Cybersecurity in the contact centre:

What are the risks and ***how can you protect yourself*** against them using the ***SaaS model?***

odigo | aws

Contents

Introduction 3

1ST PART
Cybersecurity risks 4

I. The current state of cyber threat 5

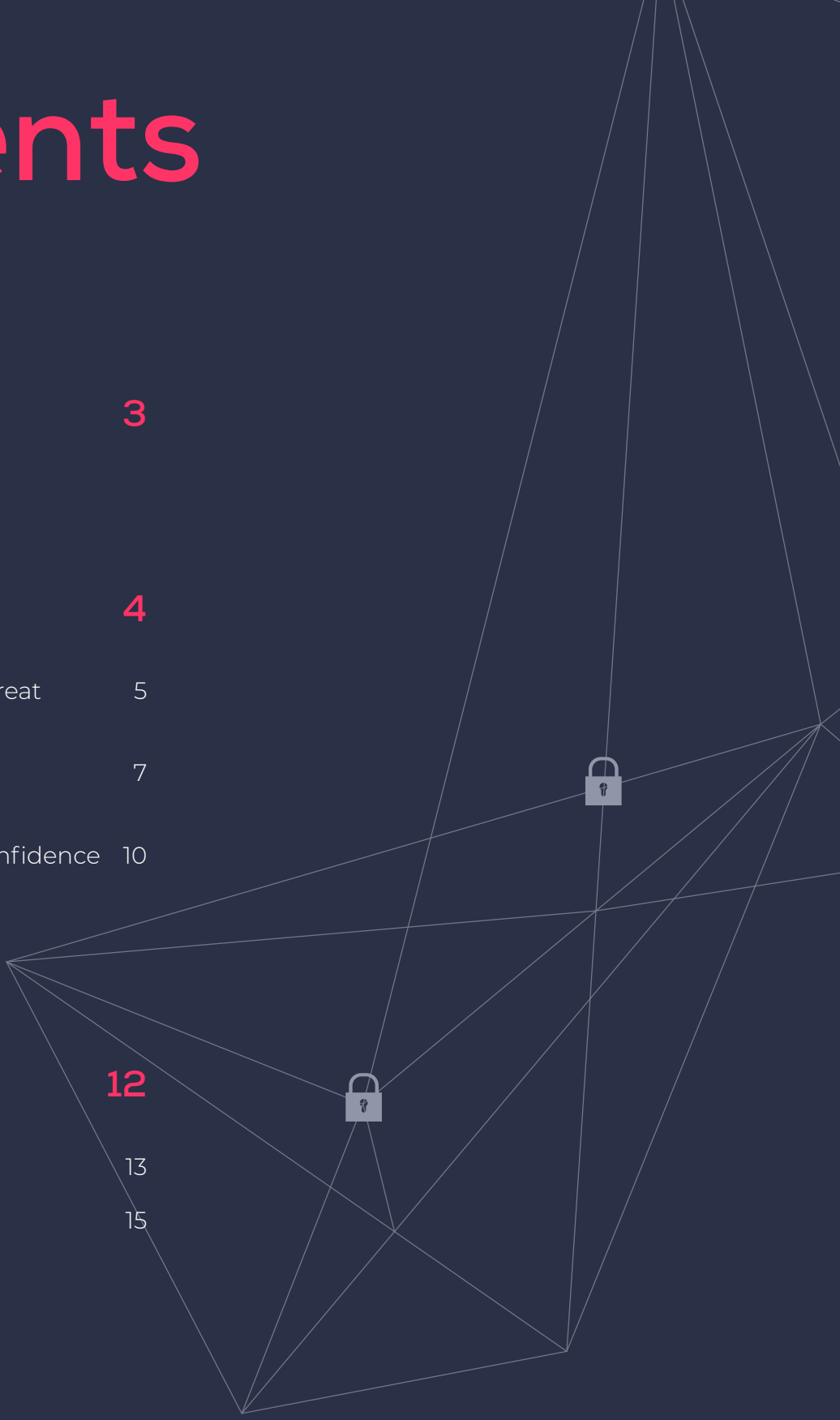
II. What threats could your contact centre be exposed to? 7

III. Data privacy, an issue of compliance and consumer confidence 10

2ND PART
How to optimise security with the CCaaS model 12

I. Best practices 13

II. Security with Odigo 15



Introduction

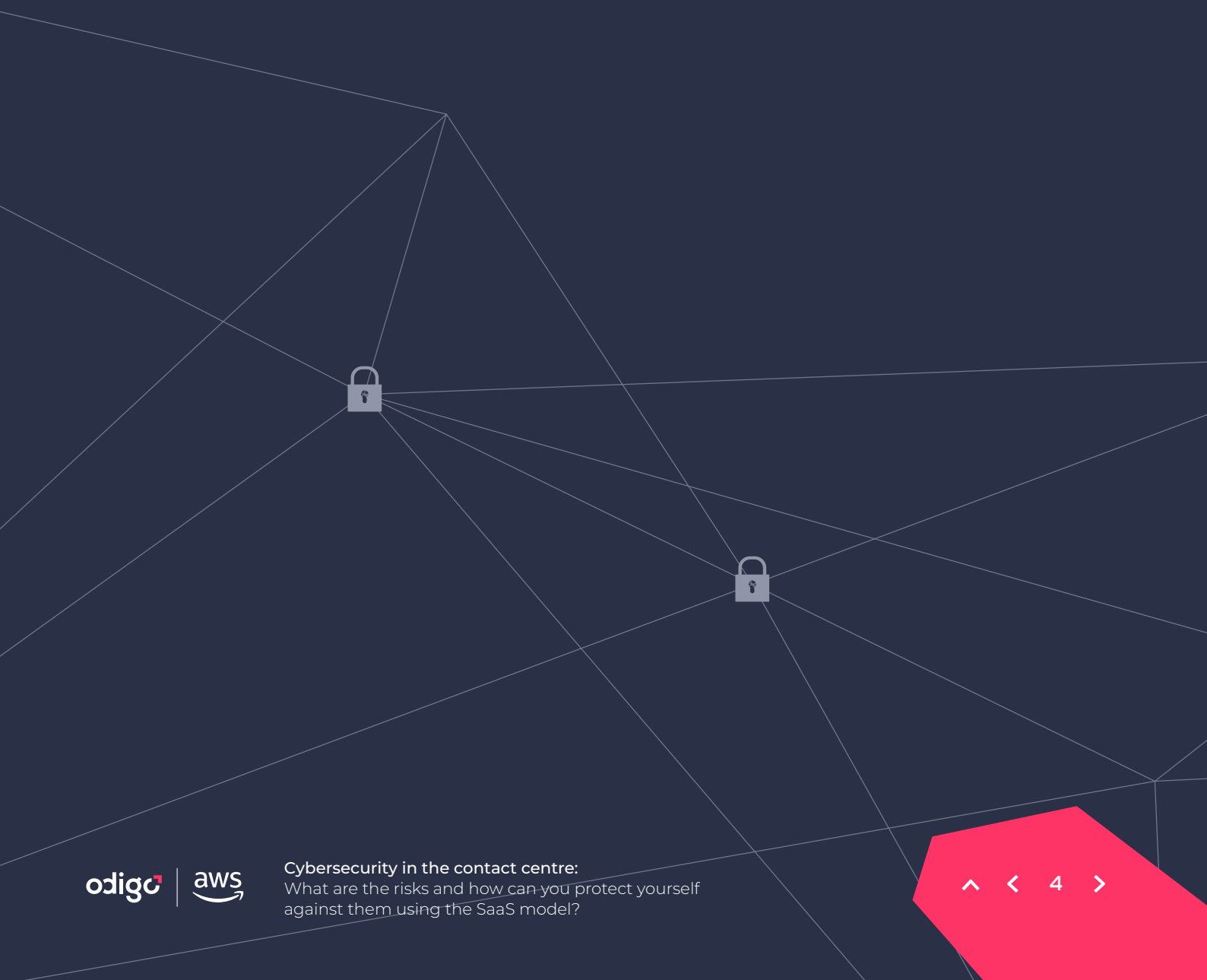
A growing number of companies are choosing to equip themselves with a Contact Centre as a Service (CCaaS) solution to increase the efficiency of their agents and optimise the customer experience. And they're achieving this with omnichannel, automation and the use of artificial intelligence (AI). According to a report published by Allied Market Research, the global CCaaS market, valued at $4.3 billion in 2021, is expected to reach $19.8 billion by 2031. Accelerated by the Covid-19 crisis, this contact centre transformation is now supporting the shift towards remote working and generating new uses.

However, the rise of CCaaS, which is often used by geographically dispersed teams, raises questions about cybersecurity. The security of customer data, in particular, has become a major issue for businesses. The challenge is twofold: to guarantee the accessibility and confidentiality of this data.

As with any cloud-based technology enabling users to access organisations' information systems (IS) and data from the Internet, CCaaS increases the exposure to cyber risks. This is driving the need for greater security and a paradigm shift from a perimeter model (with a single defence barrier) to a 'defence in depth' model, which involves securing each subset of the IS by layering numerous protection measures. The Zero Trust approach, for example, which relies on regular, granular access controls to resources, is part of this approach.

What are the main cyber security risks? How can you better secure your contact centre and protect your customers' data? And what risk management measures have Odigo put in place as a CCaaS solution world leader and an established partner of cloud provider Amazon Web Services (AWS)? This white paper gives you all the answers.

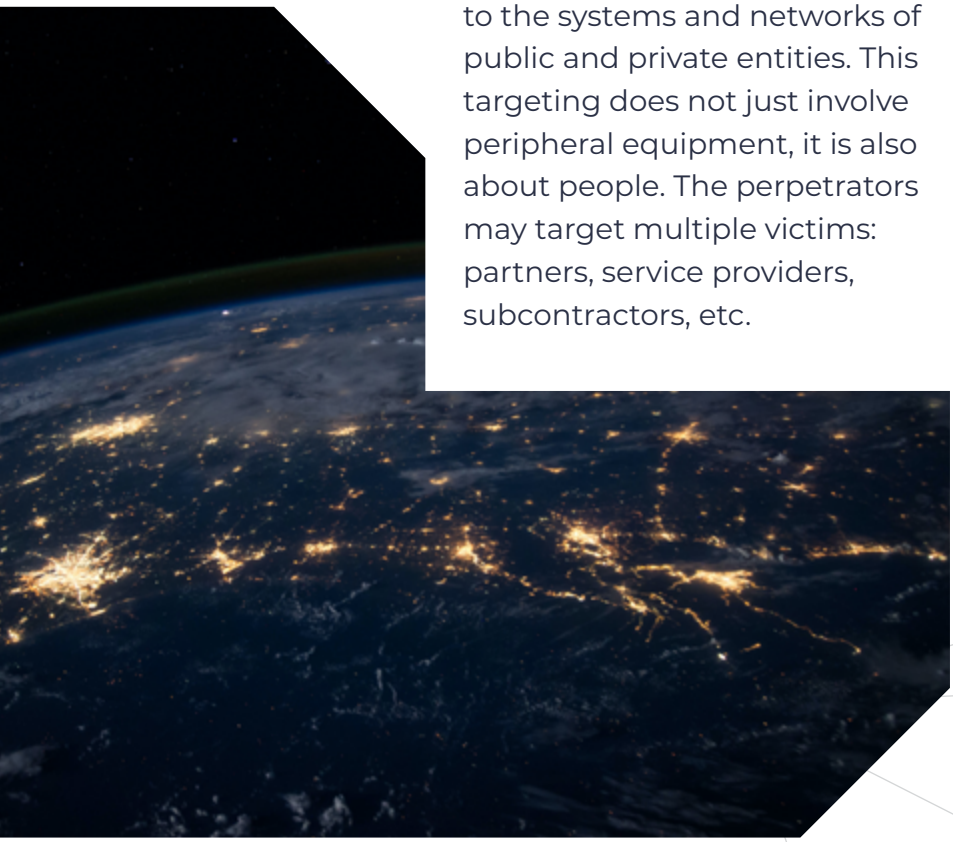
1ST PART Cybersecurity Risks

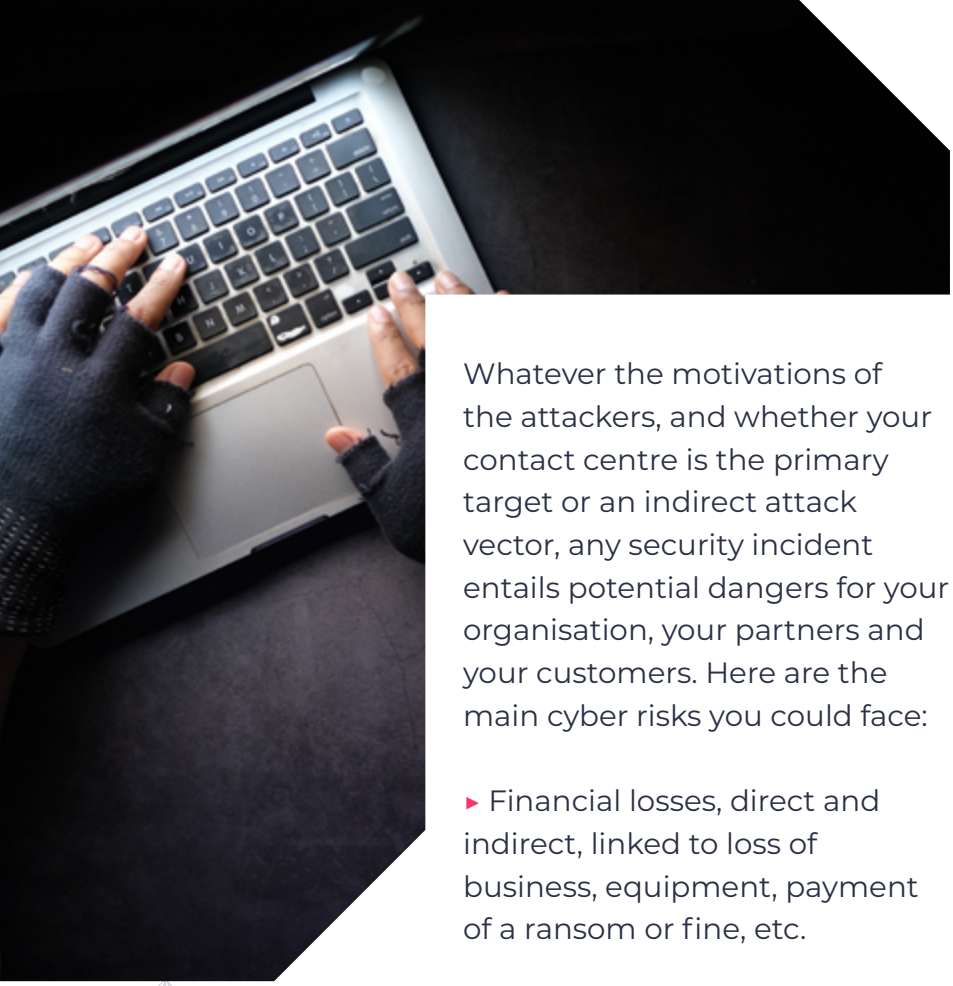


I. The current state of cyber threat

In its "Cyber Threat Overview 2022", the ANSSI (French national agency for information systems security) takes stock of the trends that marked 2022. It reports that the general level of the threat observed in 2021 will be maintained in 2022, but will shift to less well-protected entities. The ANSSI warns that criminals are continuing to hone their skills. In particular, this means "peripheral targeting" which presents a covert and more persistent access point to the systems and networks of public and private entities. This targeting does not just involve peripheral equipment, it is also about people. The perpetrators may target multiple victims: partners, service providers, subcontractors, etc.

The same is true of ENISA, which notes that malicious groups are increasingly specialising in techniques for attacking the supply chain and managed service providers (MSPs). Attacks on data are among the eight major threats identified by the European Union Cybersecurity Agency, perpetrated for financial gain (most commonly), espionage and political destabilisation.





Whatever the motivations of the attackers, and whether your contact centre is the primary target or an indirect attack vector, any security incident entails potential dangers for your organisation, your partners and your customers. Here are the main cyber risks you could face:

- Financial losses, direct and indirect, linked to loss of business, equipment, payment of a ransom or fine, etc.
- Business disruptions, due to the failure and subsequent reactivation of IT systems.
- Damage to reputation.
- Theft, disclosure or loss of data.
- Creation of breaches in your information system.

The good news is that organisations, too, are strengthening their capabilities by drawing on new approaches (Zero Trust, for example), new detection and protection tools and the expertise of external service providers.

"Thanks to the Cloud and the SaaS model, businesses can delegate part of their risk management to providers with much greater skills and resources in this area. They benefit from industrialised solutions available on demand, which are much simpler to install, configure and maintain."

Matthieu Bouthors
Security Solutions Architect at AWS

II. What threats could your contact centre be exposed to?

Contact centres, whether hosted in the cloud or not, are a target for criminals. They can operate via the telephone, interactive voice servers (IVR) or the Internet to steal money or sensitive information about companies or their customers. Fraudulent calls, Telephony Denial of Service (TDoS) attacks and phishing are just some of the attacks you need to be particularly vigilant about.

Fraudulent calls

Call fraud is one of the most common attacks on contact centres. Criminals use two types of attack:

- Hacking into equipment (such as the IP PABX).
- Spoofing and identity theft using tools to spoof telephone numbers, IP addresses and caller IDs, or social engineering techniques to impersonate real customers or employees.

Toll fraud is a global problem, costing organisations millions of dollars every year. It occurs when an unauthorised user gains access to the contact centre's telephone system (usually by infiltrating the IVR system) to make a large number of long-distance calls, resulting in exorbitant bills. This type of fraud can also have the effect of overwhelming the victim's telephone lines, draining their IT and human resources and creating the conditions for a Telephony Denial of Service (TDoS) attack.

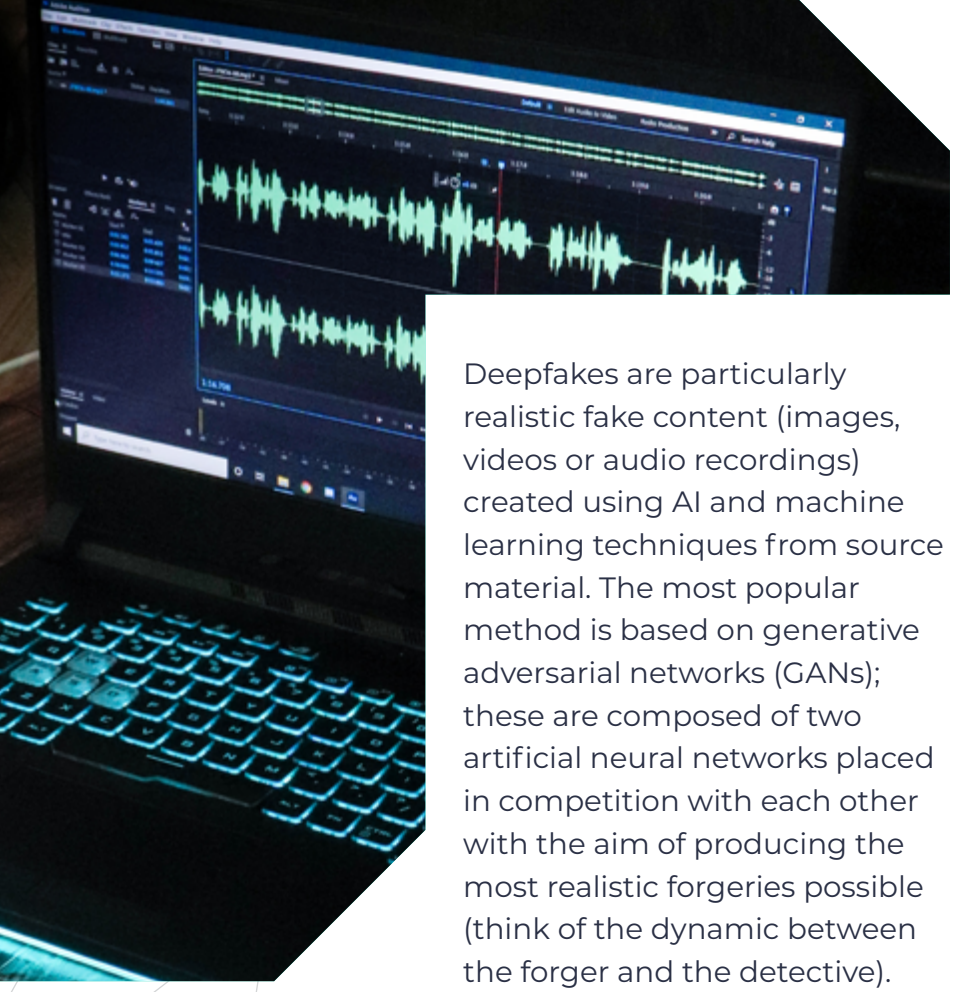
Cybercriminals can interact with contact centre agents using stolen information, such as personal data (a real customer's name, social security number, date of birth, etc.) or a credit card number, which they may have tested by entering it into an IVR. They then seek to obtain more information about the legitimate user, to convince the advisor to give them access to his or her account, or to trigger certain actions, such as purchasing products, transferring money, or changing login details. They may also try to gather information about the organisation and internal workings of the company.

Robocalls and the emerging use of AI-based tools are making it more complex to evade and detect these scams.

Deepfakes, a new threat?

In recent years, spectacular advances in AI have led to the emergence of technologies that can produce ultra-realistic dummy audio content. These tools are becoming increasingly sophisticated, but also increasingly easy to access.

Several research teams have succeeded in creating very convincing voice clones using so-called "generative" models, using recordings of real people just a few seconds in length. Although this technology opens up exciting new possibilities, it is already being used for malicious purposes. It can be used, for example, as part of a fraudulent call to interact with IVRs, and even to deceive human agents, by reproducing real voices and manipulating audio content. Deepfakes, in particular, are attracting growing interest from security specialists and the general public.



Deepfakes are particularly realistic fake content (images, videos or audio recordings) created using AI and machine learning techniques from source material. The most popular method is based on generative adversarial networks (GANs); these are composed of two artificial neural networks placed in competition with each other with the aim of producing the most realistic forgeries possible (think of the dynamic between the forger and the detective).
In the case of faked audio, the process makes it possible to capture, analyse and reproduce voice characteristics and speech patterns from voice samples (extracts from speeches, telephone conversations, etc.).

Audio manipulation is a source of concern for contact centres, as it could facilitate attacks based on social engineering, such as voice phishing, by making imitations and manipulations undetectable. While some deepfakes are impressive, specialists point out that they do not always produce perfect results. Some attack scenarios, particularly those involving real-time interaction, require significant computing capacity and a wealth of source material, both in terms of quantity and quality.

Telephony Denial of Service (TDoS) attacks

Telephony Denial of Service (TDoS) attacks are another real threat to contact centres. They aim to make a telephone system unavailable to legitimate users by draining all resources so that it becomes impossible to receive or make calls.
They are sometimes used by cybercriminals to extort money as part of a ransom demand, or by hacktivists to harass or hinder their target's activity.

"Elasticity in the cloud, i.e. the ability to adapt IT resources to demand quickly, and the greater potential to automate the provision of these resources, make it possible to be less sensitive and/or better manage this type of attack."

Matthieu Bouthors
Security Solutions Architect at AWS

III. Data privacy, an issue of compliance and customer confidence

The attacks described can result in a data breach (any security incident that compromises the integrity, confidentiality or availability of data), a particularly serious situation. According to a study carried out by IBM Security, 83% of companies have fallen victim to a data breach more than once. In addition to the financial impact, the damage to the target's reputation and to its employees and customers should be acknowledged as a significant concern.

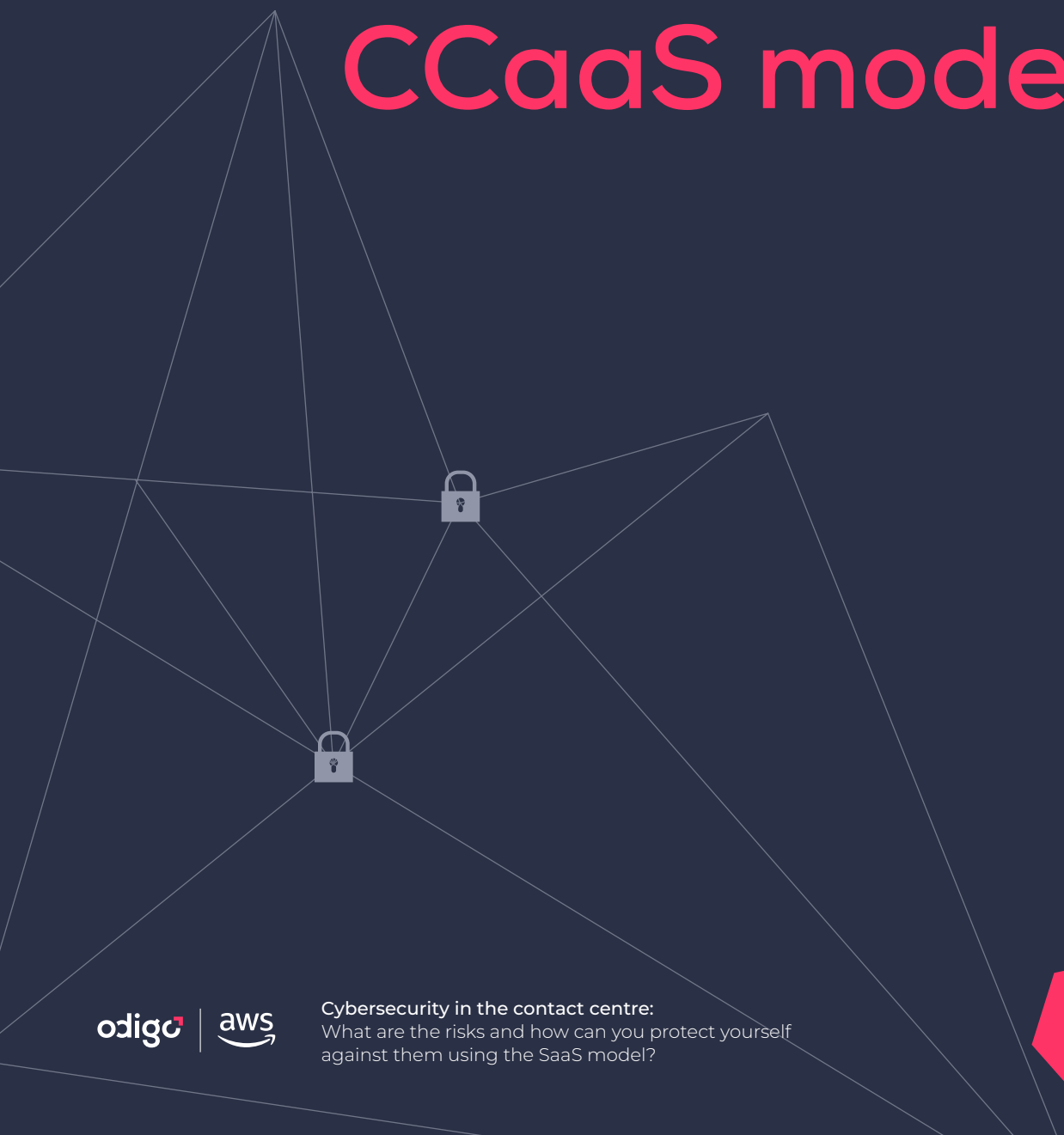
According to the latest Verizon data breach investigation report (DBIR), published in 2023, authentication information and personal data are the two most sought-after types of data. The latter represents an "inexhaustible source of revenue" for cybercriminals, 90% of whose motives, according to the report, are financial. Not only can it be used to perpetrate financial fraud, it can also be sold on the black market.

Protecting customers' personal data is therefore an important issue for companies, who are now required by law, as "data controllers", to take the necessary precautions to guarantee data security and confidentiality. This subject is all the more important because data privacy is of growing concern to citizens. It's become a matter of customer confidence. According to an EY survey on consumer privacy carried out during the Covid-19 pandemic, 63% of respondents said they would only share their data with an organisation if they were sure it would be collected and stored securely. In this "new landscape of personal data protection", companies can no longer be satisfied with simply strengthening their own defences. They need to ensure that their cloud solution providers have the necessary expertise in data security.

At the current threat level, the question is not whether a cyber-attack will occur, but when. However, while the increase in risk is unavoidable, the vulnerability and consequences of attacks are not. A solid, long-term contact centre risk management strategy (including a strict access control policy) and the development of incident detection and handling capabilities in coordination with your CCaaS provider will help minimise the risk of an attack and its impact on your organisation.

2ND PART

How to optimise security with the CCaaS model



I. Best practices

Everyone is responsible for security!

Three main players are involved in the CCaaS model, working together to secure the platform and the data hosted in the cloud, in accordance with a series of standards and/or regulations.

- The cloud hosting provider manages the security of the cloud. It ensures the protection of the infrastructure running the services, which includes software, network and servers. It offers different levels of security configuration and provides advanced security and compliance services.

- The CCaaS service provider manages the security of the platform hosted in the cloud. It provides updates and data management tools to make the contact centre software as secure as possible.

Note : *Digital service providers will soon be subject to the new NIS directive (NIS2), which strengthens security requirements and introduces obligations to report incidents.*

- Finally, the organisation contracting the services oversees all aspects of contact centre security and deploys the resources needed to protect access to services and data hosted in the cloud (securing workstations and mobile equipment, access policy, user training and awareness, etc.). As the data controller within the context of the General Data Protection Regulation and UK GDPR, the business itself must implement the technical and organisational measures required to protect personal data and ensure that its subcontractors and suppliers also provide sufficient guarantees.

When you choose an Odigo contact centre solution, you benefit from the combined expertise of our teams and that of our cloud partner AWS, who takes responsibility for part of the security under a shared responsibility model.

Our recommendations for contact centre risk management

Our first piece of advice is to put in place a robust Identity and Access Management (IAM) policy to prevent unauthorised users from accessing your resources. This involves implementing a set of processes and tools to manage the digital identities of your users and the associated access authorisations (who can access what and for how long). Many companies choose SaaS-based IAM solutions because they are easier to deploy and oversee.

Our second piece of advice is to ensure that your CCaaS solution provider has sufficient resources in terms of cybersecurity and data protection. To do this, check that it has recognised certifications (such as ISO-27001) and complies with the standards specific to your business sector. You can also carry out audits and tests to assess the security of its infrastructure and solutions, and their compliance with your security policy.

Finally, take full advantage of the latest innovations when you migrate to the cloud! SaaS solutions give you access to new capabilities for cybersecurity and data protection, while controlling the costs and complexity of on-premise deployment. These capabilities include detecting vulnerabilities using AI, securing customer interactions using intelligent IVR, encrypting and segmenting customer data using cutting-edge techniques, and monitoring activities in real time using Security Information and Event Management (SIEM) tools.

II. Security with Odigo

Our approach: risk management and continuous improvement

Odigo adheres to the principle of 'Security by Design', which involves integrating security into the design of our products, and adopts a risk-based approach to security, based on threat detection and needs assessment. These needs may arise, for example, from new standards or regulations. The implementation of STIR/SHAKEN provides a solution for combating caller identity theft, but it also entails risks because it introduces new mechanisms, in this case digital certification, into the product delivery process.

"Cybersecurity isn't something that can be solved once and for all, it's a continuous improvement cycle, which means you have to constantly evolve your security architecture and always keep up to date with threats."

Matthieu Bouthors
Security Solutions Architect at AWS

Our approach is based on the analysis, categorisation and treatment of risks, including sensitivity analyses, constant monitoring of threats and vulnerabilities, and measures to protect against spoofing and Distributed Denial of Service (DDoS) attacks. This is reflected in the implementation of regular measures aimed at continuously improving security: implementation of industry best practices, certification efforts, design of customised solutions for our clients in line with their corporate strategy and previously identified business needs, and constant enhancement of our catalogue of services to incorporate the latest technological innovations. This continuous monitoring and improvement approach applies equally to safety, quality and compliance.

Our resources: a coherent, comprehensive and responsive safety system

So how can Odigo and its AWS partner help you identify risks, protect your contact centre and detect and respond to security incidents?

Bertrand Deroubaix, Risks, Quality & Security Director at Odigo, explains: "Our system integrates threat management, vulnerability prevention and control & monitoring. We ensure that all these essential functions are interoperable and communicate with each other, to build a coherent and responsive security management system capable of meeting all our clients' challenges. All the while ensuring enhanced data protection and compliance." He also adds: "Our key words are governance, resilience and sovereignty".

These measures include:

- Intrusion prevention systems, anti-malware, firewalls and patches, reducing your exposure to threats and vulnerabilities.

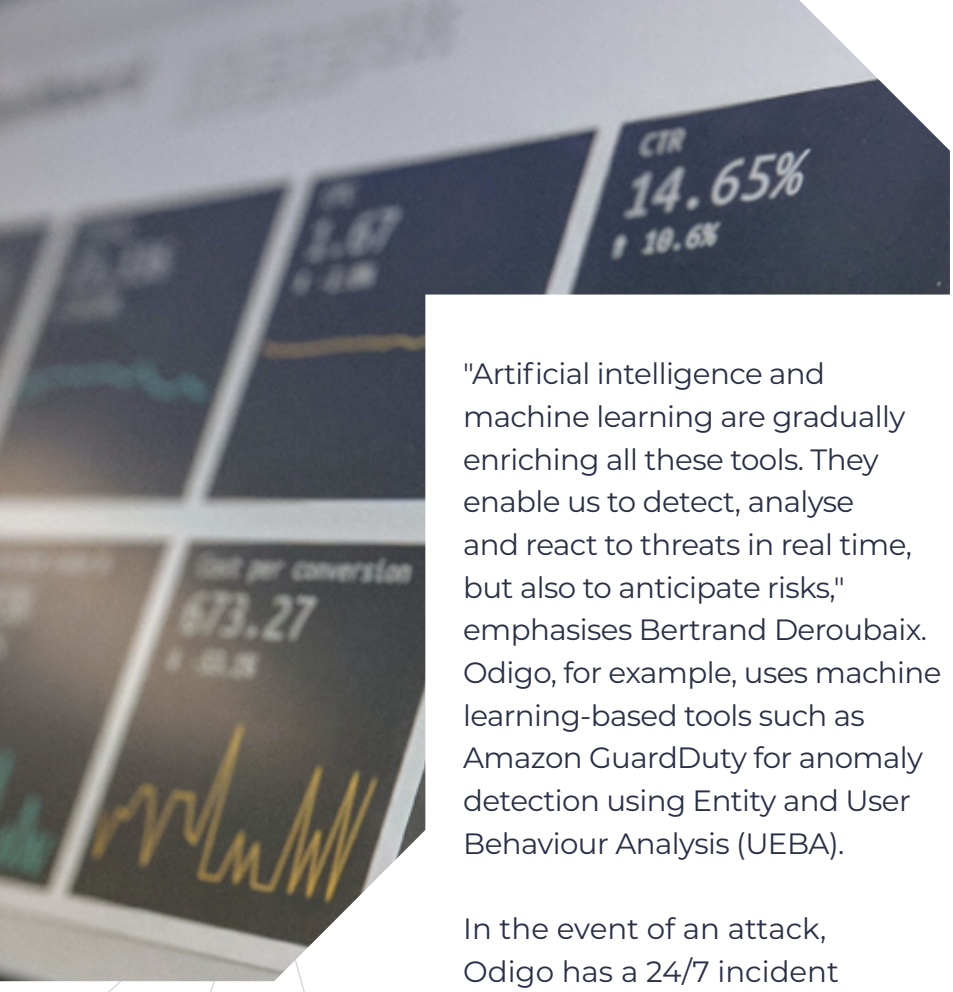
- Micro-segmentation systems, encryption of data stored and in transit, and single sign-on (SSO), to guarantee the confidentiality and integrity of your data.

- SIEM tools, which monitor incidents in real time and transmit alerts to our Security Operations Centre (SOC). These are supplemented by annual audits and intrusion test campaigns.

- High-availability mechanisms in our data centres, spread across different sites, guaranteeing the availability and resilience of our services.

"All customers who host their applications in the AWS cloud benefit from a number of tools that are activated by default. For example, protection mechanisms against DDoS attacks or on-the-fly encryption of network flows. It is then possible to go further, thanks to AWS on-demand services. For example, Odigo has set up data-at-rest encryption using AWS Key Management Service."

Matthieu Bouthors
Security Solutions Architect at AWS

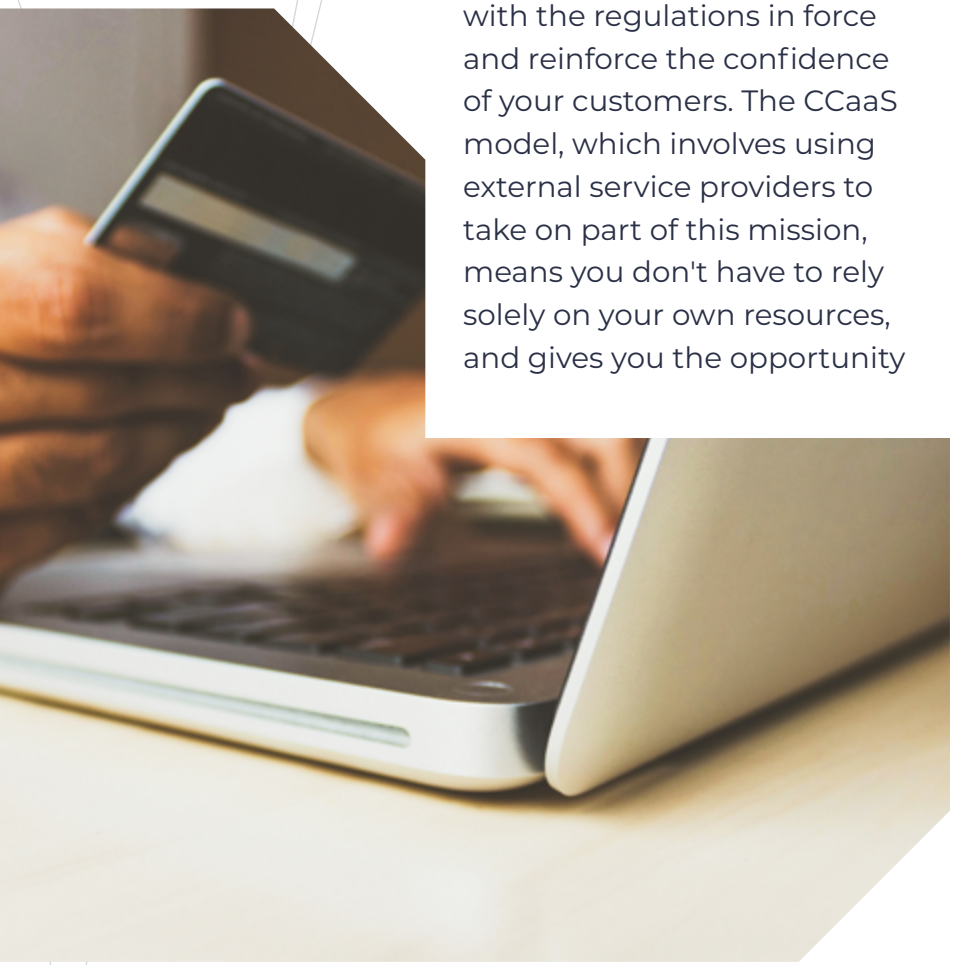


"Artificial intelligence and machine learning are gradually enriching all these tools. They enable us to detect, analyse and react to threats in real time, but also to anticipate risks," emphasises Bertrand Deroubaix. Odigo, for example, uses machine learning-based tools such as Amazon GuardDuty for anomaly detection using Entity and User Behaviour Analysis (UEBA).

In the event of an attack, Odigo has a 24/7 incident management system. We inform the targeted client of the incident and restore services to normal within two hours, minimising the negative impact on contact centre activity.

Our certifications: high standards

When you choose Odigo, you benefit from a certified solution and infrastructure. Odigo and its partner AWS are ISO-27001 and ISO-9001 certified, demonstrating our expertise in data security (ISO-27001) and quality management for all our services (ISO-9001). We seek to obtain international cross-industry certifications, complemented by local certifications, demonstrating compliance with industry-specific standards. For example, Odigo is HDS certified for hosting personal health data and PCI DSS certified for hosting payment card data. "Today, many clients choose Odigo's payment services modules because we are able to collect payments via the contact centre on a global scale, and then route them to their information systems with improved security and compliance," says Bertrand Deroubaix. For its part, AWS has signed up to CISPE. This data protection code of conduct guarantees organisations that their cloud infrastructure service provider meets the requirements of the GDPR. More than 100 AWS services have been declared compliant with the CISPE code.



Risk management in your contact centre should be an integral part of your cyber security strategy. It enables you to prevent cyber-attacks and protect data to ensure business continuity, compliance with the regulations in force and reinforce the confidence of your customers. The CCaaS model, which involves using external service providers to take on part of this mission, means you don't have to rely solely on your own resources, and gives you the opportunity to go further in terms of security and compliance. This choice gives you access to advanced detection and protection capabilities and new automation possibilities. It simplifies the use of certain technologies that are difficult to implement on-premise. Odigo and its first-class partners will support you at every stage of securing your platform.

odigo

About Odigo

Odigo provides Contact Centre as a Service (CCaaS) solutions that facilitate communication between large organisations and individuals using a global omnichannel management platform. With its innovative approach based on empathy and technology, Odigo enables brands to connect through the crucial human element of interaction, while also taking full advantage of the potential of digital. A pioneer in the customer experience (CX) market, the company caters to the needs of more than 250 large enterprise clients in over 100 countries.

Visit us:
www.odigo.com/uk

Contact us:
contact.uk@odigo.com

Customer experience inspired by empathy, driven by technology