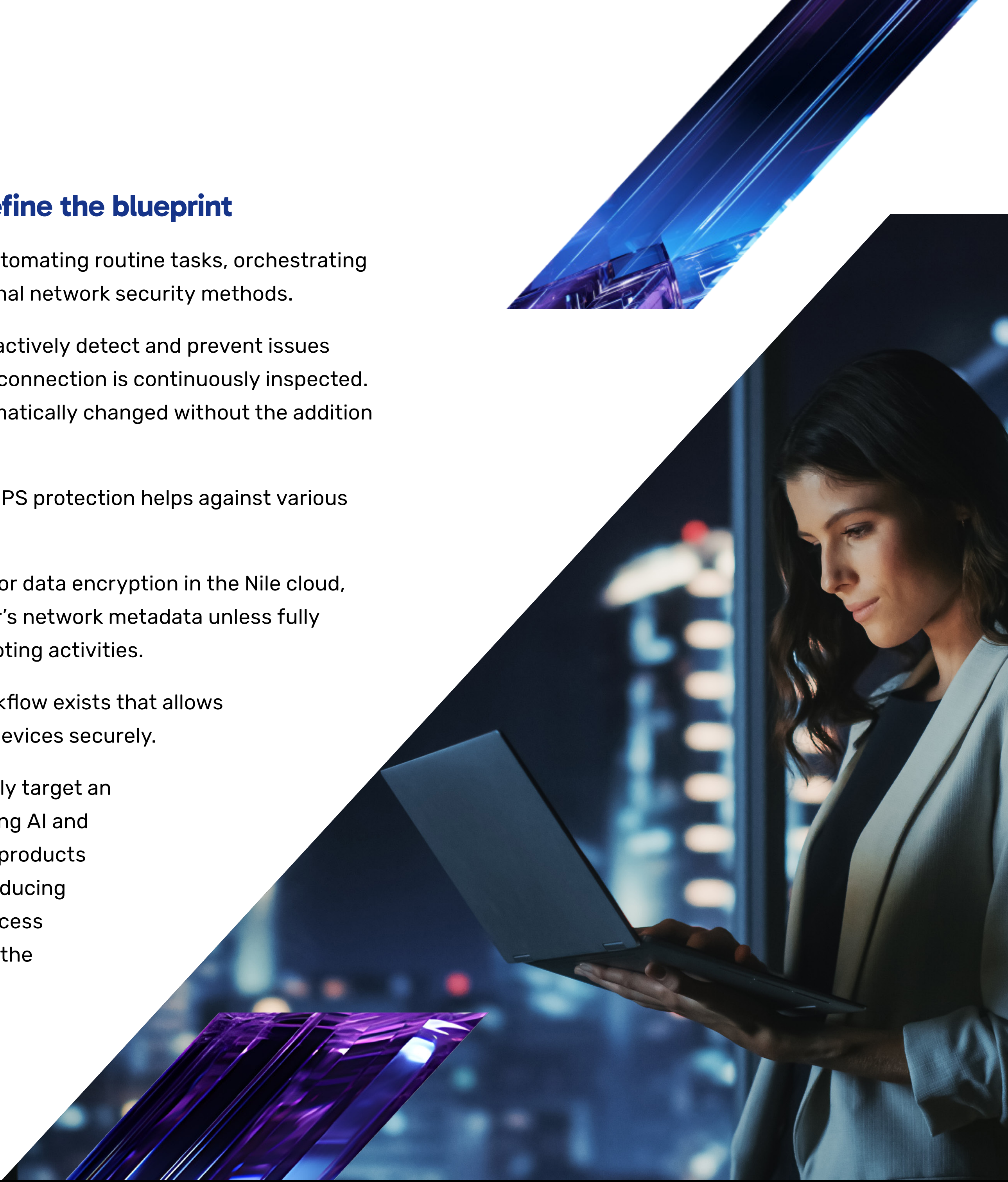
Streamlined operations where you define the blueprint

Nile streamlines network security operations by automating routine tasks, orchestrating manual security workflows, and redefining traditional network security methods.

Nile's automated approach offers the ability to proactively detect and prevent issues from escalating into incidents as traffic from each connection is continuously inspected. For instance, an endpoint's privileges can be automatically changed without the addition of a complex NAC solution.

- Full stack visibility via integrated wireless IDS/IPS protection helps against various wireless threats.
- Organizations can bring their own key (BYOK) for data encryption in the Nile cloud, ensuring that not even Nile can see a customer's network metadata unless fully authorized by the customer during troubleshooting activities.
- From an IT and user perspective, a built-in workflow exists that allows users to onboard their own endpoints and IoT devices securely.

As user behavior evolves, and attackers increasingly target an organization's network and resources, Nile is utilizing AI and automation to integrate 10+ traditionally separate products and services into a single solution - significantly reducing the potential attack surface. With an active Nile Access Service subscription, APIs and webhooks allow for the simplified integration of best-in-class third-party security solutions.



Conclusion

As organizations build or refresh their wired and wireless networks, the security profile of such infrastructure remains top of mind. Nile has extended zero trust networking principles to campus and branch locations and has eliminated the need for complex siloed solutions and vulnerable out-dated technology.

With Nile, enterprise IT teams can move beyond fragmented security and automatically instrument zero trust access and isolation for each user and device, while reducing cyber insurance costs. It's time for IT teams to explore Nile's campus zero trust approach to seamlessly protect their organization's resources, data and reputation.

To learn more, view Nile's White Paper on the same topic.

> "As part of renewing our insurance, the carrier reviewed our network security and were so impressed with the quality of the Nile network, they actually lowered our premium."
>
> **Neil Clover**
> CTO at SDI

nile

hello@nilesecure.com | **nilesecure**.com