White Paper

HardenStance

Learnings from Real World Telco Security Incidents

By Patrick Donegan, Principal Analyst, HardenStance

Sponsored by

January 2021

Executive Summary

- Recent cyber security incidents demonstrate how vulnerable telcos and their customers are to a wide variety of threats including DDoS, ransomware and SS7 attacks, as well as attacks that exploit vulnerabilities in APIs and web servers.
- Telco security must not just be viewed through the prism of 3GPP security standards; perceived risk associated with Chinese vendors; and advanced nation state threats. Most telco security incidents arise independently of these factors.
- As they evolve with digital transformation and a cloud native deployment model, telco security strategy should prioritize applying more rigour - and up to date thinking and techniques - to addressing long-standing vulnerabilities.

Many incidents have occurred that telco victims haven't even discovered yet.

Security Incidents Exploiting a Wide Variety of Vulnerabilities

Unfortunately, telco security is often viewed mainly through the lens of advanced nation state attacks and compliance with 3GPP security standards – as well as, more recently, in terms of the perceived risk associated with using Chinese telecom vendors. It's unfortunate because the day-to-day operational experience of telco security teams demonstrates that these three very high profile factors that tend to dominate most discussion of telco security in politics and the media are often wholly absent in explaining the cyber security incidents that regularly impact telecom operators and their customers.

This White Paper describes eight very different security incidents that had a variety of impacts on telcos and their customers in several different countries during 2019 and 2020. It also extracts high level learnings from them. These eight have been selected to reflect the variety of incidents that telcos are vulnerable to – some of which are unique to the telecom sector, some of which are common to all large organizations. While these eight incidents cited were publicly reported in local and international media, it's important to put them in the broader operational context of day-to-day telco security:

- Many more besides these eight have been publicly reported over the last two years.
- There are many more that have not been cited in the public domain – instead, where appropriate, they've been reported to national regulators or not reported at all.
- Many incidents have occurred that the telco victims don't even know about yet. The recent hack of software provider, SolarWinds, was discovered six to nine months after Russian hackers first accessed customer systems. In one telco security incident cited below, attackers were able to dwell in a telco's environment for two years.

Figure 1: Real World Examples of Telco Security Incidents

#	Reported	Country or Region	Telco/ISP	Description of Incident/Attack
#1	Oct 2020	Israel	Partner Comms	Theft from crypto executives via SS7 exploit.
#2	Sep 2020	Hungary	Magyar Telecom	Volumetric DDoS on banking sector customers.
#3	July 2019	Not disclosed	Ten telcos	CDR exfiltration started with initial foothold in public facing web server then lateral movement.
#4	Sep 2020	Benelux	Several ISPs	Disruption from application layer DDoS attacks.
#5	Sep 2019	South America	Telcos in Mexico, Peru, Colombia.	Foreign nation state monitoring of location and other data of tens of thousands of mobile users.
#6	July 2020	Argentina	Telecom Argentina	Targeted with a $7.5 million ransomware attack.
#7	Sep 2019	USA	Verizon	Phishing campaign targeting employees.
#8	Dec 2019	India	Airtel	API flaw in mobile app exposed customer data.

Source: HardenStance

Telcos block a colossal number of cyber-attacks every day. Those that get through and actually impact customers represent the tiniest fraction of total attempts. But the ones that get through can cause substantial financial and reputational damage.

#1 Partner Comms – Cryptocurrency Theft via Signaling Exploit

In October 2020, Haaretz, a leading local newspaper, reported that 20 cryptocurrency executives in Israel were asked to pay digital currency after their phones were hacked and their identities stolen. Citing a local cyber security company brought into investigate, the report pointed clearly to a sophisticated signaling attack leveraging access to a foreign mobile network. This allowed messages exchanged with Israel mobile operator, Partner Communications, to be manipulated by exploiting well known vulnerabilities in either SS7 or Diameter signaling protocols.

This is the third case of attackers exploiting telco signaling protocols to hack into consumer phones to steal money from their accounts in the last three years. Telefonica Deutschland was impacted in May 2017 (though the impacted bank or banks weren't publicly named). Then Metro Bank in the UK was hit in February 2019 (though the impacted telco or telcos weren't named). What's significant isn't just that this is the third such incident in three years. Just as importantly, the telcos impacted were in the UK, Germany and Israel. These are three countries that are amongst the world's leaders in cyber security generally as well as in telecom security specifically. If this can happen in these countries, it can happen anywhere.

The incident in Israel is the third case of attackers exploiting telco signaling protocols to hack into consumer phones to steal money from their accounts in the last three years.

Signaling firewalls are the key requirement for protecting against these attacks and there are still far too many mobile operators – almost certainly a sizable majority world-wide – that don't even have them deployed. Available products are being enhanced with managed options and with GSMA-led industry efforts to enable better signaling threat intelligence sharing among operators and vendors.

#2 Magyar Telecom – DDoS Attacks on Bank Customers

In September 2020, Reuters cited Magyar Telecom's statement that Russian, Chinese and Vietnamese hackers had launched DDoS attacks that disrupted the services of Hungarian banks and caused lapses in service in parts of Budapest. The volume of data was ten times higher than usual in DDoS attacks, making it what Magyar Telecom said was "one of the biggest hacker attacks in Hungary ever, both in its size and complexity."

From a global perspective, this was a fairly routine volumetric DDoS attack. These target limited bandwidth in the last mile connection of a target organization or a point of presence at the edge of a telco's metro network. There is no evidence that extortion was attempted, although this is often the motive; targets are warned they will be attacked unless they pay a ransom.

Bad DDoS experiences do prompt businesses to change telecom providers. HardenStance has knowledge of local banks that switched telco providers shortly after the huge DDoS attacks on Turkey's national infrastructure in 2015. But while this does motivate some telcos to provide DDoS protection for their largest customers, many are still relying on approaches that are no longer fit for purpose.

Specifically, a lot of telcos still rely on Border Gateway Protocol (BGP) blackholing - using BGP to drop all traffic based either on its source or destination IP address. Because it's such a binary approach - because it blocks both good and bad traffic – this often achieves a DDoS attacker's objectives by other means. For the victim, the end result can be exactly the same – a service outage until their traffic can be re-routed.

Investing in more intelligent, more granular, DDoS protection allows telcos to be a lot more surgical in how they detect and mitigate volumetric DDoS attacks. Most businesses expect to pay a premium for this – either as a DDoS mitigation service or baked into a 'clean pipes' service. Either way, telcos can grow revenue and reduce churn while securing key business customers.

#3 Ten Telcos – CDR Exfiltration via a Web Server Vulnerability

In July 2019, details of 'Operation Soft Cell' were published by Endpoint Detection and Response (EDR) vendor Cybereason. This was an Advanced Persistent Threat (APT) assumed to have been carried out by Chinese nation state hackers on a number of telcos. The attack successfully exfiltrated Call Data Records (CDRs). The initial point of entry was one or more public facing servers. The attack then moved laterally within the telco organization over a two year period to achieve the target exfiltration. It has never been publicly confirmed but the chances are quite high that the impacted parties may have been a group of telco affiliates rather than several individual telcos.

The protections against an attack like this are routine enterprise IT security hygiene rather than measures that are specific to telco security. Public facing web servers need to be regularly patched. Additional protections include a Web Application Firewall (WAF) and End Point Detection and Response (EDR) tools.

The more fine-grained a solution's ability to identify different types of normal and abnormal, behaviours, the more effective enforcement actions can be.

#4 Telcos in Benelux – Disruption from Application Layer DDoS

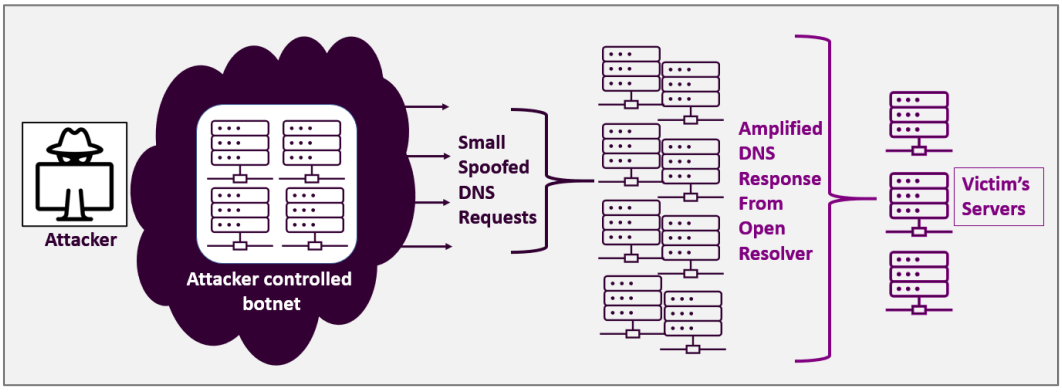
In September 2020, NBIP, the national association of Internet providers in the Netherlands, reported disruption to the services of some its member ISP companies throughout the Benelux region. This arose from application layer DDoS attacks, most of which were DNS amplification and LDAP-type attacks. NBIP reported that some of the attacks lasted more than 4 hours and hit close to 300 Gbit/s.

Telcos need to look to multiple layers of protection to mitigate the impact from these types of DDoS attacks at the application layer:

- The first layer is high quality threat intelligence sources to identify the open servers out on the Internet that are vulnerable to amplification attacks and are known to behave maliciously so they can be black-listed.
- Defensive solutions also need to distinguish between normal and abnormal behaviour of key applications like DNS and SIP as the basis for blocking malicious traffic. The more fine-grained a solution's ability to identify different types of normal and abnormal behaviours, the more effective enforcement actions can be.
- As well as that, a further layer of machine learning or AI-supported analytics can be leveraged to spot attack patterns that are independent of the specific application. For example, they can flag abnormal patterns of automation in the origination of traffic which indicate malicious factors like the presence of botnet malware. These attacks haven't been attributed to any specific group, at least not publicly.

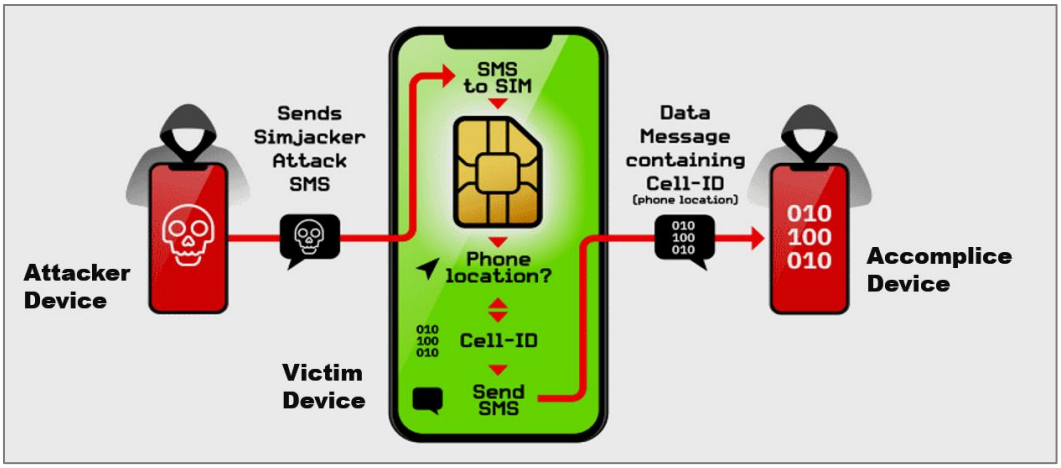
General, widespread disruption of this kind is more likely to be politically motivated, originating either from specific interest groups or nation states. However, it's also entirely possible that those responsible were simply trialling out new attack tools with a view to unleashing something bigger and 'better' in the future.

Figure 2: Anatomy of a DNS Amplification Attack



Source: HardenStance

Figure 3: Anatomy of a Simjacker Attack



Source: AdaptiveMobile Security/HardenStance

#5 Simjacker – Location Tracking via a SIM Card Exploit

Discovered in the summer of 2019 by researchers at AdaptiveMobile Security, and then disclosed to the wider telecom security community in September, Simjacker is a SIM card vulnerability that affected tens of thousands of mobile subscribers in Mexico, Peru and Colombia spanning 2018 and 2019.

At the time of the disclosure, hundreds of millions of customers of 61 mobile operators in 29 countries were vulnerable to Simjacker.

Simjacker exploited a vulnerability in a SIM Alliance library embedded in SIM cards, which had access to a subset of SIM Toolkit (STK) commands. These allowed mobile devices in targeted operators to allow remotely executed commands without any authentication, many without any user interaction. The vulnerability is believed to have been used by a surveillance company to retrieve the location and device information of targeted individuals on behalf of at least one nation state for at least twelve months.

At the time of the disclosure, hundreds of millions of customers of 61 mobile operators in 29 countries were potentially vulnerable to Simjacker. Indeed many of them still are. Because the application had – and still has – many genuine uses like operator credit-checking, disabling it entirely has proved problematic for some operators.

The industry has worked on providing a variety of fixes. The SIM Alliance has updated its Recommendations around using it. The industry has collaborated within the GSM Association's Community Vulnerability Disclosure (CVD) program and the GSMA is working on guidance on Binary Security Messaging. Network filtering of signaling messages is also effective as a part of a holistic approach to protecting against all types of signaling borne threats.

#6 Telecom Argentina – Targeted with a Ransomware Attack

In July 2020, ZDnet was among several news outlets reporting that attackers gained control over an internal domain admin of Telecom Argentina's IT infrastructure. Having installed a ransomware payload onto 18,000 of the company's workstations, it was reported that a $7.5 million ransom was demanded for unlocking and removing the malware, doubling to $15 million if the amount wasn't paid within three days.

This was at least the third ransomware attack on a telco over the last spring and summer of last year. It followed a similar attack on Sri Lanka Telecom in May. In July Orange Business Services confirmed it had been subjected to a ransomware attack by the group behind the Nefilim ransomware.

Many – perhaps most – ransomware victims do pay the ransom. However, consistent with standard practice, there doesn't seem to be a record of any of these three telcos publicly disclosing whether they did or did not pay it. In any case, paying such ransoms is becoming harder as some governments start to introduce specific legislation to outlaw

it. Additional impacts of these attacks included websites being taken out of service in the Telecom Argentina case and public exposure of some enterprise customer data in the Orange case in order to try and further intimidate the telco into paying the ransom.

Protecting against ransomware requires adhering to multiple aspects of cyber security best practice. Data should be routinely and frequently backed up. Active filtering and blocking should prevent most malicious code from ever reaching its target endpoint. Malware protection products can protect against those threats that do make it past the filtering and blocking layer onto the endpoint.

#7 Verizon – Employees Targeted with Phishing Attack

Examples #7 and #8 should be thought of as attacks or vulnerabilities discovered rather than 'incidents' per se because there was no evidence of any specific impact arising from the attacks or vulnerabilities discovered. Nevertheless the potential for such attacks or vulnerabilities to escalate into actual incidents is clear.

Verizon has been the subject of numerous phishing attacks, some targeting employees via either email or SMS and some targeting its customers.

Beginning with #7, in September 2019, Verizon was notified of a new phishing campaign targeting Verizon employees. It targeted employees as they attempted to login to the company's internal apps portal with the goal of stealing login credentials and multi-factor authentication passcodes. This particular attack was mitigated by identifying the malicious URL and other activity originating from the source IP address. Phishing monitoring, detection and mitigation solutions are available but they can only be deployed effectively in conjunction with comprehensive employee training.

In common with many other telcos, Verizon has been the subject of numerous phishing attacks, some targeting employees via either email or SMS and some targeting its customers. Telcos are also vulnerable to other types of social engineering. In 2017, an Iranian threat group was found to have been targeting telco operations personnel on LinkedIn by befriending them via a fake LinkedIn account. Attackers used the fake persona to establish a rapport with their targets over a period of time. Eventually they sent targets a document to open with malware embedded in it designed to provide access to the telco's operations environment.

#8 Airtel – Customer Data Exposed by API Flaw

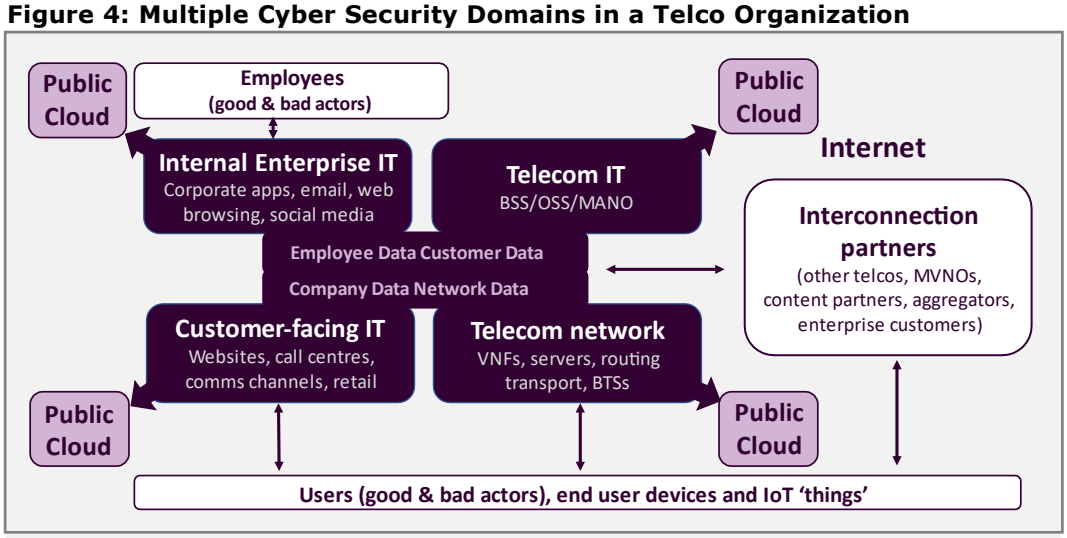
In December 2019 the BBC and several other news outlets reported on the discovery of an API flaw in the mobile app of India's Bharti Airtel. This had left the customer data – name, address, email, mobile number and IMEI numbers – of around 300 million Airtel customers potentially exposed. Such data can easily be harvested and used by fraudsters to contact customers and sound convincing when they pretend to be representing the network operator. Airtel stated that having been advised of the issue, it then fixed it promptly.

Other telcos have suffered from similar API flaws. In October 2017, T-Mobile USA announced it had notified 2.3 million customers of a risk that a subset of their personal information had been exposed by an identity and access management flaw in the APIs served up when customers were accessing their accounts via T-Mobile's website. Strong API security is founded on an Identity and Access Management engine to authenticate legitimate requests and authorize access only to the information that each API call needs; API management features from an API gateway; as well as threat detection and mitigation controls, such as via a WAF.

Old and New Security Challenges to Address

Just two of the eight incidents cited in this White Paper can be attributed to nation states. Just one – the 'Soft Cell' attack – was an APT. All but one vulnerability – 'Simjacker' – are very well known throughout the telco security and broader cyber security worlds. Only two – #1 and #5 – are unique to the telecom sector insofar as they exploited telco signaling or other telecom protocols. In the case of the other six, the vulnerabilities exploited are IT vulnerabilities that are common to all large organizations.

Figure 4: Multiple Cyber Security Domains in a Telco Organization



Source: HardenStance

There are three primary learnings for telcos from the eight examples cited here and the many others like them that routinely impact telcos all over the world now.

Telcos must:

- Double down on basic cyber security hygiene.
- Adapt to a changing landscape and available defensive techniques.
- Where possible, claw back security costs through smart security monetization.

Verizon has been the subject of numerous phishing attacks, some targeting employees via either email or SMS and some targeting its customers.

Double Down on Basic Cyber Security Hygiene

Everyone in telecom is familiar with the risk associated with the idea of nation-state controlled telecom vendors enabling eavesdropping by somehow melting so-called 'Trojan' malware into their code in a way that can't be detected. Only a small fraction of those same people knows of the 'Soft Cell' attack - even though it enabled much the same thing via the more mundane route of a vulnerability in a public facing web server as an initial point of entry.

Doubling down on basic cyber security hygiene therefore has to be a key priority for telcos. That means extensive security monitoring as well as frequent and increasingly automated patching. As shown in **Figure 4,** this needs to be done systematically across all four of a telco's IT and telecom infrastructure domains – telco IT; telco network; customer facing IT and internal enterprise IT.

As shown throughout in the examples cited, telcos are vulnerable in all four domains. Incidents #1,#2,#4 and #5 exploited vulnerabilities in different parts of a telco's telecom infrastructure – the last mile where limited bandwidth exposes business customers, as well as vulnerabilities in signaling and application protocols like SS7, Diameter and DNS. Incidents #3 and #8 exposed customer data arising from different flaws – a web server flaw and an API flaw – in a telco's customer-facing IT. The phishing and ransomware incidents cited in examples #6 and #7 targeted telco's internal IT systems and employees.

Doubling down on the basics also means according security higher priority in a telco's development environments so that API flaws are identified and fixed early in the development cycle rather than leaving customer data exposed until its discovered by a researcher in a live production environment. And it means investing to protect against threats that are proven to have impacted telcos and their customers as well as against higher order threats posed by nation states and other APT actors.

Adapt to a Changing Landscape and Available Defensive Techniques

From a telco perspective, adapting to a changing landscape means a lot more than just adapting to changes in the threat landscape (important though that is). Telcos themselves are undergoing profound digital transformation-driven change, including evolving to a fully cloud native telecom network infrastructure and operating model. This is having a huge impact on where and how telcos host their own and their customers data – hence also on how they protect it.

Telcos are following industry-wide trends in terms of leveraging the cost saving and revenue accelerating potential of public clouds. And they're doing this across all four domains depicted in **Figure 4.** That includes in their telecom infrastructure where initial deployments of 5G Stand Alone (SA) cores in public clouds such as AWS are underway now. Adapting telco security models to ensure consistent security policies across all four of a telco's technology domains, as well as the different on-premises, own cloud, and third party public cloud environments they host them in, is a key requirement.

Moreover, operators deploying Multi access Edge Computing (MEC) face additional challenges in terms of having to extend threat protection, detection and mitigation to these many more, smaller, more remote, distributed MEC sites. These sites are likely to require very high levels of network or service availability, potentially tied to a stringent Service Level Agreement (SLA). Critical telco or enterprise customer data stored at these locations also need protection that requires using widely available techniques but in more space-constrained environments.

Many of the incidents highlight how telcos are often failing to invest in mature techniques and technologies that are already widely used by more security-savvy peers.

Many of the incidents cited do not point to telcos always needing to be early adopters of the latest cyber security technologies. On the contrary, they highlight how telcos are often failing to invest in mature techniques and technologies that are already widely used by more security-savvy peers in the telecom and other sectors. Investing in available automation capabilities should again be prioritized here. This includes more automation in detecting and mitigating the colossal volume of mostly well-known threats that telcos see every day. As well as enabling faster response times, this also frees up security teams to focus on more complex threats that pose the greatest risk.

Claw Back Security Costs through Smart Monetization

Many telcos are either not investing enough in cyber security or they're getting poor efficiency – not enough 'bang for their buck' – out of their investments. It's unfortunate but investment in security is an inevitable cost of doing business in an increasingly software-driven economy. There is constant pressure to increase that spending but like any other business, telco CFOs can't just write their security teams a blank cheque.

Security costs are likely to increase for the telecom sector for two reasons. First, in common with other industries, the risk posed to telcos by the threat landscape is increasing and digital transformation is creating exposure to new risk. Second, many telcos have high hopes of incentivizing enterprise customers to increase their spend with them - and they're expecting those businesses to take on more cyber security risk as they do so. An obvious example of this is 5G where many telcos are already trying to coax business customers into investing in advanced 5G use cases. As previously shown, many of these use cases involve networking functions, enterprise data and data analytics being hosted beyond the generally pretty secure confines of highly centralized telco data centres – and hosted, instead, in a variety of different cloud environments, including distributed MEC environments.

A key way for telcos to justify increased spending on security is to map it to increased revenue, including by charging for some premium security services. Charging a premium to protect against the DDoS incidents cited in this paper is a good example of what telcos can already do – and what some are already doing. Enterprises fully expect to pay for DDoS protection services when their organizations come under attack.

The 5G era will take this a step further in terms of generating new use cases and new, custom security requirements for enterprise customers. Depending on what they expect from a dedicated 5G use case, many business customers expect a basic level of security from their telecom provider. But they also expect to pay a premium for services that fulfil the specific security requirements of the 5G use case they want to invest in. ■

More Information

- AdaptiveMobile blog on Simjacker
- A10 Networks: The State of DDoS Weapons Report

About the Sponsors

The sponsors of this White Paper are AdaptiveMobile Security and A10 Networks.

About AdaptiveMobile Security

AdaptiveMobile Security is the world leader in mobile network security, protecting more than 2.2 billion subscribers across 82 mobile networks worldwide. With deep expertise and a unique focus on network-to-handset security, AdaptiveMobile's award-winning security solutions and services provide its customers with advanced threat detection and actionable intelligence, combined with the most comprehensive security product-set in the market today.

AdaptiveMobile Security was founded in 2006 and counts some of the world's largest carriers, Governments and Regulators as customers. The Company is headquartered in Dublin with offices in North America, Europe, South Africa, the Middle East and Asia Pacific. To learn more, visit www.adaptivemobile.com

About A10 Networks

A10 Networks provides secure application services for on-premises, multi-cloud and edge-cloud environments at hyperscale. Our mission is to enable service providers and enterprises to deliver business-critical applications that are secure, available and efficient for multi-cloud transformation and 5G readiness. We deliver better business outcomes that support investment protection, new business models and help future-proof infrastructures, empowering our customers to provide the most secure and available digital experience.

A10 Thunder TPS® (Threat Protection System) is the world's highest-performance DDoS protection solution, leading the industry in precision, intelligent automation, scalability, and performance and helping leading global service providers to build cloud scrubbing centres that protect their networks and customers infrastructure. A10 Thunder® Convergent Firewall (CFW) is the first consolidated security solution for service providers, cloud providers and large enterprises that includes integrated application delivery and security solutions in a single, standalone product. Founded in 2004, A10 Networks is based in San Jose, California and serves customers globally. For more information, visit www.a10networks.com

About HardenStance

HardenStance provides trusted research, analysis and insight in IT and telecom security. HardenStance is a well-known voice in telecom and enterprise security, a leader in custom cyber security research, and a leading publisher of cyber security reports and White Papers. HardenStance is also a strong advocate of industry collaboration in cyber security. HardenStance openly supports the work of key industry associations, organizations and SDOs including NetSecOPEN, AMTSO, OASIS, The Cyber Threat Alliance, The GSM Association and ETSI. To learn more visit www.hardenstance.com