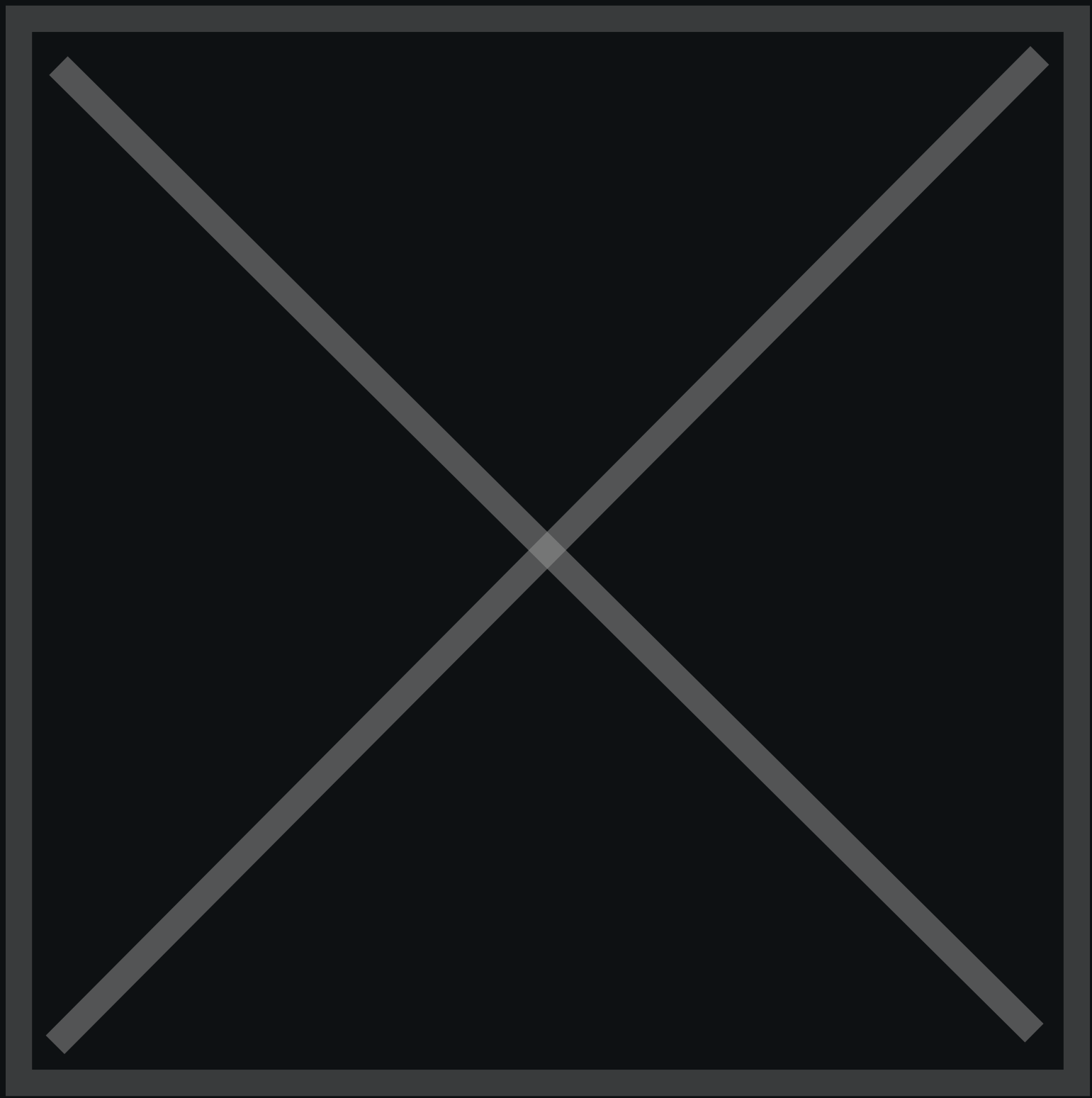

nile

Zero Trust Security. Design Without Complexities

17M

new malware detected every month[1]

95%

of cyber security breaches are a direct result of human error[2]

$6.9B

Total loss in 2021 from cyberattacks in the US[3]

A big network problem

The growing network infrastructure within a business has enabled malicious actors to level up the frequency and sophistication of their attacks, breaching even a strong security defense.

Cloud adoption, the explosion of IoT/BYOD devices, and a hybrid workforce have introduced new attack vectors. This adds to an ever-growing list of physical and cyber vulnerabilities for hackers to exploit using attack techniques like social engineering, snooping, sniffing, and Man-in-the-Middle (MitM).

Holistically secure network

Nile has holistically engineered from the start to have security natively built into the network with zero security configurations needed from SecOps.

This means from the moment the customer brings up the service, they can enjoy aspects like automated security patches, protection against rogue devices, and protection from sniffing/snooping. All designed to protect your business from any disruptions using a blackbox architecture.

Engineered around Zero Trust

Zero Trust Access

Providing authentication mechanisms for all users and devices across wired and wireless networks can be frustrating and overly complex. Zero Trust Access delivers a simplified and unified access approach by delivering functionalities like 802.1X, MAB, and SSO, for both wired and wireless networks. Always available and enabled on every component of the Nile service.

Zero Trust Network

Securing the network traditionally usually resulted in making a complexity vs risk tradeoff. Zero Trust Network by Nile protects data by default by ensuring all components powering the network infrastructure are authenticated and the data passing through the service are encrypted end-to-end to protect against attacks like MitM.

Zero Trust Isolation

When trying to protect users and devices from malware and malware proliferation, security teams often had to bolt on multiple security products or implement inconsistent security configurations to gain visibility and control. With Zero Trust Isolation, every connection flows through a central policy enforcement point. Zero configurations needed.