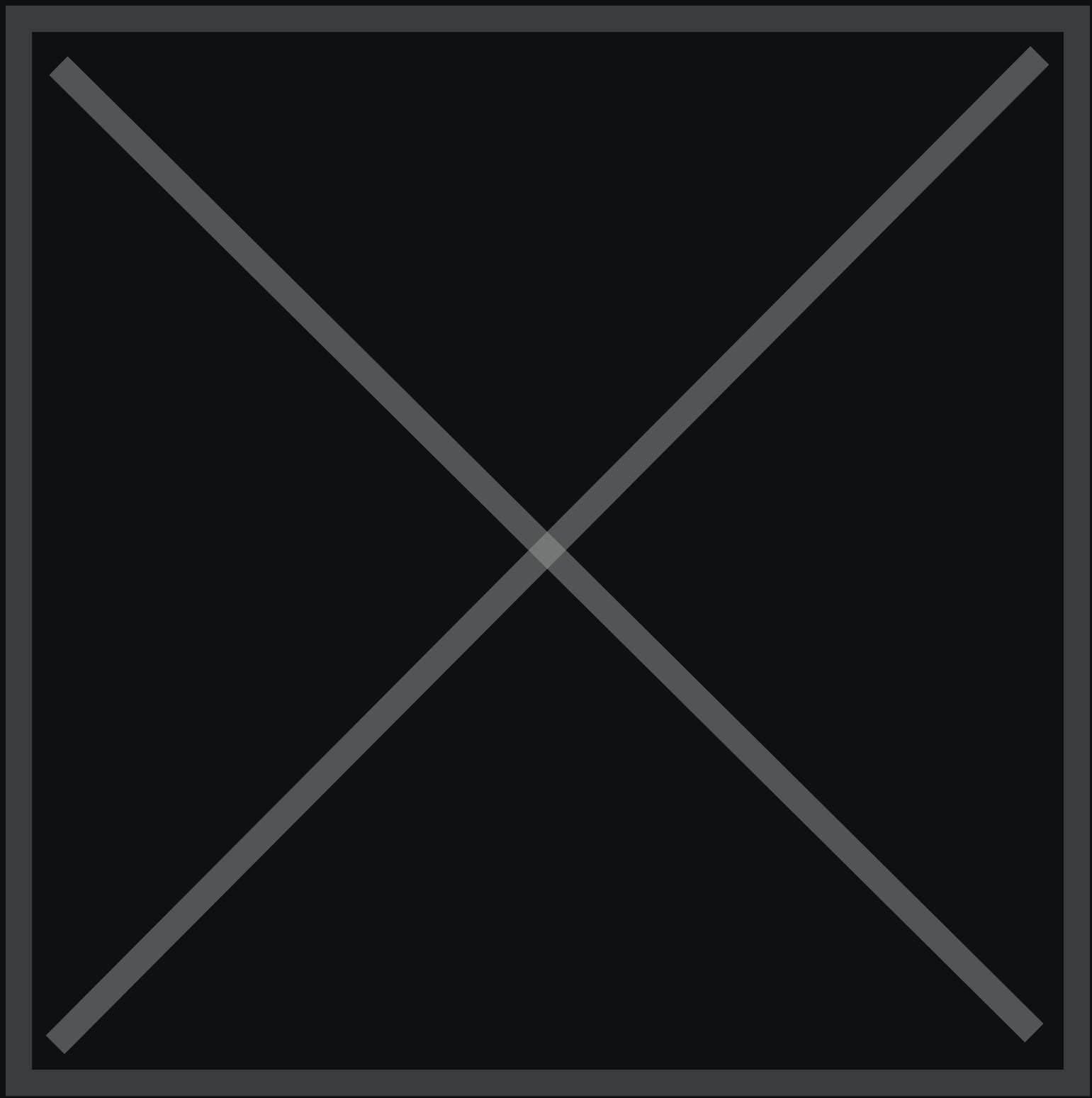

nile

The Top-5 IT Pain Points And How Nile Solves Them

5

Software Updates & Security Patches

Software updates are an inevitable truth. Similar to security patches, they are scary to implement. Any change to the network causes consternation: “will this impact the performance of my network, will something break?” The natural reaction is to avoid these software updates, which contribute to potential poor performance for enterprise networks.

NILE’S SOLUTION

All software updates are performed in-service thanks to Nile’s use of microservices based cloud software and agile software development principles. Gone are the days of procrastinating network updates out of fear of possible performance impacts.

4

Performance Needs vs. IT Budget

There is always the negotiation between the network performance needs and available capital as part of the IT infrastructure budget. When they are not aligned, performance, security and operations for your enterprise network suffers.

NILE’S SOLUTION

With Nile, whatever the site survey results mandate for high performance and secure connectivity, that’s what you will get. With no upfront capital expenditure required, a Nile network will deliver guaranteed coverage, capacity and availability with monthly billing based on a per-user or per-square-foot pricing.

3

Attracting and Retaining Expertise

Attracting expertise for enterprise network engineering, security and operations is becoming more difficult every year. And, leveraging the strategic value of those experts on long hours of manual configuration, system setup, network troubleshooting delivers low ROI.

NILE’S SOLUTION

With the Nile Access Service, we share the responsibility of guaranteed network performance with our customers. With traditional lifecycle management operations automated in software, IT organizations get to eliminate the traditional burden of network operations and focus on items that deliver strategic value to their critical IT initiatives.

2

Being Ready for Advanced Threats

There are too many ways to attack the network and hold companies hostage. From vulnerable IoT devices, to using social engineering to gain access to the network, and to infecting employee devices in order to initiate malware and ransomware attacks.

NILE’S SOLUTION

A Nile network extends the principles of zero trust security to campus and branch locations. With Nile, every connected device is isolated from each other preventing any present threats from moving laterally from device to device. Network security teams retain full control over policies, easily translating user, device, and app specific rules to network enforcement.

1

Tackling Inefficiency and Complexity

Traditionally, enterprise access networks are delivered as a package of 10+ separate products, each delivered as a self-contained technology in separate boxes. Each product requires a multitude of SKUs to choose from, software releases to keep track of, and advanced licensing requirements to invest in. Vendors offering these legacy solutions ask for additional taxes in the form of consulting, professional, support and financial services to ease the pain around this inherent inefficiency.

What if this complexity did not exist in the first place?

NILE’S SOLUTION

A Nile network experience is completely simplified, inclusive of Day -1 to Day N operations. From site survey to install to refresh, Nile Access Service integrates lifecycle management services as part of its full wired and wireless enterprise network tech stack.