Research Report

The State of the Signaling Firewall Landscape

November 2021

Published by:

mobileum

Mobilesquared
Communicating data

Introduction

Signaling networks are coming under increasing pressure from rogue companies exploiting weaknesses to defraud subscribers. To date, only a small percentage of mobile operators have deployed a truly-effective signaling firewall to detect and deflect attacks, leaving the majority of mobile networks prone to fraud, damage to their brand, and the ultimate threat of losing loyal customers.

Since early 2020, the world has fundamentally changed as consumers and businesses alike turn to their mobile devices to address and overcome the societal changes that have been forced upon the world by the pandemic and lockdowns. eCommerce and finance are two sectors that have become increasingly reliant on smartphones, in particular during the pandemic. However, the growth in financial transactions and information traversing mobile networks have not gone unnoticed by fraudsters and hackers who are attracted to any potential network weaknesses like a shark to blood.

Not surprisingly, then, network security specialist Mobileum says that there has been an exponential increase in security attacks on mobile operator networks since the start of the pandemic. Mobileum's Threat Intelligence researchers observed that these attacks are increasing in frequency and will only get worse.

A lot of the attacks fail to register with the mobile operator being targeted, but when an attack is successful, it can have a devastating impact on the mobile operator and its subscriber base as well as its reputation. The press is quick to jump on a hard-luck consumer story as a result of potential negligence or neglect from a mobile operator. And typically national security and nation state espionage stories are becoming an all-too-common feature on front pages in recent years.

To date, mobile operators have been slow to respond to the threat posed to their signaling network. But as the threats become more real, more frequent, and increasingly more public, signaling firewalls are becoming more of a priority to mobile operators big and small, but also within trade bodies such as the GSMA, tasked with the role of protecting its mobile operator members.

Mobile operators are now starting to look at either investing in a signaling firewall or investing on their already existing signaling firewall, to improve their signaling security layers.

To understand how signaling firewalls are being deployed, what level of protection they are providing, and how mobile operators are looking to harden the security of their networks, Mobilesquared conducted research into the implementation of signaling firewalls on behalf of Mobileum in 1H2021. The research was based on an online survey of 40 participating mobile operators, predominantly Tier 1. The findings have been shared in the following report.

Executive Summary

- Mobilesquared's industry research reveals that 17% of mobile operators had installed a signaling firewall as of 2020, with a further 34 deployments expected during 2021, taking the total to just under one-quarter (24%) by the end 2021. Mobilesquared predicts sustained growth in the number of mobile operators investing in a signaling firewall up to 2025, by which point 49% of all mobile operators will have a signaling firewall, providing protection for at least one protocol (SS7).

- Mobileum says that there has been a dramatic increase in signaling attacks on mobile operator signaling networks over the last 18 months

- Mobile operators must strive to achieve 100% detection of threats and attacks over their signaling network.

- A dedicated cross-protocol signaling firewall is the most secure protection available to an MNO.

Key MNO research findings

Majority of mobile operators yet to invest in signaling firewall; only one-third of active signaling firewalls capable of protecting across multiple protocols:

- Just under one-fifth of MNOs believe their signaling firewall can detect and prevent over 90% of network security attacks. The majority of respondents (44%) believe their signaling firewall can detect and prevent an average of 80% of attacks.

- One quarter of MNOs stated that 75% of security attacks cannot be detected by their signaling firewall. Just 31% of MNOs said that their signaling firewall could perform cross-protocol correlation. All signaling firewalls protect SS7, but that drops to 56% for Diameter, one-quarter for GTP, and 19% for SIP.

- Diameter has been identified as the one protocol that is under increasing pressure from security attacks.

- Attack typology is constantly changing. MNOs stated that an attack resulting in network information disclosure is the biggest network security threat they face in 2021, followed by badly formed or unexpected messages, call interception, CLI spoofing, and SMS interception.

Too many MNOs are adding needless complexities and ineffective bolt-ons to try and protect their signaling network:

- There is a 50-50 split between MNOs that use a single, dedicated firewall provider and those that use multiple suppliers to cover different protocols.

- A number of MNOs mistakenly use STP, DRA, or SBC as signaling firewalls in the belief that this offers the same level of protection as a dedicated signaling firewall.

- Half of MNOs with a signaling firewall (primarily those using the above approaches) said that they have identified vulnerabilities and weaknesses in their signaling firewall because of misconfigurations due to complexity of design and user interface.

Machine learning, advanced firewall features, and threat-sharing intelligence are critical if a MNO strives to achieve 100% threat and attack detection level.

- MNOs rate the importance of machine learning as part of their signaling firewall as “4 out of 5”, with 5 being critically important.

- As of 2021, just over half of MNOs said that their signaling firewall was applying machine learning.

- Two-thirds of MNOs with signaling firewalls will have at least five of the advanced options listed in the research on their signaling firewall within the next 12 months; recurring updates, intuitive user interface, explainable AI, cross-protocol correlation, architecture flexibility, and firewall as a service.

- One-third of MNOs subscribe to a threat-sharing intelligence service.

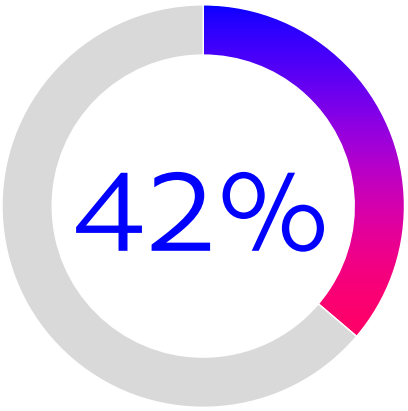
- MNOs require education on signaling firewalls.

The State of the Signaling Firewall Landscape

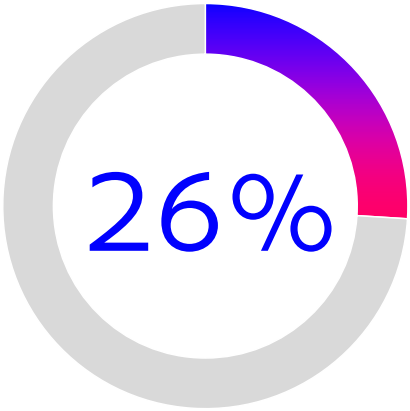
Research into the threats faced by mobile network operators (MNOs) over their signaling network, reveals the constant changes in attack typology across multiple signaling protocols, in particular over DIAMETER, allied with the sheer volume of attacks, that MNOs' networks face on a regular basis. The research of MNOs in 1H 2021 by Mobilesquared on behalf of Mobileum, uncovered that just 6% of total MNOs would be classified as having a fully-protected signaling network, despite the growing threat of attacks posed by rogue groups and individuals determined to unleash chaos and disruption in the pursuit of financial gain.

Before we explore the research data, let's look at where the market is in terms of signaling firewall deployments. Mobilesquared market data estimates that 17% of MNOs globally had deployed a signaling firewall by the end of 2020, with a further 34 deployments expected during 2021, taking the total to just under one-quarter (24%) by the end of 2021.

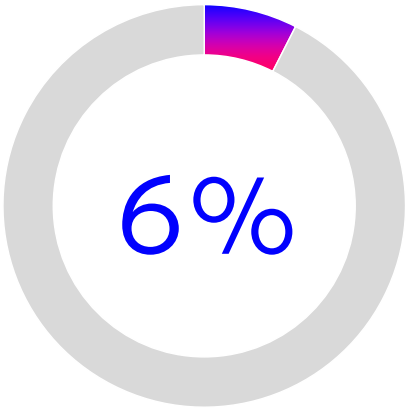
If we breakdown the deployments of signaling firewalls to date, Tier 1 MNOs are clearly ahead of Tier 2 and Tier 3s when it comes to protecting their signaling network. At the end of 2020, Tier 1 MNOs accounted for 50.4% of total signaling firewall deployments, followed by Tier 2 (31%), and Tier 3s (18%).



of Tier 1 MNOs have deployed a signaling firewall by end 2020



of Tier 2 MNOs have deployed a signaling firewall by end 2020

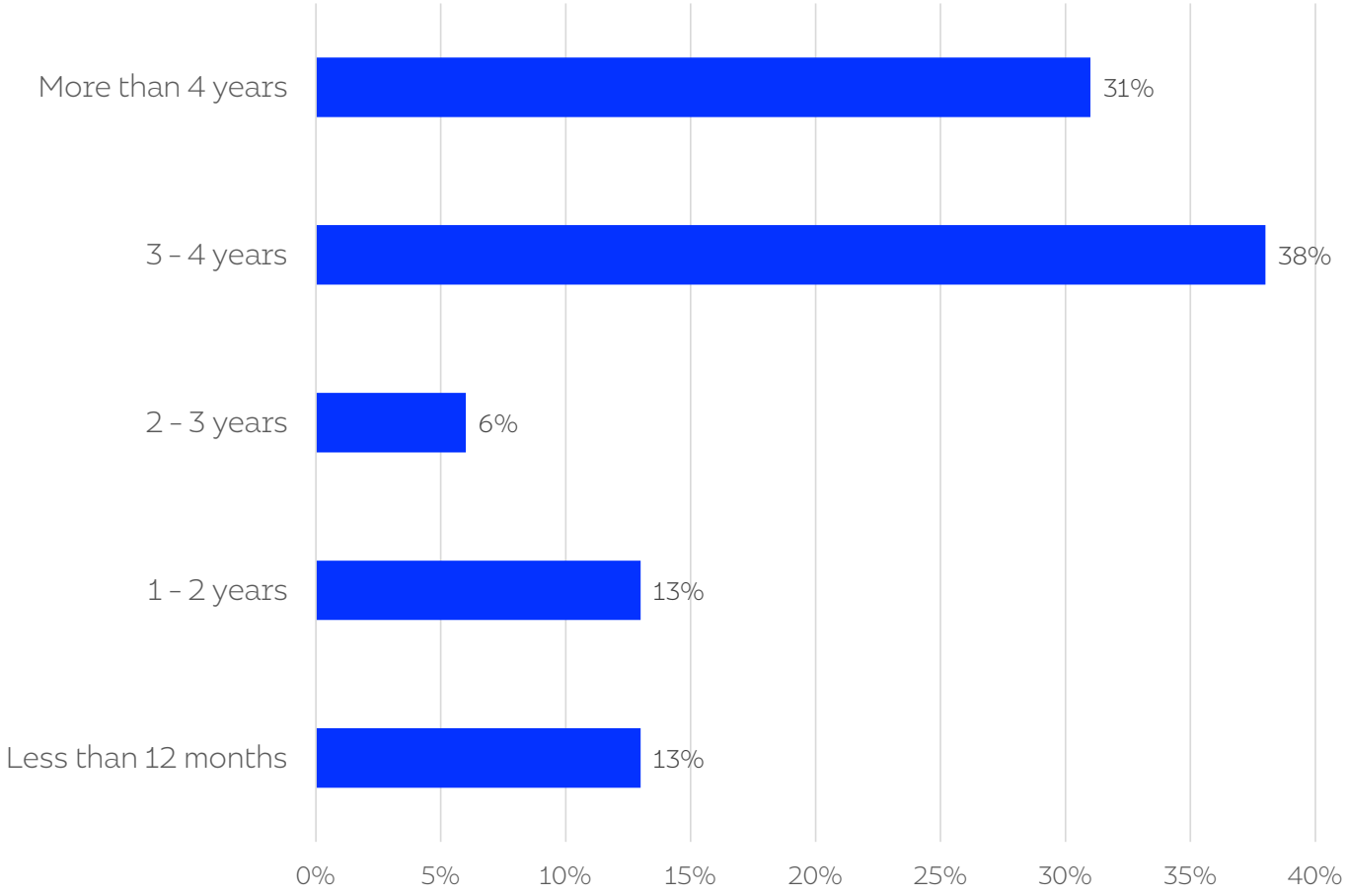


of Tier 3 MNOs have deployed a signaling firewall by end 2020

By overlaying the 2021 mobile operator research to the Mobilesquared market data, it provides significantly deeper insight into the state of the signaling firewall landscape.

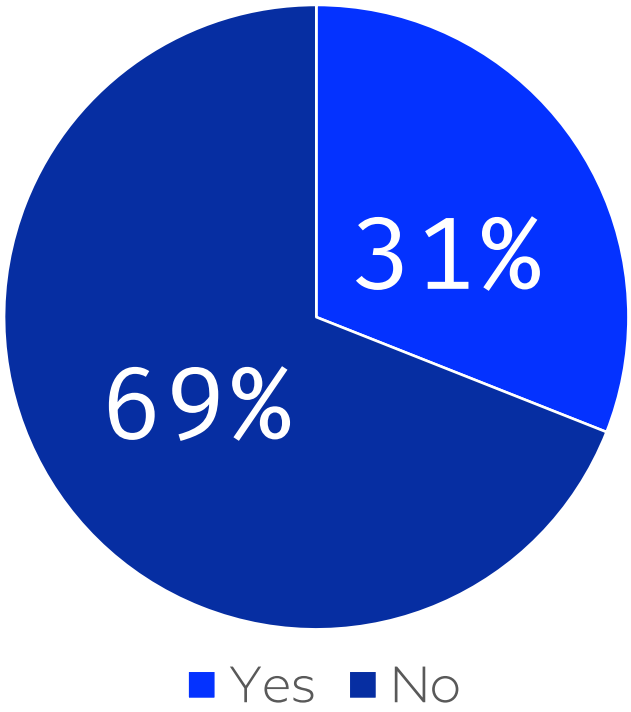
For instance, the 2021 MNO research revealed that 69% of operators that have deployed a signaling firewall have been operating it for more than 3 years, with the majority of these respondents being Tier 1s, closely correlating with the market data. The research also highlighted that, typically, Tier 2 and Tier 3 MNOs have increasingly looked to invest in protecting their signaling network in the last 3 years, with this trend set to continue in the coming years. Forty percent of MNO respondents intend to invest in a signaling firewall over the next 24 months.

For how long have you been operating your signaling firewall?



According to those MNOs that have deployed a signaling firewall, less than one-third (31%) said that it could perform cross-protocol correlation, such as correlating information and identifying abnormal patterns across different signaling protocols. This is actually an alarming statistic because attacks often occur over multiple protocols, so unless a signaling firewall can provide cross-protocol protection, the network remains exposed to the hackers and fraudsters looking to systematically exploit all points of entry that they can identify.

Does your signaling firewall perform cross-protocol correlation?

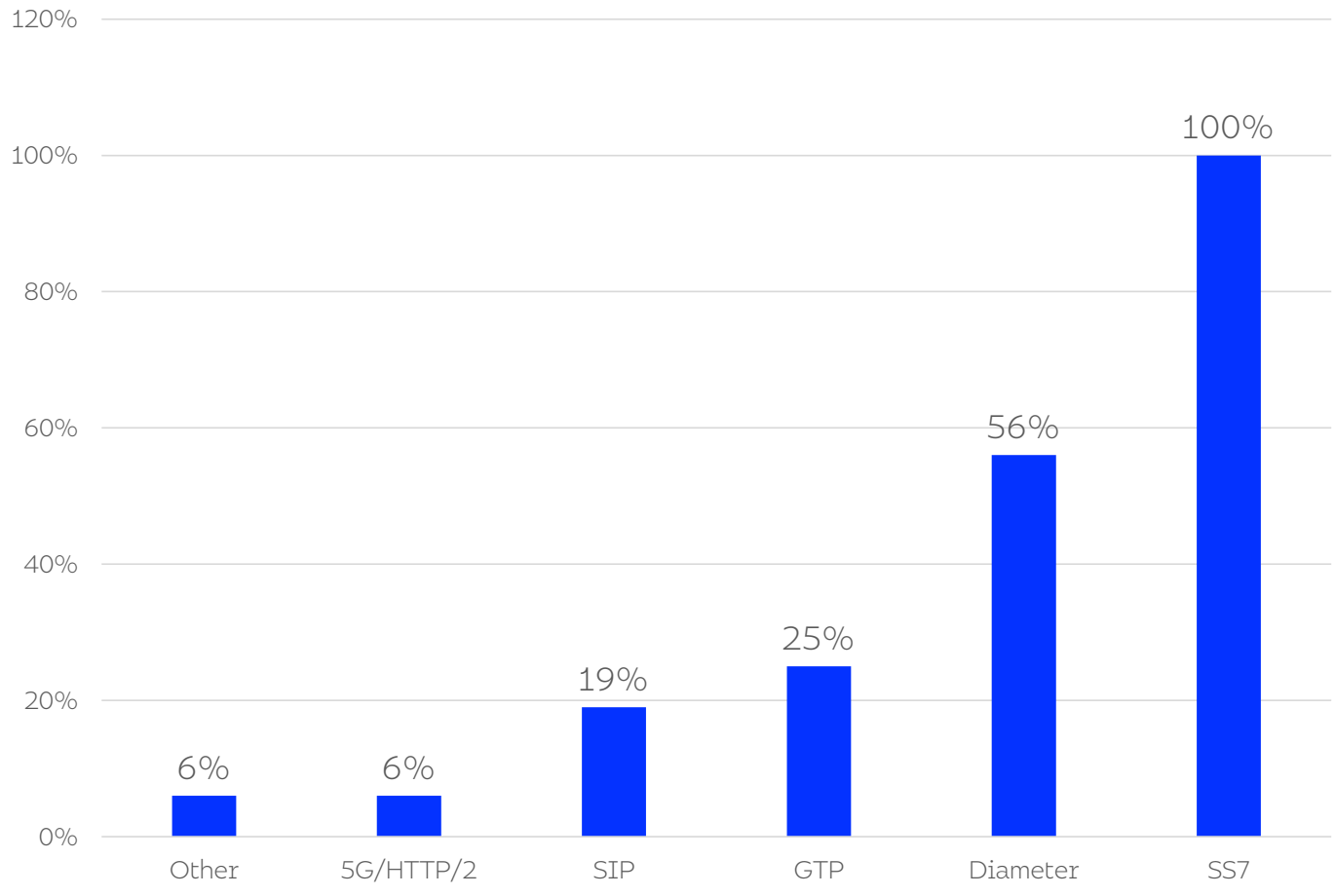


Source: Q12; Does your signaling firewall perform cross-protocol correlation? By cross-protocol correlation, we mean correlating information and abnormal patterns across different signaling protocols to identify likely network security threats.

When we apply this research (31% of signaling firewalls performing cross-protocol correlation) to the market data, it indicates that only 6% of mobile operators are likely to have cross-protocol protection provided by their signaling firewall.

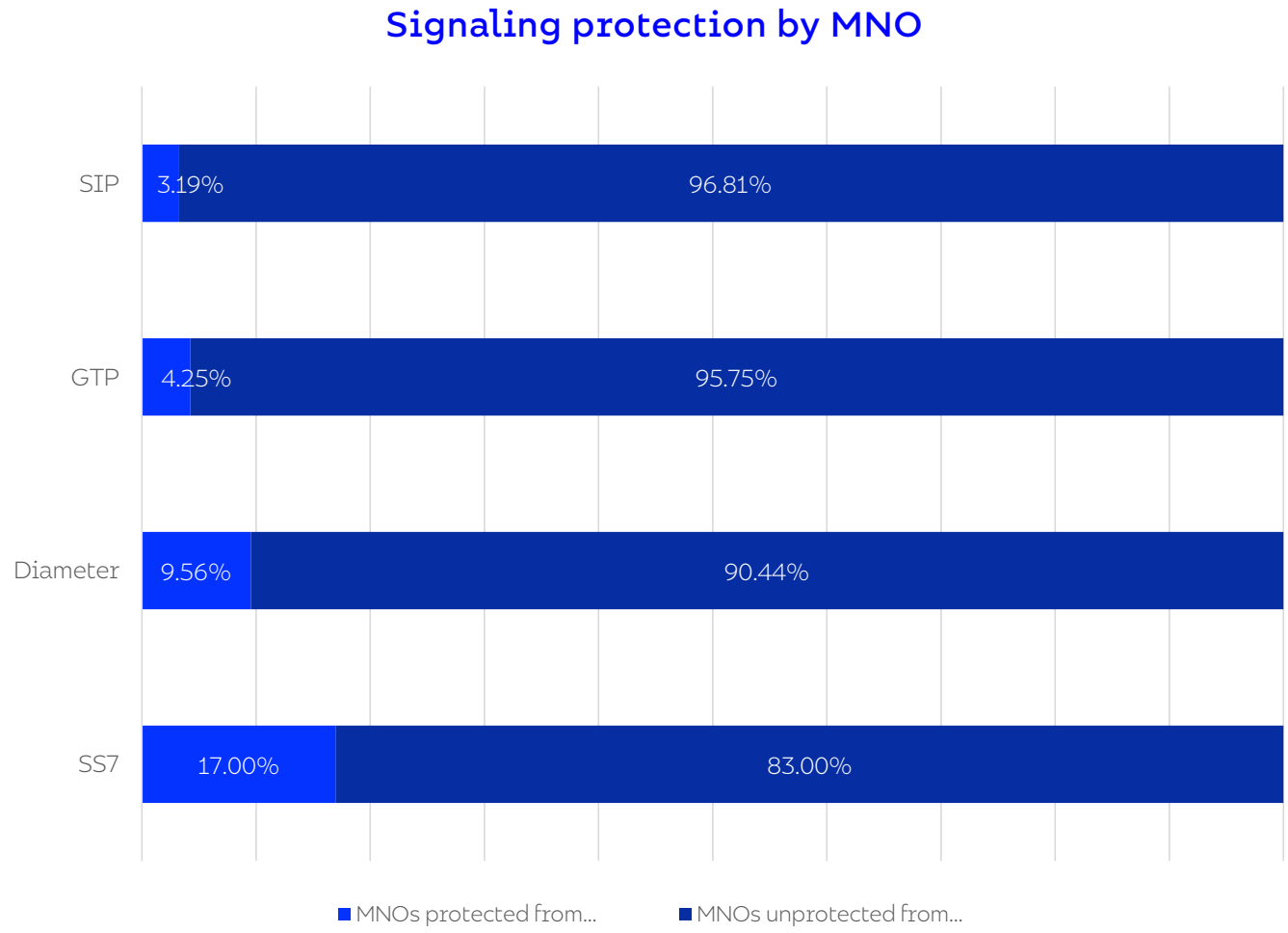
The one protocol that is most protected is SS7, with 100% of signaling firewalls protecting it. Then, there is a significant drop to the next protocol, with just over half of firewalls protecting Diameter (56%), a quarter protect GTP, and just under one-fifth protect SIP. Given that Diameter has been identified as the one protocol that is under increasing pressure from security attacks and has been highlighted as an area of key concern, it is not surprising that it is featuring more prominently among multi-protocol signaling protection, and highlights that mobile operators are reacting to the threat.

For what protocols does your signaling firewall provide protection?



Source: Q10; For what protocols does your signaling firewall provide protection? Please select all that apply?

When the research data is applied to the market data, it reveals that SS7 is protected on every mobile operator that has deployed a signaling firewall (17% of total MNOs) , whereas Diameter features on a total of 10% of MNO networks, GTP 2% and SIP on 1% of total deployed signaling firewalls.



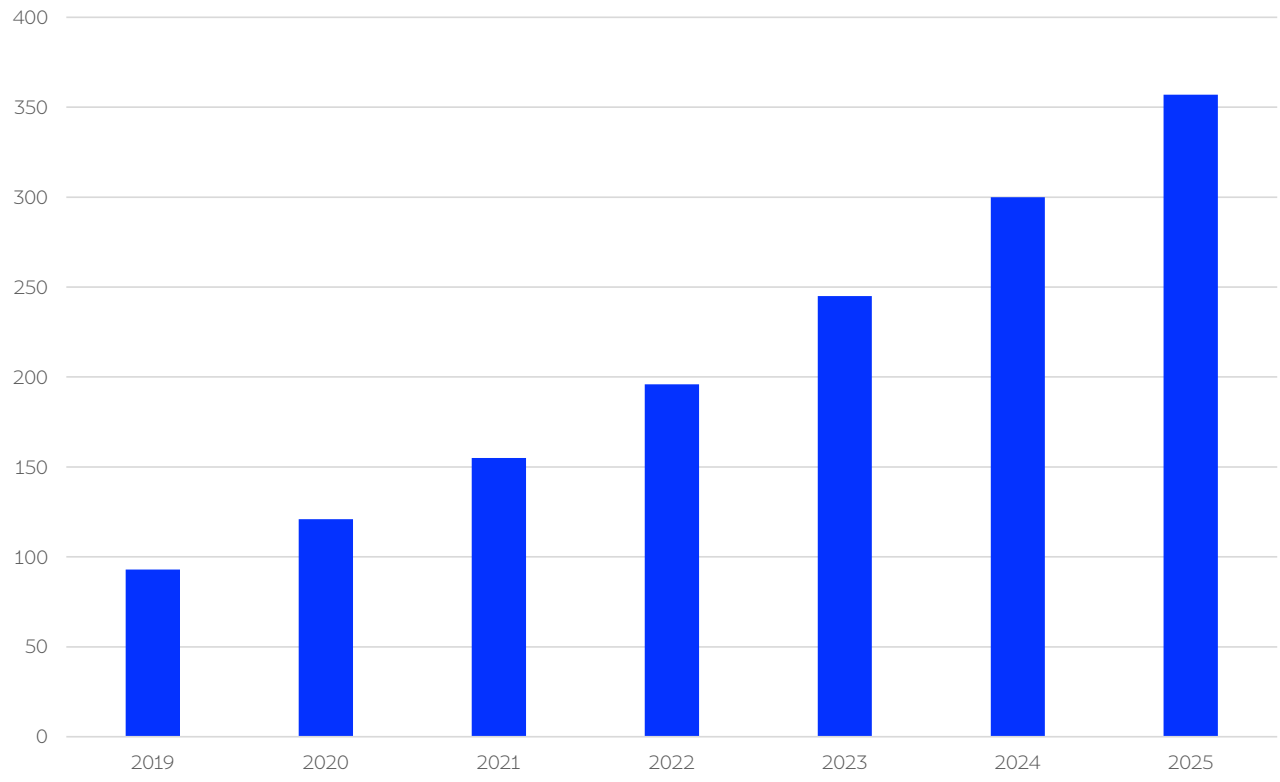
44% of respondents claim their signaling firewall provider covers all protocols required, while the same number said they relied upon different suppliers to cover different protocols.

The 17% of MNOs with signaling protection looks set to grow considerably in the coming years. The Mobilesquared market data reveals that sales of signaling firewalls will overtake sales of SMS firewalls in 2022, providing the first indication that MNOs are evolving beyond network monetisation (of A2P SMS) and towards network protectionism, which has to be seen as a positive customer-driven initiative.

Mobilesquared predicts sustained growth in the number of mobile operators investing in a signaling firewall up to 2025, by which point 49% of all mobile operators will have a signaling firewall, providing protection for at least one protocol (SS7). At this point, 100% of Tier 1 mobile operators will have a signaling firewall, 80% of Tier 2s, and 28% of Tier 3s.

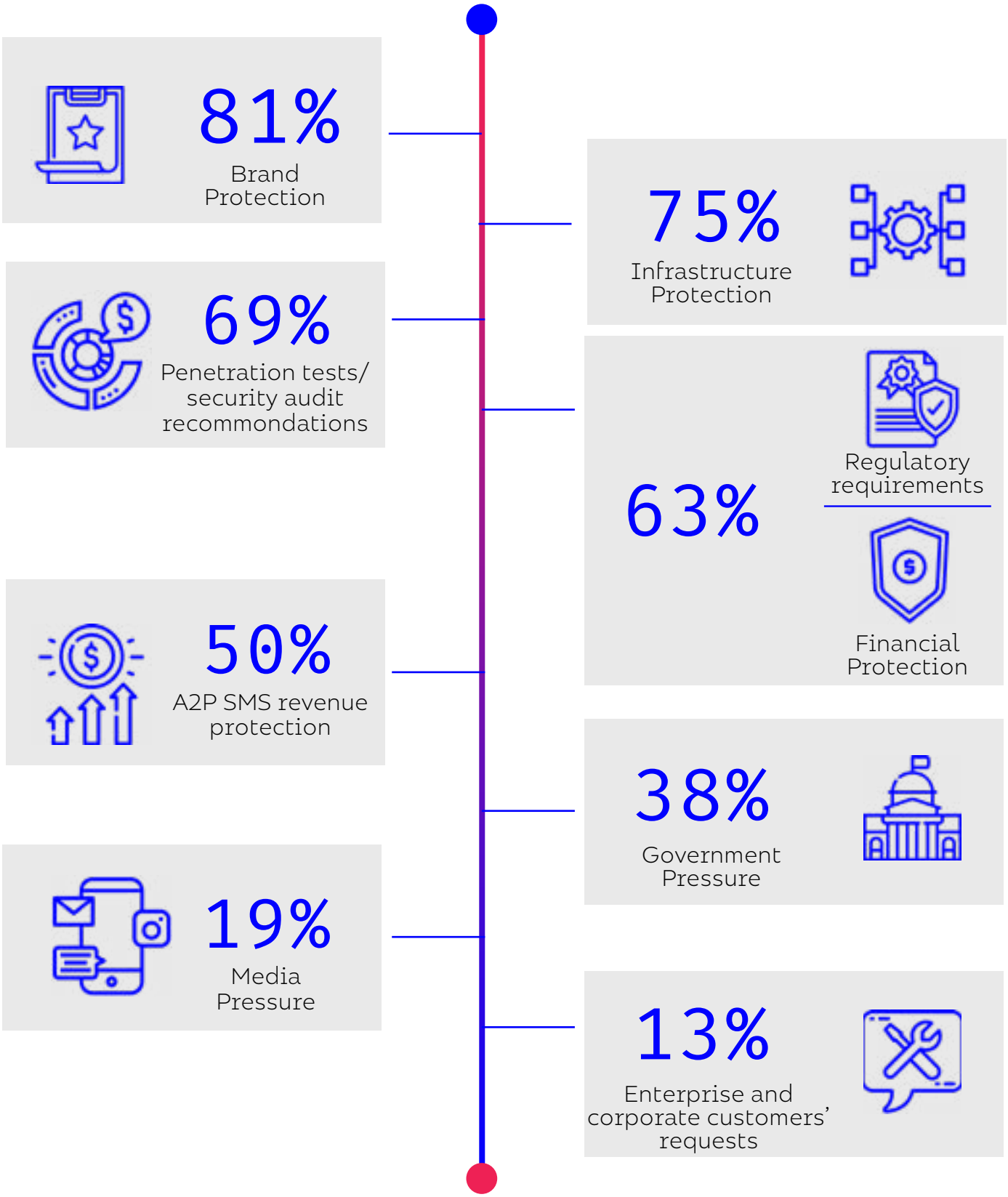
That is not to say their investment stops. As this section has highlighted, the need to provide cross-protocol protection is paramount, and if a signaling firewall is only protecting SS7, the mobile operator's network remains extremely vulnerable still to attacks.

Signaling Firewalls deployed



Signaling protection has not been seen as a priority investment for mobile operators more focused on areas that generate a direct return, such as 5G and IoT. The primary motivation to invest in a signaling firewall – aside from brand protection – is to protect network infrastructure, and to be in a position to defend against penetration tests and meet security audit recommendations, leaving the monetisation component as more of a secondary reason.

What are the motivations and business case behind your investment in a signaling firewall?



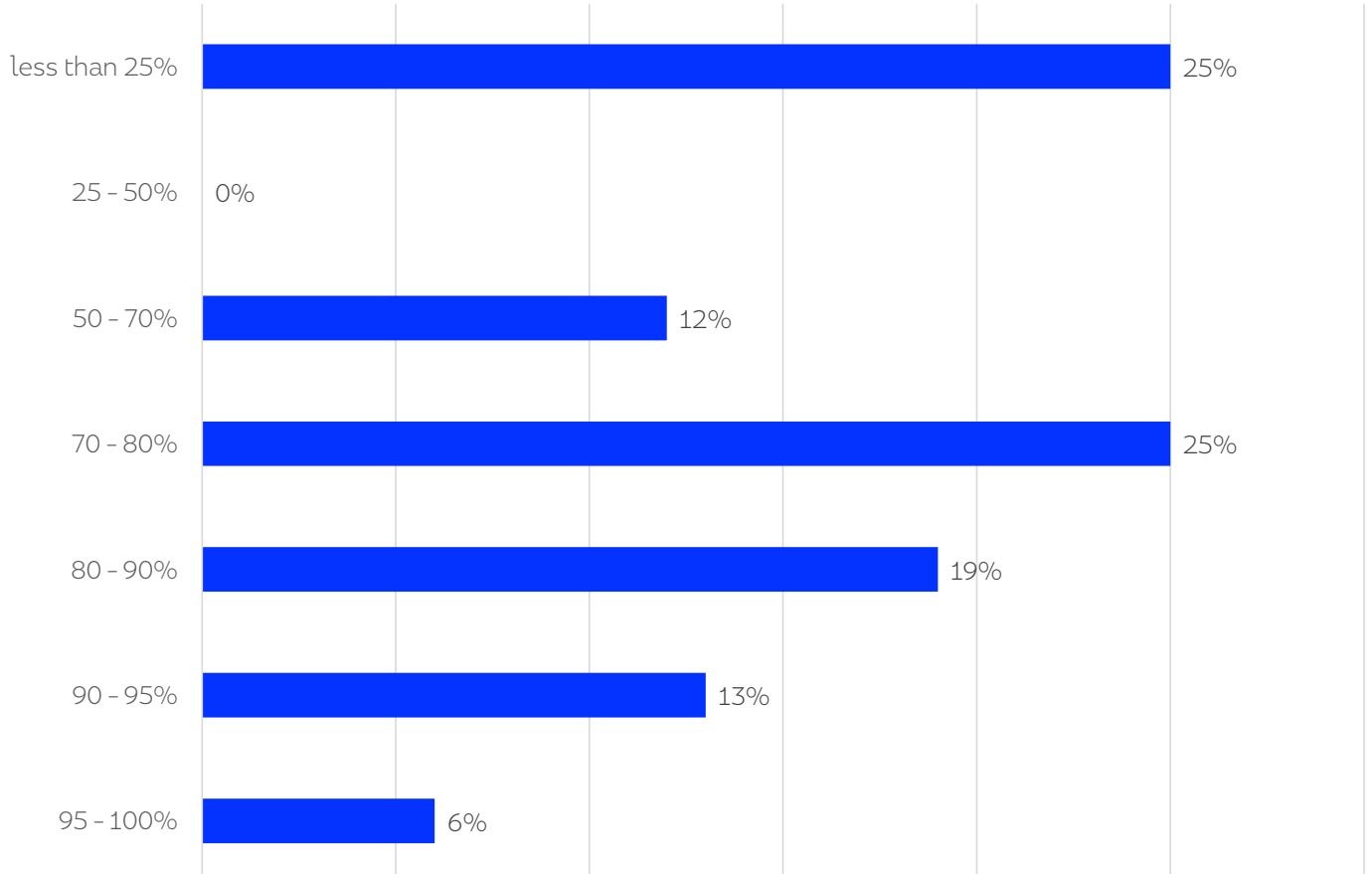
Source: Q21; What are the motivations and business case behind your investment in a signaling firewall?

Enhancing signaling firewall performance

One of the biggest lessons learnt by MNOs since deploying a signaling firewall, according to the research, is trying to grasp the constant threats their networks face on a regular basis by changes in attack typology across multiple signaling protocols.

To ascertain how signaling firewalls are performing, just under one-fifth of MNOs believe their signaling firewall can detect and prevent over 90% of network security attacks. The majority of respondents (44%) believe their signaling firewall can detect and prevent between 70 and 90% of attacks. Even more startling is the fact that one-quarter of MNOs believe they can only detect 25% of security attacks. In other words, a quarter of MNOs believe that 75% of security attacks go undetected even if they have a firewall.

What percentage of network security attacks do you think your signaling firewall is able to detect and prevent?



Source: Q16; What percentage of network security attacks do you think your signaling firewall is able to detect and prevent?

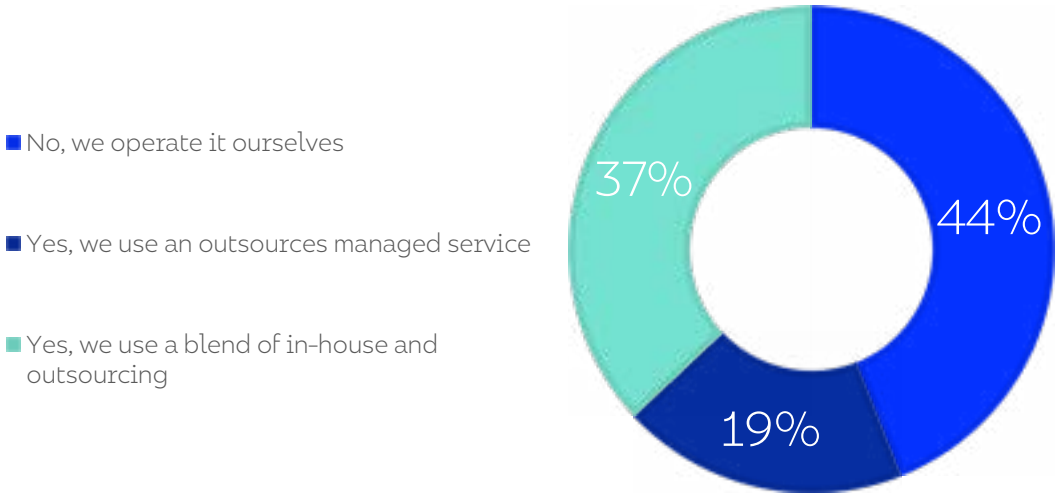
The research highlights that even for what is considered the most secure MNO capable of detecting 95-100% of network security attacks, the issue they face is that up to 5% of attacks that go undetected could be the ones that are the most damaging.

So, the aim for any mobile operator has to be 100% detection, but how can they achieve this?

How to achieve 100% detection

The first action concerns the operation of the signaling firewall. According to the research, the majority of MNOs (44%) operate the signaling firewall in-house, with 19% opting for an outsourced managed service provider, and 37% a blend of in-house and outsourced.

Do you rely on managed services solutions for operating your signaling firewall?



Source: Q10; Do you rely on managed services solutions for operating your signaling firewall?

The research also revealed that half of MNOs use a single, dedicated firewall provider, whereas the remainder use different suppliers to cover different protocols. In addition, a number of MNOs state that they do not use a signaling firewall because they believe they are getting protection from their STP, DRA, or SBC. They are not, and such approaches should only be viewed as 'bolt-ons' trying to replicate a signaling firewall.

The fact remains that MNOs relying on STP, DRA, or SBC for network protection, or using multiple firewall providers, are adding unnecessary complexities as they need to be configured and managed in a coordinated manner. This is not happening to the level required to ensure network protection anywhere close to the desired 100% detection. Any inconsistencies in the configuration of these platforms leaves a window of opportunity open to attackers.

Consequently, half of MNOs with a signaling firewall said that they have identified vulnerabilities and weaknesses in their signaling firewall because of misconfigurations due to complexity of design and user interface. Clearly, a dedicated cross-protocol signaling firewall is viewed as the most secure protection available to an MNO.

What are the greatest threats?

Interception is one of the attacks that has, and will continue to be picked up by the press and feature with a damning headline. Something that every MNO is keen to avoid.

An MNO must identify the primary network security attacks that signaling firewalls are trying to detect. Based on the research, in 2021 'network information disclosure' remains the biggest network security threat for an MNO, followed by 'badly formed or unexpected messages', 'call interception', 'CLI spoofing', and 'SMS interception'.

Call interception and SMS interception are network privacy issues that will have a direct impact on subscribers. Similarly, as a result of the pandemic, the use of one-time passwords over SMS has increased exponentially, and that could provide access to an email account and become an infringement on personal privacy. Network information disclosure could lead to user tracking, fraud, and ultimately threaten the user's safety, not to mention a host of other unwanted outcomes.

The least relevant threats, as identified by the MNOs in 2021, are profile modification and PBX hacking. Although for the purposes of the research we presented 13 fraud types, the fact remains that there are a multitude of unidentified security threats and the overall list will only expand, making the requirement for a signaling firewall all-the-more pressing.

What are the biggest network security threats that you have to deal with?

1. Network information disclosure
2. Badly formed or unexpected messages (potentially causing system outages)
3. Call interception
4. CLI spoofing
5. SMS interception
6. Subscriber information disclosure
7. Subscriber location disclosure
8. Data session hijack
9. DDoS (subscriber or machine)
10. DNS tunnelling
11. IoT device inflection
12. Profile modification (e.g. for free calls
13. PBX Hacking (SIP password or device hacking)

Source: Q17; What are the biggest network security threats that you have to deal with? Please rank based on importance, 1 being the biggest threat, and 13 the least relevant

MNOs need to be able to keep up with developments of security threats. Machine learning is going to play a critical role in the future in terms of network security, and is the only way an MNO can efficiently sift through 100 million event detail records over a network on a daily basis. There are simply too many records to process manually. Not surprisingly, MNOs rate the importance of machine learning as part of their signaling firewall as "4 out of 5", with 5 being critically important. As of 2021, just over half of MNOs said that their signaling firewall was applying machine learning.

Feature advancement of signaling firewalls

Aside from machine learning, new features are being added to signaling firewalls. By looking at what is available today on existing signaling firewalls, according to our MNO respondents, it reveals the most popular feature is recurring updates on threats, followed by architecture flexibility, and intuitive user interface. Explainable AI and cross-protocol correlation are the least deployed features among respondents, along with firewall as a service.

In contrast, to highlight what is the next wave of features to be applied to signaling firewalls, we can look at what is being developed. Cross-protocol correlation and intuitive user interface are the most popular, followed by firewall as a service.

If we assume that "being developed" covers the next 12 months, then 88% of respondents' signaling firewall will feature recurring updates on threats, within 1 year. 81% believe that their signaling firewall will feature an intuitive user interface. Just under two-thirds of respondents expect their signaling firewall to feature cross-protocol correlation, and 38% with explainable AI.

What is the status of the following features in your current signaling firewall?

	Available/being developed	Not available / not priority
Explainable AI	38%	62%
Firewall as a Service	56%	44%
Cross protocol correlation	63%	37%
Architecture flexibility	69%	31%
Intuitive User Interface	81%	19%
Recurring updates on threats	88%	12%

Source: Q19; What is the status of the following features in your current signaling firewall?

For an MNO network to approach anywhere near 100% detection of security threats, the majority of the six categories listed will need to work in unison. But the research results provide visibility on how MNOs anticipate their signaling firewalls to evolve. For instance, on average, almost two-thirds of MNOs with signaling firewalls will have at least five of the advanced options listed in the research on their signaling firewall within the next 12 months.

In addition to these enhancements, MNOs can now also subscribe to threat-

sharing intelligence services to complement and enrich their signaling firewall. As we have highlighted earlier in this report, the attack typology is constantly changing, so being kept abreast of this development is of paramount importance to an MNO.

A threat intelligence service amasses and aggregates a huge amount of information, such as new threat information and how attacks are changing, and tries to identify the evolving typology of attacks. At present, just under one-third of MNOs subscribe to such a service.

Expectations for 2021

For the minority of MNOs that have deployed a signaling firewall, the clear driving factor for the investment is to protect their brand, and ultimately their customers. The last thing any mobile operator wants is to have its brand and logo plastered all over the media because of its failure to protect even one subscriber from fraudulent activity. With attacks happening with increasing regularity, especially following the pandemic and lockdowns during which our mobile devices have played an even more prominent role in our lives, protection has become even more critical.

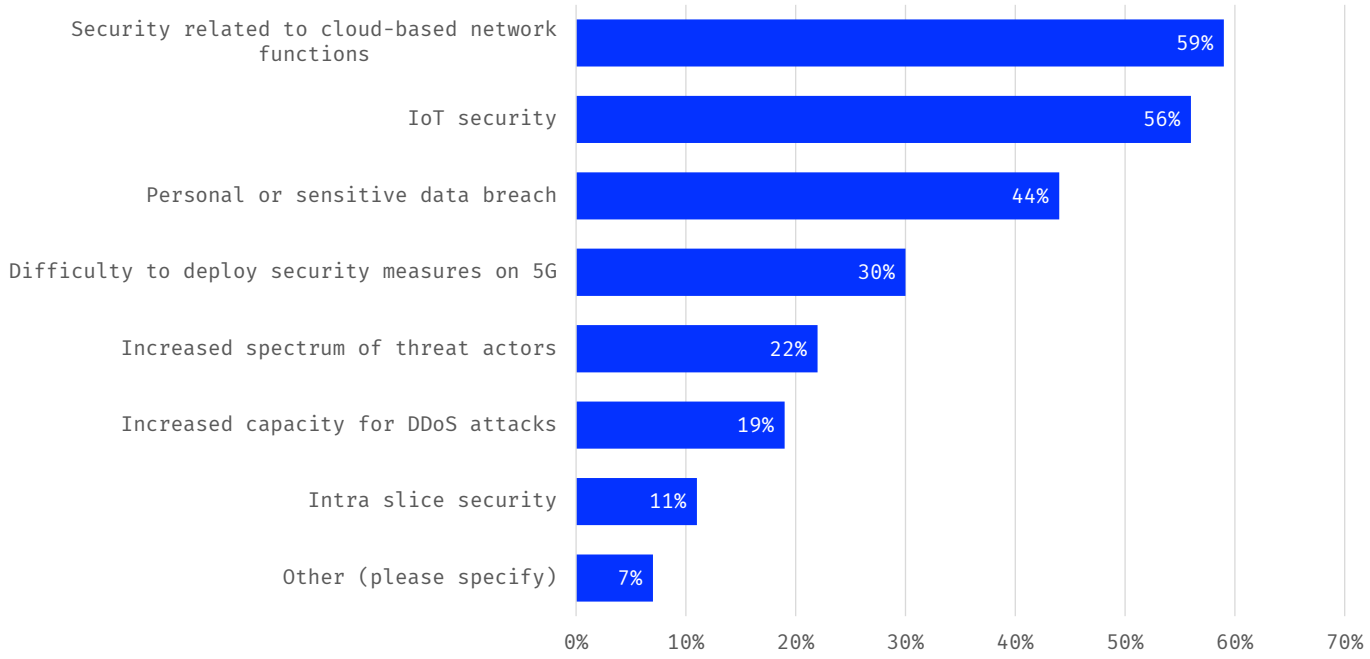
The damage to an MNO could be devastating. Over 50% of a mobile operator's subscriber base have previously said that they would potentially look to switch provider following a security breach. And even if the subscribers remain with the mobile operator following a breach, more than three-quarters would have lost trust in their provider. There is no coming back from that for a MNO.

52% of consumers and 58% of enterprises will leave or consider leaving their existing mobile provider following a security breach, up from 25% in 2017.

77% of consumers and 86% of enterprises will no longer trust/trust less their operator following a security breach.

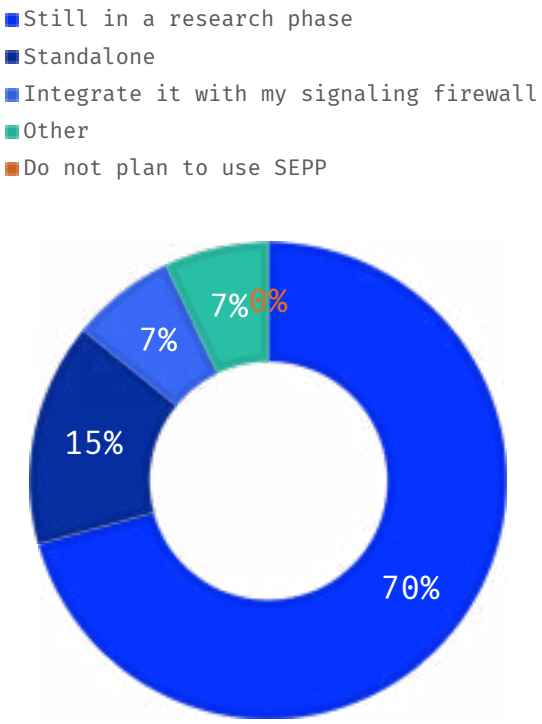
Source: Mobileum/Mobilesquared consumer research, 2018

Looking to the future – and now for a number of mobile operators – network security concerns are only going to be exacerbated with the rollout of 5G. The research revealed that 59% of MNOs stated that security relating to cloud-based network functions is their biggest network security concern based on the rollout of 5G. That was followed by IoT security (56%), and personal or sensitive data breach (44%).



Source: Q26; What are your biggest network security concerns as you start rolling out 5G?

Something that features heavily in discussions around 5G right now is that role that SEPP (Security Edge Protection Proxy) will play in enabling secure roaming between 5G networks. SEPP is already being mistaken as a 5G firewall, in the same way SBC, DRA, and STP have become confused with firewalls. As the research highlights, it is still early days, with the majority of MNOs (70%) stating that they are still researching their SEPP strategy, 15% have already adopted a standalone strategy, while 7% intend to integrate it with their existing signaling firewall.



Source: Q27; What is your strategy if you plan to use SEPP in your 5G core?

Conclusion

The majority of mobile operators are yet to invest in a signaling firewall. Only one-third of active signaling firewalls are capable of protecting across multiple protocols, with SS7 and Diameter the most protected.

The research has revealed that a significant percentage of mobile operators believe that their signaling firewalls cannot detect security attacks.

Education among MNOs is essential to understand how a signaling firewall can successfully detect the increasing number of threats and hacks that are happening on a more frequent basis. Too many MNOs have developed complex and ineffective bolt-ons designed to protect their signaling firewall. This has led to misconfigurations and compounded the threat to the mobile operator.

To work towards the 100% detection goal, each mobile operator must deploy an advanced signaling firewall allied with machine learning, and a threat-sharing intelligence service.

The research confirms the heightened importance that mobile operators are now placing on signaling firewalls and the elements required to truly protect their brand, network and subscribers.

Methodology

Mobileum worked closely with Mobilesquared to create a survey for relevant personnel working in the mobile operator environment. The survey as distributed using Mobilesquared's opt-in database in addition to being promoted at online security events. The survey ran during 1H2021.

The Mobilesquared market data is based on on-going research of the firewall sector, and is based on data and information shared by mobile operators and firewall providers. Where applicable, Mobilesquared applied the online survey data to its signaling firewall market data to provide greater perspective in terms of research findings and how this potentially impacts mobile operators.

Mobileum is a leading provider of Telecom analytics solutions for roaming, core network, security, risk management, domestic and international connectivity testing, and customer intelligence. More than 1,000 customers rely on its Active Intelligence platform, which provides advanced analytics solutions, allowing customers to connect deep network and operational intelligence with real-time actions that increase revenue, improve customer experience and reduce costs. Headquartered in Silicon Valley, Mobileum has global offices in Australia, Dubai, Germany, Greece, India, Portugal, Singapore and UK.

More in **www.mobileum.com** and follow @MobileumInc on Twitter.

#1 FOR BUSINESS MESSAGING INTELLIGENCE

Mobilesquared is the go-to partner for definitive business messaging market intelligence. We produce the most comprehensive independent global forecasts in the industry, trusted by brands including Mastercard, Vodafone, Google, Telstra, LivePerson, Telefonica, and PwC for accuracy. If you need targeted messaging market insight and future-proofed strategy, we can help. Find out more about which areas of the messaging market we're actively researching, including our databooks, reports, and precision intelligence tool MessageMap IQ.

mobileum

Action driven by intelligence

MOBILEUM, INC.
20813 Stevens Creek Boulevard, Ste. 200
Cupertino, CA 95014 USA

Phone: +1-408-844-6600
Fax: +1-408-252-1566

mobileum.com