Qualia

Datacenter, Device & Physical Security at Qualia

While many cybersecurity risks and controls exist within software applications or network communications, physical security is equally important to ensure the confidentiality, integrity, and availability of services and data. This document addresses the controls Qualia uses to ensure the physical security of the data centers, offices, and devices we use.

Datacenter security

Qualia's Software as a Service (SaaS) products utilize Amazon Web Services (AWS) to provide secure datacenters for the storage of customer data. By leveraging the best-in-class security of AWS (which you can read more about here), Qualia is able to extend those capabilities to our customers' data. These capabilities include but are not limited to:

- Implementing security controls such as cameras, alarms, and staff to ensure that only authenticated and authorized employees can access servers or other physical hardware.
- Providing redundant hardware, facilities, and data storage in the event of a disaster, such as a drive failure or extreme weather event.
- Offering robust support for secure encryption—in transit, and at rest.

Device security

This industry involves sensitive data and in order for our employees to successfully complete their jobs, their devices will have sensitive data on them. Whether our employees are working remotely or in the office, Qualia ensures that each individual employee's device and our entire fleet of devices are protected. Qualia uses a Mobile Device Management (MDM) system to make certain that a number of controls are implemented.

Device security (continued)

Qualia also safeguards devices in order to harden in the event of loss, theft, or intrusion attempt. These include but are not limited to:

- **Screen Locks:** Our employees have a strong culture of following security protocols. We go even further with even additional safeguards. Screen locks automatically lock computers after a certain period of inactivity and require the user to enter a strong password in order to unlock.
- **Firewalls:** Firewalls monitor network traffic into or out of the device, and block anything that looks suspicious. They are useful for preventing intrusion from other devices on a shared network.
- **Anti-malware:** Not all software is created with good intentions, and anti-malware solutions can help prevent malicious software from running on a device. Some anti-malware solutions are signature-based—identifying and quarantining previously-identified malware samples—while others use heuristics or anomaly detection in order to identify novel threats.
- **Patching:** Software or operating system vulnerabilities may be exploited by attackers in order to gain access to the data on a device or abuse any authenticated sessions. By enforcing the regular installation of patches, we can help prevent these attacks from succeeding.
- **Software Approval:** There is a lot of software available for download on the internet, and Qualia limits what can be installed on company devices. Qualia uses MDM to automatically push the standard Qualia software stack to laptops. There are also policies that require users to get approval from IT and InfoSec, before installing software. Finally, Qualia's MDM is used to keep an inventory of all installed software on company devices.
- **Disk Encryption:** In the event, a device is lost or stolen, disk encryption ensures that the data stored on the device cannot be accessed without the user's password. This ensures that, although the device itself may be lost, the data stored on it will not fall into the wrong hand

Office security

It is paramount—both for the safety of our employees and the security of our physical assets—that only credentialed employees (and their verified, escorted visitors) are allowed to access Qualia's offices. As Qualia has expanded to multiple offices across the United States, we've invested considerable resources to ensure that we maintain a high standard of office security.

There are numerous controls that contribute to the security of our offices, including security guards, cameras, and electronic badges provisioned to Qualia employees.

Electronic badges function similarly to physical keys, in that they open doors, but also provide a number of other advantages that improve the physical security of Qualia's offices:

- In the event that an employee's badge is stolen or lost, or if an employee resigns from the company, Qualia will immediately and remotely disable the badge.
- Electronic badges cannot be duplicated by simply taking a picture of them, unlike physical keys.
- Each time a door is opened, an electronic badge records the opened door as well as the user who opened it. This makes it easier to quickly identify suspicious events or conduct investigations after the fact.

By outfitting all of our offices with controls such as these, we can help ensure that our offices are only accessed by those with appropriate authorization to be there.

Conclusion

Qualia's team is committed to continually advancing our physical security controls both within and outside our office walls. By continuing to reevaluate and optimize our security standards to be best-in-class with the times, we can better protect our employees, our customers, and our customers' clients.