

Mobile Identity Management

Executive Summary

In today's rapidly evolving cyber threat landscape, organizations face a broad range of security challenges. From sophisticated Persistent Threat Groups (PTGs) like the state sponsored APT42, to more common risks encountered by small businesses, the need for comprehensive, reliable security solutions has never been greater.

Klök is the only active defense solution equipped to address today's diverse threat landscape: It functions as a personal Access Point (AP), dramatically reducing the attack surface by eliminating risks associated with public or unsecured networks. For high-value targets, it offers advanced features including mobile metadata anonymization, post-quantum encryption, and communication stream fragmentation across multiple MNOs. Additionally, Klök serves as a powerful 360° gatekeeper for hybrid environments, securing both cloud infrastructure and data centers. Its remote IT management capabilities eliminate user error, ensuring security configurations remain consistent, up-to-date, and reliable. By combining these features, Klök provides a comprehensive defense against modern cybersecurity threats.

Moreover, Klök centralizes control to ensure organization-wide enforcement of regulatory requirements and security policies. This centralization allows IT departments to maintain compliance with data protection regulations and internal data integrity standards, making Klök essential for organizations of all sizes. Additionally, Klök enables IT to provision global, secure data service access for remote users worldwide. IT departments can, in addition to provision, monitor and manage these remote Access Points and connections in real-time, regardless of user location, enhancing both security and operational efficiency.

Whether for large enterprise combating state-sponsored threats or small businesses needing accessible

easy-to-deploy, easy-to-use security for remote employees, Klōk offers a unified, scalable solution that adapts to the needs of any organization.

The New Threat Landscape: Metadata as an Attack Vector

PTGs include not only state-backed actors but also sophisticated transnational criminal organizations that engage in prolonged, targeted cyber operations. These groups target high-value individuals and organizations, such as political dissidents, journalists, researchers, industrialist, even US presidential candidates, using sophisticated methods including phishing, credential theft, and mobile network surveillance where mobile metadata has emerged as a critical new attack vector in the evolving landscape of cybersecurity threats.

This often-overlooked information, which includes data about calls, texts, location and internet usage, provides a rich source of intelligence for malicious actors. Unlike the content of communications, which can be encrypted, metadata is unprotected, creating a significant vulnerability. Sophisticated attackers can exploit this data to track locations, map social networks, and infer sensitive information about individuals or organizations. The ubiquity of mobile devices and the constant stream of metadata they generate make this a particularly attractive target for PTGs. As traditional attack methods become more difficult to execute, the exploitation of mobile metadata represents a subtle yet powerful means of compromising privacy and security. This shift underscores the urgent need for comprehensive security solutions that address not just the content of communications, but also the metadata trail left by mobile devices.

Tactics, Techniques, and Procedures (TTPs)

PTG tactics include:

- **Phishing and Social Engineering:** Deceptive tactics designed to trick victims into revealing sensitive information or into unknowingly facilitating the installation of malware.
- **Credential Harvesting:** Unauthorized access through stolen or manipulated credentials.
- **Mobile Network Exploitation:** Tracking individuals via their mobile device identifiers, like their IMSI and IMEI; network-based attacks, like exploiting vulnerabilities based on network connectivity.
- **Lateral Movement and Data Exfiltration:** Gaining deeper access to sensitive data once inside a network.
- **Infecting Other Devices or Networks:** Propagating malware to other devices or access points connected to the compromised system, further expanding the scope of the attack.

PTGs exploit the vulnerabilities of public networks and mobile devices, making comprehensive, secure connectivity essential for those at risk of targeted attacks.

Real-World Example

APT42, an Iranian state-sponsored Persistent Threat Group (PTG), is notorious for its cyber espionage activities, employing methods such as spear-phishing campaigns and mobile network vulnerability exploitation. A notable attack in 2019 targeted journalists and activists in the Middle East, where attackers

tracked victims' locations by leveraging IMSI and IMEI data and other identifiers exposed to public Wi-Fi networks. More recently, during the 2024 US Presidential Campaign, APT42 successfully hacked the Trump campaign, with the Harris campaign likely compromised as well. These sophisticated attacks underscore the critical need for secure, private connectivity solutions like Klök, which can protect users from such surveillance and tracking efforts. Klök offers a comprehensive defense against these types of threats, safeguarding high-profile individuals and organizations operating in hostile environments.

Klök: An Integrated Solution for Modern Connectivity

The Klök is a portable, cellular-to-Wi-Fi gateway that provides personal, secure connectivity to the Internet, ensuring users never need to rely on public, shared or unsecured networks. This capability is critical for defending against the kinds of advanced attacks deployed by APTs, as well as for offering practical, accessible security solutions for smaller businesses.

Key Features

- **Metadata Anonymization:** Klök prevents track and locate via mobile network identifiers, ensuring user anonymity and protecting against mobile network surveillance.
- **Personal, Post-Quantum Encrypted Connectivity:** Klök offers users a secure, personal connection to the Internet, bypassing the risks of public Wi-Fi. In addition, all data transmitted through Klök is post-quantum encrypted, protecting against man-in-the-middle attacks and ensuring privacy.
- **Fragmented Communication Across Multiple MNOs:** Klök can fragment the encrypted communication across multiple mobile network operators, reducing the risk posed by any compromise at the network level.
- **Klök functions as an advanced personal firewall** isolating remote workers' devices from Advanced Persistent Threats (APTs) by creating a secure barrier between the device and potentially hostile exploitation of the network.
- **Secure Access to Corporate Resources:** Klök secures remote access to both cloud infrastructure and on-premises data centers, acting as a gatekeeper that manages and controls access in hybrid environments.
- **Seamless Mobility with Global Access:** Designed for portability, Klök ensures that users can maintain secure, encrypted connections while on the move, whether traveling or working remotely, from anywhere in the world. This global access allows organizations to support their workforce no matter where they are, ensuring uninterrupted security and connectivity.
- **Real-Time Fleet Management:** IT departments can manage their fleets of Klök devices in real-time, regardless of where their users are located globally. This capability ensures that all devices are consistently updated and configured according to the latest security policies, providing comprehensive oversight and control.
- **SIEM Integration and Response:** Klök supports integration with Security Information and Event Management (SIEM) systems, enabling real-time monitoring and analysis. Devices can dynamically update configurations in response to SIEM signals, allowing for adjustments of their security postures based on security events and alerts.

- **Integrated VPN Prevents Leaks:** Klōk includes a VPN that activates before the endpoint is even turned on. This ensures that no leakage can occur, in contrast to traditional endpoint VPNs that only engage after the device is powered up. By securing the connection from the very beginning, Klōk provides an additional layer of security that prevents any exposure before the user's device is fully operational.

Real-World Relevance

Klōk not only protects against sophisticated threats like those posed by APTs but also provides an easy-to-use, accessible security solution for small businesses. It ensures that employees working from anywhere can operate securely, regardless of the resources or expertise available within the organization.

How Klōk Mitigates the Threats of PTGs

Klōk, by design, directly addresses the sophisticated tactics used by PTGs, offering multiple layers of protection to secure mobile workers and sensitive data.

Phishing and Social Engineering Defense

Klōk can integrate with browser isolation and URL filtering to block access to malicious websites, protecting users from phishing attempts and other social engineering tactics.

Anonymizing Metadata to Prevent Targeting

By regularly altering mobile identifiers, Klōk prevents APTs and threat actors from tracking users through their mobile network metadata, protecting high-value targets from long-term surveillance.

Private Connectivity Eliminates Public Wi-Fi Risks

Klōk ensures that users never need to connect to public Wi-Fi networks, which are often exploited by PTGs. Instead, users access the Internet through a personal post-quantum encrypted connection provided by Klōk, eliminating a significant attack vector.

Fragmentation of Encrypted Data Across Multiple MNOs

Klōk can fragment encrypted data across multiple mobile networks, ensuring that no single compromised MNO can intercept the full communication stream. Even if an MNO is compromised, the fragmented and encrypted nature of the data makes it nearly impossible to decipher.

End-to-End Post-Quantum Encryption

All data transmitted via Klōk is encrypted end-to-end, protecting against interception and tampering. APT42, known for MITM attacks, would find it nearly impossible to access or manipulate this encrypted traffic.

Secure Access to Corporate Resources

Klōk provides secured, controlled access to corporate resources in hybrid environments, ensuring that even if an attacker compromises a device, they cannot easily access sensitive data or move laterally within the network.

Klōk: Gatekeeper for Hybrid Environments

In addition to protecting against PTGs, Klōk serves as a gatekeeper for hybrid environments, providing unified protective layer for both cloud infrastructure and on-premises data centers. This is particularly valuable for organizations that need to manage and secure access consistently across multiple environments.

Securing Hybrid Cloud and Data Center Access

Klōk enforces strict access controls, ensuring that only persistently authenticated users can access sensitive resources, whether hosted in the cloud or within a data center. This centralized control eliminates the possibility of user error, as all configurations and permissions are monitored and managed remotely by IT departments.

Proprietary Security Measures

Klōk uses proprietary technologies to secure communication between users and hybrid environments, offering multi-layered encryption and advanced segmentation to protect data across all access points.

Unified Protection Across Environments

Klōk ensures consistent security policies are enforced across both cloud and on-premises resources, providing a seamless, unified security framework that adapts to the evolving needs of hybrid environments.

End-to-End Security for Hybrid Operations

Klōk's proprietary routing protect data as it moves between cloud and on-premises environments, ensuring end-to-end security without compromising operational flexibility.

Ensuring Compliance with Regulatory Requirements and Security Policies

In today's regulatory environment, ensuring compliance with data protection regulations and internal security policies is crucial for any organization. Klōk provides a robust framework that not only secures connectivity but also ensures that all regulatory requirements and security policies are consistently enforced across the organization. By centralizing control through remote IT management, Klōk eliminates the risk of non-compliance due to user error or misconfiguration. This centralized approach allows IT departments to implement and enforce compliance with regulations such as GDPR, HIPAA, CCPA, CIPA and other industry-specific standards, ensuring that all data handling and transmission practices meet stringent legal and security requirements. Klōk's ability to enforce these policies across both cloud and on-premises environments makes it an essential tool for organizations that must adhere to strict regulatory standards while maintaining operational flexibility.

Klōk: The Comprehensive Solution for Today's Diverse Threats

Klōk is a versatile security solution designed to meet the needs of a wide range of organizations. For large enterprises facing persistent threats from PTGs like APT42, Klōk offers high-level defenses, including metadata and mobile identifier anonymization, post quantum encrypted connectivity, and fragmented communication across multiple MNOs. These features are specifically designed to protect against complex and persistent threats.

For businesses that lack the resources to implement comprehensive security measures, Klōk provides an accessible, easy-to-deploy and easy-to-use solution that ensures work-from-anywhere employees can operate securely. By offering personal connectivity and centralized IT management, Klōk makes it possible for even the smallest organizations to protect their critical data operate effectively and comply fully with all applicable regulations.

Global Access and Real-Time Management

Klōk's ability to provide secure, reliable connectivity from anywhere in the world makes it an ideal solution for globally distributed teams. IT departments can monitor and manage their fleets of Klōk devices in real-time, regardless of where their users are located, ensuring that security and regulatory policies are enforced consistently and effectively across the organization.

Klōk Complementing Solutions Like Zscaler and CrowdStrike

While Zscaler and CrowdStrike are leading solutions in their respective domains— fulfilling the very necessary functions of securing cloud applications and protecting endpoints—Klōk fills a critical gap by securing the connectivity layer itself:

- **Zscaler/Netskope:** Focuses primarily on securing cloud-based applications and user access. Klōk complements Zscaler by securing the network paths and metadata anonymization needed for truly secure mobile work.
- **CrowdStrike:** Specializes in endpoint detection and response (EDR) to detect and mitigate malware or suspicious behavior on devices. However, Klōk addresses vulnerabilities in the connectivity that may occur before the endpoint can be defended. By providing the connectivity, securing the data in transit and anonymizing metadata, Klōk prevents a wide range of attacks before they reach CrowdStrike's layer of protection.
- **VPN on Klōk vs. Traditional VPN:** Klōk includes integrated VPN capability that activates before the endpoint is even turned on, ensuring that no leakage (in or out) can occur. This is in stark contrast to traditional endpoint VPNs that only engage after the device is powered up and connected, leaving crucial milliseconds of potential exposure. Klōk's VPN ensures a secure connection from the start, providing an additional layer of protection against leaks.
- **Zero Trust Integration:** Klōk integrates with Zero Trust models, ensuring that no single connection or data path is implicitly trusted. This approach enforces granular control over access to resources, limiting the ability of attackers to move laterally within a network, even if they gain initial access.

Unified Protection Across All Use Cases

Klōk offers unified protection that adapts to the specific needs of any organization, whether defending against sophisticated threats or providing accessible security for remote workers. Its scalable design means it can grow with the organization, providing consistent security across all environments.

Klōk's proprietary security measures, combined with its ease of use and remote management capabilities, make it a versatile tool that bridges the gap between high-level security requirements and practical needs. This makes Klōk not just a solution for today's security challenges, but a future-proof investment for any organization.

Conclusion

In a world where cyber threats are becoming increasingly sophisticated, Klōk stands out as a comprehensive solution for securing connectivity, data, and communications across diverse environments. Whether combating state-sponsored actors like APT42 and other PTGs or ensuring that businesses have the 360° security they need to protect their remote workforce, Klōk offers a versatile, scalable, and robust approach to modern security challenges.

By providing secure, personal connectivity, enforcing stringent access controls in hybrid environments, and ensuring compliance with regulatory requirements, Klōk not only addresses the most pressing security concerns of today but also anticipates the evolving needs of tomorrow. With global access and real-time fleet monitoring and management, Klōk ensures that organizations of all sizes can maintain seamless, secure operations no matter where their users are located.

For organizations looking to safeguard their most critical assets—whether in the cloud, on-premises, or on the move—Klōk delivers the tools and peace of mind needed to operate securely in an increasingly interconnected world.