

How Talkdesk Utilizes Security Measures to Prevent Data Breaches

Data security is a hot topic right now, and for good reason. A renewed conversation surrounding security has been spurred by the recent Marriott Starwood hotels data breach. If you need a refresher about what happened and are wondering how seriously Talkdesk takes data security, read on. (Spoiler alert: we take it very seriously.)

The [compromised data](#) was specifically from guests who stayed at their Starwood hotel properties. This is the [second-largest data breach in history](#), and it has affected 500 million users - potentially more. Cyber hackers gained access to credit card and passport information, birth dates, phone numbers, and other personal data that could leave many people dealing with identity fraud.

News of the hack spread quickly and left concern in its wake. In response, Marriott has [created a website](#) featuring answers to frequently asked questions about the breach and a phone number for concerned customers to call. The company has even [offered to pay for new passports](#) for individuals who can prove that they are dealing with fraud due to the breach.

This incident has brought data security to the forefront of many people's minds and influenced them to be more cognizant of how their data is stored and protected. At Talkdesk, we recognize that your data is much more than strings of numbers—it comprises your identity. We have various defenses and security certifications in place to ensure your data is protected from all angles.

Lori Stout, Senior Product Marketing Manager at Talkdesk, explains, "In addition to adhering to Privacy Shield, we are SOC2 Type II certified and GDPR compliant. To serve our diverse customer base, we strictly follow the guidelines established by the world's foremost security frameworks." These frameworks include:

- ISO
- NIST
- HIPAA
- PCI-DSS
- OWASP
- Cloud Security Alliance (CSA)

In case your head is spinning from the initialisms, let's summarize by saying that Talkdesk complies with the strictest of security regulations.

Talkdesk has Disaster Recovery processes and Intrusion Detection systems in place to protect against data loss and theft, as well as AWS availability zones to avoid service disruptions and vulnerabilities if an outage occurs. Our security team works continuously to prevent data breaches with system auditing, threat monitoring, and data protection training for all employees. Edgar Pimenta, Information Security Director at Talkdesk, shares, "We see security as a process of continuous improvement. We can never consider a job as done, as... threat

landscapes change very fast.” Talkdesk is committed to staying up-to-date with the latest data protection technology to ensure we’re at the forefront of threat detection and prevention.

Talkdesk prioritizes the protection of customer and company data and continuously strives to utilize the best security practices. For more information on our comprehensive security measures, please visit: <https://www.talkdesk.com/trust/>