4 APPROACHES TO LOWERING CYBER SECURITY INSURANCE PREMIUMS

Cyber Security Insurance Advantages by Extending Cloud Security to Enterprise Campus and Branch Networks

nile

nilesecure.com

Table of Contents

1. ZERO TRUST PRINCIPLES 04

2. ZERO TRUST ISOLATION 05

3. ENDPOINT DEVICE SECURITY 06

4. SECURE GUEST ACCESS 07

OVERVIEW

Today's networks and technology open up a world of possibilities, while also raising concerns. The premiums for cyber security insurance, also known as "cyber risk insurance" or "cyber liability insurance," have increased from years past based on evolving cyber incidents and larger payments made to bad actors. In part due to uncontained lateral movement, and increasing data breaches and successful phishing and ransomware attempts.

Cyber insurance companies now carefully vet an enterprise's network infrastructure and overall security implementation, its active configuration, and ongoing operations to ensure adherence to strict compliance requirements. In fact, acquiring cyber security insurance is increasingly challenging today as some insurers require 40 pages of supporting information versus 1 page years ago.

Security advancements that help protect data and resources, while minimizing risk are an advantage. Even though remote work has proliferated, the threat vector for wired and wireless networks within campus and branch locations remains as risky as ever. We've seen a shift of moving security to the cloud, datacenter and endpoint, but the campus network remains the easier target. In either case the network plays a role.

Compared to legacy methods where bolted-on tools are added to an existing enterprise IT infrastructure, Nile has taken an entirely new approach. We have integrated zero trust security principles that were born in the cloud into campus and branch wired and wireless deployments. This modern approach extends from the individual network elements themselves and how they are configured, to the way a network is constructed, the data associated with the network and how end user traffic flows are handled.

> **Lateral movement is not a niche issue: it is present in roughly 60% of attacks, and over 80% of attacks used privileged access. 54% of the techniques and tactics used to execute testing of lateral movement are missed.**
>
> Mandiant Security Effectiveness Report

1 ZERO TRUST PRINCIPLES

What is zero trust in networking and why is it important for a campus? The goal is to take zero trust principles, apply them to campus and branch networks, and allow customers to consume security versus buying add-ons and engineering it into the network on their own. The three main principles to look for are end-to-end encryption, authentication of every connection, and the authorization of every request.

At the foundation of Nile's zero trust campus solution, we have eliminated console ports on our access points and switches to prevent unauthorized access. Additional security measures include:

- Each access point and switch contain tamper proof technology to ensure that only authorized users have access.
- A secure boot is used that eliminates human interaction and the possibility of errors.
- Automated updates to ensure all customers are using Nile's latest software and security patches.

Upon activation, each Nile network device uses certificates to verify that they are connected to other Nile devices, as well as to the Nile Services Cloud. For added security, all device management and control traffic is encrypted.

For wireless security, each of Nile's access points include a dedicated radio for wireless intrusion and prevention (WIPs/WIDS) containment.

2 ZERO TRUST ISOLATION

Due to growing cyber security concerns tied to lateral movement within a campus LAN, every end device is completely isolated by default using next-generation security practices. All endpoint devices are isolated and their traffic encrypted and inspected as a standard practice. This removes the risk of a breach extending beyond a single device as the Nile Access Service eliminates lateral movement by design.

This modern approach to network and device security delivers a consistent framework using zero trust security principles that were born in the cloud, enabling enforcement in Layer 3 (L3) for all devices within an IP address scheme. Without authorization and authentication, no device is allowed to receive an IP address to mandate secure onboarding of any mobile or IoT device, for any wireless and wired devices.

We've taken a common datacenter construct that provides security and isolation that can now be realized across the access network to deliver similar outcomes - all consumed without additional complexity.

Nile also shares valuable user and endpoint device data with firewalls and other security solutions for policy decision processing and enforcement, as a standard practice. This integration extends the value and protection offered by Nile to other solutions within a customer's environment.

Through the use of modern principles, the Nile Access Service offers greater visibility and control, while eliminating the security challenges found in traditional switching architectures. Gone are the legacy protocols and design principles originally used in competitor's architectures meant to split up an oversubscribed network segment.

About 40% of organizations have deployed a zero-trust security architecture; those that have done so spend an average of 20% less to mitigate a data breach.

Cost of a Data Breach Report, IBM, 2023

IBM

3 ENDPOINT DEVICE SECURITY

From the perspective of users and endpoint devices such as laptops, phones and IoT, we have standardized on identity-driven access. There is no unauthenticated access allowed and unlike older network access control (NAC) systems that operate independently from the main network traffic, Nile uses a model that initiates continuous authentication requests within the traffic stream. Additionally:

- All endpoint device traffic is encrypted.
- The fingerprinting of devices is built in and a standard feature.

There is no need to introduce a secondary solution for the visibility required for granular policy creation offered via fingerprinting. Legacy or existing security solutions are supported to provide needed flexibility where required.

4 GUEST ACCESS

The expectation of accessing the Internet from anywhere also presents a certain risk that organization's must contend with today. The open nature of a guest network poses the following challenges:

- Difficulty in differentiating between an actual visitor from someone with malicious intent.
- Legacy designs that expose guest users to malicious activity.
- A misconfigured authorization rule that can easily expose corporate or business traffic to users on the Guest network.

Because you are liable for what guests do from your network out to the Internet and for ensuring your internal network is not exposed to guests and visitors, Nile's standardized isolation model for all connections provides a guest access advantage. In essence, our elimination of lateral movement is extended to the guest network by default.

An optional Secure Guest Service offers even greater security in that all traffic is forwarded to a Nile point of presence (PoP) and applied policy rules before reaching its final destination. There is zero access to the internal network, traffic is tunneled, and requires no traffic engineering, which means no chance of misconfiguration and errors.

Nile's DHCP service is included as part of the Nile Guest Service for added IP address allocation and management security. And, in the event of copyright issues originating on the guest network, IT organizations gain the added benefit of offloading to Nile for Digital Millennium Copyright Act (DMCA) occurrences.

In summary, the very core of the Nile Access Service adheres to strict zero trust security principles for the campus and branches. Additionally, the elimination of manual tasks prevent operator configuration errors that lead to increased security risk.

Nile's zero trust campus solution raises the bar regarding security and compliance based on the latest network security principles, policy enforcement, and control. And, partnerships with leading third-party security solutions ensure that the Nile Access Service offers an uncompromised foundation for securing all of your user and IoT use cases.

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

nile

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

(669) 369-6453

info@nilesecure.com
nilesecure.com