Webflow

WHITEPAPER

Webflow Security

Table of Contents

Introduction

In an age where digital presence is paramount, safeguarding the integrity and availability of online assets stands as a foundational pillar for any website hosting company. As the digital landscape evolves, so do the threats that seek to exploit vulnerabilities within it.

This technical white paper delves into the comprehensive security measures implemented by Webflow to fortify its infrastructure against emerging threats. This paper illustrates our commitment to ensuring the utmost security and reliability for our customer and community endeavors.

Product introduction

Webflow offers a visual designer that generates clean, semantic code; a CMS for dynamic content served both in and out of Webflow; different modes for editing and translating content; a set of no-code site optimization tools; and enterprise-grade, world-class hosting. Non-technical users can build, launch, host, and optimize sites on their own, freeing developers from trivial web updates so they can focus on the highest value work. Webflow allows organizations to increase efficiency, reduce costs, and generate more top line revenue.

In this whitepaper, we'll outline Webflow's approach to managing security through the following topics:

There are two core parts of the Webflow platform:

1 The Designer & Dashboard

2 Website hosting

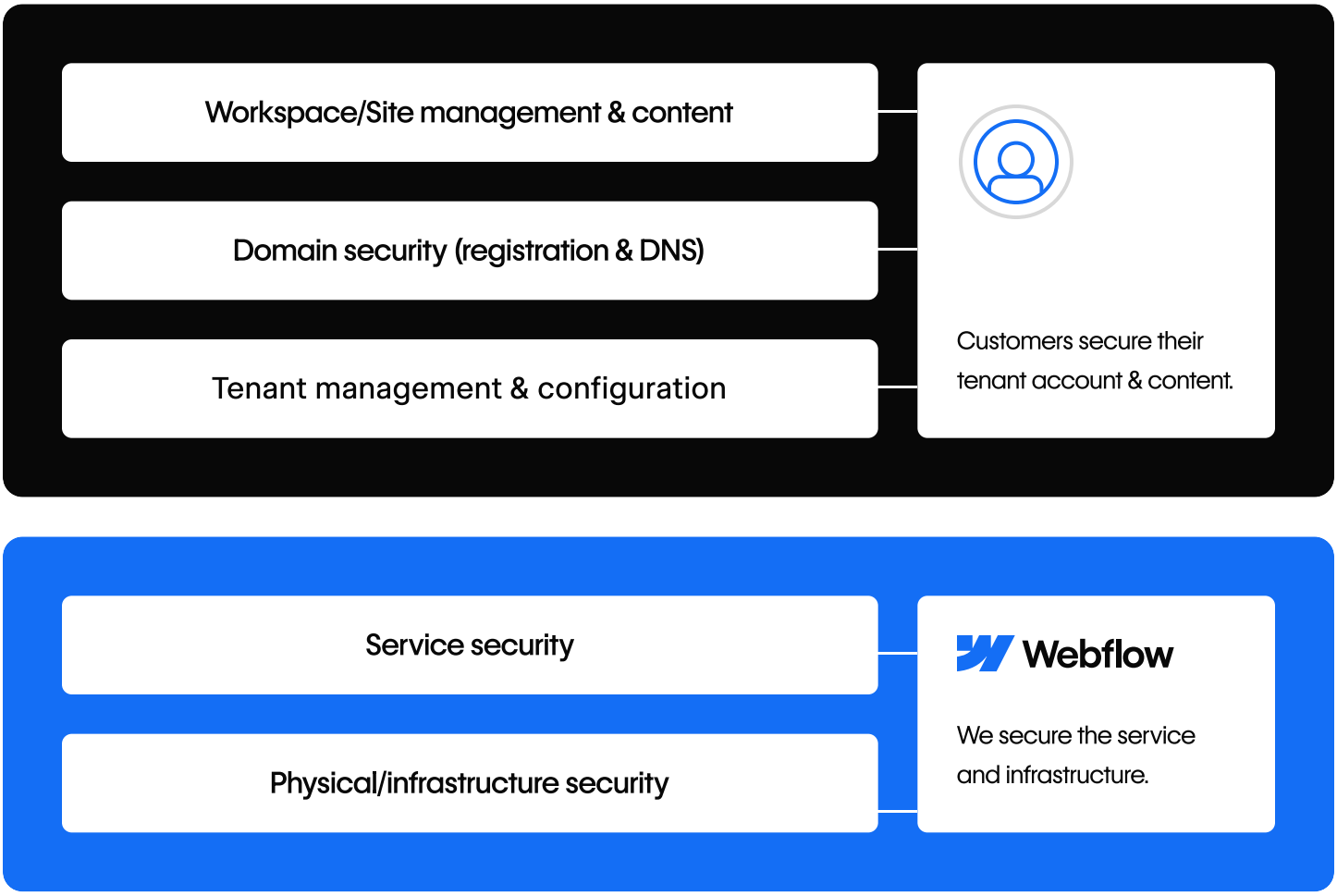
The Designer and Dashboard are hosted as a multi-tenant web application. Users are required to to authenticate in order to establish identity. Webflow integrates with SSO providers and supports OAuth and SAML connections for Enterprise customers. All actions go through authentication and authorization checks to ensure that a site you're editing is, in fact, your site — or a site you have permission to collaborate with. Authentication and authorization prevents users from modifying or uploading assets to sites that they don't have permission to modify.

All site assets are uploaded to an AWS S3 bucket which is then used to serve that content. Each site is given a path within the bucket that can only be modified by users who can edit that site. Access control checks ensure that content can not be uploaded to the path of another site. Once a site is published, pages are rendered to explicitly reference the site paths mentioned above. All site pages and assets are made available to our Content Delivery Network (CDN) which balances security and performance.

Webflow does not share production data with staging environments. Staging environments are smaller prod-like environments for developers to run tests of new code and features. They are running in similar (if not the same) architecture with smaller clusters. The production environment has tighter access restrictions and uses a larger cluster.

It is Webflow's policy to store customer data (designer or editor customers) in its databases for the duration of customer's engagement of Webflow's services and as and as necessary in accordance with applicable laws. Logs within Datadog are stored for 15 days and in Amazon Glacier for 12 months. Please note that at this time there is currently no automated method to access logs or dump site assets. If you are in need of a real-time automated access to logs, there are third party services that might help address this requirement.

Shared responsibility model



Webflow encourages customers to reference Webflow's Terms of Services, or other applicable agreement for more information about customer responsibilities when using Webflow.

Security features of Webflow

Webflow has comprehensive security built-in to its platform, such as:	
Undergoes annual SOC 2 Type II audit	All plans
Secure AWS hosting	All plans
SSL certificates	All plans
Multi-factor authentication (MFA)	All plans
Site-wide and per page password protection	All paid plans
Automatic backups	All plans
Built-in DDoS protection	All plans
Security issue monitoring 24/7/365	All plans
SAML 2.0 single sign-on	Enterprise
Custom security headers	Enterprise
Custom SSL certificates	Enterprise
Private staging site	Enterprise
Site activity log	Enterprise
Advanced roles and permissions	Enterprise
Enterprise-level uptime SLAs	Enterprise

Webflow security controls

Webflow utilizes a variety of administrative, technical, and physical controls to help protect the confidentiality, integrity, and availability of customer data.

Administrative controls

- Background checks
- Confidentiality agreements
- Security awareness training
- Security policies

Background checks

Webflow conducts background checks on all new employees during the onboarding process. For contractors from a third-party agency, Webflow requires the agency to provide proof that they conducted a background check on the contractor that will be employed. For independent contractors, background checks are conducted.

The background check needs to be cleared before contractors and employees, get access to sensitive systems. Background screenings in the USA may include:

- County and state criminal records
- Sex offender and domestic/terror watchlists
- Verification reports (e.g., identity, previous employment, SSN)
- Reference checks
- Credit reports if position requires it (e.g., finance, legal, senior leadership roles, etc.)
- Federal criminal records if position requires it (e.g., finance, legal, senior leadership roles, etc.)

For international team members hired, right-to-work checks are performed to ensure team members have the right to work in the country in which they are hired.

Confidentiality agreements

All new hires are required to acknowledge the following policies during their onboarding process:

- Employee handbook
- Code of conduct
- InfoSec policy
- Acceptable use policy

Employees are required to reacknowledge these documents when there is a new version of these documents.

Furthermore, any outsourcers, consultants, vendors or other non-employees of Webflow that require access to PII or non-public data are required to sign a nondisclosure agreement, confidentiality agreement, or data protection agreement with Webflow before such access is granted.

Security awareness training

Upon hire and on an annual basis, all Webflow employees and contractors with access to confidential information are required to participate in information security training sessions. Webflow employees are periodically tested with simulated phishing emails and are required to complete additional training if they fail the simulated phishing exercise.

Security policies

It is the responsibility of all Webflow employees to review, understand, and acknowledge related information security policy documents. These documents are posted internally and available to all Webflow staff. Webflow has the following policies in place:

- Acceptable use policy
- Information security policy
- Business continuity and disaster recovery policy
- Change management policy
- Data classification and retention policy
- Incident response policy
- AI Acceptable Use Policy
- Outsourcing and vendor management policy
- Risk management policy
- Secure configuration policy
- Systems availability policy
- Vulnerability and patch management policy
- Cryptography policy
- Background screening policy
- Trust & Security Committee policy
- Information security management system (ISMS) policy

All information security policy documents listed above are required to be reviewed on an annual basis, or when significant organizational changes occur. Any updates or changes to the policy must be approved by executive management.

Technical controls

1. Logical access control
2. Cloud security
3. Endpoint security
4. Incident response
5. Encryption
6. Web application security and vulnerability management
7. Secure development lifecycle
8. Data backups and disaster recovery

Logical access control

Webflow assigns permissions in a role-based fashion given the principle of least privilege. Webflow uses a single sign-on/access authorization product to control users and their access. Employees who require access to the application are added to the SSO product by an administrator. Access control is specified by the job title of a user, what department they are under, and the specific roles and tasks that the user must carry out. If the user requires additional access, they must submit a ticket with manager approval, and the IT team will review the business case to approve or deny the access request. Multi-factor authentication is required for access to internal systems.

Furthermore, user access reviews are performed on a quarterly basis, and customer data access is limited to only those employees with roles that require access to perform their job duties. An example of employees with access to this data is our Customer Support team.

Cloud security

Webflow is primarily hosted on AWS infrastructure, giving Webflow access to numerous benefits that AWS hosting provides to their customers. Webflow's backend infrastructure is hosted in AWS and fully monitored to detect downtime. Webflow has implemented endpoint detection and response (EDR) and intrusion detection and prevention (IDS/IPS) at the ingress/egress points at the load balancer to help facilitate timely detection, investigation by root cause analysis, and response to incidents. Webflow uses multiple tools to perform network monitoring and utilize a security information event management (SIEM) platform to centrally manage audit logs. Alerts and log events are regularly reviewed by the security and engineering staff. The virtual private cloud (VPC) environment is architected with a "defense-in-depth" security operations strategy, with numerous layers of security monitoring, protocols, and implementations protecting the confidentiality, integrity, and availability of the Webflow application. The nature and specifics of the defense-in-depth strategy are the responsibility of the security and engineering teams.

The Webflow proxy is based on an off-the-shelf tool and runs on Kubernetes. These pods automatically scale based on load. Webflow uses application load balancing (ALB) and CDN for caching.

Webflow blocks all Website traffic from OFAC-sanctioned countries and utilizes anti-bot vendors to monitor traffic at a high level and practice detection and prevention accordingly.

Webflow Enterprise utilizes a Web Application Firewall (WAF) and AWS Shield Advanced. AWS Shield Advanced is used to protect Layer 3 Distributed Denial of Service (DDoS) attacks on the SSL Terminator and the WAF is utilized for the core purpose of detecting certain kinds of brute-force attacks. When combined with a highly scaled CDN, DDoS attacks are very effectively mitigated. Webflow monitors for increased traffic patterns that indicate DDoS attacks and have on-call staff 24/7/365 to respond within minutes when services are at risk of becoming overloaded beyond the ability of automated scaling measures.

Additionally, Webflow uses both caching and a layer 7 WAF to measure and mitigate such attacks. That being said, the scale and sophistication of DDoS attacks increases all the time and our Reliability Engineers are constantly finding new ways to provide resiliency to various parts of our technology stack. If you find that your site hosted by Webflow is experiencing unusual latency or periods of unavailability, please reach out to our customer support team immediately and we will take action to both fix the issue and update our monitoring to better detect DDoS attacks before services are impacted.

Endpoint security

Webflow centrally manages its endpoints while adhering to NIST guidelines. Furthermore, the inclusion of EDR solutions bolsters the company's cybersecurity defenses. EDR tools provide real-time threat detection and response capabilities, offering enhanced visibility into potential security incidents. Additionally, vulnerability management software ensures that software and systems are regularly assessed for known vulnerabilities, enabling timely patching and remediation. Collectively, these measures form a robust security ecosystem that proactively safeguards the company's digital assets and minimizes security risks.

Incident response

Our security team performs incident response tabletop exercises on a quarterly basis to help prepare for various threats such as ransomware.

In addition, Webflow maintains a cyber insurance policy and the Certificate of Insurance (COI) is located in our security profile.

Encryption

Encryption is used throughout Webflow to protect personal identifying information (PII) and non-public data from unauthorized access. All communication between Webflow users and the Webflow-provided web application is encrypted in transit using TLS 1.2 and 1.3 while using the application.

At rest, data is encrypted by using exclusively encrypted volumes for any storage component in the Webflow SaaS cloud environment. In addition, mobile device management (MDM) enforces endpoint encryption-at-rest utilizing full disk encryption.

We utilize AES 256 to encrypt data at-rest.

Webflow uses industry best practices for production secrets management.

Webflow sites that are configured to host within a custom configured domain requires TLS certificates. For customers that prefer to manage their own certificates, it's their responsibility to rotate, maintain, and monitor.

For customers who elect to have Webflow manage their certificates on their behalf, Webflow requests certificates from the Let's Encrypt service. Each certificate is valid for 90 days and is rotated automatically by the certificate management servers. All certificates are encrypted at-rest and stored securely within an access limited database. Webflow uses TLS termination servers to serve up Webflow content with customer certificates.

We review our TLS configuration at least twice a year and adjust according to multiple requirements and recommendations. We choose TLS protocols and cipher suites based on:

- NIST 800-52 TLS Protocol Standards
- Mozilla's Security/Server Site TLS recommendations balance security with compatibility.
- Current threat landscape
- Results from SSLLabs (which are more or less aligned with the bullet points above)

Webflow Enterprise customers can utilize header customizations such as strict-transport-security for your domain. Webflow does not set HSTS headers for custom domains by default, because we believe our customers should have that control. If we set this header by default, our customers would have difficulty removing the policy in case they ever run into issues with other services running within their domain.

Web application security and vulnerability management

Webflow does not allow customers to run their own penetration test or vulnerability scan of the site, as this would violate our Terms of Service, or applicable customer agreement. We are aware that customers work with services such as WhiteHat Security, Qualys, Tenable, and other SaaS automated scanning services. When multiplied by thousands of customers, these scans and tests can cause load on our servers.

The Webflow security team runs annual penetration tests with external security firms. We make this available to you as an alternative to taking penetration testing into your own hands. You can find a copy of the Letter of Engagement from Webflow's last penetration test and summary results are available in Webflow's security profile.

Critical or high risk patches are installed within one month of release. All other patches are installed within an appropriate time frame.

If you believe you have discovered a vulnerability within Webflow's application, please submit a report to us by emailing security-bug-reports@webflow.com. Webflow does not participate in a public bug bounty program at this time, nor do we provide monetary rewards for publicly reported findings.

If you believe your account has been compromised or you are seeing suspicious activity on your account, please report it using our support contact form.

Secure development lifecycle

Webflow follows the secure software development lifecycle. Our SDLC follows an agile development process that aligns with OWASP Software Assurance Maturity Model.

All software changes at Webflow must be reviewed by peer engineers. In addition, all code changes are analyzed for security-related defects. All security-related changes must be approved by a reviewer. All code changes will be subject to static analysis security testing (SAST), secret scanning, and software composition analysis (SCA). Every new dependency involves a manual review.

Webflow does not utilize production data for purposes outside of providing the production service. Instead, non-production environments utilize test or sample data that is not related to or derived from any real Webflow customer. Webflow maintains separate demonstration, quality assurance, and test datasets that are used for the relevant environments and are unrelated to real customer data.

If any code change, upgrade, or other infrastructure maintenance activity is anticipated to cause degradation or interruption to service, this change is scheduled for after-hours, during times of minimal system activity. Any such change should be announced and receive approval from appropriate stakeholders. The customer success team will then take responsibility to notify customers of the maintenance window.

In addition, all employees and contractors that are required to review and write code are required to complete secure code training courses upon hiring.

Data backups and disaster recovery

Webflow is hosted with AWS and deployed across multiple data center segments known as “availability zones (AZ) within the USA. The Webflow service is resilient if a limited number of availability zones become unavailable.

A comprehensive database backup policy is in place that includes:

- Real-time encrypted replication to secondary database hosts
- Snapshots of the database every four hours maintained for two days
- Weekly snapshot maintained for four weeks
- Monthly snapshot maintained for 12 months

For Webflow’s data, the recovery point objective (RPO) is within four hours, corresponding to the frequency of database snapshots. Due to continuous replication, it is expected in practice that the recovery point be within one hour. For Webflow’s application, in the event of a catastrophic event (such as a full AWS region-wide failure), the recovery time objective (RTO) is 24 hours. We have a base RTO and RPO, but check on the stated RTO and RPO in your contract.

In the event of an outage, customers can visit https://status.webflow.com/ which will provide known details of the incident. Customers can also subscribe for updates on the Status page to get email or mobile text notifications whenever Webflow creates, updates, or resolves an availability incident.

Physical controls

- Data centers
- Office

Data centers

Webflow is hosted in AWS and leverages its physical and environmental controls for their data centers. All of our customer data is stored within the AWS data center.

Information around the security controls used at AWS data centers can be found at: https://aws.amazon.com/compliance/data-center/controls/.

Webflow office

The majority of Webflow staff work remotely, but Webflow does have a dedicated office for some staff members in San Francisco. Webflow applies physical security controls in its office, including:

- Smart card access control and audit trail for employees
- Video surveillance
- Alarms
- Visitor management system

Trust & Safety

Webflow's Trust & Safety team works to secure a community of stakeholders that includes the marketplace and ecosystem.

The Trust & Safety performs the following tasks such as reviewing:

- Sites/marketplace malicious content
- Sites/marketplace with adult content
- Sites with Child sexual abuse material (CSAM)
- Sites/marketplace with illegal content
- Sites with other ToS violations
- Marketplace content that violate ToS and Developer ToS
- Site/marketplace content infringing on IP or Trademark

Compliance frameworks

Webflow's security is certified annually to AICPA SOC 2 Type II Trust Service Principles. Our SOC 2 report is available for customers to view in our Whistic Security Profile.

Our payment processor, Stripe is a certified Level 1 Service Provider. Webflow never has access to sensitive payment details. Webflow regularly reviews the latest PCI Attestation of Compliance from Stripe to ensure they remain PCI compliant.

Webflow is not HIPAA compliant. Customers cannot collect protected health information (PHI) using native Webflow forms or applications. However, if you are a covered entity or business associate, you can still use Webflow to collect PHI by integrating third-party HIPAA-compliant forms — such as Jotforms or Formstack. The rationale for this configuration is that when you integrate HIPAA-compliant forms, none of the PHI touches Webflow's systems. This configuration keeps Webflow out of the scope of HIPAA and enables you to remain HIPAA compliant.

At this time, we are not ISO 27001 certified, but it's on the roadmap, and we expect to be ISO 27001 certified by Q4 2024.

Additional Webflow resources

- Additional security documentation such as our SOC 2 Type II report can be obtained in our security profile in Whistic.
- Terms of service
- Global privacy policy
- EU & SWISS privacy policy
- Customer acceptable use policy
- Copyright policy
- Cookie policy
- Trademark policy
- Data processing addendum
- Subprocessors
- CCPA notice
- Privacy FAQs
- Developer terms of service
- Webflow status page
- Webflow API documentation
- Webflow University

Launch with peace of mind thanks to Webflow's robust security features and reliable hosting infrastructure.

Webflow