Mobile Security for Enterprises

Enable the secure office anywhere

Organizations adopting a flexible approach towardAkamai mobile solutions delivered with MNO partners enable self-serve, private connectivity. remote work are facing challenges as mobile endpoints cannot be easily managed or secured outside the perimeter of the corporate firewall. Akamai partners with Mobile Network Operators (MNO) and integrates security technology in their networks that makes it easy for IT teams to maximize security, visibility, and control for all mobile endpoints.

Overview

Akamai mobile security services delivered with MNO partners protect all SIM-enabled devices. Clientless solutions can be rapidly deployed without the cost and constraints associated with traditional technologies, such as VPNs. Businesses get protections against phishing, malware, and ransomware with full visibility of traffic across the mobile estate, and can customize the internet experience of employees.

Business Challenge

More than ever, CIOs need to demonstrate leadership as organizations adopt working models where employees can be remote and offices can be anywhere. This requires a digital strategy that accounts for mobility. Becoming truly digital means business transformation initiatives must be secure by design and deliver a seamless working experience to employees regardless of where they are.

Features

Enhanced clientless solution for mobile security delivers management and protection of mobile devices and data in transit. IT teams can roll out services without the need for time-consuming integrations or hardware investments. They can also configure powerful policies to fine tune security, promote productivity, and manage data usage through an easy-to-use self-service portal.

Security and Compliance: Stop malware and malicious content before it gets to devices. Block unknown or unregistered domains that could be used for malicious purposes. Make mobile security part of a regulatory compliance strategy.

BENEFITS

Protects all SIM-enabled devices from cyber attacks before they reach the device

Removes on-device clients to eliminate exposure from client software protections being circumvented and dissatisfaction or potential disruption from slowdowns or failures

Covers all types of cellular devices including MiFis and routers regardless of operating system or manufacturer

Improves visibility of mobile traffic, allowing policies to be enforced more consistently

Supports compliance with data protection regulation applying policies at the individual or group level

Reports and real-time monitoring improve understanding of online behaviors and the impact of policies

Advanced Reporting and Analytics: Get essential data to enable better decision-making about protecting valuable mobile data and devices. Show the effectiveness of usage policies and the main drivers of data usage with mobile data insights .

Content Filtering (Acceptable Use Policies): Manage access to 165 categories of websites covering more than 1 billion domains. Deny video streaming services such as Netflix and YouTube. Ensure devices are used for business purposes or access to leisure content is managed during working hours.

Data Controls: Customize the internet experience for individuals and groups by limiting internet access speeds or setting mobile data caps. Support compliance with personal data regulations, such as SOX, HIPAA, or GDPR.

Agnostic Solution: Support any SIM (2G-5G) and all devices regardless of manufacturer or operating system.
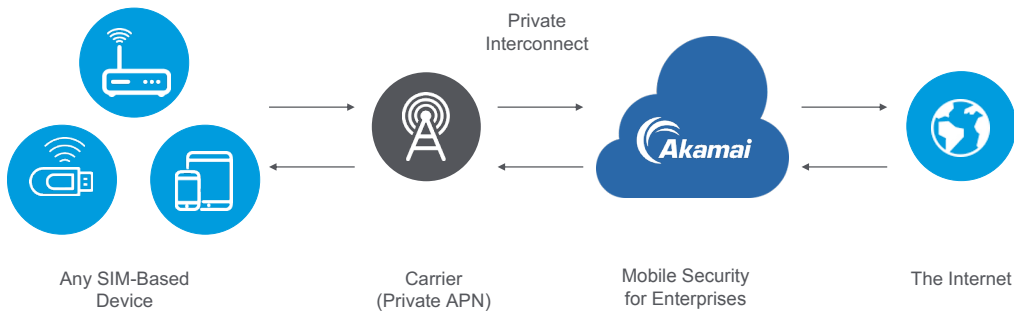
Enabling the office anywhere

Fig.1 Network-based security, visibility and control for mobile devices

Akamai mobile security services, delivered with MNO partners, are designed to help organizations become digitally secure and productively connected wherever they are. Businesses get clientless, security, visibility, and control for everything with a SIM. Devices can be enrolled at any scale with minimum effort and disruption, without the need for cumbersome hardware or client software.

To learn more click contact your Akamai representative.