VOL 20 ISSUE 1 **DECEMBER/JANUARY 2020**

Big Interview
Bevan Slattery talks to *Capacity* about the launch of the OAC subsea cable

Feature
Capacity highlights 20 leading security and anti-fraud solutions in the market

capacity

Business intelligence for the global carrier industry

A NEW YEAR

Capacity

A New Wave

capacitymedia.com

20 Security and Anti-Fraud Solutions

According to the most recent report from the GLF, 80% of carriers cite fraudulent traffic management as a "strategic" or "top priority". This among other things has highlighted the increasing need among carriers for robust security products and agile solutions. Carriers across the industry are working to mitigate the risks of cyberattacks and fraudulent activity with a host of offerings and solutions that are either built in or added to. *Capacity* has rounded a cross-section of these offerings from SMS, to networking and operations centres, all to showcase some of the work being done in this area.

Compiled by Natalie Bannerman

Tata Communications

Fraud Prevention-as-a Service (FPaaS)

In 2019, Tata Communications embarked on an initiative to consolidate all of its fraud prevention services into a new Fraud Prevention-as-a-Service (FPaaS) platform. The new offering delivers more than just the detection and blocking of suspicious traffic but also includes the deployment of advanced testing tools, the regular testing of supplier tools as well as well-known blocked fraud numbers. In addition, it also features regular numbering plan rate sheet reviews and identifies suppliers who incorporate premium rated /fraud prone breakouts. The solution has particular focus on Wangiri fraud, using AI and ML-based techniques to detect fraudulent traffic patterns.

Turkcell

Automatic fraud prevention mechanism

Leveraging its automatic fraud prevention mechanism, Turkcell offers the following benefits to its users, the blocking of international destination calls by using the calling number. The same blocking is also available for national calls. In addition, customers can block all calls using a customer IP address. Most softswitches can't identify the IP addresses of its customers as this information us owned mostly by SBCs. With this solution Turkcell carries the customer's IP address with a SIP header to the softswitch as well as the developed/configured softswitch to use this header to block fraudulent calls using the IP address.

C3ntro Telecom

C3ntro Anti-Fraud Solutions

Next, we have C3ntro Anti-Fraud Solutions, which is a proactive fraud prevention and detection service that helps operators mitigate and manage fraud on their networks according to their needs. It is a customisable service that adapts to the needs of each operator and carrier allowing them to outline the parameters and definitions of fraud. By offering its customers more than just a tool or some software, C3ntro customers also have access to all of its infrastructure including 24/7 NOC, advanced routing and even credit management for their end users. This is in addition to its fully customisable anti-fraud tools.

Orange International Carriers

SMS Protect

SMS Protect offers filtering; detection and blocking systems operate on vulnerable SMS traffic streams in real-time. The tool provides security experts with added capabilities to analyse, test, review, report and better understand of fraudulent activity. Security experts can maintain and update security mechanisms to adapt to the ever-changing methods of fraudsters. The core element is the SMS Firewall: a "black-box" server that processes and filters all SMS traffic at the SMS Network border. It is deployed logically "on-site" at the SMS network border to filter all external traffic entering the SMS network ecosystem.

Vox Technologies

Vox 360

The Vox 360 solution is a comprehensive platform for identifying, predicting and mitigating fraud across voice and SMS. It uses proprietary technology that includes AI, machine learning, anti-fraud bots and a global threat database that covers both SMS and voice to stop fraud losses and accelerate the monetisation of voice, SMS and A2P messaging services. It offers carriers a simple and powerful approach to stopping fraud across both voice and messaging. Using a single platform, carriers are able to identify, predict and mitigate fraud in challenging markets like voice where the margin is critical, while also tackling the huge problem of fraud in the A2P space.

Telefónica
TUKU Web

Telefónica's anti-fraud service, TUKU Web, is a core tool developed and patented by Telefónica International Wholesale Services (TIWS) that prevents and detects possible fraud, both in incoming traffic and outgoing traffic streams. It tackles fraud at all stages: prevention, detection and action. It is comprised of two modules: TUKU IN (detection of fraud in incoming traffic streams: Bypass (by-pass OTT and by-pass roaming), hijacking, false answer supervision, manipulated CLI, etc) and TUKU OUT (prevention and detection of anomalous traffic in outgoing traffic streams with automatic blocking linked to alarms: IRSF, detection of Wangiri, etc.

Boku
”Silent” OTP service

Using mobile operator connections, Boku has introduced a "Silent" OTP service to replace OTP's delivered via SMS. The service uses the carrier network to determine phone number possession and authenticate the user. As a direct carrier billing company Boku needs to authenticate each user before billing. The company has now separated out this authentication step and made it available as a service for any company to verify possession, silently in the background without having to involve the end-user. By using the network connection between the sim card and the local mobile phone tower, phone number possession is established in microseconds.

Infobip
sGate SMS firewall and monetization services

Winner of the 2018 Anti-fraud Innovation at the Messaging and SMS Global Awards is Infobip's sGate SMS firewall and monetisation services. The solution combines next-gen hardware with continuous in-depth business and technical support for mobile operators, helping operators fix the deficiencies in their messaging operations, be it improperly charged incoming SMS traffic (including traffic coming from SIM farms), spam or fraud messages. Through its detection and filtering system, coupled with expert analysis, continued audits and tech support for the operator starting from the pre-installation phase, Infobip enables operators to optimise their network and revenue.

BICS & cVidya
FraudGuard

FraudGuard is a state-of-the-art fraud detection platform that uses crowdsourcing knowledge to enrich the service and deliver pro-active feedback in order to fight fraud. It analyses BICS' global traffic in near real time creating a complete overview of fraud trends and allows customers to pro-actively take action and minimise a possible fraud scenario. FraudGuard customers can, in return, enrich the system with fraud details they have detected on their respective networks. The solution levrages the strengths of both partners, the extensive global reach of BICS and the deep expertise of cVidya to offer a most advanced fraud management solution.

Telenor
Fraud prevention

Telenor has developed a monitoring solution based on signalling data, which actively detects abnormal traffic towards potential misused ranges. Consequently, only calls towards genuine users are completed. This ensures that fraud traffic is discovered and stopped before its customers are affected. The service is free of charge. In the event that a fraud incident has occurred, Telenor will assist its customers in the process for stopping the payment of the fraudulent traffic. Its AI fraud solution has been developed and will be further developed in cooperation with Telenor Research to secure a fraud free voice quality product.

Airtel Business

Airtel's Intelligent Security Operation center (iSOC)

Airtel's Intelligent Security Operation centre (iSOC) is based in Manesar, India. It is one of Asia's largest network operation centre (NOC) and security operation centre (SOC) facility. The SOC in particular offers a suite of cyber-security monitoring solutions including SIEM, SOAR, UEBA, threat intelligence, network behaviour analysis etc. In addition, it also has a number of services including vulnerability management, privilege identity management, anti-phishing services, endpoint detection & response, penetration testing, identity access management, application testing, governance, risk & compliance, firewall assurance and secure device management.

NTT

SOCaaS

NTT Security's Security Operations Center-as-a-Service (SOCaaS) allows customers to rapidly build and maintain an optimal security operations model just as you would if you had your own internal SOC. While customers retain ownership of all hardware, cloud services, software and storage infrastructure, SOCaaS provides all of the SIEM management, incident response, eyes on glass monitoring, tuning, and customisation capabilities. Additionally, SOCaaS can e-bond with your existing tool sets or use ours to maintain ticketing, workflow, and reporting artefacts for compliance and auditing. The service features 24/7 monitoring and alerting of security incidents, to name a few.

Deutsche Telekom Global Carrier

Encrypted Lambda

Deutsche Telekom Global Carrier together with Ciena, has launched a new security service that encrypts all data during journey across the world. The new offering, Encrypted Lambda service, encrypts data on hardware located at the client's site and protects it over Layer 1, the physical layer, while it is transmitted. This makes it different from traditional solutions by allowing larger data volumes with higher performance, reduced costs and faster speeds. Customers that will benefit the most from the Encrypted Lambda service are those needing to transport very large amounts of confidential data very quickly.

Singtel

Trustwave Fusion platform

Trustwave, the cybersecurity division of Singtel, offers the Trustwave Fusion platform. The platform enables powerful cybersecurity capabilities to address a constantly evolving threat landscape while running completely in-country, adhering to Singapore data sovereignty laws and regulations. Once connected, the platform unifies Trustwave technologies, services and security expertise onto a single application accessed and controlled by any device including desktop, tablet or mobile phone. Organisations then have the ability to manage security programmes, which includes asset discovery to threat detection and eradication to how resources are provisioned and scaled.

Amazon Web Services

AWS Security Hub

Earlier this year saw the launch of AWS Security Hub, a service that gives customers a central place to manage security and compliance across an AWS environment. AWS Security Hub aggregates, organises, and prioritises security alerts – called findings – from AWS services such as Amazon GuardDuty, Amazon Inspector, and Amazon Macie, and from a large and growing list of AWS Partner Network (APN) solutions. Customers can also run automated, continuous compliance checks based on industry standards and best practices, helping to identify specific accounts and resources that require attention.

Colt
Network Encryption services

Colt Network Encryption services ensure secure connectivity at any network layer, with an end-to-end encryption service that can tailored to users' needs. It offers optical encryption as part of wave and private wave services. There is voice encryption, which includes both SIP signalling encryption and audio encryption. As well as Ethernet line encryption, which allows for the ability to address the growing need for effective network security solutions, driven by increasing threats and new regulatory requirements such as GDPR.

CenturyLink
Adaptive Network Security

Adaptive Network Security cost-effectively enhances a company's network security posture with a managed, network-based firewall. Users can easily add functions such as anti-malware sandboxing, data loss protection, web content filtering, application awareness and control when needed. Delivered in the cloud Adaptive Network Security can quickly adapt to new threats without requiring huge customer investments and new expertise. Additionally, by moving protection physically closer to the origins of threats, we're able to neutralize threats more efficiently and effectively. The solution also features intrusion detection, anti-virus and 24/7 security operations centre support.

Sparkle
Secure Identity Suite

The Secure Identity Suite from Sparkle allows users to securely authenticate themselves by making a simple call from their mobile phone. Designed to combat fraud, the service protects businesses as well as customers by exploiting native GSM/UMTS network features when authenticating the user and securely transmitting information and instructions to the platform. It is especially effective in the prevention of phishing, botnets, man in the middle and man in the browser, key-logger, etc.It is also user friendly as no software needs to be installed, is completely carrier and hardware neutral while delivering high levels of security.

iBasis
FraudAlert

FraudAlert was developed to combat IRSF and Wangiri scams. It has been designed to complement existing fraud prevention ecosystems by adding a final layer of protection and security. The service analyses a stream of real-time call data using an advanced algorithm. SMS/email alerts are generated and sent to customers at the first sign of suspicious activity. Fraudulent activity can then be automatically blocked based on custom thresholds, also fraudulent calls can be ended to prevent costs from incurring. In addition, the application not only prevents fraud, but also allows customers to profitably monetise previously high-risk destinations that were continually exposed to fraud.

PCCW Global
Crypteia

PCCW Global offers a suite of customisable solutions to meet the needs of the individual company. This includes the Crypteia Managed Firewall that features that includes firewall rental, installation, configuration, hardware maintenance and 24/7/365 monitoring. There's also the Crypteia Threat Intelligence & Management Service and Security Operations Centres tthat provides a 24/7 threat monitoring and identification system. In addiition, there is the Crypteia Managed Anti-DDoS Service that helps prevent distributed denial of service (DDoS) attacks against your clients' networks by re-routing traffic away from critical infrastructure assets.