Telecoms fraud and cyber risks

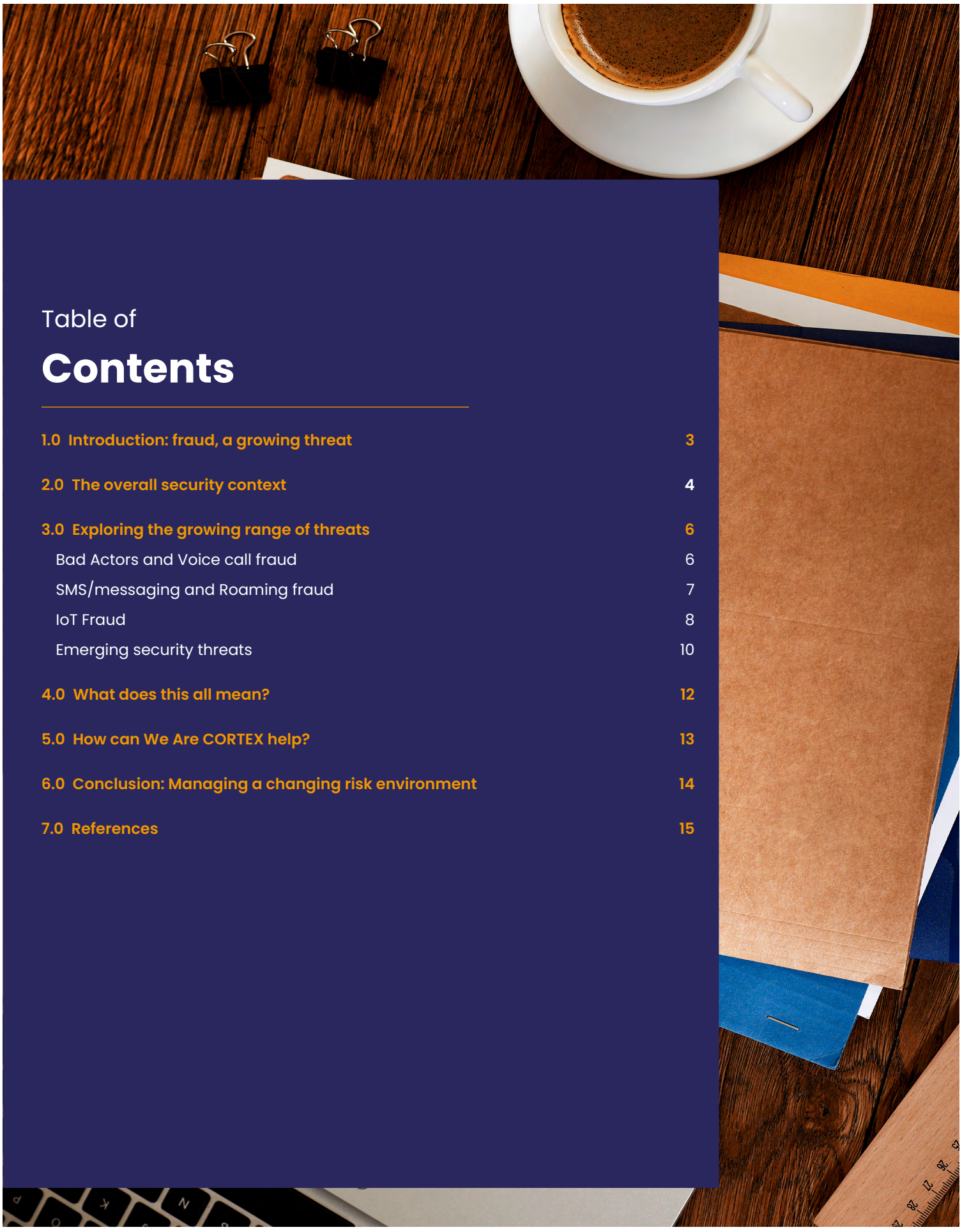
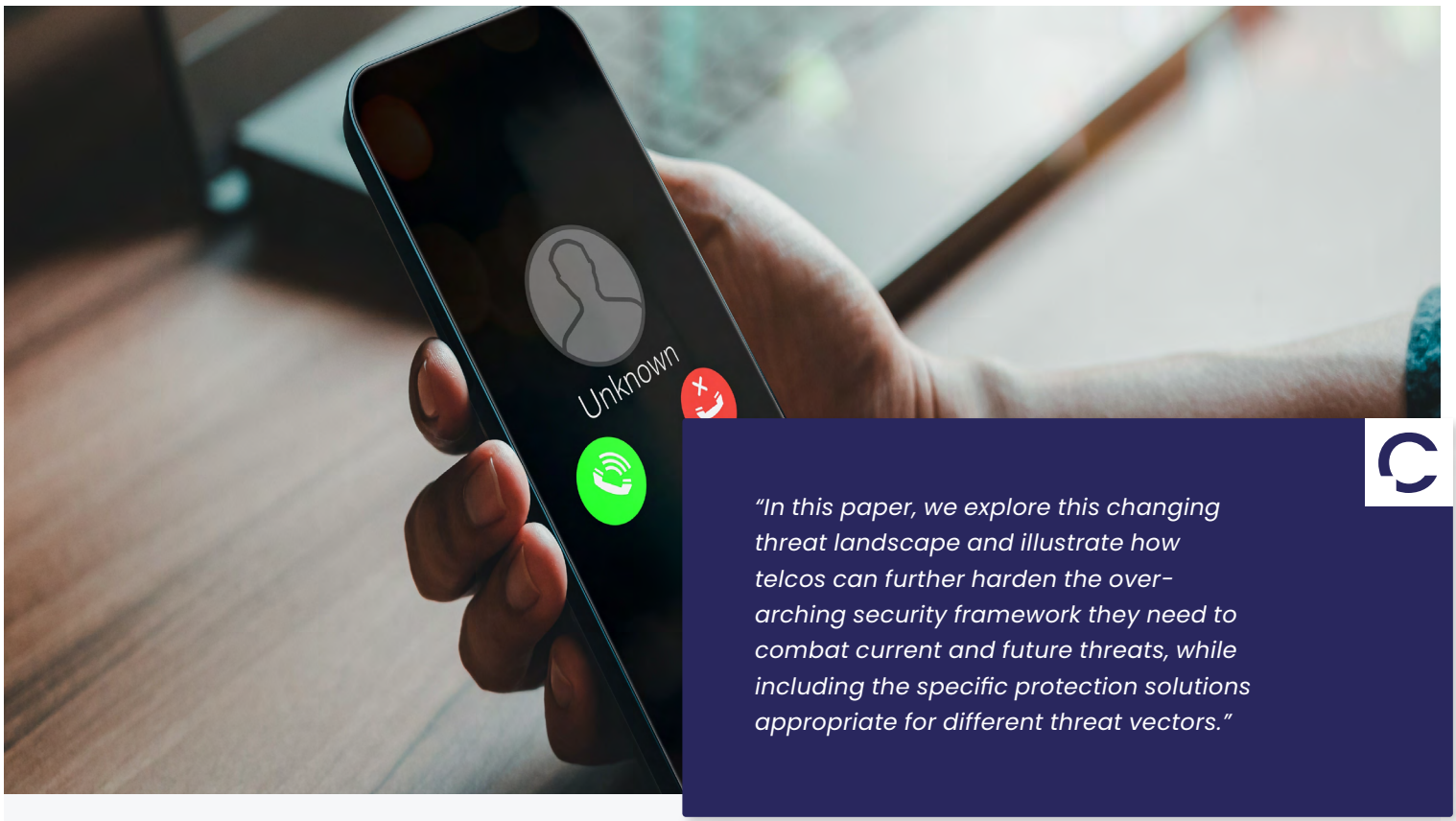


Table of

Contents

WE ARE CORTEX



"In this paper, we explore this changing threat landscape and illustrate how telcos can further harden the over-arching security framework they need to combat current and future threats, while including the specific protection solutions appropriate for different threat vectors."

Introduction

Fraud, a growing threat

Fraud continues to be a key concern for telcos. What makes it particularly challenging is that, like cyber security in general, the fraud threat landscape is constantly evolving. There are well-known threats — for voice calls or for SMS, for example — but there are also new ones that target an expanding threat surface. To complicate matters further, there are also new, stringent compliance obligations, at both national and international levels, which demand a response.

A siloed strategy that leverages point solutions to guard against specific threats — or for particular areas of operation — can help – but it's no longer adequate in the face of new, over-arching compliance requirements and the new, holistic approach to security that's required today. All of which means that operators and service providers are facing an unprecedented — and fast-moving — challenge.

In this paper, we explore this changing threat landscape and illustrate how telcos can further harden the over-arching security framework they need to combat current and future threats, while including the specific protection solutions appropriate for different threat vectors.

This ever-changing threat landscape impacts wireless, wireline, broadband, and narrowband CSPs as well as voice, data, content, and IoT providers. All in all, operators of every kind must deal with a growing spectrum of increasingly sophisticated and complex cyber threats – all within a dynamically changing risk landscape.

The overall
security context

We all know that international telecoms fraud is rising and poses a significant threat to operators – and their customers. For example, according to a report from the Communications Fraud Control Association (CFCA), companies lost $38.95 billion in 2023 to telecoms fraud. The top fraud methods included:

- Subscription (Application) Fraud
- Subscription (Credit Mule) Fraud
- PBX Fraud
- Account Takeover
- Service/Equipment Abuse

Collectively, these account for 51% of tracked fraud issues, while 42% of the top 10 fraud methods relate to customer account manipulation[1]. But that's not the end. Fraudsters target surging A2P messaging traffic, while the proliferation of IoT devices represent other areas ripe for targeting. And, as operators seek to target new opportunities presented by the introduction of 5G Standalone (SA) and network slicing, reaching new business partners and customers, fraudsters will inevitably target these too.

This new, ever-changing threat landscape impacts communications service providers (CSPs) – wireless, wireline, broadband, and narrowband CSPs – as well as voice, data, content, and IoT providers. All in all, operators of every kind must deal with a growing spectrum of increasingly sophisticated and complex cyber threats – all within a dynamically changing risk landscape.

They can never stand still, as these new threats will emerge on a continual basis. Ensuring security across all risk domains is becoming a huge challenge. The traditional way of dealing with each security domain in isolation is not enough: a holistic approach is required.

To add yet more spice to the mix, stringent regulations and legislation – such as the NIS 2 Directive and the UK's Telecoms (Security) Act 2022 – demand a joined-up approach to dealing with these threats. The requirement for a holistic approach is baked into the regulations.

It not only means that providers face a more complex, dynamic security environment with a significantly expanded threat surface, they must also ensure compliance with regulations that require an over-arching, comprehensive, cross-domain approach to this rapidly evolving threat landscape. How can operators rise to this challenge?

Exploring the

growing range of threats

As we noted, the threat surface is growing and expanding rapidly. New threats are constantly emerging, while adversaries develop more sophisticated techniques to circumnavigate providers' security systems. Essentially, it's an on-going game of cat and mouse. Let's briefly review some traditional and emerging threats to highlight the shifting landscape.

Bad Actors and Voice call fraud

Voice telephony has long been subject to a wide range of security risks and fraudulent practices.

We can classify these as 'classical' fraud attempts, and in this category, we find things like spoof calls (which appear to be from a business, for example, but which seek to obtain personal user details or money out of the user); offers of a free prize or cheap vacation if the user pays a small fee upfront first or gives away credit card information straight away; phishing calls where third parties try to extract information, loan scams that try to gain information, fake charities; calls from scammers pretending to be from a bank who then try to gain personal information, such as account numbers, to name just a few.

And then there is the infamous 'Wangiri' fraud, through which users are inadvertently tricked into thinking they have missed a call and then the return call is charged at high toll rates, leading to excessive bills – and the associated anxiety that can result. Such activities are often targeted at the elderly and more vulnerable who may not be overly technologically literate.

Carriers are often the target rather than consumers. For example, another tactic is toll-free number pumping (also known as toll-free traffic pumping), whereby a carrier injects large volumes of fake traffic into a toll-free route to generate income – as traffic passes through the network, the fraudsters take a share of the toll, or fee.

There are also multiple forms of international telecoms fraud, including International Revenue Sharing Fraud (IRSF). With this approach, malicious third parties artificially generate a high volume of international calls through expensive routes and then claim a proportion of the revenue – with large volumes of traffic this can amount to significant income. There is also an epidemic of so-called 'robocalls'.

In response, some governments have introduced legislation, such as STIR / SHAKEN. STIR (Secure Telephone Identity Revisited) offers a series of standards that add a digital certificate to SIP information to validate caller IDs.

SHAKEN (Signature-based Handling of Asserted information using toKENs) offers guidelines for dealing with calls that have incorrect or missing STIR information. So, for example, additional information in the caller ID can indicate that the number has been spoofed. There's no doubt that bad actors will continue to target voice, particularly as it remains a universal service.

SMS/messaging and Roaming fraud

Globally, an enormous 23 billion text messages are sent per day[2]. SMS is one of the most widely used forms of messaging today, used by consumers, businesses, governments, and so on. It is one of the most widely available forms of communication, as well as offering a fast and cost-efficient channel.

SMS and its evolved version, RCS (Rich Communication Services, now available on both major smartphone operating systems), are also increasingly used by businesses for Application-to-Person (A2P) messaging, allowing them to reach out and interact with customers in an easy and cost-effective manner. Its ubiquity and ease-of-use makes it an attractive communication channel. It has become widely adopted for two-factor authentication for services such as mobile banking and ID verification, for example.

So, as well as being a highly attractive form of communication for everyone, it also offers a potentially lucrative target for adversaries, who are constantly coming up with new ways to exploit the medium.

- Smishing
- Identity fraud
- Fraudulent and deceptive offers
- Malware distribution
- SMS toll fraud
- SMS pumping
- Fake notifications
- SMS boxes (or grey/black routes)

As a result, SMS fraud can have a significant negative impact on consumers and organisations. For example, in 2022, US consumers lost more than $8.8 billion to fraud through SMS fraud, particularly SMS smishing, which increased 30% increase over the previous year[3]. SMS fraud continues to grow, with research from the Mobile Ecosystem Forum suggesting that 28% of consumers receive an unsolicited SMS message daily[4].

One of the most common frauds is Smishing. Smishing message are used to trick recipients into disclosing personal data – with fraudsters masquerading as legitimate suppliers, asking consumers to re-enter or confirm personal details. SMS fraud also has a negative impact on operational efficiency, an increased burden on customer support, and a negative impact on consumer trust and experience.

The international data roaming market is also under threat. It has experienced substantial growth, reaching $84.24 billion in 2023, and projected to grow to $89.43 billion in 2024 – a CAGR of 6.2%[5]. This is a rapidly growing source of revenue for operators and so has become a target for malicious third parties.

"as the number of connected devices proliferates, it only expands the threat surface for cyber security vulnerabilities. IoT devices are particularly vulnerable to threats such as data theft, phishing, spoofing, and denial of service (DoS) attacks."

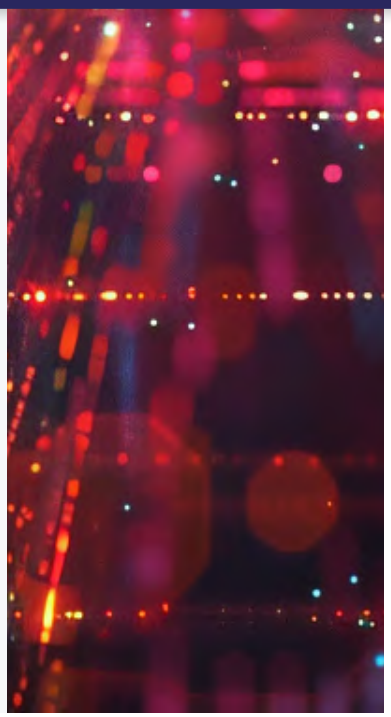
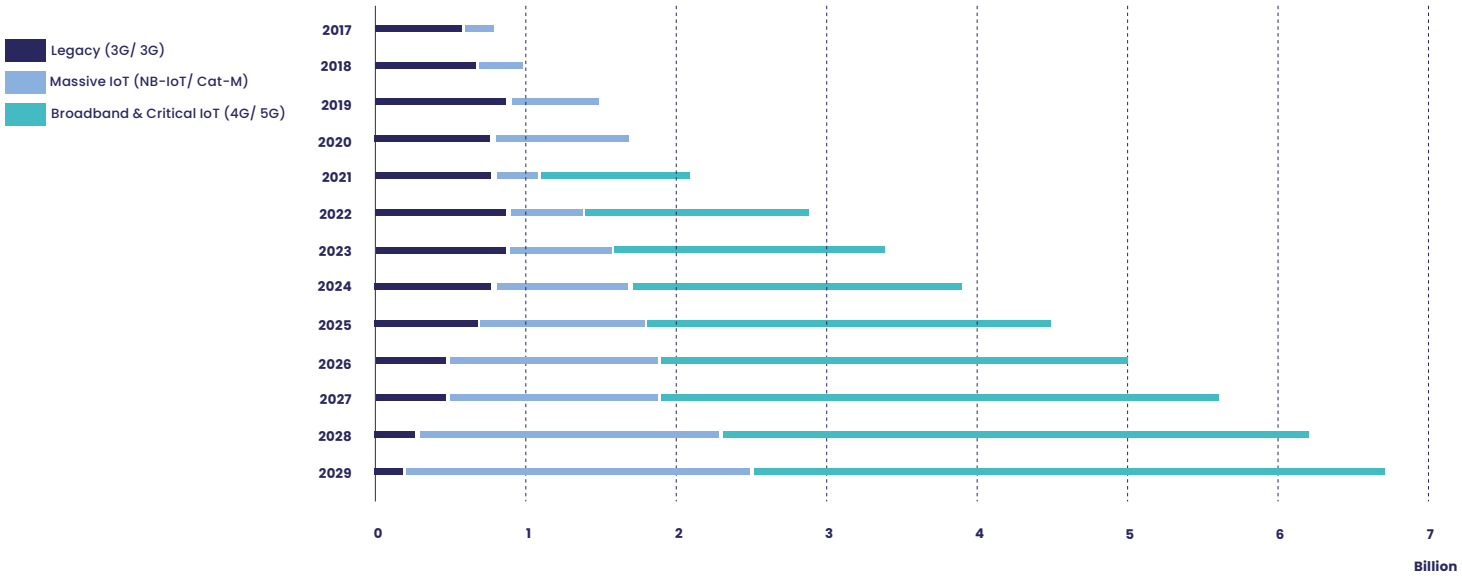


Figure 1. The exploding number of IoT connections[8]



As well as the rising ownership of smartphones and devices and the proliferation of 5G networks, the EU's 'roam like at home' policy allows residents in the region to use their phones anywhere in the EU at no extra cost has further boosted data usage.

However, the abolition of roaming charges has also contributed to increased fraud, as malicious third parties seek to exploit this growing market. For example, a study by Juniper Research predicts that global roaming fraud traffic will grow by 700% over the next five years reaching $8 billion by 2028[6]. Little wonder that the market for SMS Firewall solutions continues to be buoyant.

Similarly, many operators have deployed analytics solutions to protect their customers, screening traffic at border gateway points and using AI to predict / detect anomalous behaviour – so that it can be blocked in Session Border Control solutions are network boundaries.

IoT Fraud

According to Ericsson, the number of cellular connected IoT devices is set to reach 4 billion by the end of 2024 – up from 3.4 in 2023 – and is set to reach 6.7 billion by 2029[7].

Of course, as the number of connected devices proliferates, it only expands the threat surface for cyber security vulnerabilities. IoT devices are particularly vulnerable to threats such as data theft, phishing, spoofing, and denial of service (DoS) attacks. IoT devices include clean energy devices, smart meters, smart home devices, vehicles, fitness trackers, and many more applications.

As these IoT-connected devices proliferate, it is causing significant security vulnerabilities that carriers, operators, and service providers must deal with. Many of these devices store significant amounts of personal data, and as such represent a significant threat to both consumer privacy and organisations' ability to meet compliance obligations.

Criminals are, unfortunately, inventive and highly technically literate. As a result, the threat landscape is constantly evolving. For example, with 5G (SA) and increasingly interconnected networks and systems, there are a growing number of entry points for fraudsters and malicious parties.

Figure 2. IT – information technology / OT – Operational technology

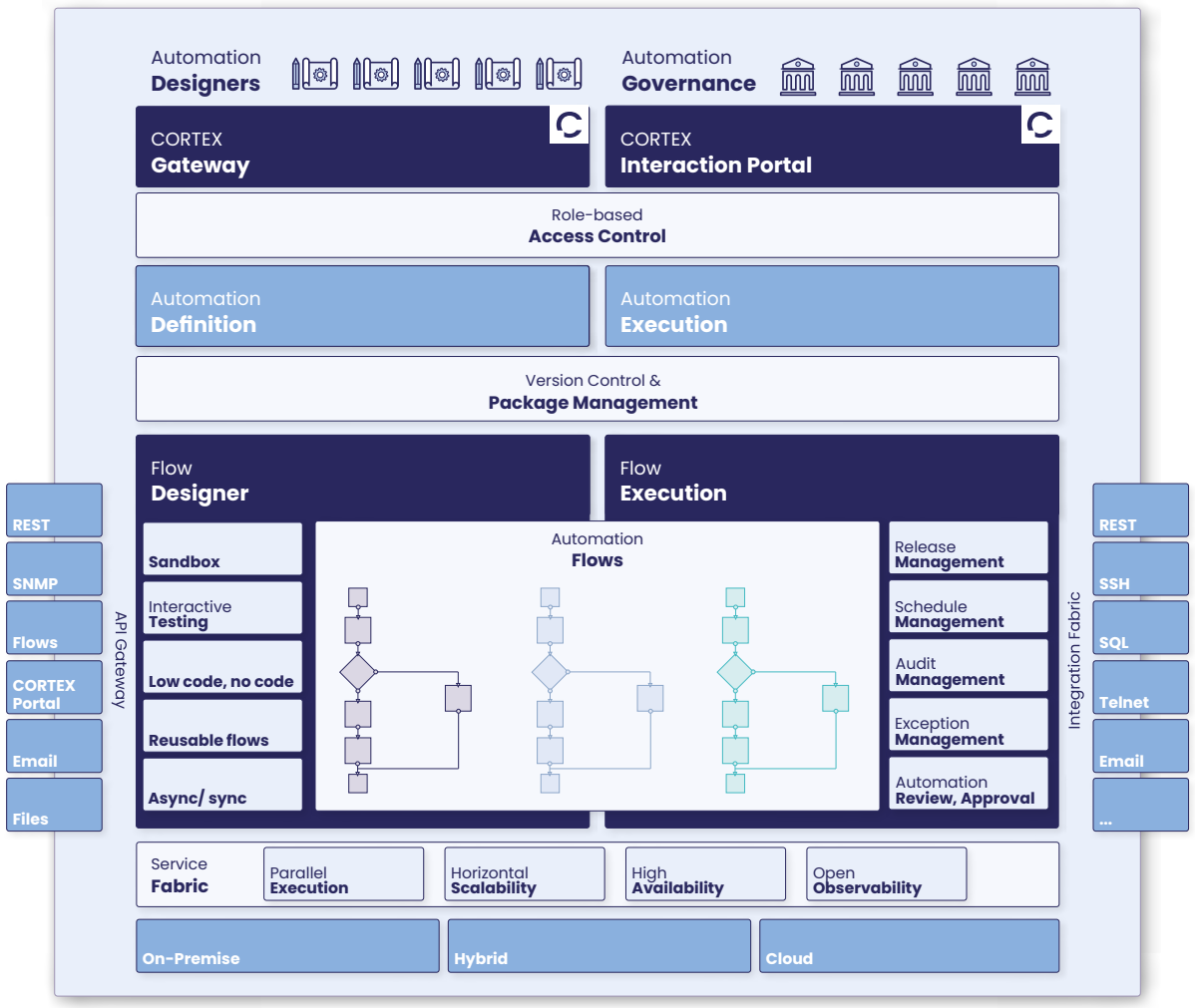
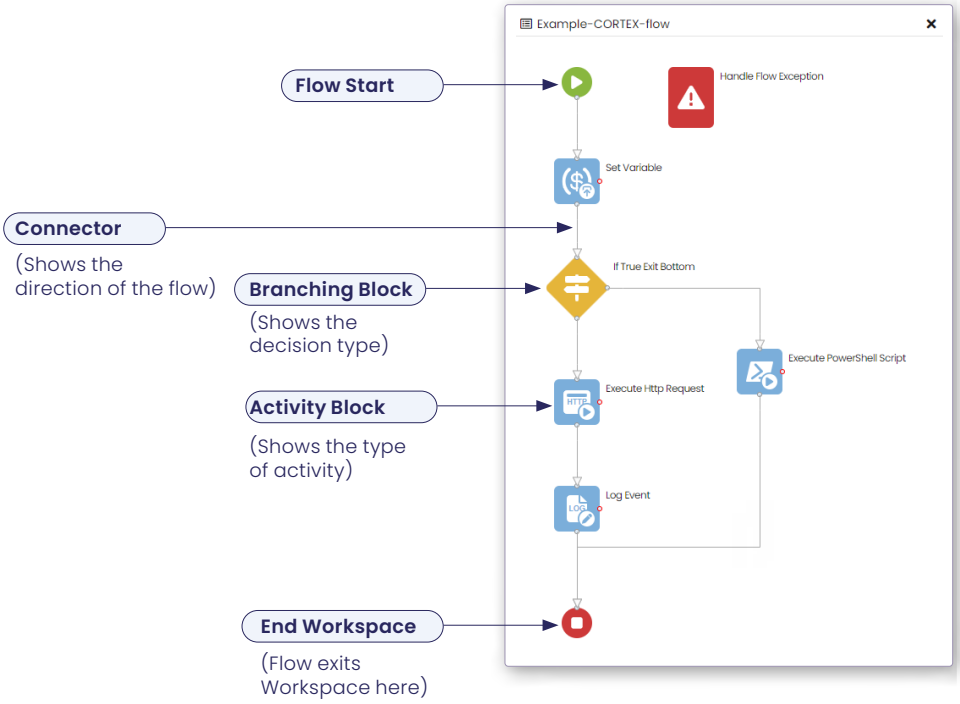


Figure 2. An example of an automated workflow



GLOBAL ROAMING FRAUD TRAFFIC WILL GROW BY 700% OVER THE NEXT FIVE YEARS

Some of the threats include: the use of default passwords that come with devices, but consumers never think to change (or don't know how to); unencrypted data transfer from devices to the network; and the ease of data theft from many devices by malicious third parties.

Take smart meters as an example. The total number globally is expected to double over the next decade, from 1.7 billion at the end of 2023 to 3.4 billion by the end of 2033[9]. In fact, smart meters already constitute over 10% of all IoT-connected devices. With global targets for climate change, this number is only set to accelerate.

However, smart meters can represent a significant security vulnerability. If hackers can gain access to these – often unprotected – devices, they can potentially manipulate energy usage readings, gain access to personal consumer data and other smart home devices. They may even find back-doors into the macro networks to which they connect – with the potential to cause significant damage to the energy infrastructure.

Emerging security threats

Criminals are, unfortunately, inventive and highly technically literate. As a result, the threat landscape is constantly evolving. For example, with 5G (SA) and increasingly interconnected networks and systems, there are a growing number of entry points for fraudsters and malicious parties. The transition to software-based and virtualised networks also opens up new vulnerabilities that must be addressed to ensure the security of the network – and operators are struggling to keep up.

To highlight one potential emerging risk area, alongside traditional — and also evolving threats to voice, messaging and data, impacting roaming and domestic customers alike — there are new threats associated with dynamic network slicing.

That's because 5G SA network slicing dynamically brings resources into play for a given service, for a given use case. Because slicing is a high-value application it means that it will inevitably become an attractive target for fraudsters. Not only could it provide significant rewards for malicious third parties (think of key B2B relationships enabled by slicing – such as between an MNO and a content provider), but any security breach could also have far-reaching consequences for service quality and data privacy, particularly as many thousands of devices or users could be affected by any breach.

Similarly, Massive IoT (MIoT) slices (which are expected to be launched commercially soon) will be designed to support a significantly increased density of connectivity in a given area – so, not only is IoT a known risk domain, the nature of IoT connectivity will also change, introducing new vulnerabilities. When we consider other slice types, such as Vehicle to Everything (V2X), the risks associated with, say, autonomous vehicles, can easily be recognised. Confronting them is, however, another challenge.

Stakeholders are already aware of these emerging threats. For example, the U.S. National Security Agency (NSA) and the Cybersecurity and Infrastructure Security Agency (CISA) have already compiled a report on some of the threats to network slicing security[10].

It notes that there are many threat vectors affecting 5G network slicing, including:

- Denial of Service (DoS) attacks on the signalling plane
- Misconfiguration Attacks (whereby security features may have inadvertently been ignored or turned off)
- Man-in-the-Middle (MITM) attacks (which involves the hacking of two communication endpoints)

DoS attacks, in particular, directly affect the availability of the slice and its functionality, including loss of access to the 5G infrastructure, loss of access to remote data, or compromised communication services.

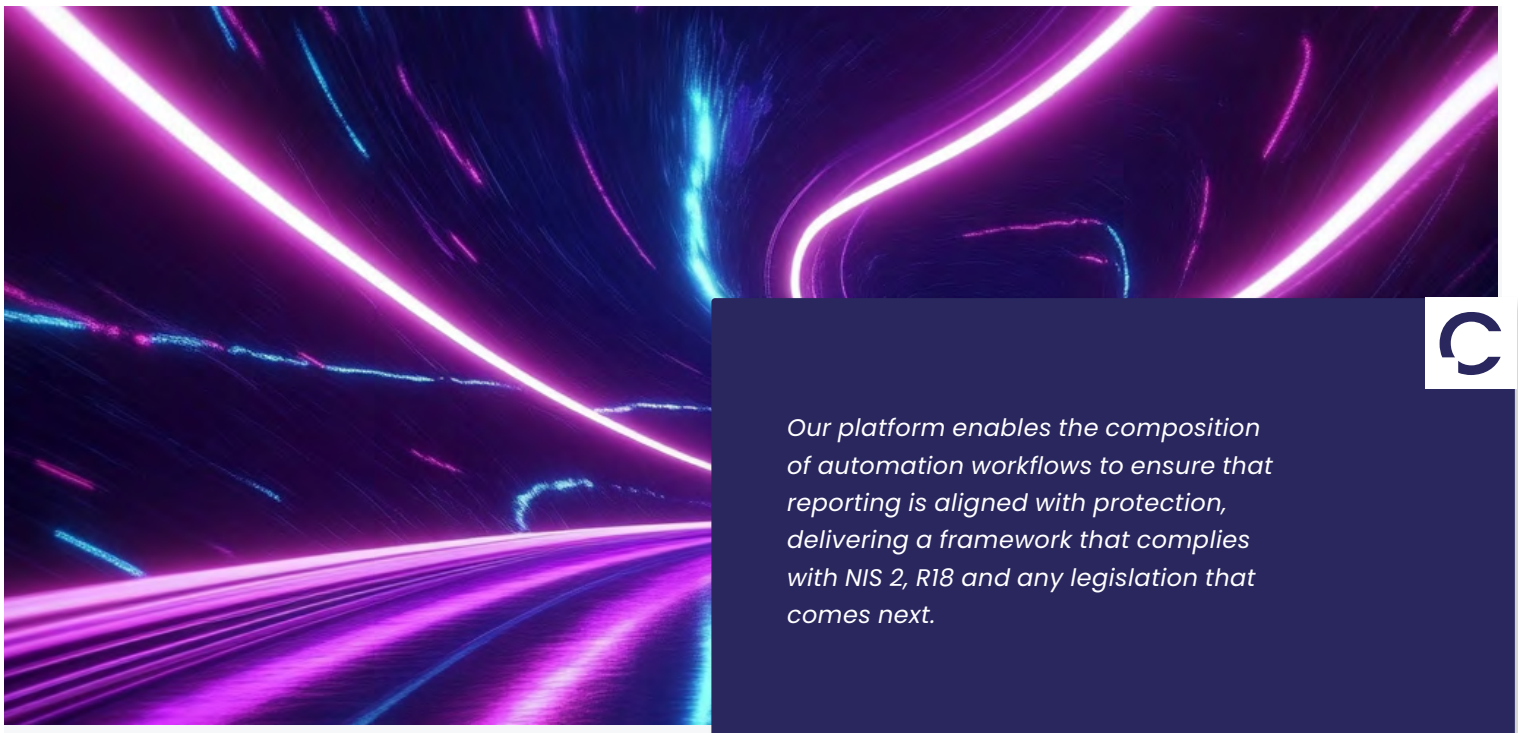
The report recommends a zero-trust architecture (ZTA) methodology through authentication, authorisation, and audit (AAA) techniques, which can help mitigate risk (in addition to basic confidentiality, integrity, and availability components).

In recognition of this, steps are being taken to mitigate potential threats. The 3GPP (3rd Generation Partnership Project), for example, has published standards that define security for the functionalities of Communication Service Management Function (CSMF), the Network Slice Management Function (NSMF), and the Network Slice Subnet Management Function (NSSMF).

In addition, it published requirements for UE Route Selection Policy (URSP). This is a particularly interesting – and entirely novel – capability, which allows an application to request the optimum data path when establishing sessions from a device to an external data network[11].

This requires another level at which network security must operate – is the device and the applications it supports secure? Is the application trusted to interact with network resources in this way? It's too early to tell – but, cognisant of the unknown risk factors, 3GPP has established a 'Coordinated Vulnerability Disclosure' reporting program so that all parties can share information about new threats and vulnerabilities[12].

Finally, in this brief tour, we have largely focused on attacks to networks or to their subscribers, be they consumers, corporations or organisations. However, it should not be forgotten that there are security risks that can arise due to human error internal to network operations. For example, employees may inadvertently misconfigure security settings through a lack of training. Similarly, passwords can be leaked, data exposed, and processes bypassed manually. Sometimes, criminals don't need to do anything to capitalise on human error.



Our platform enables the composition of automation workflows to ensure that reporting is aligned with protection, delivering a framework that complies with NIS 2, R18 and any legislation that comes next.

What

does this all mean?

The threat surface is growing significantly and rapidly. Network security has become a moving target. Left unchecked it could jeopardise the success of new service initiatives – and limit the expected gains from 5G SA enabled services or rising roaming traffic. All of this must be considered in addition to existing and known threats.

Unfortunately, the situation is only expected to get worse, because not only are criminals becoming more resourceful and creative, but there is also the issue of managing and protecting networks that have many more connected devices – for example, those enabled by Massive IoT slices.

Together, these add up to a complex network containing a myriad of potential cyber threat vulnerabilities. Hence, the introduction of legislation such as the European Union's NIS 2 Directive, The Cyber Resilience Act, The Digital Operational Resilience Act, and the UK's Telecoms (Security) Act, which jointly and severally demand a holistic approach to cyber security.

Most operators seek to protect against these individually, with silos of different solutions, policies and procedures dedicated to a particular threat. However, not only is that no longer viable, but new legislation also explicitly demands that a joined-up approach must be applied to counter the growing tide and complexity of fraud and cyber threats.

Many operators have implemented protection measures against specific fraud types or for different network domains, but a siloed approach isn't sufficient – true protection requires cross domain automation to ensure effective barriers are raised to eliminate reporting islands. At the same time, automation and stringent workflows can guard against the unfortunate consequences of human errors.

How can

We Are CORTEX help?

Security surfaces and vectors are growing – perhaps exponentially when we consider MIoT and the widening range of UEs – any device that can connect to a mobile network via SIM authentication, eSIM or otherwise. These represent back doors that could be exploited in novel ways by malicious parties. We don't yet know the vulnerabilities an innovation such as URSP could introduce – but we must take steps to prepare for them. And, attacks on new capabilities like URSP could come from existing vectors, such as smishing. A rogue message carrying malware could target applications that use URSP to threaten data connections in the underlying slice infrastructure.

Likewise, imagine a network slice itself that is used for critical purposes. This could pose a significant risk if for example, the slice is used by a smart port, an autonomous vehicle, a hospital…and so on. V2X is just one obvious target to consider.

It means that security silos are not only ineffective, but they could also lead to compliance breaches. Threat surfaces will be increasingly linked, which increases the need to orchestrate security across all vectors. You can't rely only on the SMS Firewall – we need to know when a threat has been detected and share information with other, relevant systems (e.g. the security functions behind slicing to which we referred earlier). These threats are only just beginning to be understood by the industry.

The NIS 2 Directive is just the beginning of new, stringent security regulations. The complex nature, and changing face, of security threats makes meeting NIS 2 Directive obligations a real challenge. Communications providers across the board need to have a reliable framework for reporting across all threat vectors.

In this complex and evolving landscape, We Are CORTEX offers comprehensive capabilities to help you to integrate and automate key processes across different network domains and sub-systems — from the SMS Firewall or SBC — to the 3GPP slice security functions, for example. Cross domain automation to deliver a cohesive, holistic security fabric.

Our platform enables the composition of automation workflows to ensure that reporting is aligned with protection, delivering a framework that complies with NIS 2, R18 and any legislation that comes next. Our tools can help you to realise the vision of autonomous networks in alignment with your own unique inventory and asset base – we span IT, OT, and everything in between (see Figure 2) – and they allow information and alerts from one system to be shared with another that is also involved in a potentially critical path.

Our platform is atomic and uses reusable automations that can be applied to any process or sub-domain. Importantly, we offer a cross-domain approach to orchestrating all your needs, regardless of legacy architecture, infrastructure, systems, and processes. Figure 3 shows an example of an automated workflow that we can provide.

The CORTEX platform can quickly and easily evolve with your requirements, and the changing security threat landscape. It uses reusable components and employs a cross-domain approach to orchestration, ensuring that you can not only counter cyber security threats, but also meet your compliance obligations.

Conclusion

Managing a changing risk environment

Operators and service providers are familiar with classical voice and messaging fraud – but the range and complexity of threat vectors is accelerating, while fraudsters are becoming more inventive in the ways they exploit these vulnerabilities.

IoT-connected devices present a fresh set of security challenges, while 5G SA brings a host of entirely new threats and possible vulnerabilities with the introduction of constantly changing network slicing applications. We can anticipate many new threats – but there are just as many that have yet to be conceived.

At the same time, a constantly evolving, complex regulatory ecosystem is swelling around us, with the ambition of helping us mitigate and eliminate national infrastructure security concerns. Managing this complexity, while ensuring lasting compliance with NIS 2, will require a different approach to the silos we have seen to date.

In fact, many new regulations are baking-in a joined-up, holistic approach to ensure defences meet the security obligation requirements: a hyper-automated approach to security is what you need. SMS Firewalls and SBCs need to be linked to other defences in a structured, holistic manner. CORTEX enables you to accomplish this task – while also allowing the automation of internal procedures and governance – for password management, for example.

While you may be compliant today, the constantly changing threat landscape and evolving regulations and legislation means that communications service providers must constantly, dynamically and proactively, keep up with this complexity.

You will not only need technology capable of leveraging what you have already done — and of doing more than before — but you will also need technology that will help make organisational change easier to achieve, and more quickly too, while also being able to adapt to new threats and defensive measures you implement.

While providers can introduce different protection mechanisms and systems to counter new threats continually, these will need to be connected and integrated with other platforms, so that the governance and reporting requirements for NIS 2 and others can be met, while also supporting autonomous network operations and recovery. CORTEX can help you do this.

The CORTEX automation platform provides the flexibility to help you manage this complex environment, whether it's dealing with familiar security threats or new – as yet – unknown vectors. The transit to Massive IoT, and 5G SA (and the dynamic network slicing it will bring) means that the security threat surface will become increasingly broad and complex. A technology like CORTEX can help you to provide a holistic approach to cyber security, while ensuring compliance.

To find out more, contact us today.

Footnotes

References

1. https://cfca.org/telecommunications-fraud-increased-12-in-2023-equating-to-an-estimated-38-95-billion-lost-to-fraud/
2. https://www.sellcell.com/blog/how-many-text-messages-are-sent-a-day-2023-statistics/
3. https://www.arkoselabs.com/toll-fraud/what-is-sms-fraud/#foot2
4. https://mobileecosystemforum.com/mobile-messaging-fraud-report-2016/
5. https://blog.tbrc.info/2024/08/data-roaming-market-size/
6. https://www.juniperresearch.com/press/data-roaming-fraud-to-accelerate-reaching-8bn/#
7. https://www.ericsson.com/en/reports-and-papers/mobility-report/dataforecasts/iot-connections-outlook
8. From "Ericsson Mobility Report, June 2024: https://www.ericsson.com/en/reports-and-papers/mobility-report/reports/june-2024
9. https://transformainsights.com/news/global-smart-meters-2033#:~:text=The%20key%20highlights%20are%3A,connections%20globally%20are%20smart%20meters.
10. https://media.defense.gov/2023/Jul/17/2003260829/-1/-1/0/ESF%205G%20NETWORK%20SLICING-SECURITY%20CONSIDERATIONS%20FOR%20DESIGN,%20DEPLOYMENT,%20AND%20MAINTENANCE_FINAL.PDF
11. https://www.gsma.com/newsroom/wp-content/uploads/TS.62-V1.0-UE-Requirements-related-to-network-slicing-using-URSP-1.pdf
12. https://www.3gpp.org/delegates-corner/coordinated-vulnerability-disclosure

WE ARE CORTEX

We Are CORTEX

Kings Park House
22 Kings Park Road
Southampton
SO15 2AT

Phone: +44 23 8254 8990
Email: hello@wearecortex.com
Visit: wearecortex.com