Unlock revenue opportunities with new security and personalization services
Executive summary

Recent high-profile data breaches and numerous waves of widely publicised internet attacks have made everyone nervous about security. Families, small businesses and other organisations are struggling to figure out how to protect themselves.

Accessibility of inappropriate content and concern about overuse of mobile devices by children has left parents looking for better ways to manage internet access. Small businesses are also looking for ways to ensure all their devices are protected.

As trusted brands, mobile network operators (MNOs) are ideally positioned to address these problems. In doing so they can potentially unlock revenue opportunities (ARPU) with new services deployed in their networks.

DNS-based security and personalisation services stand out as a simple, effective, and flexible way to address these problems because they typically:

• Use proven, familiar DNS infrastructure.
• Provide comprehensive threat coverage, excellent precision and are highly responsive to fast changing threats.

• Allow families to easily configure content filters and usage management features to match their preferences and values.
• Secure mobile workers in small businesses.
• Deliver a great user experience with no software or ongoing maintenance.
• Offer the same user experience as subscribers traverse converged networks.

For MNOs, DNS-based security services are an obvious opportunity as competitive pressures increase and revenue growth remains modest. Different revenue models to drive ARPU can be implemented: “freemium”, free trial linked to subscription, premium access service bundles and so on. MNO-branded offerings also demonstrate commitment to subscriber safety, increasing affinity.
1. Threat Level

Today, mobile is the dominant method of internet access and the rapid proliferation and usage of mobile apps mean MNOs, consumers and businesses face myriad threats. In an interview with Mobile World Live, James Kelly, Google’s Android security senior product manager noted securing first-time smartphone users from the threat of malware and other criminal activity is one of the most pressing challenges facing the company today. ¹

Figure 1. Phishing activity reached an all-time high in 2016

A huge range of mobile exploits exist. For example, the Anti-Phishing Working Group estimated the number of phishing attacks hit an all-time high in 2016 (see figure 1). Social networks are now targeted with malicious links and downloads. People on mobile devices are excellent targets for phishing and other kinds of social engineering because they’re generally distracted as they multitask and check their phones throughout the day, and constrained by small screens which may not offer visual cues that something is amiss.

In August 2017, researchers from Akamai and elsewhere uncovered a botnet named WireX that primarily compromised Android devices. It targeted Content Delivery Networks (CDNs) and content providers in a distributed denial of service (DDoS) attack. Traffic was observed from at least 70,000 concurrent IP addresses from more than 100 countries, which is unusual for current mobile botnets (see figure 2, P4).

In October 2017, a multipurpose malware named Loapi which infects mobile devices was reported. Among other things it can send malicious SMS, use the device as an HTTP proxy, and display unwanted advertisements (see figure 3, P5). It can even mine bitcoins, sometimes with disastrous impact on the phone. Malicious advertising networks are another plague, which present a direct threat to mobile network infrastructure. Malicious ads consume bandwidth when they are loaded, with no return for anyone except the criminals sending them.

Taking the discussion a little deeper, mobile apps present exposure in different ways. One is unauthorised or copycat apps which mimic popular verified apps and secretly gather user information. Legitimate apps can also pose a threat to smartphones and networks if they’ve been unknowingly compromised during their development, or in the deployment cycle.

Major app store providers are of course aware of the potential for vulnerabilities. They’re always searching for illegitimate apps. In a blog post in July 2017, Google said it had found 20 Lipizzan spyware apps on its Play Store. The apps and their developers were blocked from the Android ecosystem, however renegade apps still function until they’re detected so subscribers and MNOs’ infrastructure are unprotected for a period of time. ²

Malware designers go to great lengths to obscure their exploits, but they also design them to change constantly so they can be repurposed quickly. This means short lifetimes aren’t necessarily a deterrent because malware can just rise again in a new form hours (or minutes) later.

Even apps designed to protect users can pose a threat because security software adds more complexity, which leads to a larger attack surface. They also typically have privileged access to devices and operating systems, and are equipped to connect with outside resources to perform their functions. This makes vulnerabilities in these apps especially dangerous. Unfortunately, naive and underfunded developers of mobile security apps can unknowingly create this exposure. Network based security solutions don’t have these limitations (and don’t impose any load on mobile batteries, processors, and memory).

As an example, a blog on IBM’s Mobile Business Insights publication stated research had discovered a security app leaking data on more than 16,000 customers including details of their full name, email addresses, phone numbers, device information and the length of their passwords. As if this flaw is not big enough, far worse problems can arise.

To summarise the overall security trend, in its October 2016 Threat Intelligence Report, Nokia revealed the rate of mobile device malware infections increased 63 per cent in the second half of 2016, with an average of 1.35 per cent of all smartphones infected. By contrast only 1.06 per cent of all smartphones were infected in April that year, and the vendor noted the rate of infection in October 2016 was the highest it had seen since it began reporting on malware in 2012. These statistics don’t include phishing and social network exploits, discussed above.

Parents also face problems coping with the growing influence of the internet on their children: they understand the variety of inappropriate content children can access and see the constant fixation on the mobile screens. Parents are looking for ways to personalise their internet access and want oversight over content and usage. They want to instil healthy online habits, mediate time online, minimise online distractions and many other things. They don’t want endless software downloads or constant configuration headaches.

**Figure 3: Loapi malware activity in late 2017**

![Figure 3: Loapi malware activity in late 2017](image)

Source: Akamai Spring 2018 State of the Internet/Security Report
2. Operator opportunity

For MNOs, security and personalisation services are an obvious opportunity as competitive pressures increase and revenue growth remains modest. Target market segments are summarised below. Service providers of all types around the world have successfully deployed services targeted at each of these segments with different business models (as covered in the case studies section).

**Consumer**
Although consumers are aware of the level of threats they face, even the most diligent usually don’t get around to protecting themselves. Potential problems with apps from reputable providers, or those that cannot be trusted not to expose personal details, mean safety-conscious consumers face an uphill battle.

In-network DNS-based security solutions make it simple for consumers to protect their devices. There’s no software to install so all they need to do is sign up. Parents can easily configure filters to block internet content based on their family’s own unique needs and preferences. They can also set time parameters to manage internet usage or pause access when they need to get children’s attention. Services from a known and trusted third party like their MNO also eliminate the risk factor of apps and subscribers who customise their service in these ways are strongly motivated to stay.

**Public Wi-Fi**
In a survey of 500 CIOs and senior IT decision makers conducted by iPass, more than two thirds of respondents said they have introduced a ban on public Wi-Fi use: 27 per cent at all times, due to security concerns.

MNOs who have Wi-Fi in their portfolio would be well served offering a foundational layer of security to change the perception of Wi-Fi as “unsafe”. DNS-based services also allow enforcement of Acceptable Use Policies (AUP) to filter content which is not appropriate in public venues. Security and content filtering services protect consumer and business customers, and the operator brand.

**Small and Medium Businesses (SMBs)**
Large businesses are challenged dealing with a mobile workforce but small businesses are far worse off. SMBs often lack IT resources and security expertise, yet 73 per cent of senior managers in these enterprises report cybersecurity is a high priority and they are looking for ways to reduce their risks, according to the Cyber Security Breaches Survey 2017 sponsored by the UK Government.

Similarly, for its Mobile Security Index 2018, US operator Verizon commissioned an independent survey of 600 professionals involved in procuring and managing mobile devices. It found 85 per cent of respondents acknowledged their businesses face mobile security threats and 74 per cent said the dangers connected with greater reliance on mobile devices have increased over the past year.

Security services offered by an MNO make it simple for SMBs to protect mobile devices their employees use. Budget constraints may limit what SMBs can spend, but a subscription model with a modest incremental line item on a monthly bill will overcome any budgetary barriers.

These summaries show consumers and small businesses are crying out for someone to step in and deliver a solution. MNOs are ideally positioned to fill that role and in the process create a new revenue opportunity; improve customer satisfaction; increase “stickiness”; and potentially lower support costs since some security problems like crypto mining can be perceived as network or device problems.
CASE STUDY 1

Challenge: A leading fixed and mobile operator in North America sought Akamai’s help in deploying family protection services for mobile devices.

The operator wanted a solution that allowed them to deliver different service levels while offering users a high degree of control.

Solved: Akamai worked with a technology partner to deploy its AnswerX solution including managed intelligent DNS resolvers alongside additional mobile client features.

Users got a variety of controls covering internet screen time and content filters, as well as a feature that allowed families to ‘pause’ internet access.

Benefits: Akamai’s lightweight solution was easy for the operator to deploy, with automated security protections that were updated constantly.

The configuration user interface was extremely simple for subscribers to use.

Outcome: The ease of deployment let the operator deliver an improved subscriber experience while reducing overall costs.

The service offered a free trial that turned into either a basic or premium paid option.

Since launch nearly 80,000 subscribers have taken out a subscription. The underlying system allows the operator to offer regular updates to fuel further growth and increase customer satisfaction.

CASE STUDY 2

Challenge: Alarmed by the impact of increases in malicious activity on its network, a large national telecom operator in Asia-Pacific concluded it needed to do more than simply educate consumers about the risks of internet threats.

The operator saw an opportunity to boost revenue and customer satisfaction by offering security-as-a-service, while also combating the rising threats to protect its infrastructure and consumers alike.

Solved: Using Akamai’s SPS Secure Consumer product, the operator developed a broadband network protection offer which it made available to all subscribers for free. Customers did not have to sign up to access the system, but could opt-out if they wished.

The system also enabled the operator to deliver a premium service with parental controls for an additional charge on their basic internet access service or as part of a more expensive broadband bundle.

Benefits: SPS Secure Consumer delivered more comprehensive threat coverage than similar systems evaluated by the operator. The resulting improvements in consumers’ security and safety increased customer loyalty, while opening up new revenue and incentive opportunities.

Outcome: Less than 2 per cent of customers opted out of the service in the three months after it was launched. In fact, this success prompted the operator to switch the paid-for element to an opt-out model.

The security service, as part of a new package of broadband bundles, contributed to a financial boost of more than $100 million in the 12 months after launch. The boost was thanks to an increase in subscribers and a reduction in subscriber re-acquisition costs after around 400,000 customers who were at risk of leaving the company were enticed to stay by the new service bundles.
The alternatives

MNOs offering security services can take advantage of the alignment of demand from consumers and SMBs described above, and limitations of alternative security solutions. Today’s cyber threats are characterised by innovation, they’re designed to propagate and bypass detection and controls by continually modifying their complexion. No-one is immune because these threats spread randomly using software flaws or social engineering.

Traditional security solutions like endpoint software are challenged when it comes to keeping up with dynamic web exploits that change constantly to avoid being detected and disabled. They’re also not well suited for protecting the rapidly expanding base of the things being installed everywhere as part of IoT rollouts.

Endpoint protections aren’t even available for IoT devices, yet there are regular reports of these devices being exploited and used for malicious purposes. The Mirai DDoS attack in October 2016 is a highly visible example. Connected cameras were loaded with specialised software and used to execute what was, at the time, the largest DDoS attack in history. Many other IoT devices have been exploited, compromising personal privacy and valuable personal data.

Deep packet inspection (DPI) has been widely used in mobile networks to manage traffic and collect data for rating and billing. DPI vendors, anxious to expand their presence in mobile networks, are now promoting security use cases. DPI systems can be programmed to look for domains (or URLs) containing malicious or unwanted content. When a request for a target domain/URL is encountered a rule can determine how it is handled.

In order to reliably support security and personalisation use cases DPI equipment must inspect every subscriber data packet since missed packets could allow an exploit to function, or unwanted content to be transmitted in a network. Since DPI systems scale with network bandwidth, costs rise accordingly. Enabling personalised services with DPI requires additional data plane processing capacity, which raises costs. Redundancy and provisions for failover increase installation cost (and complexity) even more. DPI also increases latency, which is revealed in online benchmarks or tests conducted by regulators.

In 4G networks the cost of scaling in the data plane with DPI will be substantial; at 5G data rates it will be unsustainable.

Better alternatives are needed for security and personalisation services, which is where DNS-based solutions come in.

How DNS-enabled security and personalisation services work

The DNS performs a simple, but essential function on the internet: resolving an IP address (for example 192.164.128.24) with a given domain name (www.example.com). Because it is everywhere, highly robust, super-lightweight and has scaled in parallel with the growth of the internet for more than 30 years, nearly every legitimate and malicious application and service uses the DNS.

Adding intelligence to DNS resolvers used in every network enables incoming query streams to be evaluated against dynamically changing threat feeds to identify traffic of interest. Policies can then be applied to this traffic that dictate how it is handled (see figure 4, P9). For instance, incoming DNS queries can be compared to lists of domain names known to be associated with botnets and the queries can be dropped to prevent bots from functioning.

Different dynamic feeds can enable different services, for example, feeds tracking malicious activity can be used to secure homes and small businesses, or feeds tracking categories of website content (adult, gambling, and so on) can be used to enable a parental control service. Similarly, a wide range of policies can accommodate a wide range of threats.

“In 4G networks the cost of scaling in the data plane with DPI will be substantial: at 5G data rates it will be unsustainable.”
This is an exceptionally lightweight method of identifying malicious or unwanted activity. Comparing incoming DNS queries against entries in list feeds is an operation DNS resolvers are highly optimised to do (identical to a cache look up). There is no perceptible latency for the end-user. Servers also need to enforce policies on target domains: drop, rate limit, redirect, and log (there are others), which is a small incremental effort, especially when tightly integrated into the server code.

There are situations where domain-level visibility enabled with DNS lookups is insufficient; for example when a website has been hacked and thus has a mix of benign and malicious content (or family friendly and adult content). Obtaining URL-level visibility is straightforward to enable using policies that redirect subscriber requests for domains with URLs that host targeted content to an http proxy. The proxy can identify target URLs and apply policy accordingly. Intelligently routing traffic to a proxy, using conditional forwarding, only provides additional visibility when it is needed. This strikes the perfect balance between accurate analysis of traffic, processing burden and subscriber privacy.

Figure 4: DNS resolvers can evaluate incoming queries to determine if they signal malicious or unwanted activity.

Source: Akamai
3. The next generation of mobile security and personalisation

Akamai Security and Personalisation Services (SPS) can be deployed by MNOs in their networks, in the cloud, or as a fully managed service. Akamai research teams analyse more than 100 billion DNS queries per day. Akamai SPS uses one of the world’s most accurate and extensive domain and URL databases for identifying malicious activity, with millions of validated and categorised entries maintained by Data Science experts. Pre-populated categories are continually updated to ensure new exploits (or unwanted content) are appropriately classified and automatically filtered.

These features are designed to help MNOs get a sustainable competitive advantage with:

• Rapid time to market using tightly integrated software-only applications and deployment options.
• Engaging services that encourage personalisation and give families, small businesses or Wi-Fi admins a foundational layer of security.
• Simplicity for subscribers with a service that “just works” and personalised filters that are easy to configure with a purpose built graphical portal.
• Automated protections continuously updated with the latest threat intelligence and content categories, covering every device in homes and workplaces.
• Ongoing subscriber interaction with an integrated in-browser messaging app and campaign management tools.
• A great user experience with no data plane processing and no client software.
• Proven scalability to millions of users.

Why MNOs are well positioned

MNOs are exceptionally well positioned to offer DNS-based security and personalisation solutions that are inherently biased toward their business, deployment, and operating strengths. A key advantage MNOs hold in terms of offering security is their position as a trusted brand.

“A key advantage MNOs hold in terms of offering security is their position as a trusted brand.”

When combined with their network assets this perception leaves operators well placed to upsell security services to consumers and businesses. At a stroke they can address a rapidly changing threat level not well served by traditional alternatives which struggle to keep pace, and potentially open a new revenue stream.

Getting more value from existing network assets is operationally desirable, becoming a must both in terms of protecting their own infrastructure and fending off competition from OTT providers of security services. MNOs (and converged service providers) can build a foundational layer of security and personalisation services into their existing access offerings that drives incremental revenue. They can take advantage of billing systems (and relationships) to offer different revenue models: “freemium”, free trial linked to subscription, premium access service bundles and so on.
Conclusion

High profile cyber-attacks and an increasing desire among families and small businesses for more control over internet usage are creating opportunity for MNOs.

Combining Akamai’s Security and Personalisation Services with assets including their position as a trusted brand and billing systems, MNOs can swiftly deploy security-as-a-service as an additional revenue generator using multiple business models, in turn increasing overall customer satisfaction.

These DNS-based solutions are easy to set-up and maintain (particularly when compared with traditional security solutions), work across multiple access technologies and are simpler to update to keep pace with a rapidly changing threat landscape.
As the world’s largest and most trusted cloud delivery platform, Akamai makes it easier for its customers to provide the best and most secure digital experiences on any device, anytime, anywhere. Akamai’s massively distributed platform is unparalleled in scale with over 200,000 servers across 130 countries, giving customers superior performance and threat protection. Akamai’s portfolio of web and mobile performance, cloud security, enterprise access, and video delivery solutions are supported by exceptional customer service and 24/7 monitoring. To learn why the top financial institutions, e-commerce leaders, media and entertainment providers, and government organisations trust Akamai please visit www.akamai.com, blogs.akamai.com, or @Akamai on Twitter.

Produced by the mobile industry for the mobile industry, Mobile World Live is the leading multimedia resource that keeps mobile professionals on top of the news and issues shaping the market. It offers daily breaking news from around the globe. Exclusive video interviews with business leaders and event reports provide comprehensive insight into the latest developments and key issues. All enhanced by incisive analysis from our team of expert commentators. Our responsive website design ensures the best reading experience on any device so readers can keep up-to-date wherever they are.

We also publish five regular eNewsletters to keep the mobile industry up-to-speed: The Mobile World Live Daily, plus weekly newsletters on Mobile Apps, Asia, Mobile Devices and Mobile Money.

What’s more, Mobile World Live produces webinars, the Show Daily publications for all GSMA events and Mobile World Live TV – the award-winning broadcast service of Mobile World Congress and exclusive home to all GSMA event keynote presentations.

Find out more www.mobileworldlive.com

Disclaimer: The views and opinions expressed in this whitepaper are those of the authors and do not necessarily reflect the official policy or position of the GSMA or its subsidiaries. © 2018