TALKDESK + ZK RESEARCH WHITE PAPER

Working From Home Drives the Need for Better Contact Center Security

talkdesk® + 謀 RESEARCH

Table of Contents

Introduction

COVID-19 rapidly accelerated the digital transformation strategies of most businesses—what would normally take several years happened almost overnight.
The global pandemic hit businesses hard, with workers uprooted out of their offices into their homes.
The 2020 ZK Research Work from Anywhere Study shows the drastic change in where people work.
In North America, prior to the outbreak, about one in five (22%) employees worked remotely. That figure jumped to more than half (53%) immediately after the pandemic started and dipped to 46% as restrictions eased. The study shows that 42% of office workers will continue to work remotely even after companies clear them to return to the workplace. In addition, almost the same amount (40%)nearly double the pre-pandemic levels—will maintain their working-from-home capabilities into the future (see Figure 1).

Figure 1 • Work-From-Home Becomes The Norm (percentage of employees working remotely)

While this is a measure for all employees, the contact center is right in line. After a round of one-on-one interviews with contact center managers, ZK Research estimates that 75% of businesses plan to keep some or all of their contact center agents at home.
There are many business benefits to this, including:

- **Savings on physical space.**
  Contact centers are able to dramatically slash their real estate costs by shifting agents to home. While the amount of savings varies depending on the percentage of agents who are working from home, the majority of businesses interviewed have saved at least 30% and as much as 100% of their real estate costs with all agents working remotely.

- **Increased agent productivity.**
  Having agents work from home disables many of the common problems associated with agents being physically in the same location, such as background noise levels as well as confusion that can arise from inbound and outbound teams handling a mix of support and sales calls in close quarters.

- **Better customer service.**
  Contact center agents report they can be more focused and concentrate better on calls when they are working from home. This leads to improved customer service and shorter call times.

- **Broader talent pool.**
  Typically, businesses only hire contact center agents within a 30 -mile radius of the physical facility. Contact centers that leverage remote agents can hire from anywhere, including poaching high-quality personnel from competitors.

- **Contact center agility.**
  Relying on remote workers can allow organizations to scale up and down as the business requires. Some businesses such as retail and accounting tend to be seasonal and have dynamic calling patterns. Organizations that shift to an at-home model can scale agents on the fly.

I. Shifts in Contact Center Security

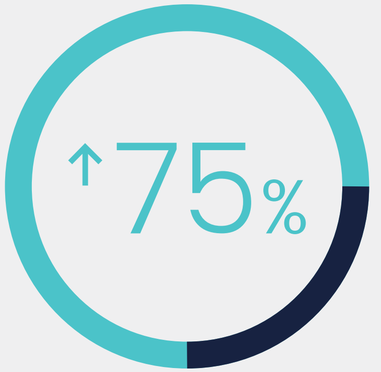
While shifting to a WFH model has many benefits, it does introduce a number of security risks that, if left unchecked, could have disastrous effects on a company. In general, company-wide security has been a greater priority for most businesses, particularly with the European Union's General Data Protection Regulation (GDPR) and the California Consumer Protection Act (CCPA), which have stiff penalties for non-compliance. This has caused the CISO in most companies to have overlapping priorities with CIOs, COOs and even CEOs. These factors are reflected in the ZK Research Work From Anywhere Study, which found that 71% of organizations have increased security spend since the pandemic started.

Historically, all contact center agents were located in the same physical location, and it was assumed all employees were trustworthy. Threat protection was aimed at the physical and network perimeters; everything outside was deemed a threat and everything inside was trusted.

The network edge was defined as the Internet connection as well as the first point of contact—typically a phone call but could be email or chat.

In reality, outsider threats were only part of the problem. Insider threats always existed, but many were mitigated from being in one location. For example, if an agent were to try and steal data with a USB stick, someone may notice the person trying to insert the drive. Now that agents have migrated to a work-from-home model, it's easier for insider attacks to happen and this needs to be addressed.

The most important point to understand is that the threat landscape has gone from something that was manageable with a physical contact center to one that requires new tools and strategies to manage workers located anywhere and everywhere.



of organizations have increased security spend since the pandemic started.

II. Understanding the Security Risks Created by WFH Agents

For many organizations, the contact center is considered the lifeblood of the company. It's often the first point of contact for customer interactions, a critical role in overall customer experience and a focal point for upsell opportunities. Over the years, the contact center has evolved from voice-only to multichannel to omnichannel (Figure 2). Conversations are now occurring over a wide range of channels including voice, chat, SMS, e-mail and others.

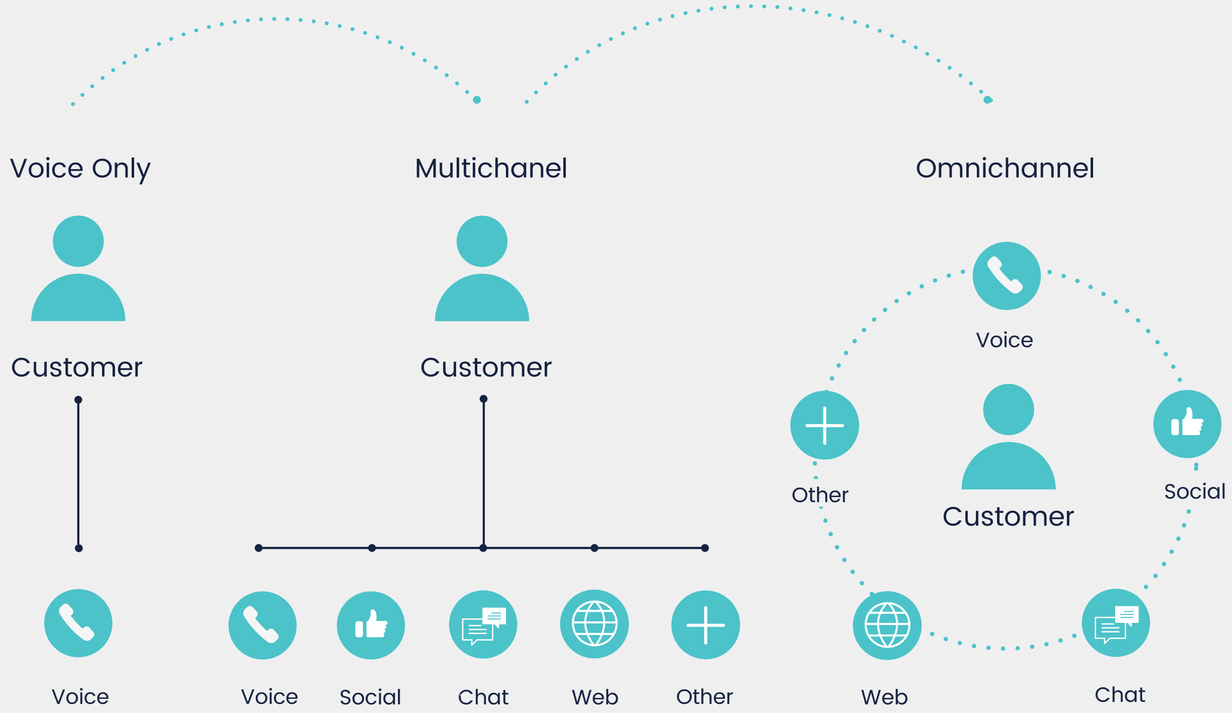


Figure 2 • Omnichannel Contact Centers Are Data Rich

One of the byproducts of the evolution to omnichannel is the contact center now holds massive amounts of data, making it a natural point of attack for threat actors. When contact centers were voice only, there was less data stored. Today, it's not just phone numbers, names and call recordings that are part of contact center records, but a wide range of information that hackers would consider a gold mine, including credit card information, social security numbers, financial statements, health records, customer demographics and more.

When agents all resided in a single, physical location, security was somewhat integrated into the architecture. Agents were using company-provided devices and the organization's network was protected by best-in-class, security technology. Now that agents are working from home, many are using personal computers and a home network with little to no security.
These systems are much easier to breach than enterprise platforms protected by state-of-the-art, next-generation security tools.

Also, the shift to WFH has created a rise in phishing attacks. A report from Google saw the number of phishing sites rise 350% from January to March 2020 (Figure 3). The reason phishing is notable, is that hackers bank on naive agents clicking links to provide access for malware to infiltrate the computer. This creates a "back door" into the contact center data.

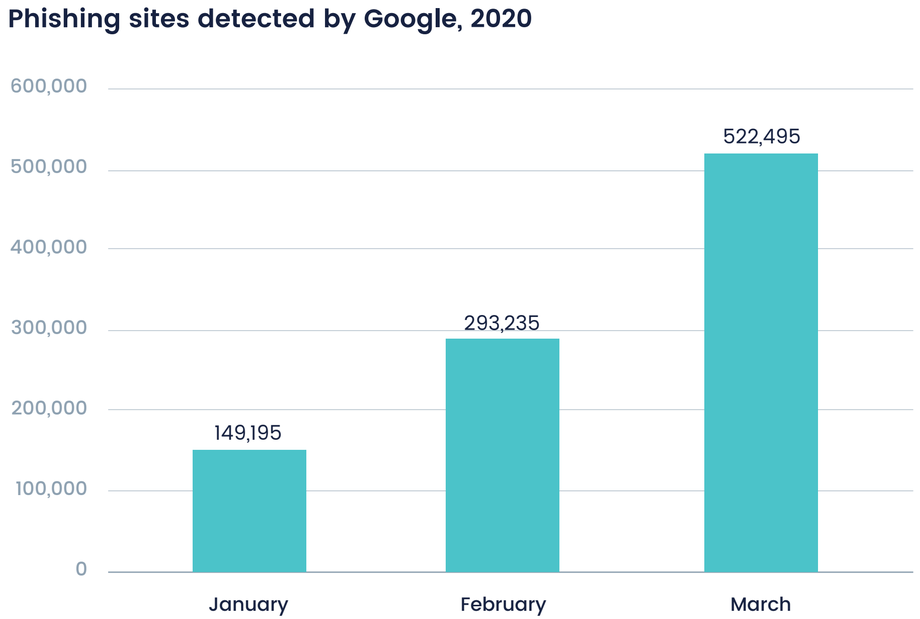


Figure 3 • Phishing Sites Are On The Risey

Contact center-specific fraud has increased as the pandemic progressed. Contact Center World (CCW) found that the annual growth rate of contact center specific fraud has increased 17% annually. This includes fraudsters that are able to navigate through a call center's automated filtering system to reach a customer service representative, who they fool into granting account access. Also, when looking across all channels, almost two-thirds (60%) of fraud incidents come through the voice channel. This is because most security tools are optimized to find threats and malware in data systems, but largely ignore the voice channel.

Another issue is the human factor, where workers intentionally or unintentionally put the company at risk. According to Egress, 75% of IT leaders believe employees have put data at risk in the past 23 months. The most common causes are storing information on personal computers or using consumer-grade cloud storage (32%); sharing sensitive information for nefarious purposes like leaking data to a competitor (22%) or to cybercriminals (21%); or even taking data to a new job (18%). Passwords present another challenge as this remains one of the top ways to hack into business systems like contact center platforms.

Lastly, home networks are highly insecure when compared to business locations, even when virtual private networks (VPNs) are used.

One resolution to the contact center security problem is to invest more in traditional security for endpoint protection, which seems to be what most businesses are doing. The 2020 ZK Research Work from Anywhere Study found that 62% of businesses have increased their investment in cloud security since the pandemic began, and 57% have upped their spend in endpoint security over the same time frame. While this can be effective, it doesn't solve all problems. One of the biggest issues with endpoint security on home computers, is the end user becomes the integration point between VPNs, anti-malware and other tools, where multiple points of failure can now take place. Software must be updated, new connection points added and licenses maintained. Also, as mentioned earlier, traditional security was never designed for the contact center.

While there are some contact center security systems, they were designed primarily to confirm the identity of external people contacting agents. This is what's known as a traditional perimeter approach, focusing on external threats, without attention paid to monitoring activity or behaviors specific to contact center agents. Below are some examples of contact center-specific threats that traditional security tools struggle to spot.

- **Unexpected calling destinations to avoid accidental bill spiking**
- **Unusual access to sensitive information to prevent data leaks**
- **Activity at suspicious hours to keep hackers out of your systems**
- **Logins from anormal origins**

III. The New Benchmark for Contact Center Security

Talkdesk® Guardian™, developed by cloud contact center provider Talkdesk, is the first security application that is designed specifically for contact center-specific threats and risks. It is ideally suited to meet the security challenges of organizations that are both distributed and dynamic—agent activity can be monitored no matter where agents are located and as a cloud application it can be deployed remotely without a heavy IT lift. It's important to note that Guardian is more than a set of tools, but rather a next-generation solution that uses artificial intelligence (AI) and machine learning (ML) to detect fraud attempts, data leakages, privacy-related breaches and identity thefts as well as monitor overall agent activity. All this information is available in real time for CISOs and information security teams to take immediate action when a threat is identified (Figure 4).

Figure 4 • Talkdesk Guardian is a Turnkey Contact Center Security Solution

The use of AI/ML is critical to finding threats as there is far too much data for even the best information security teams to manually analyze and stay ahead of malicious attacks and employee negligence.

While there are a number of AI/ML algorithms working under the hood, value is derived from the Guardian dashboards that show insights into all activity and prioritize the incidents by a calculated risk score. This enables contact center managers and security professionals to monitor agent activity for risky \behavior and discover suspicious behavior that could indicate a breach.

Key features of Talkdesk Guardian include:

Dashboards: Get at-a-glance insights into top-priority contact center security incidents and suspicious behavior based on intelligently calculated risk.

Suspicious Behavior Detection: Expose unseen behavior outliers within specific teams or across the organization and surface potential risks.

Log Analysis: **Track real-time and historic agent login information to assess suspicious behavior such as after-hours access or new device access.**

Case Management: **Spot emerging patterns as well as the most critical anomalies, so you can anticipate and immediately act on data leakage threats.**

Advanced Filters: **Quickly find the data you need by filtering, sorting and grouping information according to the time period you're interested in, or by specific case types or employees.**

Push Notifications: **Get a daily digest of clickable push notifications, alerting you to all cases that have occurred in the last 24 hours.**

Powered by Talkdesk iQ: Talkdesk iQ, a proprietary AI/ML model, analyzes data to spot irregular patterns and identify potential threats.

Guardian analyzes a rich data set including session attributes, security-specific metrics, call activity and access controls. All of this data is continually examined by Talkdesk iQ™—the native AI/ML algorithms—to provide a complete view and stay ahead of possible security breaches.

Guardian has a rich set of security capabilities that aligns the contact center with the business' overall security posture. It's also designed so that non-security personnel, such as IT or contact center administrators, can be empowered to monitor and take specific actions on security threats as the day-to-day experts. Looking ahead, it's possible for Guardian data to be fed into larger security frameworks for more advanced analytics.

Talkdesk Guardian allows the contact center to purposefully (and for the first time at many organizations) align and integrate with the strategic enterprise security posture.[1]

[1] Security posture refers to the overall security status of your software and hardware assets, networks, services and information and can include APIs.

Conclusions, Recommendations and the Future of Contact Center Security

In early 2020, the world changed in ways we could have never imagined. Many businesses were forced into doing something that was inherently uncomfortable for them: shifting their contact center agents to a WFH model. Now that the transition has happened, organizations are reaping many of the rewards, including lower costs, higher productivity and increased agility.

Like most things in life, for every Yin there is a Yang, and that's certainly true with remote contact center workers. The migration to working from home has created a number of new security breaches that organizations have never experienced before. These security risks are best addressed with a tool specifically designed for the uniqueness of the contact center. Products like Talkdesk Guardian allow contact centers to embrace WFH agents while mitigating the risks of this new way of working.

Protecting the contact center is a top priority for security, IT and business leaders. To help with the way forward, ZK Research recommends the following:

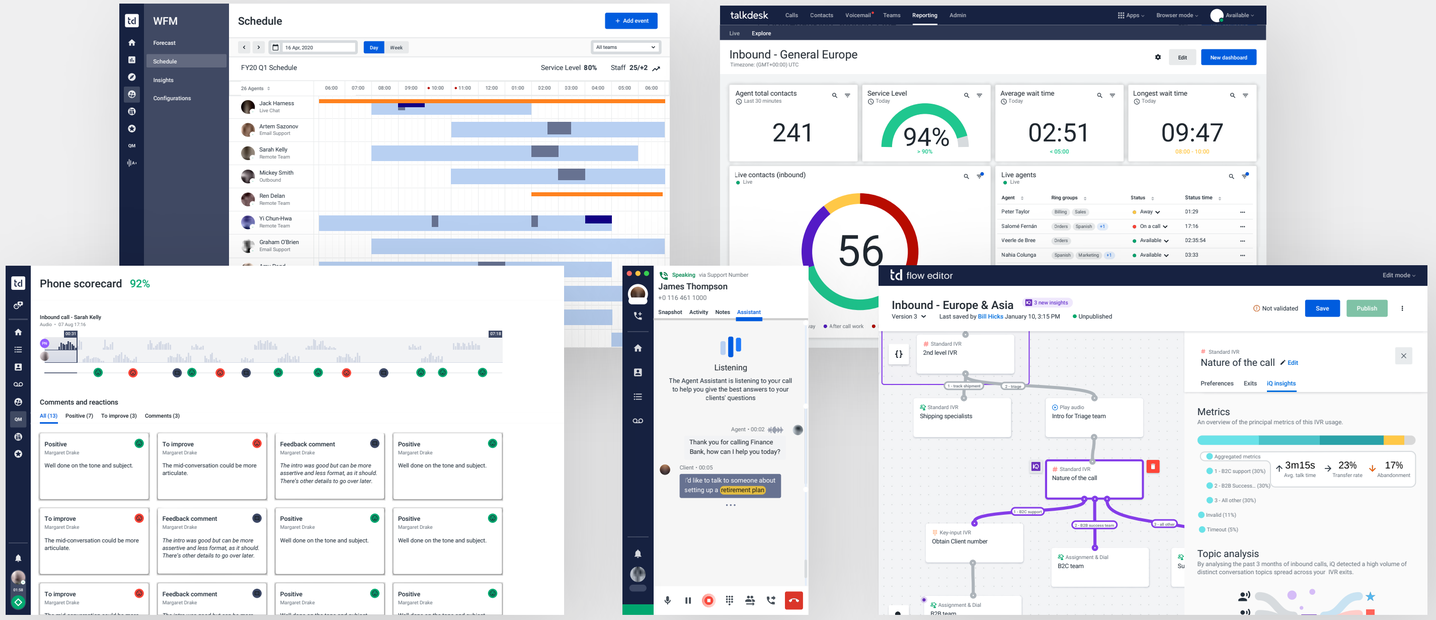
- **Embrace the use of AI/ML with security.** There is some skepticism around the use of AI/ML for security purposes as security professionals view it as a threat to their jobs. The fact is, there is far too much data for people to manually analyze. Train agents on at-home-specific threats. There has been a significant rise in the number of phishing attacks and e-mail-related threats.
- **Train agents on at-home-specific threats.** There has been a significant rise in the number of phishing attacks and e-mail-related threats. Train agents on what to look out for to minimize the possibility of them being fooled into giving up their credentials.
- **Invest in contact center-specific security tools.** Understand that traditional security tools were never designed for the demands of the contact center. Instead, look at tools like Guardian that are built from the ground up to protect agents and contact center data.

Today's secure contact center makes use of tools created to identify, manage and mitigate threats across a broader threat landscape—whether those threats are internal or external in nature, the result of a distributed workforce or unexpected disruptions to business continuity. While it uses innovative technologies like AI and ML to extract valuable insights from data, Guardian is expert-led and leverages domain expertise from the contact center to develop best practices that are fine-tuned every day. Guardian aligns with the overall enterprise security posture and integrates to larger security frameworks when possible so that security becomes a strategic priority, and customer data is always protected.

Today is the day to start making your contact center more secure. The journey begins by understanding how outdated thinking on security can put you at even greater risk for data breaches, fines and loss of customer trust.

I recommend visiting Talkdesk to learn more about their forward-thinking approach to contact center security with Guardian.

An End-to-End Solution for Delivering Great Customer Experiences



talkdesk®

+1 (888) 743-3044
www.talkdesk.com

Talkdesk® is the cloud contact center for innovative enterprises. Combining enterprise performance with consumer simplicity, Talkdesk easily adapts to the evolving needs of support and sales teams and their end-customers, resulting in higher customer satisfaction, productivity and cost savings. Over 1,800 innovative companies around the world, including IBM, Acxiom, 2U, Trivago and YMCA, rely on Talkdesk to make customer experience their competitive advantage. Learn more and request a demo at www.talkdesk.com