AKAMAI SOLUTION BRIEF

Securing Mobile Data for Financial Services

Financial services institutions (FSIs) constantly adopt new technologies to improve employee productivity and security. As more work moves outside corporate firewalls FSIs must ensure access to the internet is secured to minimize exposure to cyberattacks that target mobile endpoints in order to extract valuable personal and financial information.

Overview

Secure Internet Access Mobile is a network-based mobility service that enables FSI employees to work efficiently and securely while outside office perimeters. Secure Internet Access Mobile services delivered with MNO partners protect all SIM-enabled devices.

FSIs get protections against phishing, malware, and ransomware with full visibility of traffic across the mobile estate. Clientless solutions can be rapidly deployed without the cost and constraints associated with traditional technologies, such as VPNs.

IT teams can roll out services without the need for hardware investments or the overhead of installing and managing client software over time. They can also configure powerful policies to fine-tune security, promote productivity, and control data usage through an easy-to-use self-service portal.

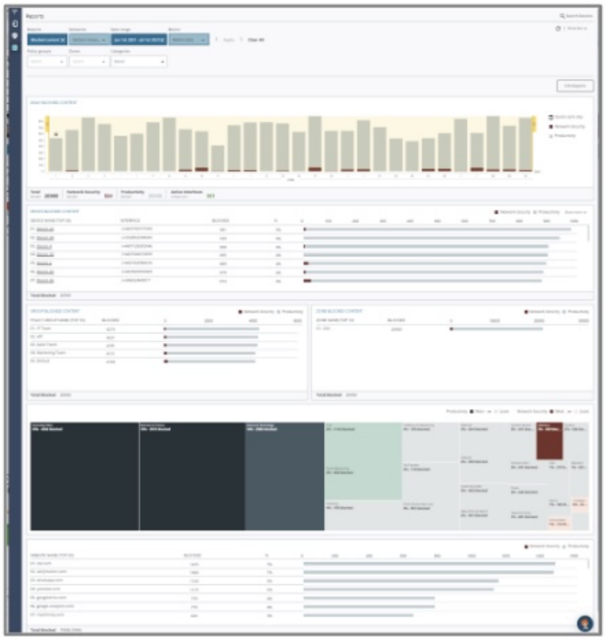
Benefits

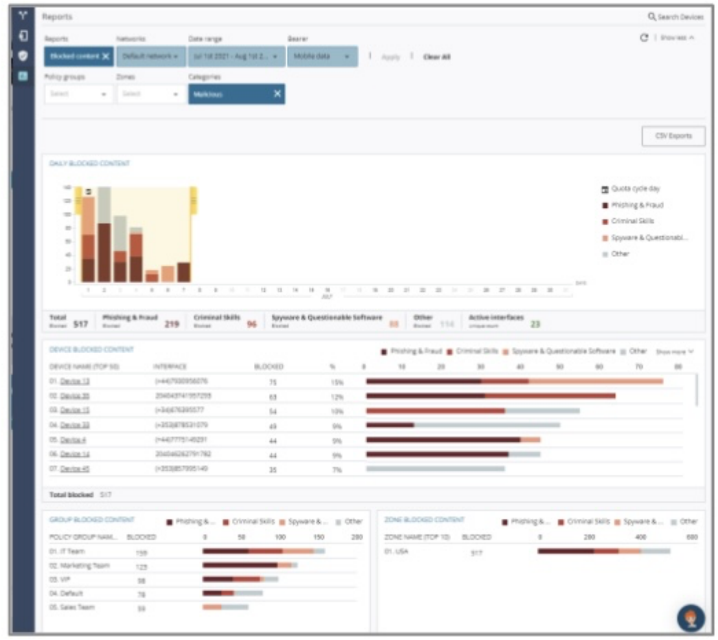
- Clientless solution compatible with any SIM-based device and mobile OS
- Covers phishing, malware and botnets with leading Akamai threat intelligence
- Enables acceptable use policy for compliance and productivity
- Provides domestic and roaming data usage policies to support cost controls
- Integrations (IDP/Active Directory, UEM/MDM) simplify deployment and management
- Delivers business intelligence with realtime threat and internet activity reports
- Speeds deployment and minimizes IT investment with self-serve provisioning
- Supports private connectivity for cellular devices that can be activated quickly through a self-service portal

Features

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.

Mobile Device Visibility: View advanced reporting and analytics to obtain essential data for 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.





Self-serve portal: Simplify deployment, support configuration of security, data controls, and acceptable use policies, and display security and usage data.

Acceptable Use Policies: Manage access to 165 categories of websites with filtering categories 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.

Device Management Integrations: Take advantage of leading Unified Endpoint Management (UEM) or Mobile Device Management (MDM) to simplify deployment and extend management visibility and control to phones and other cellular devices.

Optional Self-serve Private Network: Privately address mobile endpoints and securely route their traffic to enterprise resources.

Agnostic solution: Supports any SIM (2G–5G) and all devices.

Akamai Secure Internet Access 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.

Learn more at akamai.com