

## Introducing a Brand New Monthly Newsletter from Nile

The edge has quietly become the most exposed (and most overlooked) part of the enterprise.

Users, devices, IoT, and agentic AI are everywhere. But the architecture protecting them hasn't kept up leading to breaches, complexity and cost escalations.

Many organizations are looking for a clean-slate approach. Nile is delivering it.

The **Secure Edge** newsletter is where we provide thought leadership content, best practices and discussions that are at the epicenter of this tectonic shift.

## Thought Leadership

### Nile Brings Data Center-Class Security to the LAN reducing breaches by over 60%

On March 19th, Nile announced several industry-first capabilities based on zero-trust and identity centric microsegmentation providing lateral security in the LAN.

These reduce breaches, risk and costs.

[Read more →](#)



### Nile 2.0: Bringing Trust to Zero Trust

Nile was founded to bring radical simplicity to enterprise networks. This is the foundation for delivering zero trust security and autonomous operations powered by AI.

Nile 2.0 is about scaling security, rethinking the model entirely, enforcing identity before connectivity and eliminating the need for bolt-on controls like NAC.

[Read the blog →](#)

## Industry Perspective: Secure Networking is Being Rebuilt



The shift is becoming clear across the industry: security and networking can no longer operate as separate layers.

Coverage from Network World and The Fast Mode highlights how integrated microsegmentation, native access control, and autonomous operations are reshaping what modern networks look like.

[Read the coverage from NetworkWorld →](#)

[Read the coverage from The FastMode →](#)

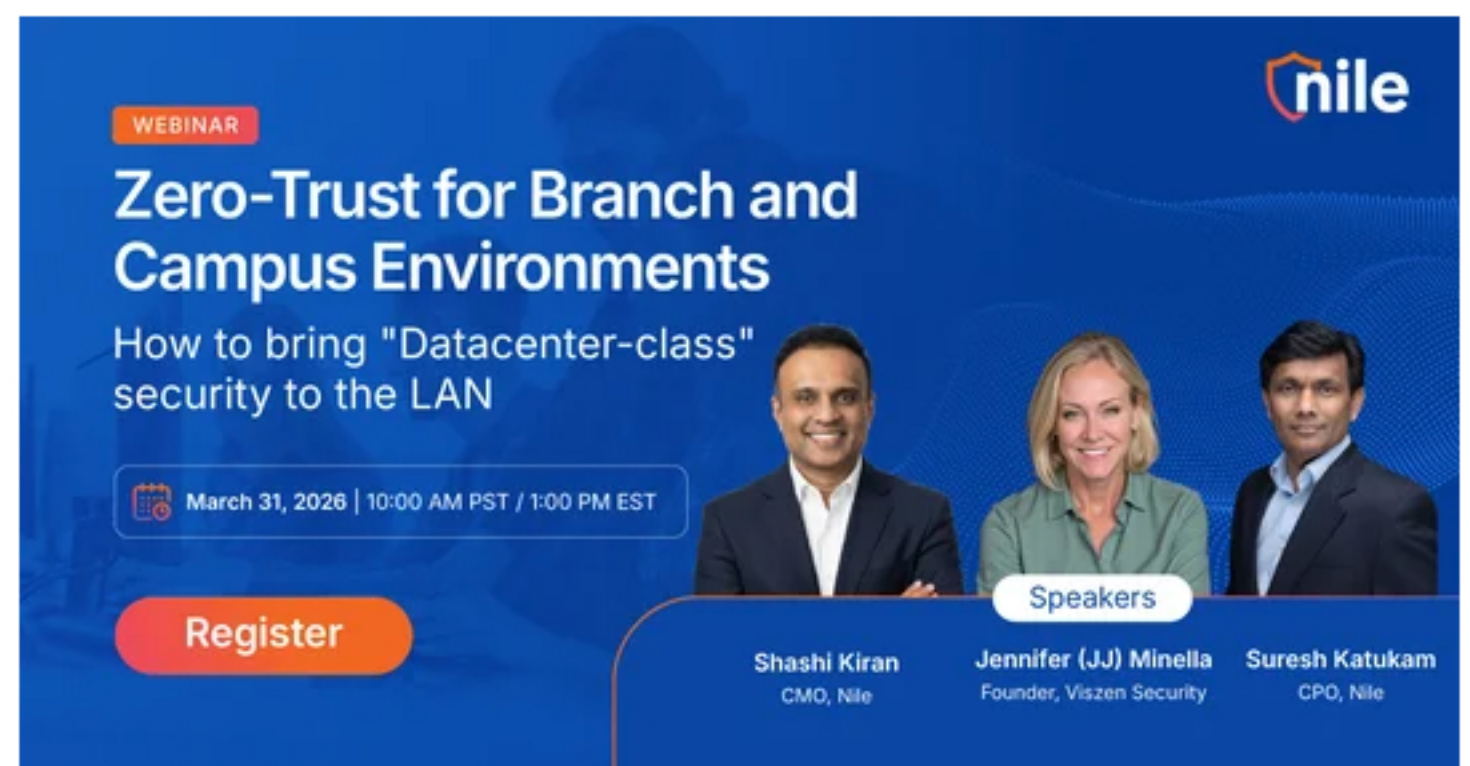
## Webinars

### Now Available On-Demand: Zero Trust for Branch and Campus

What does Zero Trust actually look like in the LAN?

This session breaks down the real attack surface and how a modern architecture eliminates complexity while improving security outcomes.

[Watch on-demand →](#)



### Why IoT/OT Is Your Biggest Security Blind Spot



IoT and OT devices are now one of the largest—and least protected—entry points into the enterprise.

Legacy networks were never designed to secure them.

This session explores how to move beyond fragmented controls and enforce identity-based security for every device, eliminating lateral risk and reducing complexity at the same time.

[Register here →](#)

## Events

### RSAC 2026

RSAC made one thing clear: AI is no longer a side conversation. It's becoming central to how networks are built and operated.

But while many are still talking about AI as an add-on, the real shift is happening deeper in the architecture.

At the booth, the conversation wasn't about layering in more tools. It was about what happens when the network itself becomes autonomous: continuously optimizing, enforcing policy, and reducing operational burden in real time.



## Security Advisory

### AirSnitch Wireless Vulnerability



Recent research uncovered a new Wi-Fi attack vector but more importantly, it exposed how much traditional networks still rely on outdated trust assumptions.

Learn why Nile is inherently protected against this class of attack due to its identity-based architecture.

[Read the advisory →](#)