Orgbrain: Overview of the security processes

1. INTRODUCTION

Orgbrain delivers a scalable Software-as-a-Service (SaaS) platform with high availability and dependability, providing the tools that enable customers to run a wide range of applications. Helping to protect the confidentiality, integrity, and availability of our customers' data is of the utmost importance to Orgbrain, as is maintaining customer trust and confidence.

2. AMAZON WEB SERVICES: GLOBAL INFRASTRUCTURE SECURITY

As one of Orgbrain's cloud-computing providers, Amazon Web Services (AWS) operates the global cloud infrastructure that we use to provision a variety of basic computing resources such as processing and storage. The AWS global infrastructure includes the facilities, network, hardware, and operational software (e.g., host OS, virtualization software, etc.) that support the provisioning and use of these resources. The AWS global infrastructure is designed and managed according to security best practices as well as a variety of security compliance standards. As an Orgbrain customer, you can be assured that we've built web architectures on top of some of the most secure computing infrastructure in the world.

Orgbrain

3. THE AWS COMPLIANCE PROGRAM

Amazon Web Services Compliance enables customers to understand the robust controls in place at AWS to maintain security and data protection in the cloud. As systems are built on top of AWS cloud infrastructure, compliance responsibilities will be shared. By tying together governance-focused, audit-friendly service features with applicable compliance or audit standards, AWS Compliance enablers build on traditional programs, helping customers to establish and operate in an AWS security control environment. The IT infrastructure that AWS provides to its customers is designed and managed in alignment with security best practices and a variety of IT security standards, including:

- SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70)
- SOC 2
- SOC 3
- FISMA, DIACAP, and FedRAMP
- DOD CSM Levels 1-5
- PCI DSS Level 1
- ISO 9001 / ISO 27001
- ITAR
- FIPS 140-2
- MTCS Level 3

In addition, the flexibility and control that the AWS platform provides allows Orgbrain to deploy solutions that meet several industry-specific standards, including:

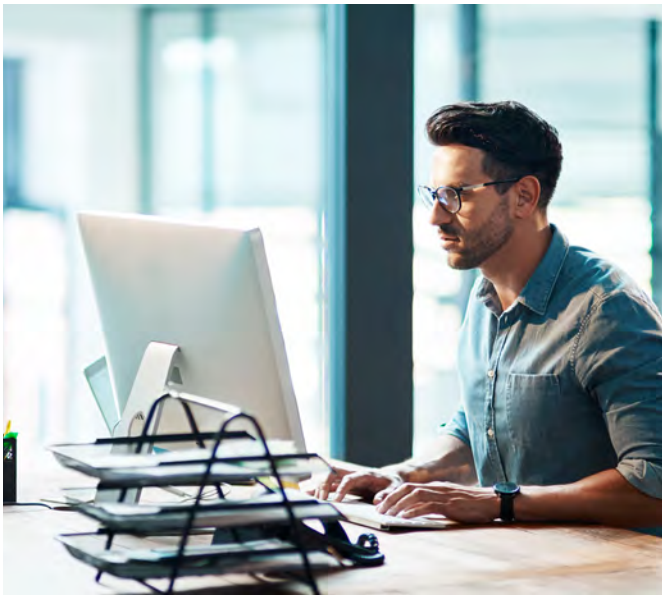
- Criminal Justice Information Services (CJIS)
- Cloud Security Alliance (CSA)
- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Motion Picture Association of America (MPAA)

AWS provides a wide range of information regarding its IT control environment to customers through white papers, reports, certifications, accreditations, and other third-party attestations. More information is available in the Risk and Compliance whitepaper available on the website: http://aws.amazon.com/compliance/

4. MICROSOFT AZURE - BUILT ON A FOUNDATION OF TRUST

Another cloud-service provider for Orgbrain is Microsoft Azure, a rapidly growing cloud computing platform that features an ever-expanding suite of cloud services. These include analytics, computing, database, mobile, networking, storage, and web. Azure integrates tools, templates, and managed services. These work together to make it easier to build and manage enterprise, mobile, web, and Internet of Things (IoT) apps faster, using the tools, applications, and frameworks that Orgbrain chooses.

As a public cloud service, Azure delivers these services to organizations of all sizes, including many of the world's leading enterprises. Additionally, Microsoft Cloud for US Government delivers Azure services, such as Azure Government, and supports mission-critical government workloads. This includes a unique cloud instance, exclusively for government customers and their solution providers, and hardened US data centers operated by screened personnel. The Azure approach to trust is based on the following foundational principles: security, privacy, compliance, resilience, and intellectual property (IP) protection.



5. AZURE COMPLIANCE TO GLOBAL STANDARDS

Compliance plays a critical role in providing assurance for customers and is an important element in the trust relationship. Through rigorous and widely recognized formal standards that are certified by independent third parties, Microsoft helps organizations comply with constantly shifting requirements and regulations governing the collection and use of individuals' data.

With Azure, Orgbrain took advantage of more than 90 current compliance certifications, including over 50 region- and country-specific offerings for the United States, the United Kingdom, the European Union, Germany, Japan, India, China, and more. Orgbrain also benefited from over 35 compliance offerings specific to the needs of such key industries as healthcare, government, finance, education, manufacturing, and media.

New legislation and regulations are constantly emerging, but Microsoft engages globally with both governmental and non-governmental regulators and standards bodies to keep Orgbrain's current and future compliance needs covered.

Azure offers a broad set of key global and industry-specific standards and supporting materials for key regulations, including, for example, ISO/IEC 27001 and ISO/IEC 27018, FedRAMP, and SOC 1, 2, and 3 Reports. Azure also meets regional and national standards that include the EU Model Clauses, EU-U.S. Privacy Shield, Singapore MTCS, and the CS Mark in Japan. More can be found here: https://azure.microsoft.com/en-us/overview/trusted-cloud/compliance/

6. THE OWASP TOP SECURITY RISKS

The Open Web Application Security Project (OWASP) is a nonprofit foundation that works to improve the security of software. Through community-led open source software projects, hundreds of local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure the web. Here are the top 10 vulnerabilities that Orgbrain has painstakingly took efforts to mitigate and/or eliminate.

A. Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization. This has been mitigated by properly sanitizing all inputted data within the Orgbrain ecosystem.

B. Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently. Orgbrain's code development undergoes a strict review and quality assurance that pinpoints weak codebase to prevent this vulnerability.

C. Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare and profile identification. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. In Orgbrain, all sensitive data are encrypted at rest and in transit as well as special precautions put in place when exchanged in the browser.

D. Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc. We have implemented strict role-based access groups in the Orgbrain ecosystem that clearly defines what type of functionality and data is available to the end-user.

E. Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. In Orgbrain, all operating systems, frameworks, libraries, and applications are thoroughly and securely configured, and are also patched/upgraded in a timely fashion.

F. XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser

which can hijack user sessions, deface web sites, or redirect the user to malicious sites. As stated in figure 1, Orgbrain's user inputs are all duly validated, escaped and sanitized to only allow correctly typed and expected values.

G. Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts. At Orgbrain, we make sure that each component or library we used is a widely known standard and has passed meticulous criticism from both enterprise and the open source community.

H. Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. By partnering with top cloud-computing providers such as Microsoft Azure and Amazon Web Services, we at Orgbrain made sure to have proper logging and monitoring in place from all over the different facets of the infrastructure. Code error and access logs are duly put in place and all returned error responses are properly transformed to prevent sensitive data from being displayed.

7. AZURE STORAGE AND REDUNDANCY

Azure Blob storage is Microsoft's object storage solution for the cloud. Blob storage is optimized for storing massive amounts of unstructured data. Unstructured data is data that doesn't adhere to a particular data model or definition, such as text or binary data. Azure Storage encryption protects and safeguards Orgbrain's data to meet our organizational security and compliance commitments. Azure Storage automatically encrypts all data prior to persisting to the storage account and decrypts it prior to retrieval.

Geo-redundant storage (GRS) is the implemented redundancy for scenarios requiring both high availability and maximum durability. Cross-regional redundancy to protect against regional outages. Data is copied synchronously three times in the primary region, then copied asynchronously to the secondary region.

8. MONGODB ATLAS CPS AND POINT-IN-TIME RESTORES

MongoDB Atlas Cloud Provider Snapshots (CPS) creates daily automatic snapshots of the cluster during the cluster's backup window. It saves the automatic snapshots of the cluster according to the backup retention period that is specified. If necessary, it can recover the cluster to any point in time during the backup retention period.

The CPS snapshot storage for each AWS Region is composed of the automated cluster snapshots and manual cluster snapshots for that Region. The snapshot storage is equivalent to the sum of the database storage for all instances in that Region. Automatic CPS snapshots occur daily during the preferred backup window. If the snapshot requires more time than allotted to the backup window, the backup process continues until it finishes, even though the backup window has ended. The backup window can't overlap with the weekly maintenance window for the cluster.

The backup retention period is the number of days an automatic backup is retained before being automatically deleted. MongoDB Atlas CPS supports a backup retention period of 2 days to 12 months.