# Secure Internet Access Mobile for SMBs

Carrier GTM playbook

# Akamai Disclaimer

Akamai makes no representations or warranties and undertakes no commitment with regard to product planning information, anticipated product characteristics, performance specifications, or anticipated release dates (collectively, “Roadmap Information”).  Roadmap Information is provided by Akamai to the recipient solely for purposes of discussion and without intending to be bound thereby. This presentation is based on Akamai’s expectations and understanding at the time of delivery; Akamai disclaims any obligation to update Roadmap Information.

This information is **Akamai Confidential and Proprietary** and is provided under the terms, conditions and restrictions defined in the non-disclosure agreement in place with your organization.

# Welcome to the Secure Internet Access Mobile GTM playbook

The objective of this playbook is to help Carriers:

- Understand the SIA mobile service strategy
- Clearly communicate the value of Secure Internet Access (SIA) Mobile to Small Business customers with relevant, targeted messaging
- Enable sales teams within the carrier organisation to effectively sell the proposition

# Contents

## Section 1: Messaging to the Carrier

- Market Context (MTD and Carrier Industry)
- SIA Mobile Executive  Summary
- Value proposition and benefits for the Carrier
- Customer success stories

## Section 2: Messaging for marketing to SMBs

- Elevator pitch
- Value proposition and benefits for the SMB
- Overview of security challenges
- Overview of business challenges
- Feature descriptions for web copy & media
- FAQs
- Sample marketing timeline
- Sample copy for marketing email and SMS campaign

## Section 3: Sales Enablement

- Messaging Focus for SMB buying personas
- Qualifying questions & responses
- Objection Handling
- Pain points vs selling points
- Sample call script and product brief copy

## Section 4: Competitors

## Section 5: Product Features

# Carrier Industry context

- **Business Challenge:**
  Globally, carriers are facing challenges to grow revenues in an increasingly commoditized and competitive market. Network operators are looking for opportunities to build value and offer innovative solutions to differentiate from competitors.

- **Carrier Business Goals:**
  - Drive growth through delivery of best connectivity products and services
  - Add value to traditional access solutions to grow subscribers  and market share
  - Provide leading innovation in digital services
  - Focus on deepening customer relationships through launch of converged customer offers
  - Extend network leadership with 5G and accelerate MEC and IoT partnerships
  - Manage costs through operational and financial discipline

- **Investment Focus**
  - Focused investment in digital products and services
  - 5G rollout and fibre deployment
  - Partnerships with global technology leaders in cloud & security

# MTD Market context

The Mobile Threat Defense (MTD) market is growing, particularly in regulated and high security sectors. Gartner estimates that the MTD market reached $350million in 2020* and it's expected that growth will continue due to the following factors:

- Mobile threat landscape is continuing to grow with the increase of mobile device sales. According to the GSMA report "The Mobile Economy 2022" there will be 400 million new mobile subscribers by 2025*
- MTD is moving from niche to mainstream adoption in organisations as security teams see MTD as a way to obtain visibility into the mobile fleet
- Regulated industries such as healthcare and financial services need to ensure compliance with data usage regulations. It's estimated that by 2025 more than half of organisations in regulated industries will have a security solution for iOS and Android devices
- IDC predicts that by 2025 35% of deskless workers worldwide will use a connected mobile device to complete daily tasks, increasing the workload on IT to efficiently manage mobile assets and users
- IDC also asserts that mobility is a critical investment for success. Mobile centric workflows enable businesses across all industries from self-employed business owners to the world's largest corporations. IDC expects to see increased spending on mobile device application management as well as mobile software and security solutions.

*Gartner Market Guide for Mobile Threat Defense March 2021
https://www.gsma.com/mobileeconomy/wp-content/uploads/2022/02/280222-The-Mobile-Economy-2022.pdf

Akamai

# SIA Mobile executive summary

SIA Mobile is a service built for mobile network operators which is designed to be rebranded and re-sold to small and large business customers to help manage security across all their SIM enabled devices.

It’s a clientless solution that can be deployed rapidly without any hardware or software investment and businesses gain full visibility of their mobile traffic across all mobile devices. Organisations can ensure a safe mobile internet experience for their employees by protecting them against phishing attacks, malware and ransomware.

New work models mean mobile devices are essential and SIA Mobile makes it simple to secure ANY mobile device. Value add features help improve productivity and support compliance initiatives and enhanced visibility drives better business decisions.

# SIA Mobile - value proposition for network operators

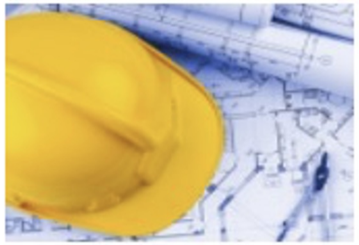
Value proposition

**A security solution for every SIM on your network**

| Key Benefit 1 | Key benefit 2 | Key Benefit 3 | Key Benefit 4 |
|---|---|---|---|
| **Protect every SIM** | **Generate new revenue** | **Differentiate from competitors** | **Deepen customer relationships** |
| ● Protect Smartphones, tablets, cellular routers and IOT devices.<br>● No need to support client rollout or VPN deployment<br>● Single APN split across multiple customers<br>● Clientless solution enables great customer experience | ● Value add service to new and existing customers<br>● Enable security on legacy as well as newer mobile devices<br>● Rapid deployment of solution enables revenue generation sooner | ● Embed security as part of service offering<br>● Simple onboarding process for customers<br>● Network branded to reinforce value proposition | ● Evolve relationship from connectivity provider to trusted partner<br>● Deliver benefits from day one |

# SIA Mobile is a proven solution applicable to all business sectors

Construction



Turner
Building the Future

Energy

enel x

solo energy

Manufacturing

glanbia FOODS

Safe Cities

CNIguard

*White-labelled by Major global carriers*

*Tens of thousands of business customers*

Retail

Camelot

Oil & Gas

HOWARD ENERGY PARTNERS

Healthcare

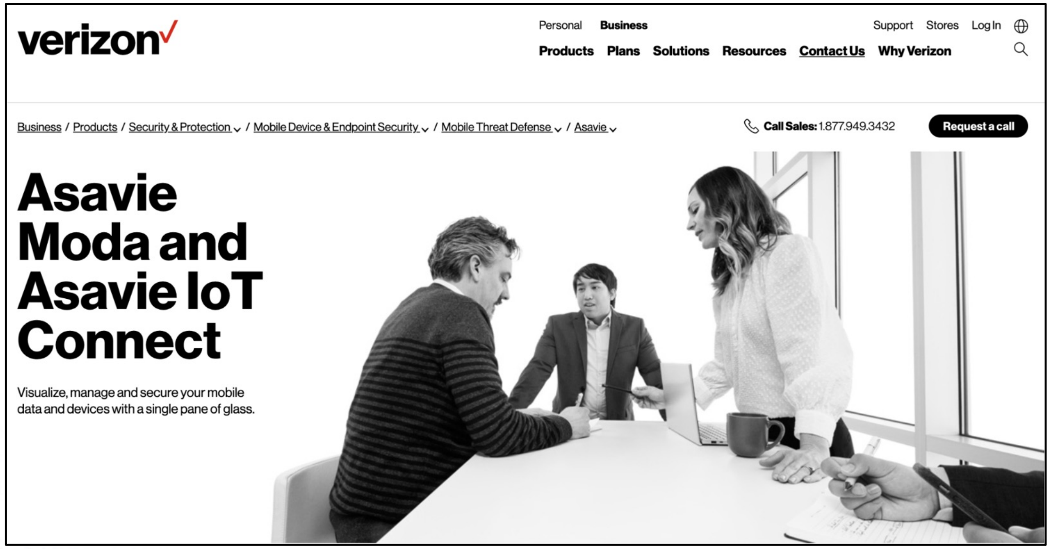
CardiLink

Transport & Logistics

Transport for London

# Examples of SIA Mobile partner branded collateral

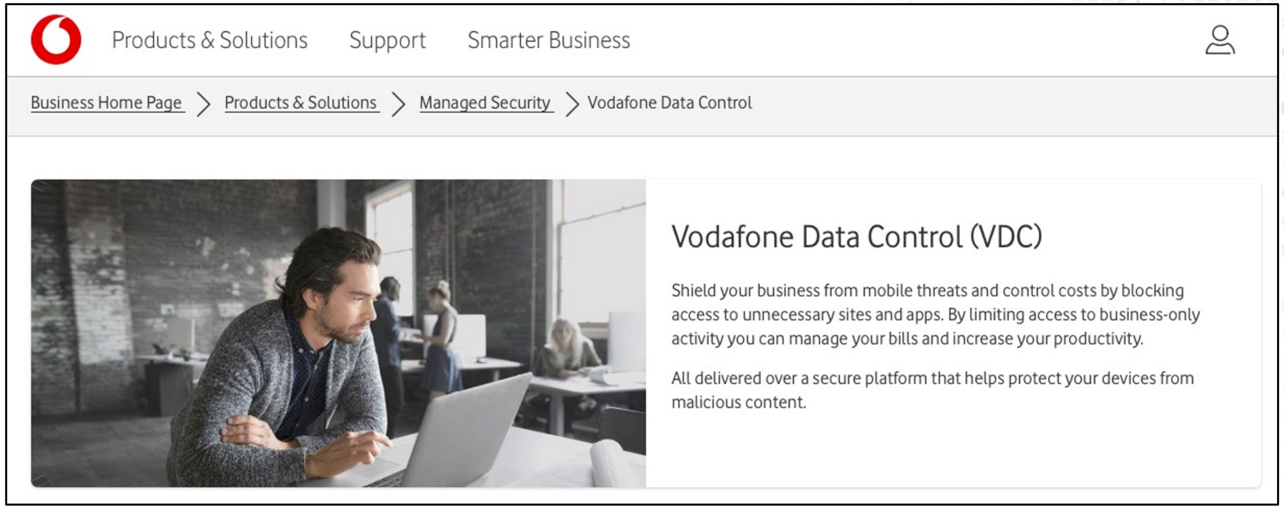
## Verizon


verizon✓
Personal
Business
Support
Stores
Log In
Products
Plans
Solutions
Resources
Contact Us
Why Verizon
Business / Products / Security & Protection / Mobile Device & Endpoint Security / Mobile Threat Defense / Asavie
Call Sales: 1.877.949.3432
Request a call

### Asavie Moda and Asavie IoT Connect

Visualize, manage and secure your mobile data and devices with a single pane of glass.

## Vodafone

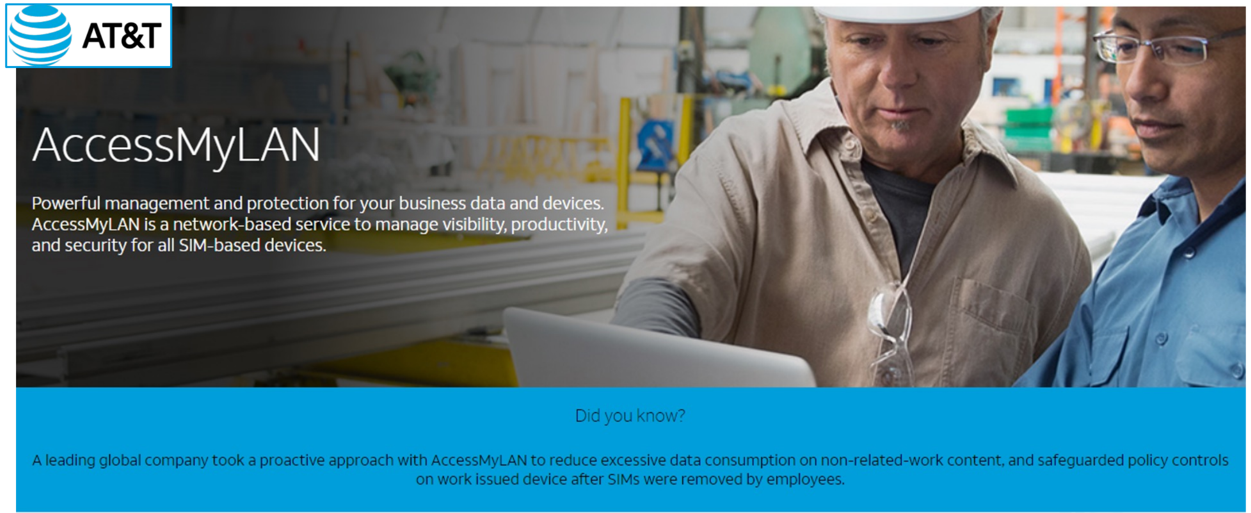

Products & Solutions
Support
Smarter Business
Business Home Page > Products & Solutions > Managed Security > Vodafone Data Control

### Vodafone Data Control (VDC)

Shield your business from mobile threats and control costs by blocking access to unnecessary sites and apps. By limiting access to business-only activity you can manage your bills and increase your productivity.

All delivered over a secure platform that helps protect your devices from malicious content.

## AT&T



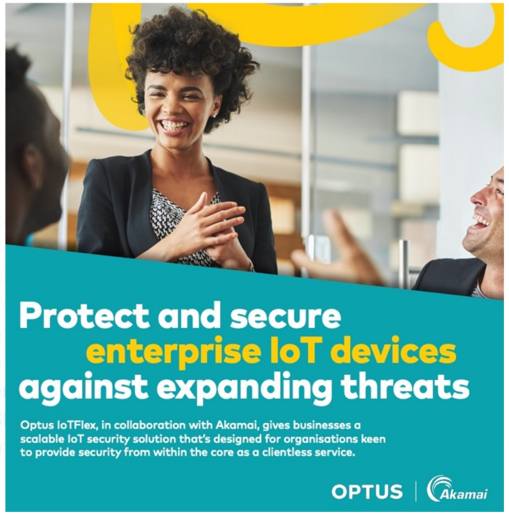
### AccessMyLAN

Powerful management and protection for your business data and devices. AccessMyLAN is a network-based service to manage visibility, productivity, and security for all SIM-based devices.

Did you know?

A leading global company took a proactive approach with AccessMyLAN to reduce excessive data consumption on non-related-work content, and safeguarded policy controls on work issued device after SIMs were removed by employees.

## Optus



**Protect and secure enterprise IoT devices against expanding threats**

Optus IoTFlex, in collaboration with Akamai, gives businesses a scalable IoT security solution that's designed for organisations keen to provide security from within the core as a clientless service.

# Customer success stories - Travel Industry

## Business Challenge

**Gray Line Tours offer customers free Wi-Fi on their fleet of tour buses**

- Manage data usage and deliver a secure browsing experience to customers
- Protect IP enabled wireless routers deployed on each bus
- Manage data costs and protect profit margins

## Solution deployed

- A solution combining a shared data plan, wireless routers and SIA mobile was deployed
- SIA Mobile enabled the delivery of a safe internet experience on board and control of data usage
- Service was deployed within two weeks with their mobile partner Verizon

## Benefits to the business

- Passengers are **protected against malicious and inappropriate content**
- **Enhanced control:** Ability to set tailored usage policies and restrict access to data hungry streaming services
- Better able to **predict monthly data costs** through the implementation of data usage policies

# Customer success stories - Security Industry

## Business Challenge

**Safe Haven security is an ADT authorised dealer with a large number of employees in the field**

- Lack of visibility into device data usage to ensure devices were being used for work related purposes
- No control over applications being accessed on devices
- High data consumption costs

## Solution deployed

- SIA Mobile rolled out across field teams
- Customised usage policies and data caps deployed on each device
- Content categorisation features to restrict access to specific websites and protect employees from malicious websites through real time threat intelligence

## Benefits to the business

- **Improved cost control:** Sales team data usage remains on target and within budget
- **Enhanced security:** Devices are protected through zero day defense blocking of online threats
- **Enhanced productivity:** employees can access relevant content in a more productive manner and avoid time wasting distractions

# Business Case Basics

## Build on trusted relationships

Providers already have business and technical/IT relationships

## Business model

Premium/secure service bundle

Add-on to mobile subscription plan

Included by default in business tariff

(e.g. Try-before-you buy or x weeks protection included)

## Customer acquisition

Opt-in

## Revenue potential

TBC

## Penetration

3-5% depending on business model

## Other business motivations

Competitive differentiation

Retain existing customers (Service personalization)

## Business case example

$2/mo * 12 mos * 3% penetration * 5,000,000 SMB mobile subs  = $3.6m ARR

# Messaging for marketing to SMBs

# SMB market context

- Small businesses are the bedrock of most countries economies providing local services, jobs and investment in their communities

- Sentiment among SMBs on economic outlook varies by region. In the US inflation remains a top concern with 71% of small businesses believing the worst is still to come regarding inflation and price increases.

- In Europe the outlook is mixed with 40% of Irish SMBs expecting to see growth of between 25 and 50% and a reduction in debt levels. In the UK the outlook is notably more pessimistic with the UK Small Business Index falling to -24.7 in Q2 2022, the second largest fall in the history of the index

- Despite the challenges in the economy small businesses are expected to continue to prioritise investment in digital transformation and technology to help them compete during challenging economic conditions.

- Cybersecurity is a growing concern for many small businesses with data breaches increasing by 152% at small companies in 2020 and 2021. A recent cybersecurity report from Comcast and Akamai highlighted 30,000 SMBs were protected from an attempted phishing attack in a single day.

- Network Operators are well positioned to support SMBs in their digital transformation by working with them to pinpoint the best solution for their business. Solutions such as SIA Mobile are embedded directly into the carrier network delivering the protection and peace of mind that enable small business to focus on growing their revenues.

# The elevator pitch

SIA mobile <replace with Carrier brand name>> is a business ready solution that delivers essential security, visibility and control for mobile devices.

It's integrated directly into the mobile network which means there's no need for client software and it protects ANY SIM-based device regardless of operating system. Businesses can roll out the service quickly without the need for costly integrations or hardware investments and it provides organisations with essential reporting and controls to ensure devices are secure and data costs are managed.

In a world where mobile is becoming the new normal it is imperative to extend the same controls and parameters typically reserved for companies private networks to mobile devices, helping to solve the challenges that come with the work from anywhere revolution.

# SIA Mobile - value proposition for small to medium businesses

| Value proposition | | | |
|---|---|---|---|
| **Secure your business to drive productivity and growth** | | | |
| **Key Benefit #1** | **Key benefit #2** | **Key Benefit #3** | **Key Benefit #4** |
| **Secure mobile devices** | **Empower employees** | **Control costs** | **Work with trusted partner** |
| • Devices and data are protected from day one<br>• Protects smartphones (including ruggedised and non-premium), tablets, cellular routers and IoT devices<br>• No app required | • Mobile workforce is secure<br>• Business resources are protected<br>• Employees empowered to be more productive and do their best work | • Manage data usage costs and prevent bill shock<br>• Protect against financial loss due to cyber attack<br>• Be compliant with data usage regulations | • Work with a provider that understands your mobile security requirements<br>• A proven solution used by multiple businesses<br>• Support to help you roll out the solution quickly and efficiently |

# Top 10 benefits for SMBs

- Enroll mobile devices quickly
- Browse safely by blocking phishing  attacks
- Protect every SIM
- Empower your mobile workforce
- Get more insights with advanced reporting
- Content Filtering per user
- Meet data compliance requirements
- Access data in real time
- Control mobile data costs
- Apply data controls when roaming

# SIA Mobile also addresses key business challenges

| Business Challenge | How SIA Mobile addresses the challenge |
|---|---|
| **1. Securing data** | ● Facilitates secure access to sensitive data over cellular and Wi-Fi networks*. |
| **2. Securing connectivity** | ● Provides high levels of security to your business with seamless and secure connectivity between your companies private network and mobile devices. |
| **3. Protecting mobile subscribers** | ● SIA Mobile can monitor all traffic to and from the device to keep it safe. |
| **4. Managing remote workers** | ● Enables seamless and secure access to essential business resources for remote and mobile employees |
| **5. Managing costs** | ● Helps businesses avoid high data charges by setting data usage policies to manage how much data employees can consume both at home or abroad |
| **6. Compliance** | ● Helps businesses meet data compliance obligations by securing the mobile device |

*Wi-Fi client available for US and Ireland customers only.

# Feature descriptions for web copy and media

**Network based security**

- Designed to block malicious content before it can reach the mobile device. Zero day threat blocking restricts devices from accessing suspicious websites which could pose a threat to the device or critical business data.

**Advanced reporting**

- Detailed reporting provides valuable insights on the effectiveness of data usage policies and helps to identify cost concerns before they become significant. Access to real-time data enables faster decision making to support your business priorities.

**Works on any SIM-enabled device**

- Security policy enforcement across all mobile devices regardless of mobile operating system or manufacturer

**Content filtering**

- Manage access to specific categories of websites or block video streaming services such as Netflix and YouTube

**Manage data and costs**

- Manage the websites and applications that can be accessed by device or device groups. Avoid high data charges by creating shared data bundles and alerting end users when they are approaching their data usage limit.

**Simple to use portal**

- Add devices and create customisable security policies via an easy to use web-based portal

**Easy to deploy**

- Can be deployed and managed without MDM integration

# Questions SMBs frequently ask providers (FAQs)

Q. **What are the benefits of SIA Mobile <<replace with Carrier brand>>?**
A. It enables businesses to protect all of their mobile devices and ensures consistent application of security policies across any SIM based device including smartphones, tablets, mobile wi-fi devices and more.

Q. **What do I need in order to take advantage of SIA Mobile?**
A. You will need to connect your businesses mobile devices to the service, which will require changing the Access Point Name (APN) on the device. There are different options available depending on the type of device you wish to connect. If your business uses a Mobile Device Management (MDM) solution, settings can be pushed out to end users devices. If your business does not have the capacity to push APN settings via an MDM solution, devices can be configured directly by your IT Administrator.

Q. **What business problems does SIA Mobile solve for SMBs?**
A. Many small businesses lack security resources or expertise yet are exposed to the same risks as larger organisations.SIA Mobile <<replace with Carrier brand>> provides a solution to help small businesses protect mobile devices against phishing attacks and malware. It can be rolled out quickly and managed centrally from an easy-to-use online portal, without the need to install costly infrastructure or hardware.

**Q. How does SIA Mobile solve these problems?**
A. As soon as devices are enrolled in the service security policies can be applied quickly, ensuring devices are protected from day one. Threats such as phishing attacks and malware are blocked before they reach the smartphone or tablet. Critical business data is secure and businesses are protected against financial loss from a cyber breach. Businesses can also apply policies to manage how mobile data is used e.g. restrict access to websites that use a lot of data such as video streaming sites. This keeps data usage costs under control both at home and abroad.

# Questions SMBs frequently ask their providers (FAQs)

Q. **What’s different about this offering?**

A. SIA Mobile is network-based security so malicious content can be stopped before it reaches the end user device. It’s also clientless which means there’s no cumbersome app installation to manage.

An easy-to-use self service portal enables security policies to be created and applied quickly.

**Q. How does SIA Mobile handle security when phones or other devices connect through Wi-Fi networks?**

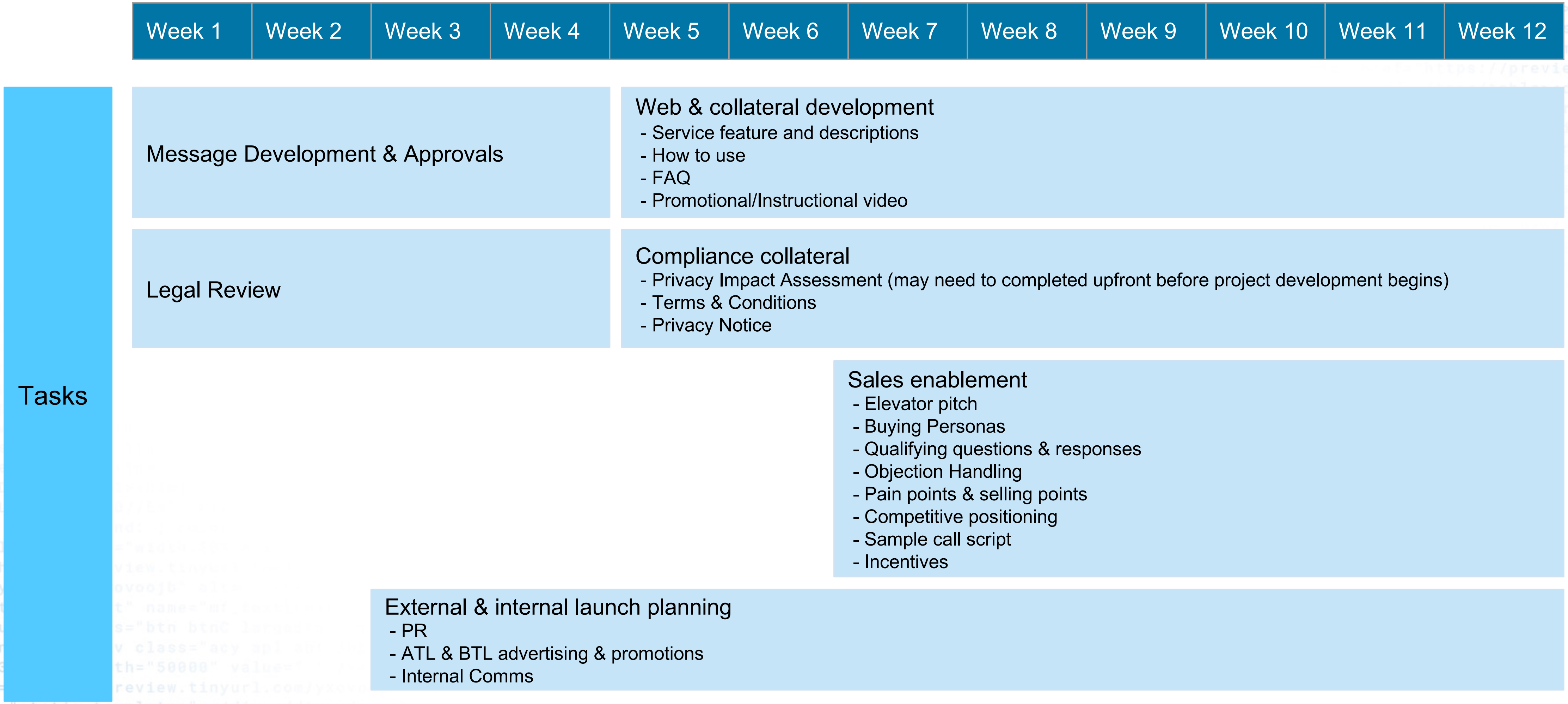
A. An optional client is available to provide protection on wifi networks, however the service is mostly deployed without a client for cellular protections*

Q. **Why is this product better than the competition?**

A. SIA Mobile is integrated in to our network so it works with any SIM-enabled device regardless of the device manufacturer or operating system. . It also works for cellular routers and all kinds of IoT devices. Competitors often depend on a client or application installed on the device in order to track usage and apply policies. SIA Mobile is a clientless and tamper-proof solution and this means policies stay with the SIM card even if it is taken out of the device.

*Wi-Fi client available for US and Ireland customers only.

# Sample marketing GTM timeline & activities



Message Development & Approvals

Web & collateral development
- Service feature and descriptions
- How to use
- FAQ
- Promotional/Instructional video

Legal Review

Compliance collateral
- Privacy Impact Assessment (may need to completed upfront before project development begins)
- Terms & Conditions
- Privacy Notice

Sales enablement
- Elevator pitch
- Buying Personas
- Qualifying questions & responses
- Objection Handling
- Pain points & selling points
- Competitive positioning
- Sample call script
- Incentives

External & internal launch planning
- PR
- ATL & BTL advertising & promotions
- Internal Comms

# Sample marketing copy

## SMB marketing email

### Grow your business securely with SIA Mobile

As more employees use mobile devices to store and access business data the risk of phishing and other security attacks increases. In order to stay ahead of the attackers it's important to ensure your business has a security strategy in place which includes securing your mobile devices.

**SIA Mobile helps protect your business**

SIA Mobile <<replace with Carrier brand>> protects your mobile devices and sensitive business data from malicious cyber attacks. It also enables you to control mobile data costs at home and abroad while ensuring your employees are empowered to collaborate securely and effectively.

To hear more about how SIA Mobile can help you secure your business contact our security solution experts today.

## SMS copy 1

Protect your business and secure your mobile devices with SIA Mobile <<replace with Carrier brand>>. Click here for more information.

## SMS copy 2

The threat of cyberattacks is growing. Protect your business with SIA Mobile <<replace with Carrier brand>>. Contact our security experts today on 1800 xxx xxx

## SMS copy 3

Protect your mobile devices and manage your data costs with SIA Mobile <<replace with Carrier brand>>. To find out more talk to our security experts today on 1800 xxx xxxx

# Sales Enablement

# Small business buying personas

| Role | Responsibilities | SIA Mobile Messaging Focus |
|---|---|---|
| **Small Business Owner** | ● Oversees the business<br>● Time constrained & results oriented<br>● May not have dedicated IT staff or formal security expertise | ● Security protection for **every SIM enabled device** used by the business<br>● **Simplicity of deployment** - no client needed on the device<br>● **Increased visibility and data controls** deliver cost savings and improved productivity |
| **Small Business Manager** | ● Runs day to day operations<br>● Manages multiple priorities to ensure business goals and priorities are met<br>● May not have formal security expertise | ● Highlight the improved visibility into mobile activity and threats<br>● **Data control features** help manage data costs and prevent bill shock |
| **IT administrator** | ● Manages computers, networks and software<br>● Internal technology expert but finds it difficult to keep up-to-date with rapid pace of change in technology<br>● May be sceptical of new security solutions | ● Highlight **ease of deployment**. No costly hardware or infrastructure required<br>● SIA Mobile protects any SIM based device, , against phishing and malware attacks<br>● If IT function is outsourced IT call out fees may be reduced |

# Sales Qualifying Questions for SMBs

1. Do your employees use business owned mobile Phones or tablets?
2. Has your business been impacted by a security breach in the past?
3. Are you concerned about the financial impact of a security breach?
4. Are you looking to manage mobile data usage and costs?
5. Do you have a process in place to  apply security policies to your business mobile devices?

# Qualifying customer responses/requirements

✓

## Good fit for SIA mobile <replace with Carrier brand>

- Needs more control around mobile devices
- Need more visibility on how devices are used
- Need a process to secure business owned employee mobiles
- Need to manage mobile data costs
- Are in a regulated industry and need to align with internal or external governance
- A customer with Field employees and mobile devices
- Have problems applying policies consistently across all mobile devices

✗

## Not a good fit for SIA mobile

- Have a BYOD (Bring your own device) mobile environment. This means the employee uses their own devices and the company does not provide them to employees
- Businesses where mobile devices predominantly connect to a Wi-Fi instead of cellular network

# Objection handling

***I already have a Mobile Device Manager. Why do I need a separate security service?***
*SIA Mobile complements mobile device managers  as they solve different problems. MDMs enable remote wipe of devices if a phone is stolen or no longer controlled by your employee or business.*
*SIA Mobile covers threats including malware and phishing attacks. . It also provides useful data management and control features, and visibility into mobile device traffic.  Both work together to protect businesses.*

***How does SIA Mobile handle security when phones or other devices connect through public Wi-Fi networks?***
*An optional client is available to provide protection on wifi networks, however the service is mostly deployed clientlessly for cellular protections.*

***Why is this product better than the competition?***
*SIA Mobile is integrated  into the mobile operator network so our services work with any SIM-enabled device regardless of the manufacturer or OS version. They work for cellular routers and all kinds of IoT devices.*
*Competitors also depend on a client or application installed on the device in order to track usage and apply policies. SIA Mobile is a clientless and tamper-proof solution and this means policies stay with the SIM card even if it is taken out of the device.*

***What business problems does SIA mobile solve?***

- *Protects your business against the financial impact of a security breach*
- *Minimises the stress of managing security on your mobile devices - simple to deploy and manage at scale*
- *Improves employee productivity restricting access to non work related sites*
- *Helps your business to manage mobile data and data roaming costs*
- *Protects your business against the reputational impact of a cyber breach.*

# Pain points vs selling points

## Pain points for a small business

- ➢ **Cyber attacks against SMBs are increasing:** A recent report highlighted that 48% of SMBs reported multiple cyber attacks over last 3 years
- ➢ **Financial loss:** Can have huge negative impact on a small business
- ➢ **Intellectual property theft:** Loss of valuable data
- ➢ **Regulatory exposure:** May be penalties for data breaches or non compliance
- ➢ **Reputational damage:** Loss of customer trust if their data is compromised
- ➢ **Lack of resources:** Small business are resource constrained so mobile security may not be a top priority

## SIA Mobile selling points

- ➢ Business can set data usage policies to ensure mobile data costs are managed
- ➢ Access to critical business data is controlled and secured
- ➢ Mobile devices are protected and access to data on the company network is secured
- ➢ Managers can configure acceptable use policies to control what content is accessible for business devices
- ➢ SIA Mobile leverages the existing relationship with their mobile provider to deploy the service quickly without significant investment costs

# Sample sales call script

Hello,  my name is <sales agent name> and I'm calling from <Carrier name> to tell you about a new service we've launched that helps you secure your business mobile devices from cyber threats such as malware or phishing attacks. If you have time I'd like to run through some questions with you to see how our service might benefit your business.

***Qualifying questions***

*<<Insert qualifying questions here>>*

***Examples of common problems or pain points***

*As we've spoken to other small businesses we've noticed that they often say:*

*<<insert some small business pain points here>>*

You may be aware that the threat of cyber attacks is growing and threats against small businesses in particular is growing with attacks against businesses with less than ten employees increasing four fold over the last year.

SIA Mobile <<replace with Carrier brand>> was designed specifically to protect mobile devices on our network and it's very straightforward to set up and roll out to your employees. There's no need to install a client on the device or get your employees to activate the service. As soon as the device has been added to the service it's protected immediately. The service costs $xx per month based on x number of devices.

I can sign you up to the service today or if you're interested in learning more about it I can send you an email now and one of our security experts can follow up with at a time that suits you. Can I just confirm your contact details <<confirm email address and contact number>>.

Great, thank you for your time today and I'll get that email out to you straight away. Please don't hesitate to contact us if you have further questions.

# Sample content for product brief

### Secure Internet Access Mobile for SMBs

SIA Mobile helps you grow your business securely by protecting mobile devices, data and employees from the risk a cybersecurity attack.

### Overview

In the new work-from-anywhere environment it’s essential to have a security strategy in place to reduce the risk of cyberattacks. Businesses need to empower employees to be productive wherever they are and to ensure business resources are protected against phishing and malware attacks. In order to stay ahead of the attackers your security policies must include protection for mobile devices.

### Business Challenge

Cybersecurity is a growing concern for many businesses with attacks continuing to increase against organisations of every size. The financial and reputational impact of a data breach can have an outsize impact, particularly against smaller companies. To ensure businesses continue to thrive it’s important that mobile security is considered as companies and employees adapt to a hybrid working world.

### Benefits of SIA Mobile for SMBs

SIA Mobile helps protect businesses against the financial impact of a cyberattack. Phishing attacks and malware are blocked before they reach the device and business owners get a real time view of the mobile threats faced by employees. It’s a clientless solution so doesn’t require an app to be installed on the device enabling a faster roll out across the business.

### Other benefits include:

- **Data Controls**: Limit access to non work-related sites and manage data costs by setting user specific usage policies and data usage caps

- **Content filtering:** Manage access to over 165 categories of websites

- **Real-time visibility**: Detailed reporting gives real time data to assess the impact of security and usage policies

- **Works on any SIM-enabled device:** regardless of device manufacturer or operating system

SIA Mobile delivers a secure internet experience across all mobile devices and empowers your employees to do their best work. Working with a trusted partner we will support you in ensuring your mobile resources are protected so you can focus on ensuring your business continues to grow and thrive.

# Competitors

# Competitor product overview

## SIA Mobile is unique as it positions the network operator as an embedded component of the SMBs security portfolio.

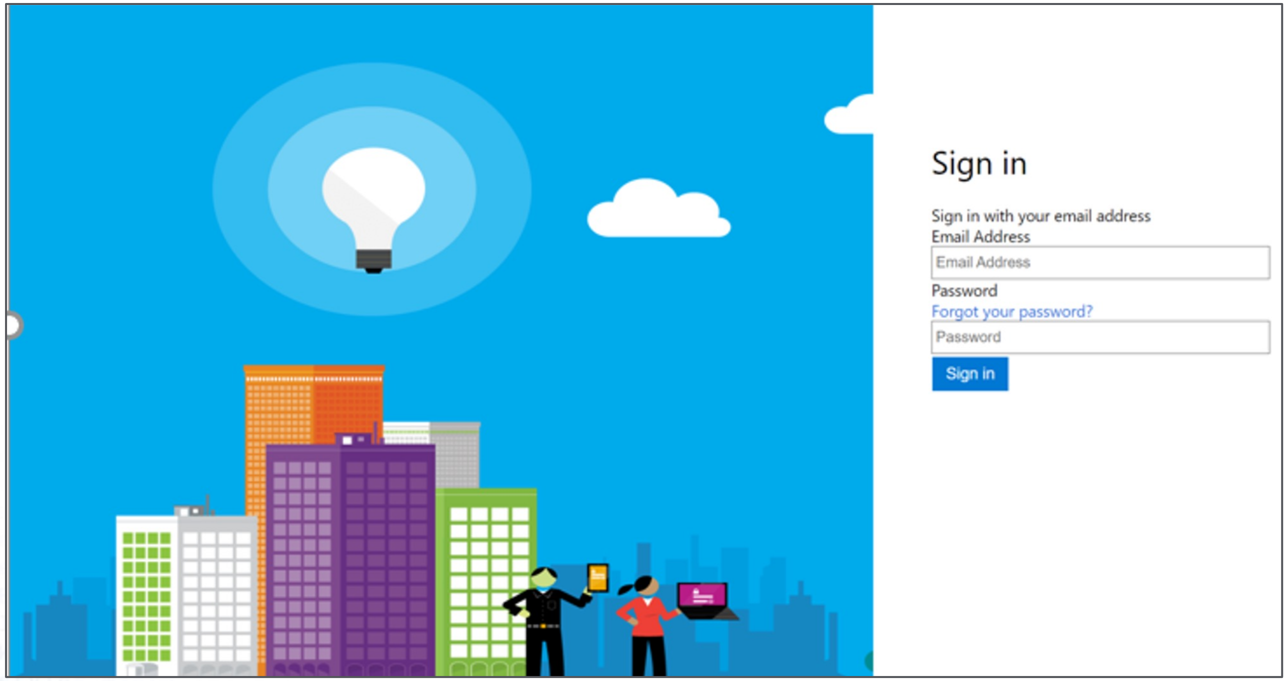
| Competitor | Value proposition | How SIA Mobile wins |
|---|---|---|
| Lookout | Protection for Smartphones, Tablets and Chromebooks and uses artificial intelligence to analyse telemetry data from nearly 200 million devices and over 120 million apps. | ● **Clientless solution** - no need to install an app on end user devices<br>● **Works on ANY Sim-enabled device including mobile broadband dongles and IoT devices** |
| CHECK POINT | Checkpoint Harmony unifies 6 cloud based security products to keep  remote workforce 100% safe. Supports any device ownership programme (BYOD, COPE) | ● **Works on ANY SIM-enabled device including mobile broadband dongles and IoT devices** |
| ZIMPERIUM | Provides continuous on-device monitoring and analysis capabilities to detect mobile cyber attacks in real time. | ● No app required - impact on device battery life is significantly reduced |
| SOPHOS | Sophos Mobile supports BYOD environments to ensure business data is safe and personal information is private. Intercept X for Mobile leverages a market leading Intercept X deep learning engine to protect devices and corporate data from known and new mobile threats | ● No app required - impact on device battery is significantly reduced<br>● Device agnostic - works well on Apple, Android and other Device OS |

More detailed competitor summaries included in Appendix

# SIA Mobile Product features

# Self Serve Portal

White label Portal



Sign in

Sign in with your email address

Email Address

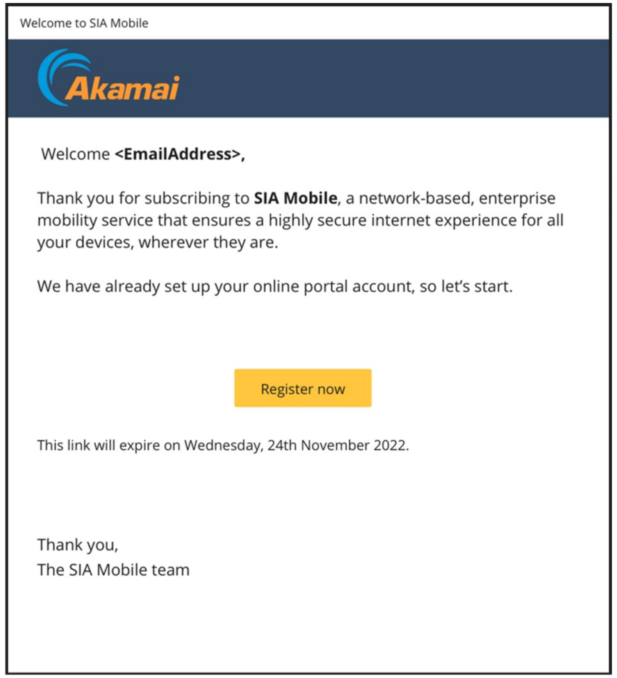
Email Address

Password

Forgot your password?

Password

White label Welcome email



Welcome to SIA Mobile

Welcome **<EmailAddress>**,

Thank you for subscribing to **SIA Mobile**, a network-based, enterprise mobility service that ensures a highly secure internet experience for all your devices, wherever they are.

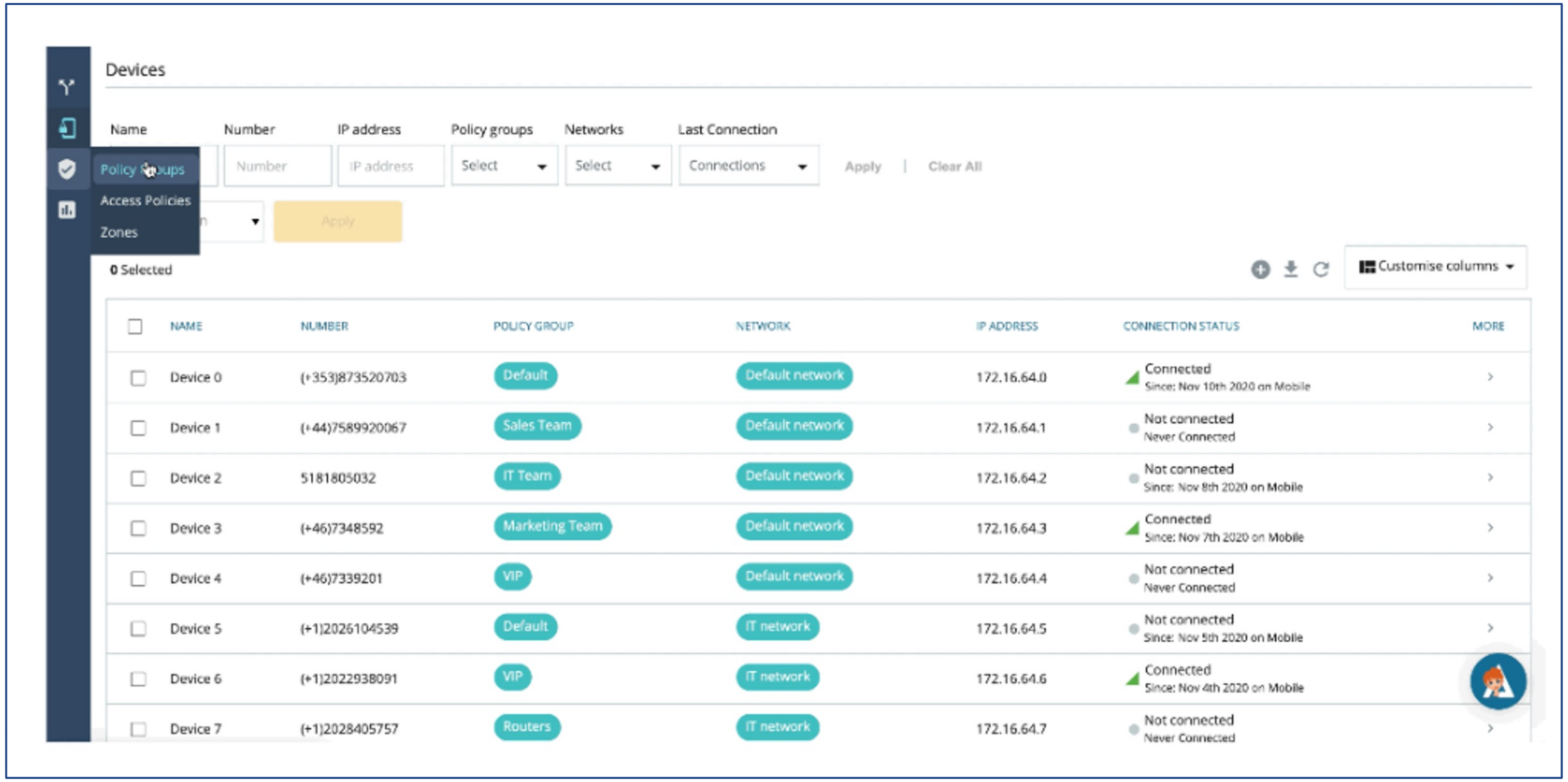
We have already set up your online portal account, so let's start.

This link will expire on Wednesday, 24th November 2022.

Thank you,
The SIA Mobile team

- Welcome Email - can be re-branded with Carrier branding
- Self-Care onboarding – web UI built on Public Developer API
- All touchpoints are white label – option to rebrand

# Create Policy Groups



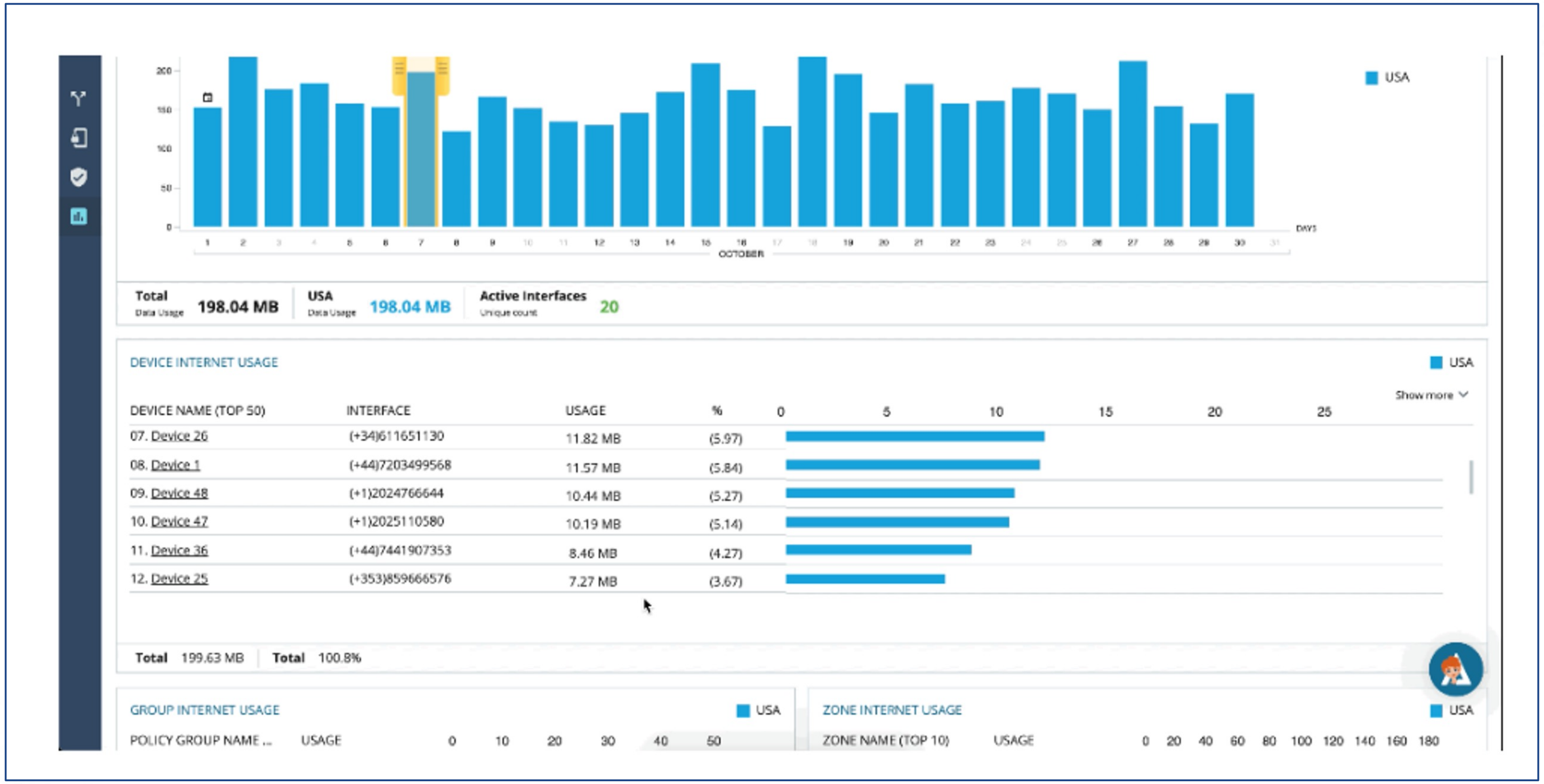
0 Selected

| ☐ | NAME | NUMBER | POLICY GROUP | NETWORK | IP ADDRESS | CONNECTION STATUS | MORE |
|---|---|---|---|---|---|---|---|
| ☐ | Device 0 | (+353)873520703 | Default | Default network | 172.16.64.0 | Connected<br>Since: Nov 10th 2020 on Mobile | › |
| ☐ | Device 1 | (+44)7589920067 | Sales Team | Default network | 172.16.64.1 | Not connected<br>Never Connected | › |
| ☐ | Device 2 | 5181805032 | IT Team | Default network | 172.16.64.2 | Not connected<br>Since: Nov 8th 2020 on Mobile | › |
| ☐ | Device 3 | (+46)7348592 | Marketing Team | Default network | 172.16.64.3 | Connected<br>Since: Nov 7th 2020 on Mobile | › |
| ☐ | Device 4 | (+46)7339201 | VIP | Default network | 172.16.64.4 | Not connected<br>Never Connected | › |
| ☐ | Device 5 | (+1)2026104539 | Default | IT network | 172.16.64.5 | Not connected<br>Since: Nov 5th 2020 on Mobile | › |
| ☐ | Device 6 | (+1)2022938091 | VIP | IT network | 172.16.64.6 | Connected<br>Since: Nov 4th 2020 on Mobile | |
| ☐ | Device 7 | (+1)2028405757 | Routers | IT network | 172.16.64.7 | Not connected<br>Never Connected | › |

**Group devices and assign mobile and Wi-Fi access policies and access times**

- Apply restrictions by individual device or group of devices once data usage limits have been reached
- Choose specific policies to be applied when devices are used on Wi-Fi networks
- Create Access Times polices to allow devices to be connected during certain times e.g. weekdays

# Data usage reporting



**Total** Data Usage **198.04 MB** | **USA** Data Usage **198.04 MB** | **Active Interfaces** Unique count **20**

DEVICE INTERNET USAGE

■ USA

Show more

| DEVICE NAME (TOP 50) | INTERFACE | USAGE | % |
|---|---|---|---|
| 07. Device 26 | (+34)611651130 | 11.82 MB | (5.97) |
| 08. Device 1 | (+44)7203499568 | 11.57 MB | (5.84) |
| 09. Device 48 | (+1)2024766644 | 10.44 MB | (5.27) |
| 10. Device 47 | (+1)2025110580 | 10.19 MB | (5.14) |
| 11. Device 36 | (+44)7441907353 | 8.46 MB | (4.27) |
| 12. Device 25 | (+353)859666576 | 7.27 MB | (3.67) |

**Total** 199.63 MB | **Total** 100.8%

GROUP INTERNET USAGE ■ USA

POLICY GROUP NAME ... USAGE

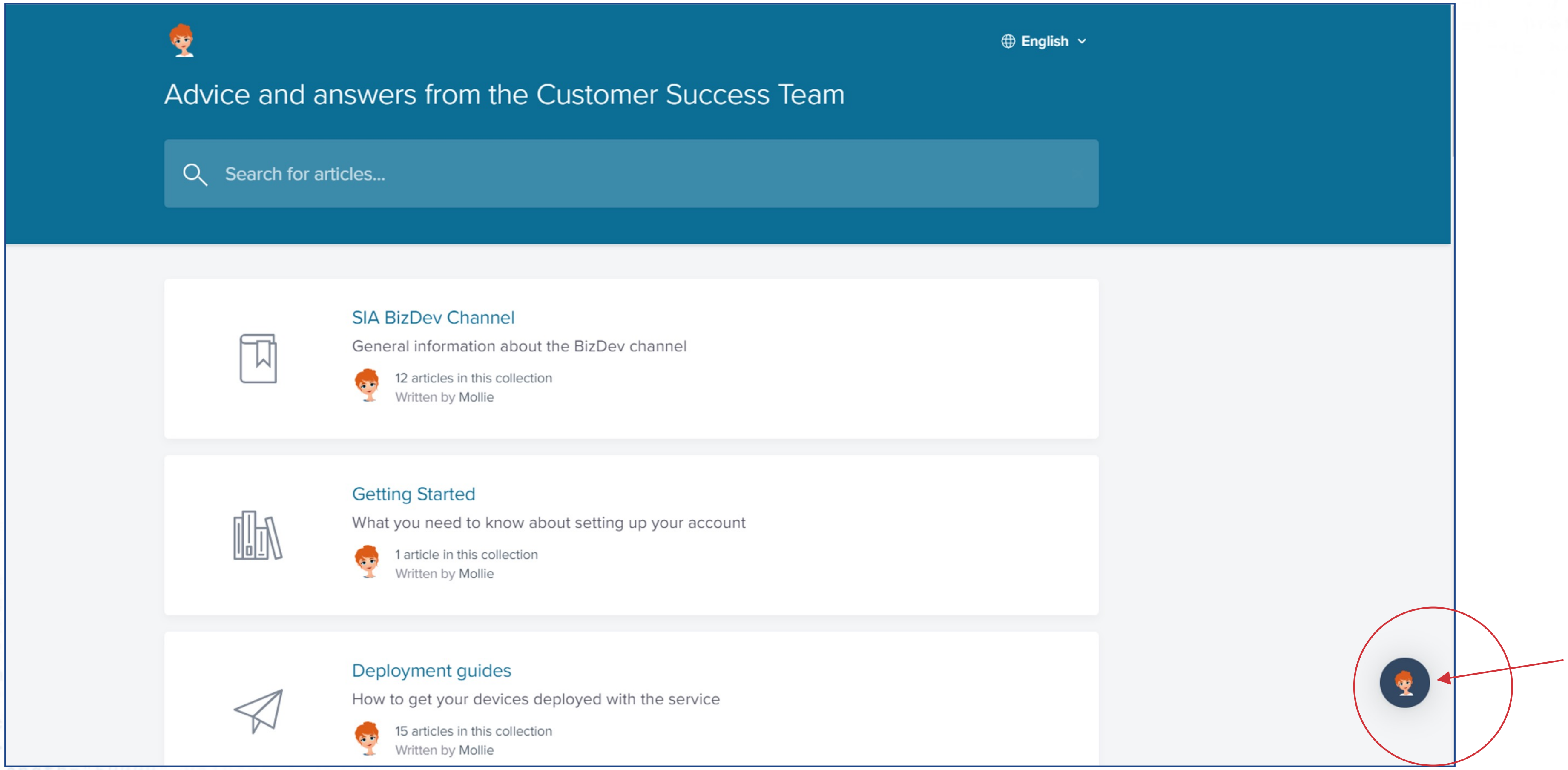
ZONE INTERNET USAGE ■ USA

ZONE NAME (TOP 10) USAGE

**Get visibility on your internet traffic and policy blocks**

- Internet usage can be viewed by device, by zone or by category
- A list of pre-defined reports is available to use
- Internet blocking reports analyse how policies are being enforced.
- Visibility of the entire device fleet or a single device

# Customer support chatbot



Advice and answers from the Customer Success Team

SIA BizDev Channel

General information about the BizDev channel

12 articles in this collection
Written by Mollie

Getting Started

What you need to know about setting up your account

1 article in this collection
Written by Mollie

Deployment guides

How to get your devices deployed with the service

15 articles in this collection
Written by Mollie

Customer support available with chatbot "Mollie"

# Appendix

# Competitor - Lookout Mobile Endpoint Security

## Description

Lookout is an integrated endpoint-to-cloud security company. Their mission is to secure and empower our digital future in a privacy-focused world where mobility and cloud are essential to all we do for work and play. They enable consumers and employees to protect their data, and to securely stay connected without violating their privacy and trust.

## Value proposition/selling point

Lookout offers protection for Smartphones, Tablets and Chromebooks and uses artificial intelligence to analyse telemetry data from nearly 200 million devices and over 120 million apps. Algorithms search the internet daily to find websites purpose-built for phishing and countless custom apps have been analysed via their API. Lookout MES is powered by the Lookout Security Graph and can be scaled to hundreds of thousands of end points.

## Main products offered

Lookout MES product bundles:

Essentials: 2 Modules - Modern Endpoint Protection and Phishing and Content Protection

Advanced: Adds Mobile risk and compliance and Mobile Vulnerability and Patch Management modules

Premium: Proactively hunt for mobile threats with Mobile Endpoint Detection and Response

## How we win

1. **Clientless solution** - no need to install an app on end user devices
2. Sales channel strength and presence
3. Works on any SIM based device, regardless of operating system

| Product Comparison | Own | Lookout |
|---|---|---|
| Client on Mobile | No | Yes |
| Malware/Phishing detection | Yes | Yes |
| DNS Security | Yes | Yes |
| Website Whitelisting/Black | Yes | Yes |
| MDM Integration | Yes | Yes |
| Self serve portal | Yes | Yes |
| Data Control Cap/Throttling | Yes | Yes |
| Data Control - Roaming | Yes | No |

Lookout customer reviews taken from Gartner Peer Insights

## Strengths

- Simple to use web interface
- Large amount of detail provided on each threat detected
- Strong engineering and technical support
- Easy integration with MDM

According to customer reviews:
“Very easy to work with. Our rep and tech service support are both highly responsive. Managing the dashboard, portal, staying on top of risk and vulnerabilities has been straightforward.”

## Weaknesses

- Requires app to be activated on the device. User must log in to the app in order to begin protecting the device
- Challenge to identify devices with specific apps
- Deployment to IoS can be cumbersome
- Lack of integration with MS tenant

According to customer reviews:

- “Small to medium sized businesses are going to experience significant challenges managing IoS devices”
- “Device management/filtering could be better”
- “Better alerting features would be beneficial”

# Competitor - Checkpoint Harmony

## Description

Checkpoint Harmony Endpoint is a complete endpoint security solution built to protect the remote workforce from today's complex threat landscape. It prevents the most imminent threats to the endpoint such as ransomware, phishing or drive-by malware, while quickly minimizing breach impact with autonomous detection and response.

## Value proposition/selling point

Checkpoint Harmony unifies 6 cloud based security products to keep  remote workforce 100% safe.  It protects devices and internet connections from the most sophisticated attacks while ensuring zero trust access to corporate applications.  Whether it's a phishing attempt, malicious email attachment, or zero day ransomware, Harmony protects users from all cyberthreats across all attack vectors.

## Main products offered

- Harmony Endpoint - Complete endpoint protection
- Harmony Browse - Secure Internet Browsing
- Harmony Email & Collaboration - Secure mailbox
- Harmony Mobile - Mobile Threat Defense
- Harmony Connect - Securely connect users to anywhere

## How we win

1. **Clientless solution** - no need to install an app on end user devices
2. Sales channel strength and presence
3. Works on any SIM based device, regardless of operating system

| Product Comparison | Own | Checkpoint |
|---|---|---|
| Client on Mobile | No | Yes |
| Malware/Phishing detection | Yes | Yes |
| DNS Security | Yes | Yes |
| Website Whitelisting | Yes | Yes |
| MDM Integration | Yes | Yes |
| Self Serve portal | Yes | Yes |
| Data Controls - Cap/Throttling | Yes | No |
| Data Controls - Roaming | Yes | No |

Checkpoint Customer reviews taken from Gartner Peer Insights

## Strengths

- Integrates with any mobile management solution
- Supports any device ownership programme (BYOD, COPE)
- Elegant user experience - no impact on device usability
- Privacy by design - user and corporate data kept completely separate

According to customer reviews:
"Harmony mobile is light software in terms of load on mobile but powerful in terms of security"

## Weaknesses

- No thin client
- Difficulty working together with an EDR
- Resource intensive

According to customer reviews:

- "Endpoint resource usage is something that needs to be tweaked as it is resource intensive when running all features"
- "At times over intrusive malware detection in web browsers, OS support and compatibility with new OS versions

# Competitor - Zimperium

## Description

Zimperium empowers enterprises to secure their mobile endpoints, enabling employees to access sensitive data and mission-critical systems safely and securely. Their enterprise-focused, advanced mobile security solution integrates with IAM, UEM, XDR platforms and is deployable on any cloud, on-premises, and air-gapped environments.

## Value proposition/selling point

The Zimperium MTD platform provides continuous on-device monitoring and analysis capabilities to detect mobile cyber attacks in real time. The Zimperium app doesn't require signatures, a cloud based sandbox, or even an internet connection. End-users get contextual alerts & remediation recommendations. IT gets best-in-class visibility with dashboards & detailed reporting with actionable phishing, network, device and malware threat forensics

## Main products offered

- Mobile Threat Defense Platform - continuous on-device protection and detects attacks in real time
- zIPS Mobile Device Security - On device protection for COPE and BYOD devices
- z3A Advanced App Analysis - Detailed app privacy and risk analysis
- Z9 Detection Engine - Dynamically identifies attacks

## How we win

1. **Clientless solution** - no need to install an app on end user devices
2. Sales channel strength and presence

| Product Comparison | Own | Checkpoint |
|---|---|---|
| Client on mobile | No | Yes |
| Malware/Phishing detection | Yes | Yes |
| DNS Security | Yes | ? |
| Website Whitelisting | Yes | Yes |
| MDM Integration | Yes | Yes |
| Self Serve portal | Yes | Yes |
| Data Controls - | Yes | No |
| Cap/Throttling | Yes | No |
| Data Controls - Roaming | | |

Zimperium customer reviews taken from Gartner Peer Insights

## Strengths

- Easy integration with MDM solution
- Good account and technical support
- Scalability
- Strong threat component which gives meaningful visibility to an organisations mobile risk posture

According to customer reviews:

- "Zimperium zIPS offers the most advanced on-device detection engine and can detect threats from all mobile threat vectors including phishing"

## Weaknesses

- More APIs required
- Enhancement of console functionality/granularity
- Impact on battery consumption

According to customer reviews:

- "Endpoint resource usage is something that needs to be tweaked as it is resource intensive when running all features"
- "At times over intrusive malware detection in web browsers, OS support and compatibility with new OS versions
- "The only problem we have is support. It must be better and faster in responses".

# Competitor - Sophos Mobile

## Description

Sophos Mobile is a secure Unified Endpoint Management (UEM) that helps businesses manage and secure traditional and mobile endpoints.

## Value proposition/selling point

Sophos Mobile supports BYOD environments to ensure business data is safe and personal information is private. Intercept X for Mobile leverages a market leading Intercept X deep learning engine to protect devices and corporate data from known and new mobile threats. Organisations can manage mobile end users via a easy to use, unified, web based admin interface which gives visibility across endpoint, network and server security

## Main products offered

- Intercept X for Mobile: Device, network and app security for Android and iOS devices
- Sophos XDR): Checks devices for vulnerabilities or unwanted apps

## How we win

1. **Clientless solution** - no need to install an app on end user devices

1. Sales channel strength and presence

| Product Comparison | Own | Checkpoint |
|---|---|---|
| Client on mobile | No | Yes |
| Malware/Phishing detection | Yes | Yes |
| DNS Security | Yes | ? |
| Website Whitelisting | Yes | Yes |
| MDM Integration | Yes | Yes |
| Self Serve portal | Yes | Yes |
| Data Controls - | Yes | ? |
| Cap/Throttling | Yes | ? |
| Data Controls - Roaming | | |

## Strengths

- Comprehensive Man-in-the-Middle (MitM) threat detection
- Microsoft Intune conditional access
- Easy to install and deploy

According to customer reviews:

- “Mobile device coverage is extensive, covering most OS. Application and content control is also very easy to manage”

## Weaknesses

- Support issues for more technical complex issues
- Some features (virus remediation) don’t work well on MACs
- Can make other apps on a device run very slow

According to customer reviews:

- “Usage on Linux not as straight forward as Windows. Usage on Chrome OS needs some work.”
- “Currently multiple applications are required to install on the endpoint. Work on combining all the applications in one package for easy installation”

Sophos Mobile customer reviews taken from Gartner Peer Insights