Four megatrends that could threaten your contact center SECURITY

GTS

GENESYS™

Introduction

In the face of rapid technological change, contact centers are quickly evolving. And the security measures they use to safeguard their customers, employees and company need to keep up.

The costs of poor security are high: a tarnished reputation, loss of consumer trust and confidence, potential lawsuits, and deteriorating bottom lines. Technology moves so fast that companies that fail to adapt with the right security solutions will be left behind.

Some contact centers have responded by migrating their operations to the cloud — a secure option when working with the right vendor. But even as cloud-based ecosystems become more prevalent and sophisticated, companies must remain vigilant to ensure stringent security standards are maintained.

By analyzing some of the larger forces at work — "megatrends" that shape the security landscape for years, if not decades — we learn that moving to the cloud not only guarantees the security of data better than on-premises systems, but the cloud also places contact centers in a perfect position to capitalize on emerging trends and maximize their success.

Contents

MEGATREND 1

The remote/hybrid workforce brings unique security challenges

With companies of all sizes going remote, it's only a matter of time before most companies deploy a hybrid, if not fully remote, workforce.

Remote work has a wide range of benefits — happier, healthier employees; low operating costs; and a smaller carbon footprint. But it's not without security risks.

An **HP study** found that 70% of remote office workers said they use work devices for personal tasks, and 69% use personal laptops or printers to do their work.

So **with more agents working from home**, call centers need updated and clearly defined security protocols about how data moves through their operations in a remote environment.

Fence your data

Because of how data is accessed and flows differently in a hybrid workforce, companies need to set up perimeters around their data to guarantee its security. Data fencing — restricting access to data by location — is table stakes in the age of restructured labor.

Whether data is on internal servers or in the cloud, on employee devices, or transiting between endpoints, it all moves through the ecosystem. And no matter whether it's at rest or in motion, you must prevent that data from crossing compliance boundaries.

The size, focus and location of your fencing depends on your operations. For example, it can start at the level of the individual remote employee — where contact centers first ensure that only workers with appropriate permissions can view restricted workloads. It then encompasses external third parties that manage data. Regardless of scope, data protection standards must be established for and followed by all.

KEY TERMS

- **Data residency:** The geographic location upon which data is stored
- **Data sovereignty:** Laws that govern where the data is stored
- **Data localization:** Laws dictating the boundaries in which data must remain
- **Data fencing:** The ability to restrict data within geographic borders

Data localization in the time of remote workers

Abiding by data sovereignty laws has become increasingly difficult with the growing remote and often transient workforce.

Let's take Brenda, an agent working remotely in Germany, as an example. Brenda's mother lives in Spain and has become ill. So Brenda rushes to her mother's side, forgetting to inform her manager. Brenda grabs her computer so she can continue to work while overseas, thinking that as a remote worker she can work from anywhere.

While in Spain, Brenda starts helping her first customer from Germany. She uses her internet browser to view the German citizen's data. This is where things get tricky. By accessing that data, Brenda has moved the customer data from Germany to Spain via the internet. Depending on Germany's data localization laws, Brenda and her employer could be breaking the law.

Situations like Brenda's aren't uncommon anymore. Fortunately, technology can help — especially when managers don't know the locations of their employees. For example, some technology platforms will limit data access automatically using geographic attributes and data fencing to protect your customers, employees and company.

Shore up web browser vulnerabilities

An ongoing weak spot, the web browser remains vulnerable to having sensitive information like user credentials and passwords targeted. This information can be used to access personal information, such as credit card details, or company information like proprietary technology or consumer data.

Exploiting the browser to obtain information is done in a variety of ways, from the browser cache, the browser's physical memory (using the Back button and Refresh feature of the browser), the stored password in the browser, or leaked through the URL from the browser's history.

To address these vulnerabilities, install robust web application firewalls on all company devices and networks; insist that employees only connect using private, secured Wi-Fi networks; and train employees about cyber-threats like phishing attacks and browser security warnings.

Think beyond the VPN to context-based multifactor authentication

Virtual private networks (VPNs) have become increasingly common in organizations, especially as employees access corporate networks and data off-premises.

VPNs offer secure data transmission, but they're still subject to frequent cyberattacks. That's because they often have only a single point of access for corporate networks and are based on a single password. When every employee enters the same password, it's easy to penetrate the entire network through mass phishing attacks, ransomware and insecure home routers.

Selecting a VPN with multifactor authentication, such as facial recognition or a text message sent to an employee's company-issued smartphone, adds extra layers of security that are essential for contact centers that rely on VPNs for hybrid or remote workers.

Balance employee monitoring with personal privacy

Remotely monitoring your employees through actions like browser activity and keystrokes can be controversial. But as more employees work from home and use their own devices for company activities, guaranteeing data security requires oversight.

Many high-performing employees value personal responsibility and trust when doing their work. By remotely monitoring employees, you could jeopardize your relationship with top performers and possibly even cause them to leave.

As a first step, companies need to ensure they have the right to monitor their employees, as it's only legal in some jurisdictions and under certain circumstances.

If monitoring is permitted, companies should be transparent with employees about how and why they'll be monitored, as well as what happens to captured data. For example, if employees are using their own devices, gain consent from employees to access those devices. This is the ethical thing to do — and it offers some legal protection if there's a termination or data breach.

GOOD NEWS:

Personal responsibility is the strongest motivating value in high-performing contact center employees.

"Human values: The operating system for a high-performing contact center"

Genesys, 2022

MEGATREND 2

Consumers demand more control over their data

With compliance measures finally catching up to some of the more brazen data-mining tactics of new advertising technologies, the struggle between consumer data and privacy has swung in favor of the consumer. This doesn't mean that concerns surrounding data privacy and protection have disappeared. Rather, these issues are more important than ever.

Customer data is increasingly positioned as the key to successful marketing at a time when consumers are still very concerned about privacy issues — consumers who, paradoxically, now expect more personalized customer experiences.

Prioritize data privacy and protection

Given the long and very public history of massive data leaks, it isn't surprising that data privacy remains one of the most important social and ethical concerns for consumers and businesses around the world.

A 2021 **survey by KPMG** found that consumer anxiety about data remains high: 86% of consumers worry about data privacy and 78% worry about the amount of data collected — both figures up from previous years.

Despite this growing anxiety, data collection has increased, even while security measures seem to lag: the same KPMG study found that 70% of companies expanded their collection of personal consumer data over the past year. And 62% admitted they could do more to strengthen their existing data-protection measures.

Consumers are still willing to share their data, but it's with the expectation that it'll be secure and used to improve their customer experiences.

DATA PROTECTION AND PRIVACY is the number one environmental, social or ethical concern for consumers worldwide.

"State of customer experience"

Genesys, 2022

Exchange experience for data

Rather than buy into the generic messaging of traditional marketing, consumers increasingly want content personalized to their specific needs and preferences. And they're willing to exchange their data for this improved experience.

People now expect the type of personalization they get from Netflix or Spotify — streaming services that collect data about users to deliver better and more tailored recommendations.

Not only have **two out of three** consumers said they receive better service from companies that collect their data, but **91% are more likely to shop** with brands that personalize their offerings. In fact, 72% of consumers said they ***only*** **engage with personalized messaging.**

PRO TIP:

Remember: Trust is earned through years of positive experiences. But it can be lost due to a single broken promise.

Earn trust through transparency

There's a paradox: Consumers are very concerned about data privacy but they also want personalized experiences. By including transparency into their everyday data operations, businesses can overcome this challenge and find the right balance.

Transparency involves being very clear about what you intend to do with user data and ensuring that, whenever possible, data collection is anonymized. Being transparent also directly involves your customers — giving them more control over what data they want to share and getting permission where applicable.

PRO TIP:

When you champion transparency and disclose your data intentions, people see you as more genuine; this authenticity is the bridge to building trust.

MEGATREND 3

Housing massive amounts of data can pose a security threat

As a call center adopts new technologies to streamline operations and improve customer relationships at a wider array of touchpoints, it produces exponentially more data. This is great to power AI, develop insights and further refine customer experience strategies. However, increasing amounts of customer data pose a logistical and security threat to both businesses and customers. Strategies are necessary to capture this growth and store data securely.

Prepare data infrastructure

Customer interaction recordings, whether they're screen, chat or voice, offer call centers a wealth of benefits. They provide companies with training material and deliver more granular data to power omnichannel experiences — and that creates better customer experiences. Call centers can also leverage quality evaluation tools to track compliance and keep an audit trail that demonstrates — to regulators and customers — how your company follows information collection procedures.

These recordings are robust tools that generate volumes of valuable data and insights that need to be stored in a consistently secure and compliant way — or not stored at all in certain instances. To take advantage of all the benefits of new technology like interaction recordings, call centers must be prepared with the right IT infrastructure in place.

PRO TIP:

Building services on a microservices foundation inherently allows for security walls or layers within the solution. This means any potential attack surface is smaller than the whole, which limits the impact and reach of threats.

Layer your security

Given the sophistication of current cyberattacks, companies can't assume one methodology will solve all security problems. The key is to secure all your data — not just your network.

To minimize the impact of a potential data breach, part of building the right IT infrastructure is to integrate security at various layers. This includes:

- Encrypting data at rest and in motion
- Instituting company-wide, role-based access rules according to job function
- Integrating a strict password management system
- Keeping abreast of your industry's compliance standards and ensuring you have the tools to meet them

PRO TIP:

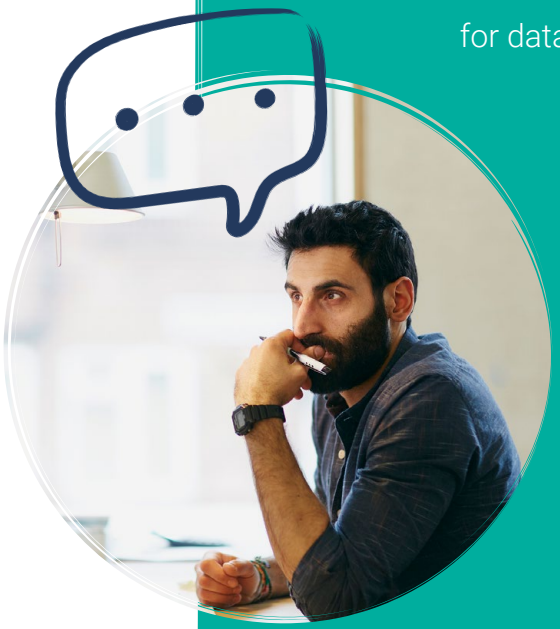
When building security layers, think past the conventional CIO role of passive intervention. Partner with your technology leaders early and at strategic levels to ensure that security is prioritized and operationalized across the entire organization.

Weigh your options

Managing the storage of huge tracts of important business data will become part of every company's future security posture. And it's a major consideration for call centers as they move to new digital solutions.

With access to the sheer amount of data, there's game-changing potential to enhance everything from training to bottom lines. But how you anonymize the data and store it safely makes the difference in the long term.

Regulations like GDPR dictate how long data can be stored and how it should be removed. At the outset, deciding on how long you store data and how you dispose of it will save you security and storage headaches down the road. Also, many cloud service providers provide elevated security layers like encryption at rest and in motion.



PRO TIP:

When experimenting with data to improve AI models, data scientists should handle only anonymized data to further reduce the scope for data breaches.

MEGATREND 4

Cloud is now the baseline for better security

With its host of reliable and consistently proven benefits, cloud technology is here to stay. As more companies opt to streamline their operations from it, the overriding necessity for cloud security is paramount.

Data can be more secure in the cloud than in a data center — if handled properly. With their reputation and bottom lines at stake, cloud service providers cannot afford the slightest lapse in security. Often, they have their own dedicated security specialty teams that few organizations can match or afford.

Implement cloud security best practices

Cloud services are multi-purpose, from data storage to productivity tools and even IT infrastructure. These services let businesses move faster, cheaper and more efficiently. But data security is still a challenge that, ultimately, remains the responsibility of the cloud customer.

Here are some best practices to reliably guarantee data security in your organization.

- **Apply data protection policies.** Determine the policies that will classify and govern the types of data you're storing in the cloud.
- **Implement encryption — with your own keys.** Encrypting your data is standard and can be done by cloud services, but make sure you use your own encryption keys.
- **Train staff.** Train employees on how to recognize security threats and initially respond to them, including the perennial importance of creating a strong password.
- **Limit data sharing**. Establish which users, groups and roles are granted internal and external access to data, under which circumstances, and across which devices and cloud services.
- **Control unmanaged devices**. Block access to your cloud services from unmanaged devices (e.g., personal phones) or control it by requiring security verifications before access.
- **Secure your user endpoints.** You must protect all network endpoints used to access the cloud, including end-user devices such as laptops, mobile phones and desktops.
- **Conduct audits and penetration testing.** Whether relying on an outside security firm or an internal team, run intermittent security audits and penetration tests to assess current cloud security levels.

> "Increased security, disaster recovery and business continuity are cited as the greatest benefits of migrating to the cloud by almost half of CX leaders."
>
> **"State of customer experience"**
> Genesys, 2022

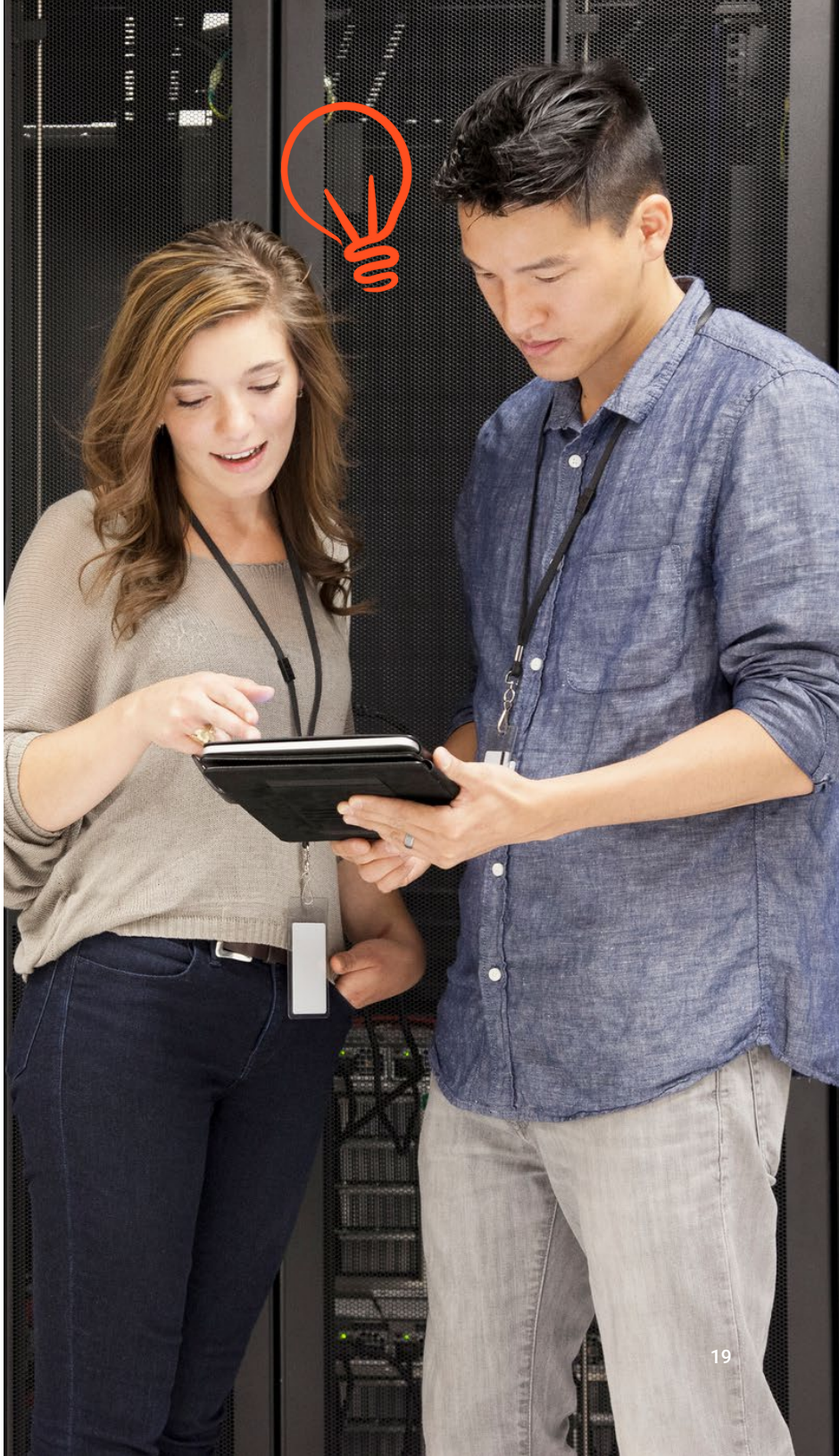
Screen cloud vendors for security

It's imperative for businesses to only partner with third-party cloud vendors who can be trusted to consistently deliver the best and latest in security protocols that conform to industry and regulatory standards. A trusted cloud provider will hold a range of security certifications — and they need to make this information publicly available.

To guarantee your cloud service vendors meet your stringent security standards, we've developed a series of questions you can ask based on four major security pillars: compliance, data protection, information security and business continuity.

Security pillars:

- Compliance
- Data protection
- Information security
- Business continuity



Security pillar questions

Compliance

Your third-party vendors are an extension of your business, so it's essential they — as well as their partners — meet the same stringent regulatory and compliance standards.

- Does your cloud solution comply with all necessary audits and certifications?
- Can customers audit the cloud solution?
- How does your cloud solution provide tools to manage TCPA compliance and Do Not Call lists?
- Does your cloud solution meet GDPR?
- Does your cloud solution comply with Payment Card Industry Data Security Standards?

Data protection

Data breaches put companies at risk of losing both public trust and revenue; protecting that data is essential. **IBM research** found the total average cost of a data breach increased 10% year-over-year in 2021, and increased an additional $1.07 million, on average, when remote work is what contributed to the breach.

- Does your cloud solution provide enterprise-grade security?
- Does the cloud data center have adequate monitoring and processes to address excessive, suspicious or unauthorized attempts to access?
- Is customer data, including sensitive data, encrypted while at rest and in transit?
- Does your cloud solution use web application firewall products to protect against application-layer attacks? If so, do you have documented configuration controls?

Security pillar questions

Information security

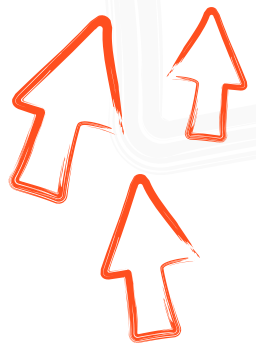
Regardless of size, all vendors should understand the global network design and where any points of vulnerability might exist. They also should have strict policies that protect against both internal and external threats. And vendors must consistently and systematically test and review their code using various tools and vulnerability assessments.

- Do you understand the global network design and where any points of vulnerability exist?
- Does a third-party company perform intrusion tests on your cloud solution? If so, how often?
- How does your cloud solution protect against malicious internal data threats?
- How does your cloud solution protect against Distributed Denial of Service attacks? Does it use Amazon Web Services Shield and load balancers?

Business continuity

After a disruptive incident, returning to normal operations depends on accessing cloud data and services. Vendors must demonstrate how they would first address any disruptions and then seamlessly pick up from where operations dropped off.

- What strategy does your cloud-based contact center use for high availability?
- What's the cloud solution's business continuity plan?
- Does your cloud solution have an additional charge for geo-redundancy?
- Is your cloud architecture designed with inherent geo-redundancy with at least three data centers configured with active-active resiliency?
- Does your solution provide autoscaling to handle substantial increases in demand?



To the cloud — and beyond

These four megatrends are already changing how businesses operate. Too often, however, companies don't have the financial or human resources to meet even basic security standards with their on-premises computing solutions.

Companies that neglect security will see their customers look to others to provide it. And if outpaced by technology, a deteriorating security posture can lead to costly data breaches.

To tackle these challenges, contact centers must form strong partnerships with cloud providers that have the resources and technological know-how to offer digital solutions that meet higher security standards and leverage the power of data for better customer and employee experiences.

And a strong partnership means you'll always have stability in a shifting security landscape: a secure cloud infrastructure, data encryption at rest and in motion, full regulatory compliance, transparency in data processing and intentions, and an unwavering commitment to data privacy.

NEXT STEPS:

Get a personalized demo to see the true power of Genesys.

GENESYS

ABOUT GENESYS

Every year, Genesys® delivers more than 70 billion remarkable customer experiences for organizations in over 100 countries. Through the power of the cloud and AI, our technology connects every customer moment across marketing, sales and service on any channel, while also improving employee experiences. Genesys pioneered Experience as a Service℠ so organizations of any size can provide true personalization at scale, interact with empathy, and foster customer trust
and loyalty.

For more information, contact:

GTS

Global Technology Solutions LLC (GTS) http://www.globo-tek.com

sales@globo-tek.com

+1.855.245.6285