LOXADA™

SAFE, SECURE, REMOTE

WHITE PAPER

# **Securing the Uncontrolled Network Edge:** Why Traditional Cybersecurity Measures Can Fall Short and What to Do About It

## Executive Summary

The rapid growth of remote and hybrid working has reshaped the cybersecurity landscape, bringing critical vulnerabilities into sharper focus, specifically, the uncontrolled network edge. This refers to networks and devices beyond the direct management of internal IT teams, including home networks, unmanaged office setups, and IoT devices used to access corporate resources.

Traditional security tools, such as VPNs, Zero Trust frameworks, endpoint security, and SASE solutions, were not designed to secure these unmanaged environments. As cyber threats targeting these areas increase, organizations must secure this overlooked frontier directly.

> “More than half of devices accessing enterprise networks are unmanaged; operating outside direct IT control.”
>
> Source: Telefónica Tech

## **Introduction:** The Uncontrolled Network Edge Explained

The uncontrolled network edge comprises personal or third-party managed networks and devices that employees, contractors, or partners use to access data and organizational resources remotely.

With remote data and system access now commonplace, organizations often unknowingly rely on insecure home routers, third-party networks outside their direct control, public Wi-Fi, and IoT-heavy environments, all of which significantly expand their attack surface whilst being beyond their ‘reach’.

Global cybersecurity authorities, including CISA, the UK’s NCSC, and Australia’s ACSC, have raised alarms about this increasingly targeted threat landscape, highlighting the necessity for immediate action.

> “Corporate access points now extend far beyond traditional IT oversight, significantly widening the attack surface”
>
> Source: Spectrum Enterprise

## 1. Why Existing Security Frameworks Fail

**Traditional cybersecurity tools leave critical gaps at the uncontrolled edge:**

**VPN Limitations:**
VPNs offer broad access to corporate networks once authenticated. However, exploits like TunnelVision (CVE-2024-3661) allow attackers to bypass VPN encryption entirely, underscoring that VPNs secure connections, but not the environments from which they originate. (Source: Zscaler)

**Endpoint Blind Spots:**
Endpoint protection secures user devices but cannot address vulnerabilities in underlying infrastructure, such as compromised routers or IoT devices, which remain invisible to typical endpoint security measures. (Source: NinjaOne)

**Zero Trust Shortcomings:**
Zero Trust models rely on reliable contextual data; however, compromised home networks can provide false or tainted information, thereby undermining trust verification. (Source: Microsoft Learn)

**SASE Limitations:**
SASE secures paths to applications but remains infrastructure-agnostic, primarily at the local network layer, and is unable to prevent compromised networks and devices from manipulating traffic. (Source: ZPE Systems)

## 2. Emerging Threats Targeting Edge Devices

**Attackers increasingly exploit vulnerabilities in devices at the uncontrolled edge:**

**Home and SOHO Routers:**
Often insecure by design, these devices have vulnerabilities actively targeted by state-sponsored actors. The Volt Typhoon attacks leveraged compromised SOHO routers to infiltrate critical infrastructure. The persistent vulnerabilities and lack of automated firmware updates further exacerbate these risks.

**IoT Devices:**
IoT devices often present widespread vulnerabilities, including default credentials and infrequent updates, making them prime targets for large-scale botnet recruitment (e.g., Mirai). Compromised IoT devices can be gateways into corporate networks, providing attackers easy pivot points.

These examples highlight the systemic nature of uncontrolled edge threats, demonstrating that isolated measures are insufficient.

## 3. The Human Factor

Human behaviour significantly compounds technical vulnerabilities at the uncontrolled edge. Limited cybersecurity awareness, weak passwords, neglected firmware updates, and poor security hygiene amplify risks, creating easily exploitable pathways.

> “Human errors amplify technical vulnerabilities, creating easily exploitable pathways.”

SOURCE: INFOSEC INSTITUTE

Organizations must address the human factor through consistent and comprehensive training and awareness initiatives.

## 4. Why 'Secure by Design' is Critical

> **"Secure by Design" principles require security to be built into products from the outset. Despite clear guidance from authorities, many consumer-grade routers and IoT devices continue to ship with fundamental flaws. Over 80% of off-the-shelf routers remain vulnerable despite regular updates."**

SOURCE: PACKETLABS

There is a substantial gap between recommended best practices and real-world device manufacturing, underscoring the need for inherently secure, managed solutions. Regulatory and industry pressures are increasing on manufacturers to adopt secure-by-design practices more comprehensively.

## Recommendations:
## How to Secure the Uncontrolled Network Edge

**To effectively secure this overlooked area, organizations should:**

01 **Deploy Secure Routers with Managed Firmware:** Replace consumer-grade routers with enterprise-grade, securely managed solutions to protect at the network level.

02 **Extend Visibility into Uncontrolled Environments:** Gain visibility and control of remote networks through centrally managed infrastructure and proactive monitoring.

03 **Implement Comprehensive Employee Training:** Provide clear and concise training that emphasizes router security and best practices in environments outside the organization's direct control.

04 **Integrate Network Edge Security into Zero Trust and SASE Models:** Ensure Zero Trust and SASE architectures include securing local network infrastructure as a fundamental component, embedding network edge security into broader cybersecurity strategies.

05 **Conduct Regular Risk Assessments:** Continuously assess exposure by regularly auditing network edge environments and adapting policies and solutions accordingly.

## Practical Checklist:

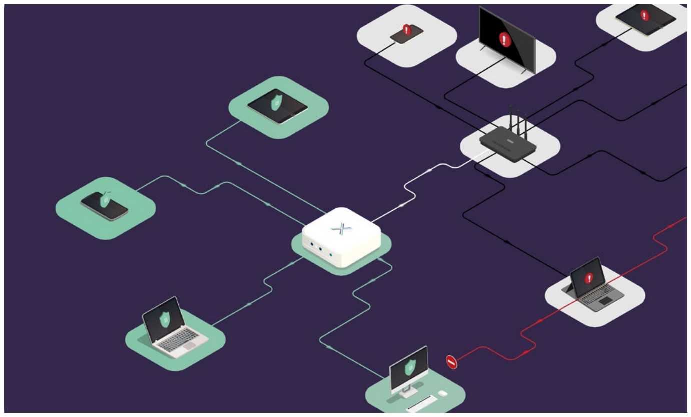
- ✓ Do you have visibility into the networks and routers outside your control that employees use?
- ✓ Are secure, managed routers provided to employees that connect to your data and systems from unknown networks?
- ✓ Do your security frameworks explicitly address home and third-party networks?
- ✓ Are your staff trained regularly in router and IoT security practices?

## Conclusion

Securing the uncontrolled network edge isn't optional. It's essential.

The combination of vulnerable network devices, inadequate traditional cybersecurity frameworks, and increasing human error creates a dangerous trust vacuum. Organizations that recognize and act upon these challenges now will be best positioned to protect their critical data and infrastructure.

**For a straightforward discussion on securing your uncontrolled network edge, contact Loxada today.**



> "Securing the uncontrolled network edge isn't optional. It's essential."