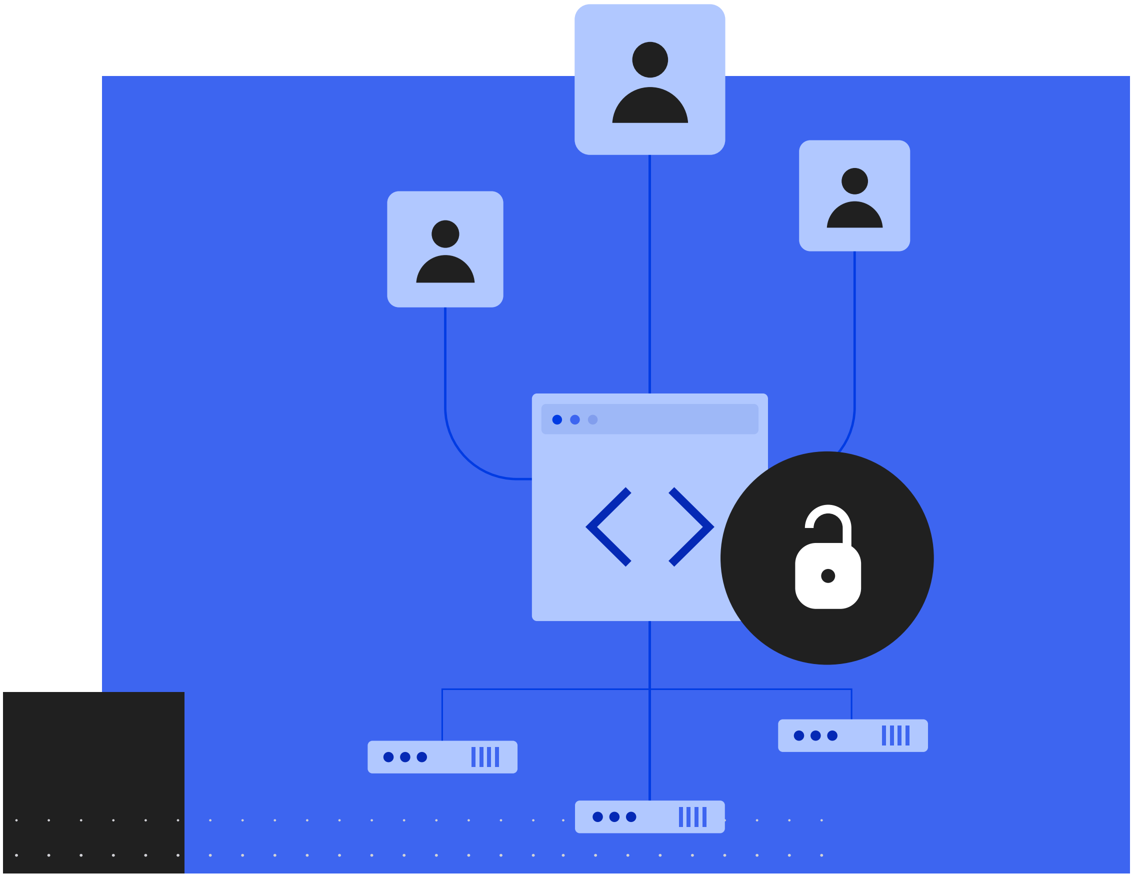
frontegg White Paper

The Frontegg Security Approach: Software Design, Architecture, and Philosophy



frontegg.com

As more and more of technology infrastructure has moved to SaaS and services delivered via the Internet, web security has become a critical concern. Cyberattacks targeting weaknesses in web application and web site security have become one of the most critical risks facing all companies, and especially companies delivering SaaS or other services via the Internet. The rapid growth of APIs which serve as both internal and external connection points for web applications has created even greater web security risks. Attackers often target managed services and SaaS applications as a way to leverage web services and APIs to attack the many customers of these services. User Management providers, like Frontegg, are among the most sensitive and critical third-party SaaS subsystems, regularly processing and storing critical customer and business information.

To address these growing threats, Frontegg has designed its processes, systems and environments to match the best standards of security. Security was a crucial part of the initial design process for the Frontegg architecture, PlatformOps and DevOps, and software lifecycle development processes. This architecture incorporates modern cloud native methodologies focused on loosely coupled microservices running on scalable containerized infrastructure with full redundancy at each point of failure and segmentation of services and functionality across multiple availability zones to ensure that code and infrastructure is strongly secured. Frontegg utilizes a multi-layered defense built around principles of Zero Trust, least privilege, segmentation and testing. We put in place security controls and automated tests at every stage of operations. We also continuously test and audit our security, both internally and with third-party testing systems and white-hat hackers.

> **Frontegg built its entire application development, deployment and operations around the concept of "security-first" through the lens of cloud-native computing and infrastructures.**

Deep Security Roots and a Culture of Security

Frontegg sees world-class Information Security as a core component of its services.

We have deep security roots in web application and cloud security. Our co-founders, Sagi Rodin (CEO) and Aviad Mizrachi, CTO, designed, architected, and scaled the cloud platform for Check Point, a leading provider of cybersecurity solutions. This platform was the primary vehicle for deployment and delivery of all SaaS products and managed and web services provided by Check Point to its thousands of customers including the majority of the Fortune 500. As part of this process, Frontegg leaders built and scaled a full-featured, multi-tenant user management system to manage authentication and user administration across multiple Check Point SaaS cybersecurity products leveraging a single platform. The engineering and security management team also came from Check Point and other security-focused companies, providing an additional layer of secure coding and secure application design experience. This management team operationalizes on a daily basis and in every process the lessons learned from building out Check Point's web products and many other mission critical SaaS products for other companies. Collectively, Frontegg's engineering and software development team have over 50 years of experience architecting, coding and operating secure software. The team also was educated in the elite Israel Defense Force (IDF) information security and software development programs and has been immersed in a culture of secure code for all of their working lives.

A Methodology of Continuous Security Development and Operations

To create a rigorous security culture, Frontegg has developed a methodology of continuous security with checks at every stage of the development process. The methodology includes the following stages:

- **Plan**
  Developers and engineering managers whiteboard and plan for new features and code
- **Code**
  Developers write code and use inline formatting, linters, and other basic security checks
- **Test Phase 1**
  Code put through unit tests and other more advanced security checks
- **Peer Review**
  All new code must be reviewed by designated secure code experts on the team
- **Test Phase 2**
  Code is stress-tested in staging and subjected to additional security checks
- **Deploy, Monitor and Observe**
  DevOps team deploys the code to production and security team monitors all application behaviors
- **Update and Remediate**
  Code is continuously updated to ensure the latest security advisories are addressed

This methodology is built on a foundation of transparency and adherence to a systems of processes, checks and balances that enforce security at every technology stage and in every operational practice.

> **Frontegg documents all procedures and policies and assigns explicit security ownership at every stage of the software development lifecycle from code development through deployment and integration through end-of-life**

This includes a set of regular mandatory checklists and audits that are a part of every development, integration, deployment and operational process at Frontegg. (Frontegg is happy to provide documentation for these processes, audits, and checks upon request.) This rigorous accountability ensures that security is part of the core job function of every member of the engineering team at Frontegg. To ensure that these audit and checklist processes continue to accurately reflect the constantly evolving application codebase and architecture, Frontegg conducts annual risk assessments to identify any newly introduced coverage gaps and swiftly remap any workflows or security checks to precisely mirror the attack surface of the application and infrastructure. In the following sections, we provide a summary of Frontegg's organizational and technical measures that help us keep your information secure.

Third-Party Audits, Code Testing, Certifications

To provide a higher degree of security assurance and to meet rigorous compliance standards, Frontegg relies on third-party tests and services under the philosophy "With many eyes, all bugs are shallow." Audit and security verification efforts include:

Pen Testing: A penetration test of Frontegg's infrastructure and application is carried out by an external independent security firm semi-annually. Frontegg rotates this process between different third-party g companies to ensure a wider variety of penetration testing strategies, tools and methodologies are applied, better validating the security posture of Frontegg.

Bug Bounty: Frontegg conducts a Security Bug Bounty program facilitated by an ethical hackers platform to incentivize ad-hoc community audits of our application. This puts Frontegg in a continuous security testing process, thus ensuring that our application is always secure.

Access Control Verification: All access controls of the application are subject to automated tests. The tests are run against every software and configuration change and against every new code, feature, or product release.

Automated Code and Integration Test: All changes to applications are subject to an extensive suite of API and integration tests as well as unit tests. Frontegg also utilizes software composition analysis (SCA), to rigorously test all code prior to integration and deployment.

Full Transparency of Security Processes and Testing: Any Frontegg customer is welcome to view all auditing, testing and certification process documentation. In addition, customers are welcome to conduct their own penetration tests upon request. Our security team will coordinate these and other security analyses.

Full Dependency Map, Software Bill of Materials (SBOM) Available on Demand: Customers that wish to know the full composition of the Frontegg application including software components and third-party dependencies (packages, services, libraries) may request a dependency map and SBOM. Frontegg consistently tracks these artifacts and can automatically generate them through its Continuous Integration solution.

ISO and SOC2 Certification: In recognition of these security processes, verification and accountability practices, Frontegg has achieved two critical certifications required for inclusion by many customers in regulated industries: ISO27001:2013 and SOC2 Type 2. These certification and audits provide 3rd party assurance of the robustness and reliability of our security program. Frontegg has also completed a CSA STAR level 1 self-assessment certification, which is publicly available for review.

Application Design and Architecture

Frontegg's infrastructure and application design leverages modern, cloud-native architectural approaches to integrate Zero Trust principles into processes and practices across development, deployment and operations of the application. The infrastructure is composed primarily of services linked via APIs, including internal services, managed cloud services, and external services.

> **All services are segmented, to minimize blast radius and horizontal traversal attacks.**

Frontegg's application runs in containers orchestrated by Kubernetes. Each of the dozens of backend services runs as a microservice with its own container (containers) security rules, database, certificate and redundancy across cloud availability zones and physical data centers. All back-end (East-West) services are continuously authenticated and protected with signed digital certificates. East-West traffic is encrypted via TLS. This approach minimizes the blast radius of any compromise and allows Frontegg to quickly isolate and shut down any compromised portion of its infrastructure.

External traffic and requests entering the Frontegg application front-end and back-end pass first through a Cloudflare WAF and then through a Kubernetes Ingress Controller. The Ingress Controllers serve as an external API gateway, filtering traffic and applying security rules and policies to all API requests before they can pass into the Kubernetes environment and impact back-end services. Frontegg also implements AWS security groups to further prevent malicious traffic from accessing the application.

Application Security Measures: Detail

Frontegg applies a long list of specific security measures to ensure greater application security. These measures include the following:

Granular Security Policies: Granular security policies are applied to user interactions with higher levels of security applied to the most sensitive interactions. For example, sensitive cookies are set with secure- and HTTP-only flags. This limits the scope of the cookie to "secure" channels so that the user agent will pass the cookie in an HTTP request only if passage happens over a secure channel using TLS.

Validation of User Input: All user input is validated before processing to identify and block OWASP top 10 threats. This step can prevent common and serious application level vulnerabilities like Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF) and SQL Injection.

Password Hardening: Frontegg enforces robust passwords. User passwords have a minimum length of 10 characters. Passwords must contain at least one lowercase character, one uppercase character, and one non-alphabetic character. Passwords are stored as salted hashes, rendering them useless to attackers who might gain access to the password database. Frontegg also supports most SSO types as well as multi-factor authentication with tokens, authenticator apps or SMS. Frontegg is one of the first B2B SaaS applications in the world to support Passkeys for passwordless security.

Rapid Code Pushes for Fast Patching: Because Frontegg is a cloud-native application based on microservices, R&D teams can push new code into production in a matter of minutes. This enables Frontegg to push patches more quickly than most organizations, with CI/CD that enables instant rollbacks and infrastructure that provides “Blue-Green” testing capability to quickly validate patches on a small groups of live users prior to a full rollout.

Production Environment Security

Protecting code deployment and production environment tools from attacks is another key element of Frontegg's multi-layered security design. Frontegg's production environment resides in Amazon Web Services (AWS), a highly secure compute cloud guarded 24/7 by the AWS security team. Frontegg takes numerous steps to lock down production and ensure that access is provided only after rigorous authentication of a requester's identity and verification of key attributes such as IP address, geolocation, device type or agent, and use of proper authentication systems.

Least-Privilege Principles: Access to any of the production environments or services is on a need to know basis, and limited to the environments required for specific tasks. There are no super admin roles and no engineer has global access to all production systems from a single log-on or authorization system.

Mandatory Multi-Factor Authentication: Any access to production environments and to DevOps toolchains used for deployment (CI/CD) requires 2-factor authentication (2FA). All pass-word only access modalities have been disabled.

Access Limited to DevOps: A limited group of DevOps engineers has access to the servers in the production environments. Activities of these engineers are closely monitored to ensure that an account takeover or other form of identity compromise will be quickly identified and mitigated.

Firewall, Gateway, DDOS Protection: The production environment is protected by both a network firewall and a web application firewall (WAF) tuned specifically to block web attacks, such as the OWASP Top 10. In addition, the ingress controller in front of the Kubernetes cluster provides an additional layer of protection and resilience for API traffic accessing back-end services. Frontegg uses Cloudflare for DDOS protection, tapping into a global service that has repelled a number of the world's largest DDOS attacks to date.

Endpoint Protections on All Exposed Endpoints: Although Frontegg is a 100% cloud company, its resources are accessed by its endpoints. To mitigate this risk, Frontegg has deployed an EDR solution on all endpoints. All endpoints are also managed by an MDM system to ensure that endpoints accessing sensitive assets are properly secured and patched.

Extensive Encryption Measures to Protect Traffic, Data

Robust encryption is table stakes for security of any complex SaaS application. Frontegg encrypts data wherever practical and uses proven encryption protocols and algorithms throughout their infrastructure.

Data Encrypted in Transit and at Rest: Frontegg encrypts all data through its lifecycle inside the application. This ensures that, at any point in a process or interaction, data is encrypted. Customer data is encrypted at rest using the AES-256 algorithm.

TLS 1.2 (and above), 2048 Bit RSA Keys: All communication over public networks uses HTTPS with TLS 1.2 (and above). Frontegg has disabled the older, weaker SSL protocol for all traffic. Frontegg deploys RSA keys with a length of 2048 bits (where supported by the client) and can deploy 4096 bit keys upon request.

Strict Secure Coding Practices

With many decades of practice writing secure software for mission critical cybersecurity applications, Frontegg's engineering leadership follows strict secure coding practices designed to institute best practices during the development process.

Completely Separate Development Environment: To prevent any vulnerabilities or security gaps in development code from affecting production, Frontegg separates all development environments from testing and production environments. Further, production data is never used for testing purposes and is never transferred out of production environments.

All Code Reviewed, Tested Prior to Push: All code goes through multiple reviews, including SCA, before it is merged into the main branch. This includes peer-review by senior developers with extensive knowledge of application security and experience in securing coding best practices. Frontegg runs automated test suites against every code change. Changes are not allowed to deploy until all tests pass. In addition, Frontegg's QA engineering team performs manual code tests to verify security and performance in an isolated test environment.

Incident Response, Disaster Recovery and Business Continuity

Frontegg realizes that security never sleeps and that even the best security preparation must be paired with plans for rapid recovery from problems and contingencies to ensure business continuity. For this reason, Frontegg has developed an Incident Response Plan, Disaster Recovery Plan and Business Continuity Plan. All plans have been audited and approved by external parties. All plans are tested on a regular basis as part of the company's ongoing readiness drills program.

To accelerate incident response, Frontegg uses a managed Network Operations Center (NOC) staffed 24/7 with human analysts. These analysts can instantly direct a response to any incidents, identifying and contacting the right Frontegg experts to engage in the response. Frontegg also has detailed incident response plans that assign ownership and establish workflows and processes. Frontegg's team has quarterly incident response exercises to identify potential problems with response plans and to improve teamwork and response abilities as well as ensure that all stakeholders maintain the necessary competencies.

> **Frontegg also contracts with AWS for the highest level of incident response assistance, with a 10-minute response time SLA.**

A Culture and Methodology of Continuous Security

Rock-solid web security is now table stakes for any B2B SaaS provider. As a core capability of B2B SaaS, user management services like Frontegg must meet an even higher bar for web application security. To meet this need, Frontegg has designed its processes, systems, and environments to address the growing threat of cyberattacks on web applications and websites. Unlike other providers of user management SaaS, Frontegg's leadership, engineering and operational management, and development teams all have extensive experience in web application and cloud security building global scale SaaS products and user management platforms for multi-tenant, multi-SaaS infrastructure. Based on this experience, Frontegg deploys a methodology of continuous security with checks at every stage of the software development lifecycle process. Across all operations, Frontegg has implemented a multi-layered defense based on principles of zero trust, least privilege, segmentation, and testing, and has automated tests at every stage of operations. As evidence of this commitment, Frontegg has obtained the two highest-level SaaS compliance certifications. Frontegg continuously tests its applications and operations using both internal and external checks and services such as penetration testing and code review.

> **Frontegg understands that user management is a core capacity for any B2B SaaS and we have designed a rigorous security practice that adheres to the highest industry standards to ensure that our customers' trust is rewarded with secure, resilient and industry-leading user management services.**