

Securing the Last Mile

Executive Summary

In today's digital landscape, with the dissolution of traditional network perimeters, organizations have widely adopted Zero Trust architectures to secure their data and systems. However, a critical vulnerability often remains unaddressed: The Last Mile and the Access Point (AP) through which remote and hybrid employees connect to organizational resources and the wider Internet. While not overlooked, this aspect of network security is presumed to be beyond an organization's control and therefore, not addressable. This white paper challenges that presumption, explaining how Zero Trust principles can and must be extended to securing this fundamental element in the network connectivity chain.

Organizations whose employees connect remotely face a myriad of threats. These range from rogue networks luring unsuspecting remote employees to sophisticated and targeted attacks that take advantage of vulnerabilities and protocols in cellular networks, and of course, human error. We examine the threats emanating from Last Mile connectivity and infrastructure: unknown APs, uncontrolled WiFi, public networks, mobile network operators (MNOs) and discuss Klök's solution for addressing these threats.

Introduction: The Rapidly Dissolving Network Perimeter and the Gauntlet at the Edge

The traditional network security model, often described as a "castle and moat" approach, has become obsolete in recent years. This model, reliant on securing a well-defined network perimeter, fails to address

the realities of modern enterprise IT environments and the full scope of threat vectors facing organizations from remote connections.

The following factors have contributed to the dissolution of the traditional network perimeter and a geometric increase in the attack surface:

- **Cloud Computing:** The widespread adoption of cloud services has moved critical data and applications outside the organization's physical infrastructure.
- **Mobile Devices:** The proliferation of smartphones and tablets has created a vast array of endpoints accessing corporate resources from anywhere.
- **Remote Work:** The global shift towards remote and hybrid work models has further blurred the lines between corporate and non-corporate networks.

The "Last Mile" of connectivity refers to the final leg of the network connection between the end-user device and the broader internet or corporate network. This Last Mile ordinarily involves connecting through various public and shared networks and APs that are traditionally outside and therefore, beyond the organization's control. They include among others:

- Public WiFi networks in cafes, airports, and hotels
- Home WiFi networks
- Mobile Network Operators (MNOs), especially when roaming

Because remote workers use public and shared network infrastructure in disparate locations to remain productive, organizations must instead adopt an "elastic" and comprehensive approach to security that protects employees, data and resources regardless of where they are accessed from, rather than rely on securing a single, well-defined network boundary.

The following are examples of the threats faced by organizations from remote workers:

- **"Evil twin" WiFi attacks:** Malicious actors set up fake WiFi access points at expected locations such as airports or hotel that mimic legitimate networks to lure employees and intercept data.
- **Lateral attacks through malware:** Compromised devices on shared networks can spread malware (or worse) to systems and other connected devices. An example might be a consultant whose compromised device accesses and infects their client's network.
- **Man-in-the-Middle Attacks:** Attackers can potentially intercept and manipulate traffic.
- **Malware Injection:** Compromised APs and networks can be used to distribute malware to connected devices and infect systems.
- **Data Theft:** Sensitive corporate data can be exposed when transmitted over these networks.
- **Rogue Access Points:** In the case of WiFi, fake networks (similar to Evil Twin) are easily set up to trick users into connecting.
- **Human Error:** Accidental or engineered by malicious actors to induce human targets to connect to

rogue APs.

Additional risks when relying on MNOs include:

- **IMSI (International Mobile Subscriber Identity) Tracking and Location Privacy:** MNOs necessarily track the location of devices connected to their networks using the IMSI. This information can potentially be accessed by malicious actors, leading to:
 - **Physical Security Risks:** Users' real-time and historical locations can be tracked, posing a significant threat to personal safety, especially for high-profile individuals or those working with sensitive information.
 - **Corporate Espionage:** Tracking patterns of employee movements could reveal sensitive business activities or partnerships.
 - **Privacy Violations:** Detailed location data can provide insights into personal lives, routines, and associations.
- **IMSI Catchers (Stingrays):** The cellular equivalent of Rogue Access Points, they mimic legitimate cell towers and can force nearby mobile devices to automatically connect allowing attackers to:
 - Intercept communications by forcing changes in the security protocol of the connecting device
 - Track precise user locations
 - Potentially manipulate or block communications
- **SS7 and Diameter Protocol Vulnerabilities:** These foundational protocols in telecom networks have known weaknesses that can be exploited by sophisticated attackers:
 - **SMS Interception:** Attackers can potentially intercept SMS messages, including those used for Multi-Factor Authentication (MFA).
 - **Call Redirection:** Incoming and outgoing calls can be redirected to attackers.
 - **Location Tracking:** Like IMSI tracking, these vulnerabilities can be exploited to determine a user's location.
 - **MFA Compromise:** By intercepting SMS-based MFA codes, attackers can bypass this critical security measure, potentially leading to account takeovers.
 - **Zero Day Attacks:** Make use of network tools and protocols to inject malware or exploit vulnerabilities of targeted devices.

The sheer variety and sophistication of these threats underscore the need for a comprehensive solution that can reduce the attack surface and make employee devices less visible and thus less vulnerable.

To effectively combat these threats, the solution must:

- Make employee devices less visible to public networks and MNOs, and thus less vulnerable to attack.

- Reduce organizations' attack surface by minimizing the profiles and number of potential entry points for attackers.
- Enable control of the APs and enable remote independent provisioning of the network(s) employee devices connect through to reach organizational resources and the wider Internet.
- Remote Route network messages to and meta-data from, in a manner that keeps users protected from digital and physical attacks.

Klōk has developed such a solution in an integrated portable AP that eliminates the need for employees to connect their devices to public or shared WiFi, or to an MNO, thus rendering employee devices both immune and invisible to infected or malign APs. Its advanced cellular and routing technology provisions service independently of the MNO, prevents tracking (even by MNOs) and protects users from network-based attacks using Zero Trust principles.

Understanding the Zero Trust Architecture and Its Application to Last Mile Security

Zero Trust is a security model that addresses the limitations of traditional perimeter-based security by operating on the principle of “never trust, always verify.” This approach assumes that no user, device, or application should be trusted by default, even if they are within the corporate network perimeter.

Key principles of Zero Trust include:

- Verify explicitly: Always authenticate and authorize based on all available data points.
- Use least privilege access: Limit user access with Just-In-Time and Just-Enough-Access (JIT/JEA).
- Assume breach: Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to gain visibility on threats.

While many organizations have begun implementing Zero Trust models, these implementations often focus on securing access to applications and data, neglecting crucial aspects of vulnerability: the AP and the network connection itself. This oversight leaves remote workers vulnerable to the range of threats (and then some) discussed above.

Extending Zero Trust to the Last Mile (ZTLM): The Klōk Solution

Adapting these principles to encompass remote connectivity, including connections through MNOs, means that to truly implement comprehensive Zero Trust, organizations must:

- Adopt a mindset that treats all networks as potentially hostile, compromised or at least vulnerable, including home WiFi, public WiFi, and even MNOs' cellular networks (especially when roaming).
- Have no reliance on any single MNO or uncontrolled AP.
- Implement strong independent authentication and independent provisioning for all network connections, regardless of the underlying infrastructure employees connect through.

- Have visibility and control over the entire path from the end-user device to the AP to corporate resources, independently of any network infrastructure used.
- Reduce the attack surface by minimizing the number of potential entry points for attackers.
- Making employee devices less visible and less vulnerable to attack.
- Persistent authentication of the APs used by employees to access network resources.
- Provision APs and Last Mile services with JIT/JEA on an “as-needed” basis to relevant network resources.
- Eliminate opportunity for human error (and the need for training) by controlling connectivity and cyber-security remotely.

Klōk’s solution addresses these requirements by providing a secure, remotely controllable “connectivity hub” that as the AP for employees’ devices, provides the Last Mile connection, is a gateway between the organization and the resources accessed and protects users from being tracked and located, among other things.

- Creates a secure, isolated and controlled network connection for each remote worker, regardless of their physical location worldwide, or the network they’re connecting through.
- Implements granular access controls and security policies on the AP and at the network level, ensuring consistent security.
- Monitors, manages and provisions all remote connections and all APs from a central platform, providing visibility and independence that’s impossible when relying directly on MNOs or other last-mile providers.
- Ensures consistent security measures across all remote APs, eliminating the variability introduced by different manufacturers, firmware, configurations and network providers.
- Implements real time multi-network Last Mile to Edge provisioning to fragment traffic and meta-data across multiple MNOs.
- Protects against IMSI tracking and IMSI catcher attacks by:
 - Implementing dynamic IMSI rotation
 - Using advanced and post quantum techniques to obfuscate content and metadata
 - Providing alerts for suspected IMSI catcher presence
 - Offering options for anonymous connectivity that doesn’t expose the user’s real IMSI to the network
- Mitigate risks associated with SS7 and Diameter protocol vulnerabilities:
 - Implement alternative MFA methods that don’t rely on SMS.
 - Provide secure communication channels that bypass cellular networks’ delivery protocols for

sensitive token exchange or authentications.

- Offer real-time monitoring and alerts for SS7 or Diameter-based attacks.
- Enable rapid response and isolation of affected APs and devices if an attack is detected.

By taking control of the APs and by provisioning MNO services, organizations control the Last Mile to their remote employees and mobile connections anywhere, worldwide and render their network perimeter elastic while wrapping employees in a “bubble” that achieves end-to-end Zero Trust security for the organization and its distributed workforce.

Implementing Last Mile Zero Trust with Klōk

ZTLM is a paradigm shift in how organizations manage remote connectivity, but its implementation is straightforward. The core of this implementation revolves around the Klōk secure connectivity hub and its supporting cloud infrastructure as the AP, gateway and the Last Mile to the Internet:

- Deploying Klōk Secure Connectivity Hubs:
 - Provide each hybrid worker with their own dedicated hub.
 - The hub becomes the sole means for an employee to connect work-related devices to the Internet, significantly reducing the attack surface.
 - Cloud Infrastructure Setup:
 - Multi-tenant Cloud Option (Klōk as a service):
 - Utilize the pre-configured, multi-tenant Kubernetes environment hosted in Klōk’s secure cloud.
 - Train IT teams on using the web interface / API to manage their organization’s section of the secure cloud’s multi-tenant environment.
 - Single-tenant Cloud Option (on Prem):
 - For organizations requiring dedicated infrastructure, rapidly deploy the solution into their preferred cloud environment (e.g., AWS, Azure, Google Cloud).
 - Provide IT teams with documentation and training for seamless integration with their existing cloud infrastructure.
- Device Distribution Plan:
 - Conduct a Needs Assessment:
 - Determine the total number of users requiring hubs.
 - Identify the geographic distribution of users to ensure appropriate coverage.
- Mobile Services Provisioning Strategy:

- Develop a plan for acquiring the necessary SIM cards.
- Consider multi-carrier agreements to ensure optimal coverage across all required geographies to optimize cost.
- Negotiate bulk purchasing agreements with mobile network operators to optimize costs.
- Establish a process for managing, activating tracking and auditing SIMs, including handling of roaming agreements where necessary.
- IT Team Training:
 - Managing the hubs through the web interface or API.
 - Deploying and managing the single-tenant solution in their cloud environment (if chosen).
 - Implementing security policies and configurations.
 - Monitoring and responding to alerts and events.
 - Troubleshooting common issues and performing updates.
 - Manage escalations to Klōk NOC.
- Policy Development and Enforcement:
 - Create comprehensive security policies that mandate the use of the secure connectivity hub for all work-related network access.
 - Develop guidelines for employees on proper use and handling of the hub.
 - Configure policies within the cloud management interface to enforce security standards across all hubs.
- Integration with Existing Security Infrastructure:
 - Integrate the secure connectivity hub system with existing security information and event management (SIEM) systems.
 - Ensure compatibility with current identity and access management (IAM) solutions.
 - Utilize APIs to enable seamless data flow between the hub management system and other security tools.
- Monitoring and Management Setup:
 - Configure the cloud-based management console to monitor all secure connectivity hubs.
 - Set up alerts for any anomalies or attempted policy violations.
 - Establish protocols for IT teams to respond to alerts and manage devices remotely.
- User Education and Training:

- Conduct training sessions for all hybrid workers on using the secure connectivity hub.
- Educate employees about the risks of connecting through unsecured networks and the importance of using the hub exclusively for work-related activities.
- Operations Plan Development:
 - Distribution Strategy:
 - Determine the most efficient method for distributing secure connectivity hubs to all hybrid workers.
 - Consider factors such as geographic dispersion of workforce, shipping logistics, and local regulations.
 - Establish a process for tracking hub distribution and ensuring all workers receive their devices.
 - Loss and Replacement Policies:
 - Develop clear policies for reporting lost or damaged hubs.
 - Establish a streamlined process for quickly replacing compromised or non-functional hubs.
 - Implement security protocols to remotely disable lost hubs to prevent unauthorized access.
 - Create guidelines for proper disposal of old or damaged hubs.
 - Gradual Rollout and Testing:
 - Begin with a pilot group to identify and address any implementation challenges.
 - Gradually expand to the entire hybrid workforce, ensuring smooth adoption and minimal disruption.
 - Use the cloud management interface to monitor adoption rates and identify any issues during rollout.
 - Continuous Assessment and Optimization:
 - Regularly review the performance and security efficacy of the implemented solution using the cloud-based analytics tools.
 - Continuously update policies and configurations based on emerging threats and changing work patterns.
 - Utilize the flexibility of the cloud infrastructure to quickly adapt to new requirements or scale as needed.

By leveraging either the multi-tenant environment or deploying a dedicated solution in their preferred cloud, in combination with Klōk hubs, organizations can effectively extend their network perimeter to their employees. This approach to remote connectivity provides the flexibility and scalability needed to

manage all hybrid workers with robust tools for monitoring, policy enforcement, rapid response to security events and to actively protect organizations and employees from bad actors.

The combination of personal APs and a powerful cloud-based management platform allows for the application of consistent security configurations, conduct thorough enforcement, and maintain visibility over all remote connections, truly embodying the principles of Zero Trust to the Last Mile of connectivity.

The Future of Zero Trust and Last Mile Security

As technology continues to evolve, so do the challenges and opportunities in securing the Last Mile of connectivity. While advancements are being made, new vulnerabilities are also being discovered, underscoring the need for a flexible and adaptable security approach.

- Evolving Cellular Network Security

The transition to 5G networks promises enhanced security features, including:

- Improved encryption algorithms
- Network “slicing” for better isolation of traffic
- Enhanced authentication mechanisms

However, recent research has exposed significant vulnerabilities in 5G networks, such as:

- Successful attacks on the 5G authentication protocol
- Location tracking despite enhanced protections
- Vulnerabilities in the interaction between 5G and legacy networks

These findings highlight that even as cellular network security improves; it cannot be blindly trusted as a complete solution for last-mile security.

- The Key to Future-Proof Last Mile Security

The fundamental principle for robust last-mile security lies in avoiding dependence on any single connectivity source. The Klök solution embodies this principle by:

- Multi-Network Capability: The ability to seamlessly switch between different MNOs, independently of them, provides resilience against vulnerabilities in any single network and avoiding all traffic flowing through a single network.
- WiFi Avoidance: By keeping users off public WiFi, Klök eliminates a major attack vector that has historically been a significant source of security breaches.
- Intermediation: By acting as an intermediary between users and MNOs, Klök:
 - Applies consistent security policies across all network connections
 - Responds rapidly to newly discovered vulnerabilities in specific networks

- Implements additional encryption and security measures on top of what MNOs provide and across MNOs
 - Adaptability to New Threats: Klōk’s management platform allows for rapid updates and policy changes in response to emerging security threats
- Addressing Future Attack Vectors

As new attack vectors emerge, the Klōk solution is well-positioned to address them:

- AI-Powered Threat Detection: Integration of machine learning algorithms to identify and respond to novel attack patterns in real-time.
- Quantum-Resistant Cryptography: As quantum computing threatens current encryption standards, the solution can be readily updated with post-quantum cryptographic algorithms.
- Edge Computing Security: With the rise of edge computing, Klōk can secure the critical Last Mile between edge devices and edge computing nodes.

By providing a flexible, multi-network solution that keeps users off public WiFi and acts as an intelligent intermediary, Klōk is well-positioned to adapt to future security challenges. This approach ensures that organizations can maintain a strong security posture in the face of evolving threats, without being tied to the limitations and risks associated with a single network provider.

Conclusion: Is your network ZTLM ?

Securing the Last Mile of connectivity is no longer optional -- it’s a critical component of a comprehensive Zero Trust strategy. By extending Zero Trust principles to encompass all remote and mobile connections, including those through MNOs, organizations can significantly reduce their attack surface and better protect their people, data and resources.

The Klōk solution addresses the gauntlet of threats faced by remote workers at the Edge, from “Evil twin” WiFi attacks to sophisticated cellular network vulnerabilities and human error. By reducing the attack surface and making employee devices less visible at the Edge, Klōk provides an actionable solution for implementing true end-to-end Zero Trust security.

We urge CISOs and security leaders to review their current Zero Trust strategies and consider how they can be extended to address the often-overlooked vulnerabilities of the Last Mile. With the Klōk approach and technologies, it’s possible to create a truly end-to-end Zero Trust environment that provides robust security without sacrificing productivity or user experience, while also safeguarding the physical security and privacy of employees.