fauna

Security overview

A technical overview of Fauna's end-to-end information security, data protection and privacy practices.

March 2023

Contents

Introduction

Fauna is a distributed, document relational database that we deliver to customers as a cloud API. With Fauna, developers can simplify code and ship faster by replacing their database infrastructure (on-premises or cloud hosted) with an intelligent Cloud API that brings the full power of a distributed, strongly consistent, relational database to a document based store. Development teams around the world rely on Fauna to build and scale applications without the need to compensate for eventual consistency, or manage any database related infrastructure.

Fauna's underlying globally-distributed storage and compute fabric is fast, consistent, and reliable, with a modern and secure infrastructure. At its core, Fauna utilizes an algorithm inspired by Calvin[1] to deliver strict serializability, the highest level of transactional consistency possible. As a result, applications built on top of Fauna can assume data correctness without implementing complex validation and retry logic.

Fauna is natively multi-cloud, and can be run on any public cloud environment. The majority of Fauna's current multi-tenant regions operate on Amazon Web Services (AWS). In those Fauna region groups, Fauna typically runs across multiple regions to increase availability and decrease read-latency. For more demanding applications or for customers that want to choose a different geographic or cloud provider footprint than is available in Fauna's public regions, Fauna also offers a Virtual Private Fauna offering that delivers customers a single tenant, serverless experience with VM level isolation.

At Fauna, ensuring that our cloud service is secure, available, and performant is our top priority. This paper outlines Fauna's approach to security across all aspects of the company, from recruiting the engineers building the product to the design of the database and our corporate infrastructure and processes.

Fauna's implementation of security & compliance controls offers significant advantages to Fauna customers. In this paper we will cover:

- How Fauna's offering differs from other datastores
- How Fauna builds secure systems:
  - Personnel Security
  - Application Security
  - Business Continuity
  - Data Center Security
  - Privacy & Regulatory Compliance

1 http://cs.yale.edu/homes/thomson/publications/calvin-sigmod12.pdf

Security & Reliability: Fauna vs Traditional Database Systems

The security considerations when developing an application based on Fauna differ significantly than when using a traditional database within the application stack. The areas of difference can be categorized as administrative security, data resiliency, and native application authentication and authorization:

Administration Security

Fauna's serverless model dramatically reduces administration and thus configuration errors during provisioning and eliminates operational changes likely to introduce errors & data mismanagement. Rather than requiring a dedicated team of technology experts to manage a growing datastore, Fauna assumes the responsibility for key administration tasks to avoid common issues altogether.

- Fauna's endpoints are global, cluster-aware and automatically route requests to the nearest node
- Developers and DB admins no longer need to manage application endpoints, simply point to Fauna and the application consumes data
- Absolutely no database management
    - No servers or containers to provision and management
    - No patches to apply or update on the backend
    - No shards or replicas to manage as the data is always available via the API
    - No risk of downtime due to inaccurate scaling projections
    - HTTP endpoints remove session constraints

Built-in Resiliency

Fauna is built to ensure availability even during major public cloud outages and typically runs across multiple data regions and datacenters within those regions. In addition:

- The disaster recovery & failover work is Fauna's responsibility
- Secure database connections occur via https which eliminates connection limits and guarantees encryption of data in transit
- Data is distributed to multiple locations to avoid data loss to ensure data can be served even in the event of a full regional outage

Application Security

Fauna brings cloud-native security that leverages both built-in fine-grained security as well as standards based authentication using leading 3rd party enterprise identity services.

- Identity and attribute-based authorization and access controls
    - Role-based access control (RBAC) governs authorization within the database
    - Attribute-based access controls (ABAC) allows fine-grained query access

- Native authentication via 3rd-party market leaders
    - Out-of-the-box integration with Auth0 and Okta

Personnel Security

Fauna's security strategy starts with our people. Our recruiting process was developed to ensure we attract and retain a competitive workforce that prioritizes secure development and data security while mitigating the risks of code loss or data mishandling. To those ends, we have incorporated the following:

Background Checks

We pride ourselves on recruiting highly capable and qualified people at Fauna. We also recognize that people are a critical part of upholding a secure environment. When each new employee joins Fauna, a background check is completed prior to granting access to company systems.

Security and Privacy Training

All employees are required to participate in an Information Security and Privacy orientation when hired and annually thereafter. Awareness training provides our staff with skills to prevent, detect and respond to common security threats and includes topics such as password management, phishing, social engineering, physical security, data security, global privacy regulations and how to report security incidents.

New hires are required to acknowledge corporate policies, including their expectations regarding their conduct, and sign non-disclosure agreements as part of their onboarding process to ensure they understand their responsibilities while performing work for Fauna.

Organizational Focus on Security

Fauna's leadership team has appointed a group of individuals to form a security leadership committee with the responsibility to formally oversee security efforts within the company.

These individuals have requisite expertise in secure architecture, engineering, security operations, and compliance, including CISSP-certified professionals and privacy professionals.

The security leadership committee team proactively:

- Issues policies to ensure the accessibility, reliability, protection, and proper use of electronic resources available for use within the company
- Pursues strategies to develop secure applications, ensure the security of the SaaS infrastructure, and establish protected and stable data storage
- Is a stakeholder in the software development lifecycle process with approval authority for code review and proper release management

- Mitigates security risk to the environment through outreach, awareness, assessment, policy, and best practices
- Participates in monitoring of systems and infrastructure to protect against and detect malicious activity
- Audits the environment, identifies vulnerabilities and recommends resolution strategies
- Responds to security events to contain the incident and improve protocols

The security leadership committee at Fauna drives continuous assessment and improvement of Fauna's security program and fosters a security culture within the organization.

Access Control

Internal user accesses are granted using a role-based access control model that follows the least-privilege principle and requires a documented request and approval. We observe a similar procedure to manage access for individual contractors that perform work on behalf of Fauna and require access to corporate systems.

If an employee or contractor changes roles, their access is reviewed to ensure excess privileges are removed. In the event that an employee is terminated, access is removed.

User entitlement reviews are performed quarterly for privileged accounts and every 6 months for non-privileged accounts for critical systems, applications and infrastructure. User access reviews are focused on identifying access errors, removing overlapping or excessive permissions, and removing orphaned accounts.

Software Development Lifecycle (SDLC)

Fauna's SDLC centers on change management and code review to ensure that all updates to the core database and UI are legitimate, linked to an approved requirement, and produce reliable results. Code authors cannot promote their own code and all code requires peer review prior to merge to validate correctness and promote stability. Each production change to infrastructure and application source code is evaluated for security and performance impact to minimize release risks, and Fauna's integrated testing framework runs at release prior to code promotion to the production environment.

Customer Application Security

Fauna incorporates application security by design, allowing Fauna customers to build natively secured applications. Key aspects include:

Multi-factor Authentication

With multi-factor authentication (MFA) support for the Fauna database, Fauna customers can secure their developer environments by requiring a second layer of identity verification at sign-in using one-time password (OTP) applications such as Google Authenticator and Microsoft Authenticator. MFA is an industry best practice that

dramatically increases the security and safety of business data hosted in Fauna. To learn more about MFA, refer to the Fauna docs.[2]

Authentication using Third-Party Identity Providers

Fauna's API security model enables developers to query the database over any HTTPS connection, whether the connection originates from a web browser, a desktop app, or a mobile app. Using the newly-built integration with third-party identity providers (IdP), developers can now secure access to their Fauna databases with the same tools they use to protect other APIs that their applications consume.

Modern apps frequently use cloud-based IdPs to manage access to their apps and resources. Fauna now offers standards-based integration with third-party IdPs, such as Auth0 and Okta, to help developers manage and secure access to their database resources. Setting up this integration requires minimal code, allowing developers to bypass a typically complex, time-consuming, and error prone component of application development.

Attribute-Based Access Control

For database accounts, attribute-based access control (ABAC) provides a flexible, fine-grained strategy for managing identity-based operations within Fauna. ABAC extends the default Fauna authentication and authorization mechanisms[3] to gate access to data based on query metadata, attributes of the documents being accessed, or the time of day.

Encryption

To protect data in transit between users and Fauna servers, Fauna uses Transport Layer Security (TLS) version 1.2 or better, creating a secure data transmission method protected by 128-bit or higher Advanced Encryption Standard (AES) encryption. Connections to the service that do not utilize this level of encryption are not permitted.

Data uploaded to the Fauna service is encrypted at rest using 256-bit AES. Data storage spans multiple data centers to provide a consistent, unified, and global view of all data in real time that remains protected. Backup copies of primary data stores also leverage 256-bit AES.

Incident Management

Fauna's incident response program is based on documented, tested policies & procedures linked to our on-call cadence. All employees are empowered to declare an incident, which is treated as a critical event requiring executive engagement through the identification, mitigation and post-event documentation stages. We're proactive about monitoring for security and operational incidents.

2 https://docs.fauna.com/fauna/current/integrations/dashboard/mfa.html
3 https://docs.fauna.com/fauna/current/security/

The key components include:

- Classify the incident using an initial analysis
- Limit the immediate impact of the incident
- Take corrective action to contain the impact
- Investigate and collection evidence
- Inform the relevant authorities (where applicable)
- Inform impacted customers

Customers can view Fauna's historical uptime and subscribe to updates about operational incidents by visiting the status page at https://status.fauna.com/.

Patching

To reduce the risk posed by outdated or vulnerable operating system libraries or code packages across our infrastructure we use an automated service to notify code owners of patching requirements and related vulnerabilities, which are prioritized for work according to severity. Patching status is reviewed by Engineering leadership on a weekly basis.

Virtual Private Fauna

As a further security measure, customers may opt to leverage the Virtual Private Fauna offering. Virtual Private Fauna is a Fauna managed service that is deployed into a separate cloud account and offers VM-level isolation from other Fauna customers. Customers can choose the specific geo footprint and cloud provider to meet their business and data residency requirements. For more information, visit https://fauna.com/virtual-private-fauna.

Business Continuity

At Fauna we understand that we are the critical layer for our customers' applications and ensuring that our services are hyper-resilient. Our staff functions as well as our technical infrastructure are designed to ensure our service offerings are highly available and resilient to outages.

Service Reliability

Fauna uses an innovative new architecture that guarantees low latency and transactional consistency across all replicas and indexes while replicating data globally. Fauna transparently manages operational concerns such as replication mechanisms, data consistency, and high availability. Each replica consists of many geographically-aware nodes, each with a partition of the full dataset in a single region. Scaling replicas or adding new replicas can be accomplished with no downtime, manual configuration, or changes to drivers.

Fauna caters to enterprise workloads by prioritizing data integrity and correctness without compromising scalability, flexibility, or performance. Fauna is designed to be resistant to real-world failures, and data remains consistent even in the face of node outages, network partitions, and clock skew.

Disaster Recovery

The Fauna team has a robust plan in place to respond to any major disaster or significant incident that poses a threat to business operations. The plan includes considerations for continued operations by the work unit as well as the technical recovery of the service and checklist, tabletop, and parallel test exercises are carried out throughout the year to test the effectiveness of these plans.

Data Center Security

Fauna is delivered using state of the art, innovative architectural and engineering approaches. Cloud computing technologies are utilized from Amazon Web Services and Google Cloud Platform data centers in the United States and the European Union.

Physical Security

The data center facilities have implemented a robust physical security and environmental protection program to ensure adequate safeguards for equipment. The facilities are located in non-descript locations, maintain professional security guard personnel 24 hours a day with video surveillance monitoring, and feature electronic access controls to control access at the perimeter and building ingress points.

Environmental Security

Environmental protections prevent impact from fire, loss of power, flood, humidity and temperature changes. This includes automatic fire detection and suppression equipment, uninterruptible power supply (UPS) units for backup power in the event of an electrical failure, climate control to maintain atmospheric conditions at optimal levels and leakage detection and removal mechanism.

Data Center Compliance

Both Amazon Web Services and Google Cloud Platform have achieved and continue to maintain a multitude of certifications, compliance and attestations for globally recognized laws, regulations and frameworks.

The AWS cloud infrastructure has been designed and managed in compliance with regulations, standards, and best practices, including HIPAA, SOC 1/SSAE 16/ISAE 3402 (formerly SAS70), SOC 2, SOC 3, PCI DSS Level 1, ISO 27001, FedRAMP, DIACAP and FISMA, ITAR, FIPS 140-2, CSA, and MPAA among others. To learn more about Amazon Web Services compliance programs, please visit: https://aws.amazon.com/compliance/programs/.

An independent third-party auditor has granted Google Cloud Platform a formal certification, attestation, or audit report based on an assessment that affirms compliance

with ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 27701, SOC 1/SSAE 16/ISAE 3402 (formerly SAS70), SOC 2, SOC 3, PCI DSS, HITRUST CSF, FIPS 140-2 Validated, FedRAMP among others. To learn more about Google Cloud Platform compliance programs, please visit https://cloud.google.com/security/compliance.

Compliance & Privacy

Fauna was designed to comply with global data protection regulations and is compliant with major regulatory requirements out of the box. Fauna has chosen the AICPA's SOC2 framework as the basis for its security & compliance program with control criteria informed by the ISO27001 framework.

Among the global privacy & data security requirements that Fauna tracks, the European Union's General Data Protection Regulation is a core focus, and Fauna provides key advantages for companies developing applications for EU data subjects.

Service Organization Controls (SOC)

Fauna's leadership team has adopted a security control governance model consistent with the SOC 2 audit standard. Since 2021, Fauna has maintained its conformance with the trust services criteria relevant to security, availability, and confidentiality as set forth in the 2017 Trust Services Criteria for Security, Availability, and Confidentiality, and Privacy (AICPA, Trust Services Criteria) as certified by an independent auditor.

Fauna's current security and compliance initiatives include a SOC 2 Type II audit covering the period from 1 December 2020 through 31 November 2021, available for review under NDA. The current SOC2 Type II audit period covers 1 December 2021 through 31 November 2022.

Penetration Testing

Fauna's leadership team is committed to partnering with trusted leaders in the cybersecurity industry to further support Fauna's information security and risk management strategy. A key part of that effort is our ongoing bug bounty program, which enlists the help of independent security researchers to identify vulnerabilities in our service. To supplement these efforts we also conduct regular (at least twice annual) external penetration tests with a leading vendor in this space.

Privacy Regulations

Fauna has employed legal counsel and privacy experts to help build a foundation for a privacy program that considers existing and emerging laws and regulations aimed to protect consumer personal information.

We have developed processes and technical capabilities to support compliance with various privacy regulations in jurisdictions where our business operates and the requirements set forth by our customer's geographic needs, including the General Data

Protection Regulation (GDPR), California Consumer Privacy Act of 2018 (CCPA), and Health Insurance Portability & Accountability Act (HIPAA).

We have developed processes to record and respond to consumer requests to exercise their rights. Considerations for privacy are embedded in our approach to designing and delivering software and our legal team helps guide new business objectives in a manner that considers our privacy obligations. For US customers in the healthcare industry, Fauna is willing to discuss signing HIPAA Business Associate Agreements (BAAs) to facilitate processing of covered ePHI.

GDPR Compliance

With the launch of data localisation capabilities, customers can choose to store their data in a multi-datacenter European Union region, ensuring that applications built on this region group can be hosted entirely within the same geographic region to ensure no application data is transferred to countries outside of the bloc. As part of our GDPR compliance strategy, we strictly limit the operational metrics we collect and forward to our US-based monitoring tools to ensure that we are not transferring personal data.

In addition to offering low-latency data connections, this native GDPR-compliant application stack removes the need for legal transfer mechanisms from the application developer, the data controller, to Fauna.

Our cluster monitoring tools that selectively gather operational metrics and metadata fields which may contain personal data are sanitized prior to ingestion in our dashboards and alerting pipelines. Fauna reviews monitoring data feeds on an ongoing basis to ensure personal data on EU data subjects is not processed outside of customer clusters -- another advantage we offer for companies subject to the GDPR.

Further, we understand that some customers have complex global data pipelines which require transfer of personal data from the EU to US-based clusters for performance or operational reasons. For these cases we rely on data processing agreements incorporating the European Commission's standard contractual clauses which outline the security & compliance responsibilities of both the data exporter and Fauna as data importer.

Vendor Risk Management

Fauna expects critical vendors to observe industry standard security practices and, where applicable, provide assurance that they comply with global privacy regulations. Fauna's security team has implemented a process to evaluate the security posture of its data centers and service providers used in delivering the Fauna service. All vendors are subject to a risk assessment and annual review of security, however, different focus and scrutiny are applied based on the service being provided by the vendor.

The review areas may include an evaluation of the following criteria:

- Compliance, Certifications, and Attestations
- Contractual Terms (confidentiality, availability and data protection)
- Data Retention Practices
- Data Security Controls
- Disaster Recovery / Business Continuity Capability
- Security Incident Management

If a review has identified a potential risk to customers or other areas of concern, Fauna will work closely with the vendor to develop a remediation plan. For a list of Fauna's current data centers and service providers used in delivering the Fauna service, please reach out to the security team at security@fauna.com.

Conclusion

Fauna was founded by engineers who believe in the need for security & compliance by design, and is led by an executive team that has built products where security is paramount. At Fauna, we prioritize continuing work on our security practices to ensure that, as our product evolves, it continues to offer best-in-class safeguards for customer data.

For more information about Fauna's security and compliance measures, please contact Fauna's Security team at security@fauna.com.