2017 SaaS Security Study

ABSTRACT

Data security is a key element of selecting any SaaS provider. Qualtrics surveyed over 200 SaaS security and privacy officers to understand which security and privacy protocols the typical SaaS company follows, and compared those results to Qualtrics' security and privacy protocols.

SAAS IS A POWERFUL TOOL FOR BUSINESS

SaaS services have become a key tool for executing on strategy and driving business outcomes. These services have grown to provide crucial functionality without requiring on-site implementation.

Because SaaS companies have made massive investments in data protection, they are generally better equipped to maintain higher standards of security than companies that choose to keep their software on premises. Even the security-obsessed CIA uses cloud services provided by Amazon AWS[1].

But how well are SaaS companies protecting the data they store for customers? Qualtrics conducted a study to find out.

FOUR KEY AREAS OF DATA SECURITY

The 2017 SaaS Security Study is a blind survey designed to better understand the security and privacy standards that companies in the SaaS space uphold. Over 200 information security and privacy officers at SaaS providers were asked to describe their security protocols in four key areas:

- Data protection
- Data ownership, privacy and processing
- Employee training and independent certification
- Disaster recovery and business continuity

The following sections will address the security standards that Qualtrics meets in these four areas compared to how many other SaaS providers meet the same standard.

1. Data Protection

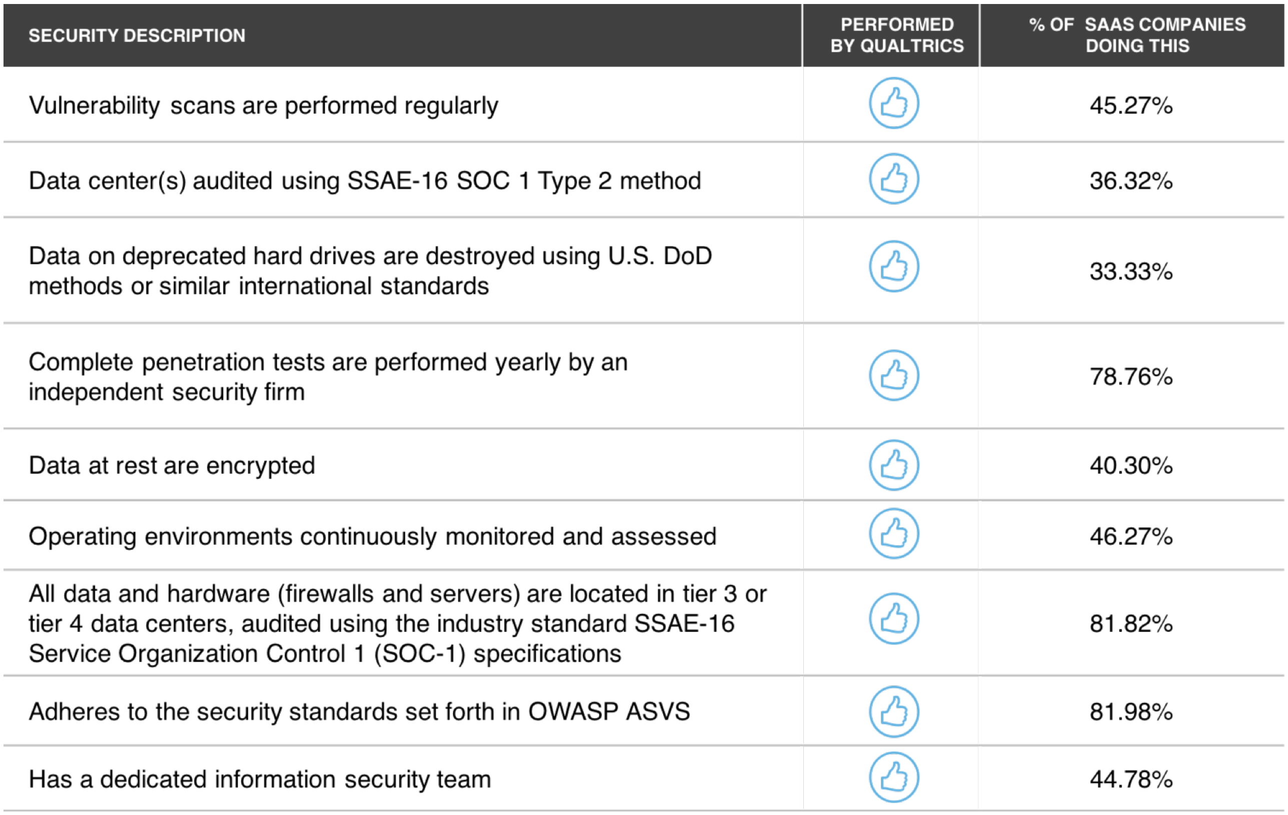
Qualtrics recognizes that to fully take advantage of cloud computing, its customers must be able to entrust them with one of their most valuable assets – their data. Data integrity has become a top priority for businesses working to earn trust and positive brand reputation with customers. Qualtrics' top concern is adhering to the highest standards of data protection.

Qualtrics takes a multi-faceted approach to protecting your data. Scans are performed to provide a vulnerability snapshot, allowing you to see the security footprint your systems expose to the web. For secure data disposal, all data on deprecated hard drives are destroyed using U.S. DoD methods or similar international standards. Qualtrics utilizes data center auditing in a Tier 3 or Tier 4 facility with SSAE-16 SOC 1Type 2 Method.

[1] http://www.infor.com/content/industry-insights/security-of-cloud-vs-on-permise-deployments.pdf/

The associated table shows the data-protection protocols performed by Qualtrics versus the percent of other SaaS companies performing the same protocol.

Data Protection: Qualtrics vs. Other SaaS Providers



SECURITY DESCRIPTION	PERFORMED BY QUALTRICS	% OF SAAS COMPANIES DOING THIS
Vulnerability scans are performed regularly	👍	45.27%
Data center(s) audited using SSAE-16 SOC 1 Type 2 method	👍	36.32%
Data on deprecated hard drives are destroyed using U.S. DoD methods or similar international standards	👍	33.33%
Complete penetration tests are performed yearly by an independent security firm	👍	78.76%
Data at rest are encrypted	👍	40.30%
Operating environments continuously monitored and assessed	👍	46.27%
All data and hardware (firewalls and servers) are located in tier 3 or tier 4 data centers, audited using the industry standard SSAE-16 Service Organization Control 1 (SOC-1) specifications	👍	81.82%
Adheres to the security standards set forth in OWASP ASVS	👍	81.98%
Has a dedicated information security team	👍	44.78%

2. Data Ownership, Privacy and Processing

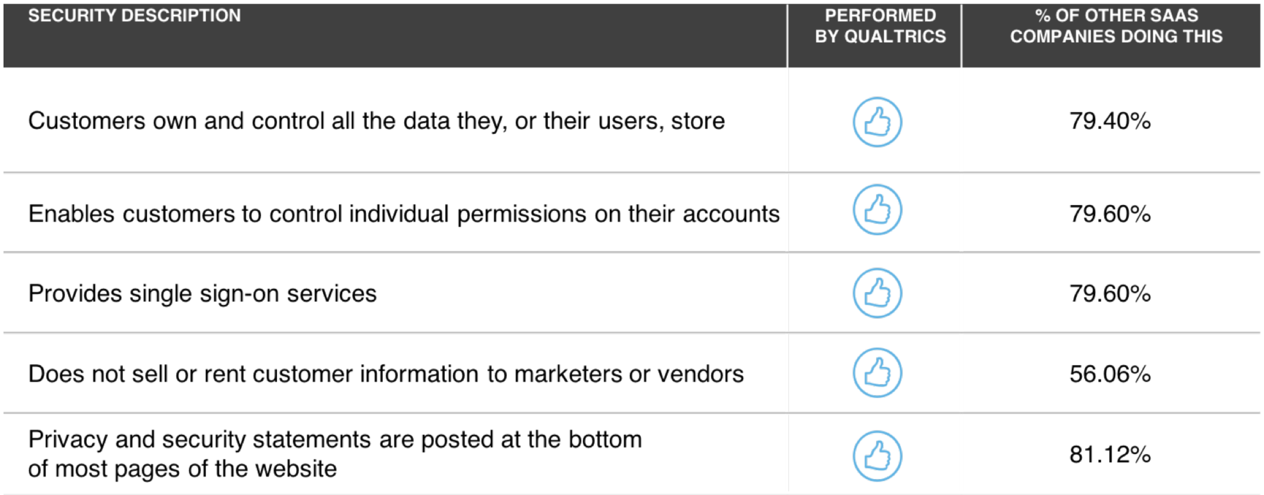
Because a key benefit of using a SaaS provider like Qualtrics is the ability to own your data without owning the burden of maintaining on-premises software, using the cloud should not mean losing any degree of ownership or control.

Qualtrics does not rent, sell or share your data with anyone else because you are Qualtrics' customer, not Qualtrics' product. Customers have wide-ranging freedom to set up individual permissions making the user experience more convenient. Qualtrics allows customers to be "self service" by owning and controlling all the data they, or their users, store. Qualtrics also offers single sign-on services for convenient authentication access.

> *You are Qualtrics' customer, not Qualtrics' product.*
>
> *Qualtrics does not rent, sell or share your data with anyone else.*

The associated table shows the data ownership, privacy and processing protocols performed by Qualtrics versus the percent of other SaaS companies performing the same protocol.

Data Ownership, Privacy and Processing: Qualtrics vs. Other SaaS Providers



SECURITY DESCRIPTION	PERFORMED BY QUALTRICS	% OF OTHER SAAS COMPANIES DOING THIS
Customers own and control all the data they, or their users, store	👍	79.40%
Enables customers to control individual permissions on their accounts	👍	79.60%
Provides single sign-on services	👍	79.60%
Does not sell or rent customer information to marketers or vendors	👍	56.06%
Privacy and security statements are posted at the bottom of most pages of the website	👍	81.12%

3. Employee Training and Independent Certification

Ninety-five percent of all security incidents involve human error. According to a report by BakerHostetler[2] the top human-factor mistakes leading to data breaches are:

- Phishing or malware
- Employee actions/mistakes
- External theft
- Vendors
- Internal theft
- Lost or improper data disposal

For many SaaS companies, the human factor is the missing factor in data protection. That’s why Qualtrics conducts *face-to-face* trainings with all of its employees to instruct them how to avoid or detect security problems.

In addition, Qualtrics’ privacy and security officers are accredited by both the International Association of Privacy Professionals (IAPP) and ISC(2). These formal certifications help ensure that Qualtrics’ security professionals are both knowledgeable and current in the area of security. The IAPP and ISC(2) organizations provide up-to-date programs to disseminate information regarding privacy laws, security operations, compliance and risk mitigation.

The associated table shows the employee training and independent certification protocols performed by Qualtrics versus the percent of other SaaS companies performing the same protocol.

[2] https://www.dataprivacymonitor.com/cybersecurity/deeper-dive-human-error-is-to-blame-for-most-breaches/

Employee Training and Independent Certification: Qualtrics vs. Other SaaS Providers

SECURITY DESCRIPTION	PERFORMED BY QUALTRICS	% OF OTHER SAAS COMPANIES DOING THIS
Employees trained on privacy law compliance	👍	62.20%
Employees trained on physical security	👍	60.98%
Employees trained on email acceptable use policy	👍	62.20%
Employees trained on access control	👍	71.95%
Employees trained on internet security	👍	78.05%
Employees trained on personal devices in the company	👍	65.85%
Employees trained on information security Incidents	👍	63.41%
Employees trained on password policy and tips	👍	63.41%
Customer support employees are permitted to access to sensitive customer data on a business need-to-know basis	👍	67.51%
Regular employee trainings conducted in-person or online	👍	40.80%
Security updates and reminders sent to employees	👍	47.26%
No employee has unfettered access to customer data	👍	25.87%
Organization's privacy officer is accredited by IAPP	👍	75.51%
Security officer accredited by ISC(2)	👍	71.65%
New employees are given security training quickly after onboarding	👍	40.30%
Background checks prior to hiring	👍	42.29%
Employees sign a confidentiality agreement that specifically addresses data security	👍	49.75%
Policy of access prohibition to data without customer permission	👍	38.31%

4. Disaster Recovery and Business Continuity

Data can't help when it's missing. Data is currency and even on a small scale, data loss can damage your company's financial stability. Seventy percent of small and medium businesses that have lost significant amounts of data have gone out of business within a year of the loss[3].

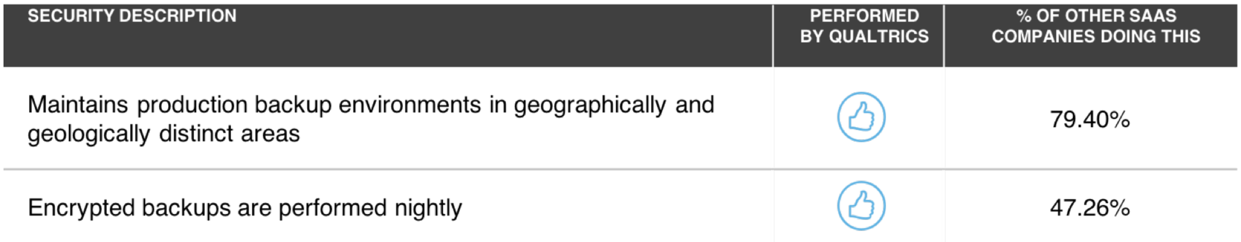
[3] http://spanning.com/blog/4-real-life-examples-of-saas-data-loss/

Hackers, natural disasters, user error and malicious deletion are common causes of downtime and data loss, but Qualtrics has taken action to minimize these and other risks of data loss while also preparing a detailed data redundancy and recovery plan. Qualtrics' Recovery Time Objective (RTO) is 24 hours to resume normal operations in the event of a disaster, with the goal of a full data restoration due to extensive backup measures. Qualtrics' disaster recovery and business continuity plans are tested biannually.

Seventy percent of small and medium businesses that have lost significant amounts of data have gone out of business within a year of the loss.

The associated table shows the disaster recovery and business continuity protocols performed by Qualtrics versus the percent of other SaaS companies performing the same protocol.

Disaster Recovery and Business Continuity: Qualtrics vs. Other SaaS Providers



SECURITY DESCRIPTION	PERFORMED BY QUALTRICS	% OF OTHER SAAS COMPANIES DOING THIS
Maintains production backup environments in geographically and geologically distinct areas	👍	79.40%
Encrypted backups are performed nightly	👍	47.26%

SUMMARY

Because hackers are increasingly organized and sophisticated, data security should be at the top of the list for any company considering a SaaS provider. Hackers prefer soft targets and easy payoffs, rendering SaaS companies with best-practice security standards both less likely to be targeted and less likely to be breached in the case of an attack. Qualtrics has taken steps to be a leader and set an example among SaaS providers with standards quantifiably higher than many other SaaS companies.

ADDITIONAL REFERENCES

Qualtrics Security Statement	https://www.qualtrics.com/security-statement/
Qualtrics Privacy Statement	https://www.qualtrics.com/privacy-statement/
Contact Qualtrics About Security	https://www.qualtrics.com/support/