Eckoh

Moving your contact center to the cloud?

How to stay secure when launching a cloud contact center

01
The march to the cloud is unstoppable

Organizations are moving their contact centers to the cloud in vast numbers. They're often attracted by greater scalability, flexibility, simpler management, and tools for greater insights into the customer journey. Switching to a CCaaS (Contact Center as a Service) may also deliver savings.

There's movement within the cloud too. Early adopters are switching providers for a better deal — or contact center features that align better with their roadmap.

But when you're up and running in the cloud, who's responsible for security?

Is security something that's now outsourced to a cloud provider? Can you relax completely?

This is an issue that the C-suite, contact center leaders, security leaders, and migration teams must have at the front of their minds.

Let's take a closer look →

The numbers are only pointing one way

The global cloud-based contact center market is estimated to be growing from $17.1 billion to $54.7 billion in the five years to 2027 – that's a compound rate of about 26% a year

Source:
Global Forecast to 2027
MarketsandMarkets

02
How far does cloud security extend?

"Our cloud provider has military-grade security, so everything inside our contact center is protected, right?"

Answer: No.

Cloud platforms have their own robust security. And that's a big win if you're switching away from on-premises servers and other technology.

Cloud providers' service-level agreements (SLAs) will normally cover important areas such as availability, load-balancing across data centers, and disaster recovery.

Vendors may also apply security scanning and vulnerability assessments. Machine learning and artificial intelligence may also have a role in their security practices, tools, and capabilities. Some follow leading security standards, such as SOC 2 Type II and ISO 27001. You may encounter an Attestation of Compliance (AoC) regarding cardholder data, which provides a sense of comfort.

So it's easy to assume you're completely secure ... when that's not the case.

Cloud providers give you a set of keys - but protecting what happens inside the stack they've given you is **your responsibility**. This **shared responsibility** model that cloud providers lay out means that if there's a data breach, then you're liable.

It's worth knowing ...

Out-of-the-box cloud security can lack the critical features and nuances of a contact center's previous set-up. This may have been carefully tailored and evolved over years by experts – to specific needs, such as secure integration with a payment platform and CRM. It could turn out that the new cloud service doesn't offer a security equivalent.

So where can that leave a business and its customers? There's one word for it: vulnerable.

That's because the cloud is a sweet spot for criminals. Cloud environments were frequent targets for cyber attackers in 2023, according to a recent IBM study[1]. In fact, 82% of data breaches explored in the report involved data stored in the cloud.

Did you know

The global average cost of a data breach is at an all-time high. $4.45 million global average cost (up 15% on 2020) $9.48 million average cost in the United States.

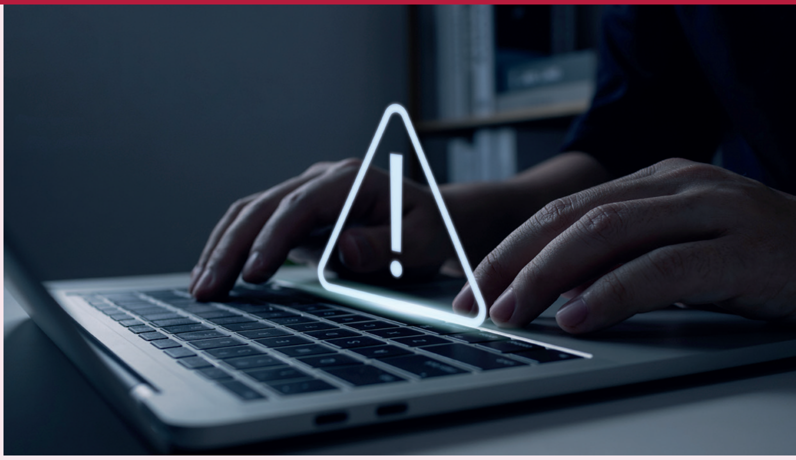
Let's see what criminals are targeting →

[1] Source: "Cost of a Data Breach Report 2023": IBM study based on independent research by the Ponemon Institute

03 What's most at risk in my cloud contact center?

Criminals target personal identifiable information (PII) – which includes payment card details and people's sensitive data – commonly processed by contact centers.

The IBM study found that 52% of all breaches involved some form of customer PII. This was the most common and costliest of data being stolen.



How might criminals target and steal PII data?

- Rogue employees listening to customers giving out details during calls
- Criminals stealing sensitive information that appears on agents' screens
- Thieves accessing PII that's stored in call recordings and transcripts
- Criminals stealing customer records through hacking or social engineering attacks, such as phishing
- Staff sharing confidential data by accident – or through lapses that leave systems vulnerable

It's your responsibility to ensure this data is secure.

Organizations must protect themselves, safeguard customers, and keep in step with PCI DSS 4.0 security, GDPR and CPRA privacy requirements, and other compliance demands. Failure can mean business disruption, lasting brand damage and lost business, and significant financial penalties.

So what's the simplest way to protect this sensitive data?

How can companies take full advantage of the cloud without worrying about data security.

Let's consider the options →

04

How can I maximize protection for sensitive data in the cloud?

Let’s take the issue of securing customers’ card details as an example.

This is a hot topic for contact centers right now – because of the arrival of the PCI 4.0 security standard, which has raised the stakes with its far more stringent rules.

Typically, there are two routes you can take to protect sensitive data:

↘

Do-it-yourself security

Here, the full weight of the PCI 4.0 security standard falls on your organization. Compliance isn’t an annual tick-box exercise, it’s an ongoing mission that must permeate your business, processes, and systems – on your premises and in the cloud.

Security relies on watertight protocols, timely updates, and company resources. You may need to recreate old security measures in the cloud – or find new, cloud-suitable ones quickly. One slip-up can prove disastrous.

↘

Work with a trusted security partner

Many forward-thinking contact center leaders work with partners to process card payments for them. A PCI DSS Level 1 Service Provider can secure payment data for you and actually shield your contact center environment from any trace of sensitive data.

Customers’ valuable payment card details will never enter your cloud-based systems or your premises, remote offices, or devices. Sensitive data can’t be seen, heard, recorded, or stored anywhere. Even if there was a security breach, there’s nothing to steal - reducing the risk of loss of associated PII data too.

This can minimize stress, cost, and risk for your organization. For example – you can remove your environment from the scope of PCI DSS 4.0 compliance as a relates to the handling of card data.

What my best next move? →

05

Next steps: What to do before you migrate

Planning ahead pays off. Here are three steps for a smoother transition for your contact center to a new home in the cloud.

Step 1: Understand your current set-up

There will be nuance and complexity around your existing contact center stack and operations, and it's best to know this – long before you launch in the cloud. Your team can then pinpoint potential areas of risk. Don't assume a simple tick-box from cloud contact center vendor will suffice.

Step 2: Engage early with specialist partner

The best suppliers – in areas such as contact center security – will have ready-to-go integrations with the leading CCaaS platforms. You can then take your robust security with you, or find someone new who's got a track record providing specialist security in the cloud. This can take a huge weight off your shoulders.

Step 3: Protect your migration, end to end

Often, cloud migrations are phased. So you need a contact center security specialist who'll be experienced in providing a shield of data protection before, during, and after you've made the switch. Migration itself will be challenging enough. Ensure someone else can save you from the added risk of a serious data breach.

Eckoh

Discover more

Eckoh has supported many contact center migrations to the cloud for a range of customers across industries. We understand the complexities and pressures involved. We'll help to safeguard your migration and help to ensure your cloud strategy delivers benefits from day one.

☎ **Call:**
US +1 866 258 9297
UK +44 (0)330 404 7330

✉ **Email:**
hello@eckoh.com

Visit:
www.eckoh.com