Last Update: March 2023

Security & Compliance Overview

HubSpot

Table of Contents

Introduction

Our Company and Products

HubSpot is a Customer Relationship Management (CRM) platform with all of the tools that you need to Grow Better and power your marketing, sales, customer service, and content management efforts. Since 2006, HubSpot has been on a mission to make the world more inbound. Today, over 150,000 customers in more than 120 countries use HubSpot's software, services, and support to transform the way they attract, engage, and delight customers.

The HubSpot products are offered as Software-as-a-Service (SaaS) solutions. These solutions are available to customers through purpose-built web applications, mobile applications, application programming interfaces (APIs), and email productivity tools.

HubSpot Security and Risk Focus

HubSpot's primary security focus is to safeguard our customers' data. To this end, HubSpot has invested in the appropriate controls to protect and service our customers. This investment includes the implementation of dedicated Corporate, Product, Infrastructure, and Physical Security programs. These teams are responsible for HubSpot's comprehensive security program, partnering with our Compliance, Legal and Privacy teams to own the governance process. Our Chief Information Security Officer oversees the implementation of security safeguards across the HubSpot enterprise.

Our Security and Compliance Objectives

We have developed our security framework using best practices for the SaaS industry. Our key objectives include:

- Customer Trust and Protection – deliver superior products and services while protecting the privacy and confidentiality of data.
- Availability and Continuity of Service – ensure availability of the service and minimize risks to service continuity.
- Information and Service Integrity – make sure that customer information is never corrupted or altered inappropriately.
- Compliance with Standards – aim to comply with or exceed industry standard best practices. Our controls governing the availability, confidentiality, and security of customer data meet or exceed the applicable SOC 2 Trust Service Principles (TSPs) established by the American Institute of Certified Public Accountants (AICPA).

HubSpot Security Controls

In order to protect the data that is entrusted to us, HubSpot utilizes a defense-in-depth approach to implement layers of administrative, technical, and physical security controls throughout our organization. The following sections describe a subset of our most frequently asked about controls.

Infrastructure Security

Cloud Hosting Provider

HubSpot does not host any product systems or data within its corporate offices.

HubSpot outsources hosting of its product infrastructure to leading cloud infrastructure provider, Amazon Web Services (AWS). HubSpot's US product infrastructure resides in AWS data centers located in the United States. The primary region is located in Virginia and the secondary region is located in Ohio. Customers also have the option to have their HubSpot data hosted in the European Union, with the primary region located in Germany and the secondary located in Ireland.

We place reliance on AWS's audited security and compliance programs for the efficacy of their physical, environmental, and infrastructure security controls. AWS guarantees between 99.95% and 100% service availability, ensuring redundancy to all power, network, and HVAC services. The business continuity and disaster recovery plans for the AWS services we use have been independently validated as part of their SOC 2 Type 2 report and ISO 27001 certification.

AWS's compliance documentation and audit reports are publicly available at the AWS Cloud Compliance Page and the AWS Artifacts Portal. HubSpot is unable to deliver these documents on your behalf; you can obtain them directly from the AWS Artifacts portal.

Additional information regarding HubSpot's Cloud Infrastructure can be found on our Cloud Infrastructure Frequently Asked Questions page and in our Regional Data Hosting Policy.

Network and Perimeter

The HubSpot product infrastructure enforces multiple layers of filtering and inspection on all connections across our web application firewall (WAF), logical firewalls, and security groups.

Network-level access control lists are implemented to prevent unauthorized access to our internal product infrastructure and resources. By default, firewalls are configured to deny network connections that are not explicitly authorized, and traffic monitoring is in place to alert on anomalous activity.

Changes to our network and perimeter systems are actively monitored and controlled by standard change control processes. Firewall rulesets are reviewed on an annual basis to help ensure that only necessary connections are configured.

Configuration Management

Automation drives HubSpot's ability to scale with our customers' needs and rigorous configuration management is baked into our day-to-day infrastructure processing. The product infrastructure is a highly automated environment that expands capacity as needed.

All server configurations are embedded in images and configuration files, which are used when new server instances are built. Each instance type includes its own hardened configuration and changes to the configuration and standard images are managed through a controlled change management process. Server instances are tightly controlled from provisioning through deprovisioning, ensuring that deviations from configuration baselines are detected and reverted at a predefined cadence. In the event that a production server deviates or drifts from the baseline configuration, it will be overwritten with the baseline within 30 minutes.

Patch management is handled using automated configuration management tools or by removing server instances that are no longer compliant with the expected baseline.

Logging

Actions and events that occur within the HubSpot application are consistently and comprehensively logged. These logs are indexed and stored in a central logging solution hosted in HubSpot's AWS environment. Security relevant logs are also retained, indexed, and stored to facilitate investigation and response activities. The retention period of logs depends on the nature of the data logged.

Write access to the storage service in which logs are stored is tightly controlled and limited to a small subset of engineers who require access.

Alerting and Monitoring

Not only does HubSpot fully automate its build procedures, we invest heavily in automated monitoring, alerting, and response capabilities to continuously address potential issues. The HubSpot product infrastructure is instrumented to alert engineers and administrators when anomalies occur. In particular, error rates, abuse scenarios, application attacks, and other anomalies trigger automatic responses or alerts to the appropriate teams for response, investigation, and correction.

Many automated triggers are also designed to immediately respond to anomalous situations. For example, traffic blocking, file quarantines, process termination, and similar functions are triggered at predefined thresholds.

Application Security

Web Application Defenses

All customer content hosted on the platform is protected by our Web Application Firewall (WAF). These tools actively monitor real-time traffic at the application layer and can alert on or deny malicious behavior based on behavior type and session rate.

The rules used to detect and block malicious traffic are aligned to the best practice guidelines documented by the Open Web Application Security Project (OWASP), specifically the OWASP Top 10 and similar recommendations. Protections from Distributed

Denial of Service (DDoS) attacks are also incorporated, helping to ensure customers' web sites and other parts of the HubSpot products are continuously available .

Development and Release Management

One of HubSpot's greatest advantages is a rapidly advancing feature set, and we optimize our products through a modern continuous delivery approach to software development.

New code is deployed thousands of times each day. Code reviews, testing, and merge approval is performed before deployment. Static code analysis runs regularly against code repositories and blocks known misconfigurations from entering the code base. Approval is controlled by designated repository owners and once approved, code is automatically submitted to HubSpot's continuous integration environment where compilation, packaging and unit testing occur. Dynamic testing for security vulnerabilities is performed continuously against our applications.

Newly developed code is first deployed to a dedicated and separate QA environment for the last stage of testing before being promoted to production. Network-level segmentation prevents unauthorized access between QA and production environments.

All code deployments create archives of existing production code in case failures are detected by post deployment hooks. The deploying team manages notifications regarding the health of their applications and if a failure occurs, rollback processes are immediately engaged.

We use extensive software gating and traffic management to control features based on customer preferences (private beta, public beta, full launch). HubSpot features seamless updates and, as a SaaS application, there is no downtime associated with releases. Major feature changes are communicated through in-app messages and/or product update posts.

Vulnerability Management

The HubSpot Security team manages a multi-layered approach to vulnerability management, using a variety of industry-recognized tools and threat feeds to ensure comprehensive coverage of our technology stack. Adherence to Service Level Agreements is accomplished via automation of ticket generation and closure, as well as escalation paths when appropriate.

Vulnerability scans are configured to scan for vulnerabilities on a daily basis, using adaptive scanning inclusion lists for asset discovery as well as the latest vulnerability detection signatures.
In addition to our SOC, HubSpot also has an internal Threats & Vulnerabilities team that works to systematically discover any vulnerabilities and ensure best practices are in place to secure our product.

We bring in industry recognized third parties to perform annual penetration tests against our applications and infrastructures. The goal of these programs is to identify vulnerabilities that may present security related risks. Relevant findings are assessed, mitigations are prioritized accordingly, and both are incorporated in the reports available to our customers. Additionally, HubSpot manages a bug bounty program where independent security researchers may submit potential issues for review. Security community members and HubSpot customers are welcome to perform security testing against trial portals, although we recommend using a different IP address for scanning than what is used to login to the portal. This mitigates any risk that customers may be unable to use their HubSpot portal due to blocks resulting from testing. Please see our Acceptable Use Policy to learn more about how to perform testing in an authorized manner.

Customer Data Protection

Data Classification

HubSpot's tools allow customers to define the type of information to be collected and stored on their behalf. Per the HubSpot Terms of Service and Acceptable Use Policy, our customers are responsible for ensuring they only capture appropriate information to support their marketing, sales, services, content management, and operations processes.

The HubSpot products should not be used to collect or store sensitive information as defined in our Terms of Service, such as credit or debit card numbers, financial account information, Social Security numbers, passport numbers, financial or health information.

Further detail on HubSpot's data classification scheme can be found within our SOC 2 Type 2 report that can be downloaded from our Security page.

Tenant Separation

HubSpot provides a highly scalable, multi-tenant SaaS solution where customer data is logically separated using unique portal IDs to associate data and objects to specific customers.

Authorization rules are incorporated into the design architecture and validated on a continuous basis. Additionally, we log application authentication and associated changes, application availability, and user page views.

Encryption

All sensitive interactions with the HubSpot products (e.g. API calls, authenticated sessions, etc.) are encrypted in transit with TLS version 1.2, or 1.3 and 2,048 bit keys or better. Transport layer security (TLS) is also a default for customers who host their websites on the HubSpot platform.

See our website setup guide and our KB article on SSL and domain security for more information about configuring TLS for your HubSpot-hosted site.

HubSpot leverages several technologies to ensure stored data is encrypted at rest. Platform data is stored using AES-256 encryption. User passwords are hashed following industry best practices, and are encrypted at rest.

Key Management

Encryption keys for both in transit and at rest encryption are securely managed by the HubSpot platform. TLS private keys for in transit encryption are managed through our content delivery partner. Volume and field level encryption keys for at rest encryption are stored in a hardened Key Management System (KMS). Keys are rotated at varying frequencies, depending upon the sensitivity of the data they govern. In general, TLS certificates are renewed annually.

HubSpot is unable to use customer supplied encryption keys at this time.

Data Backup and Disaster Recovery

System Reliability and Recovery

HubSpot is committed to ensuring the availability of our systems by using commercially reasonable efforts to meet a Service Uptime of 99.95% for our Subscription Service in a given calendar month. Please reference Sec. 7 of the Product Specific Terms for more information.

Additionally, we provide real-time updates and historical data on system status via HubSpot's status site.

All HubSpot product services are built with full redundancy. Server infrastructure is strategically distributed across multiple distinct availability zones and virtual private cloud networks within our infrastructure providers, and all web, application, and database components are deployed with a minimum of n+1 supporting server instances or containers.

Disaster Recovery

HubSpot maintains disaster recovery plans for key product infrastructure and providers that are tested annually as a part of our SOC 2 controls. Please refer to our SOC 2 report (downloadable from our Security page) for more detail.

Backup Strategy

SYSTEM BACKUPS

Systems are backed up on a regular basis with established schedules and frequencies. Seven days' worth of backups are kept for any database in a way that ensures restoration can occur easily. Backups are monitored for successful execution, and alerts are generated in the event of any exceptions. Failure alerts are escalated, investigated, and resolved.

Data is backed up daily to the local region. Additionally, backups are copied periodically to a separate AWS region for recovery in the event of a primary regional outage. Monitoring and alerting is in place for replication failures and triaged accordingly.

All production data sets are stored on a highly available file storage facility like Amazon's S3.

PHYSICAL BACKUP STORAGE

Because we leverage public cloud services for hosting, backup, and recovery, HubSpot does not implement physical infrastructure or physical storage media within its products. HubSpot does not generally produce or use other kinds of hard copy media (e.g., paper, tape, etc.) as part of making our products available to our customers.

BACKUP PROTECTIONS

By default, all backups are protected through access control restrictions and write once read many (WORM) protections on HubSpot product infrastructure networks, and access control lists on the file systems storing the backup files.

CUSTOMER DATA BACKUP RESTORATION

HubSpot customers don't have access to the product infrastructure in a way that would allow a customer-driven failover event. Disaster recovery and resiliency operations are managed by HubSpot product engineering teams.

In most cases, customers can use the recycle bin to directly recover and restore contacts, companies, deals, tickets, and custom object records, activity, and workflows up to 90 days after they were deleted. Changes to web pages, blog posts, or emails can be restored to previous versions of content using version history that is kept indefinitely.

For customers who wish to additionally back up their data,, the HubSpot platform provides many ways of ensuring that you have what you need. Many of the features within your HubSpot portal contain export options, and the HubSpot library of public APIs can be used to synchronize your data with other systems. For further details about backing up your data, please review our KB article about exporting your content.

Identity and Access Control

Product User Management

The HubSpot products allow for granular authorization rules. Customers are empowered to create and manage the users in their portals, assign the privileges that are appropriate, and limit access as they see fit.

For more information about user roles, please see the HubSpot User Roles and Permissions Guide.

Product Login Protections

The HubSpot products allow users to login to their HubSpot accounts using the native HubSpot login, "Sign in with Google" login, or Single Sign On (SSO). The native login enforces a uniform password policy which requires a minimum of 8 characters and a combination of lower and upper case letters, special characters, whitespace, and numbers. People who use HubSpot's native login cannot change the default password policy.

The "Sign in with Google" feature is available to all HubSpot customers. SAML-based SSO integrated with any SAML-based IDP is available with any Hub at the enterprise tier level.

Instructions for setting up SSO are available on this knowledge base article and HubSpot Academy. Single Sign On and Google login users can configure a password policy in their SSO provider or within their Google account settings.

Customers who use HubSpot's built-in login are strongly encouraged to set up two-factor authentication for their HubSpot accounts. Portal administrators may require all users to have two-factor authentication enabled.

Product API Authorization

As of November 30, 2022, we sunset the use of API keys (also known as Hapikeys or HubSpot API keys) and they are no longer supported. API Keys were one of three authentication methods supported by HubSpot APIs.

Application programming interface (API) access is enabled through either OAuth (version 2) or Private App access tokens. Both HubSpot's OAuth and Private App implementations are a stronger approach to authenticating and authorizing API requests than legacy API keys. These methods offer more granular control over your integrations and account data. We also require OAuth for all featured integrations.

For more information about API use and authentication, please see the Developers portal.

Portal Activity & Alerting

Customers have the ability to export portal account activity history including:

- User logins
- HubSpot employee access
- Security activity
- Content activity

Customers can also set up user notifications to alert on imports and exports.

HubSpot Employee Access to Customer Data

Access to Production Infrastructure

HubSpot's internal data stores and production infrastructure may only be accessed from the Corporate network or on Virtual Private Network (VPN), which requires device validation and phish-resistant Multi-factor Authentication (MFA). User access is strictly controlled. HubSpot employees are granted access using a role based access control (RBAC) model.

Day to day access is minimized to members of the Engineering team and persistent administrative access is restricted. For temporary or emergency access to administrative functions (e.g. alert responses/troubleshooting), HubSpot's system uses a Just-In-Time-Access (JITA) model to grant users privileged access for a limited duration (Engineering JITA).

Each Engineering JITA request is logged, along with the reason for access. After the configured session limit, access to the account expires and is automatically revoked. Daily Engineering JITA usage is available for retroactive review by Engineering management. Management reviews activities performed during JITA sessions in key datastores, the reason for access, and monitor for anomalous behavior.

Additionally, direct network connections to product infrastructure devices over SSH or similar protocols is prohibited, and engineers are required to authenticate first through a bastion host or "jump box" before accessing QA or production environments. Server-level authentication uses user-unique SSH keys and token-based two factor authentication.

Access to Customer Portals

By default, Customer Support, Services, and other customer engagement staff can obtain limited access to parts of your HubSpot account to help you with using HubSpot.

The HubSpot application also uses a JITA model to grant employees access to a customer's portal for a limited duration (Portal JITA). Each Portal JITA request is logged and requires a business reason for access. Note that access is automatically granted for certain use cases, such as an open Support ticket. Some portal JITA requests will initiate an exception process which requires manager or manager-equivalent approval. Access is tied to a specific customer's portal for a maximum 24-hour period. HubSpot also utilizes risk-based monitoring to detect unusual Portal JITA activity. HubSpot employees must be on the corporate network or VPN, which requires device validation and MFA, in order to access Portal JITA.

When accessing a portal using Portal JITA, HubSpotters are unable to perform high-risk actions such as:

- changing domain or SSO settings
- exporting users/contacts
- viewing/creating/deleting/rotating private app keys
- importing data to the CRM
- deleting contacts, companies, deals, and tickets

User logins, HubSpot employee access, security activity, and content activity is logged. The last 90 days of these logs are available as the 'Export HubSpot employee access history' within your portal.

Customers may choose to disable HubSpot employee access to their portal entirely by following the steps outlined in here.

Corporate Authentication and Authorization

Access to the HubSpot Corporate network, both remotely on VPN and while in office, requires device validation and MFA. Access to corporate systems is centralized via Single Sign On as a policy.

Password policies follow industry best practices for required length, complexity, and rotation frequency. Password vaults are in place to manage certain administrative account

passwords, and access to the vault is managed through Role Based Access Control or through the JITA process.

We have built an extensive support system to streamline and automate our security management and compliance activities. In addition to many other functions, this system sweeps our product and corporate infrastructure several times daily to ensure that permission grants are appropriate, employee events are managed, access revocations are timely, change logs are effectively collected, and compliance evidence is preserved. Employee access and permissions to key internal systems are manually reviewed semi-annually to help ensure access granted is necessary for their job function.

Organizational and Corporate Security

Background Checks and Onboarding

HubSpot employees in the US undergo an extensive third party background check prior to formal employment offers. In particular, employment, education, and criminal checks are performed for potential employees. Outside of the US, employment checks are performed. Reference verification is performed at the hiring manager's discretion.

Upon hire, all employees must read and acknowledge HubSpot's Corporate Acceptable Use Policy (AUP) and Code of Use Good Judgement (CUGJ), which help to define employee's security responsibilities in protecting company assets and data.

Policy Management

To help keep all our employees on the same page with regard to protecting data, HubSpot documents and maintains a number of written policies and procedures. HubSpot maintains a core Written Information Security Policy, which covers a variety of topics such as data handling requirements, privacy considerations, and disciplinary actions for policy violations.

Policies are reviewed and approved at least annually and stored in the company wiki. Policies requiring acknowledgment by employees are incorporated into mandatory annual training.

Security Awareness Training

We consider employees to be our first line of defense, and we ensure HubSpot employees are trained for their roles. HubSpot employees are required to complete security awareness training within 30 days of commencing employment, and training is made available annually thereafter. In addition to awareness training, HubSpot keeps employees aware of recent security news or initiatives with internal enablement.

In addition to general awareness training, HubSpot conducts phishing awareness training/simulations at least annually, and provides additional role-based training for certain roles.

Risk Management

HubSpot has an Enterprise Risk Management (ERM) program that includes a documented ERM policy, continual risk assessments, and a formal risk register. Risk mitigation and remediation activities are tracked and reviewed at a designated cadence.

Further detail on the risk assessment and risk management program can be found within the SOC 2 report (downloadable from our Security page).

Vendor Management

We leverage a number of third party service providers at HubSpot to support the development of our product as well as internal operations. We maintain a vendor management program to ensure that appropriate security and privacy controls are in place. The program includes inventorying, tracking, and reviewing the security programs of the vendors who support HubSpot.

Appropriate safeguards are assessed relative to the service being provided and the type of data being exchanged. Ongoing compliance with expected protections is managed as part of our contractual relationship with them. Our Security, Privacy, Legal, and Compliance teams coordinate with our business stakeholders as part of the vendor management review process.

We also maintain a list of our Sub-Processors within our Data Processing Agreement (DPA).

Corporate Physical Security

HubSpot offices are secured in multiple ways. Security services are leveraged at each of HubSpot's global locations to help create a safe environment for HubSpot employees. Door access is controlled using RFID tokens tied to individuals, which are automatically deprovisioned if lost or when no longer needed (e.g., employee termination, infrequent use, etc). Video surveillance, and other protective measures are implemented across HubSpot offices.

Corporate Network Protections

Centrally managed application firewalls are deployed in a High Availability architecture at HubSpot Corporate offices. Our guest networks are separate from our corporate network, and the firewall is configured to block all inbound connections unless the session is explicitly identified and allowed. HubSpot enforces system authorization checks prior to allowing a device's connection to the Corporate network. Unauthorized devices are disconnected immediately or moved to containment VLANs.

Endpoint Protection

Company issued laptops are centrally managed and are configured to among other things, maintain full disk encryption.

Endpoints are also protected by a market leading Endpoint Detection and Response (EDR) solution and we incorporate extensive automation into our detection and response capabilities, capitalizing on signaling from our robust security stack to create a highly integrated ecosystem that is continually optimized to detect anonymous behavior.

Incident Management

Incident Response

HubSpot's Security Operations Center (SOC) team provides 24x7x365 coverage to respond quickly to all security and privacy events. HubSpot's rapid incident response program is responsive and repeatable. Predefined incident types, based on historical trending, are

created in order to facilitate timely incident tracking, consistent task assignment, escalation, and communication. Many automated processes feed into the incident response process, including malicious activity or anomaly alerts, vendor alerts, customer requests, privacy events, and others.

Our Security Leadership reviews all security related incidents, either suspected or proven, and we coordinate with affected customers using the most appropriate means, depending on the nature of the incident.

Compliance

Sarbanes-Oxley (SOX)

As a publicly-traded company, HubSpot's key IT controls are audited on a recurring basis as part of its SOX compliance.

Public information about HubSpot's SOX compliance and our annual financial statements are available as part of our SEC filings. You can find more information on our Investor Relations page.

System and Organization Controls (SOC 2)

HubSpot undergoes rigorous SOC 2 Type 2 and SOC 3 audits on an annual basis to attest to the controls that we have in place governing the security, availability, and confidentiality of customer data and the HubSpot products. These controls map to Trust Service Principles (TSPs) established by the American Institute of Certified Public Accountants (AICPA). Our SOC 2 Type 2 and SOC 3 are available for public download from the HubSpot Security page.

Sensitive Data Processing and Storing

Please see our Terms of Service for details about prohibited data types.

HubSpot should not be considered a solution for processing or storing electronic Protected Health Information (ePHI) and is not HIPAA compliant, or HITRUST certified.

Similarly, while HubSpot customers pay for the service by credit card, HubSpot does not store, process or collect credit card information submitted to us by customers and is not PCI-DSS compliant. We leverage trusted and PCI-compliant payment card processors to ensure that our own payment transactions are handled securely.

Privacy

The privacy of our customers' data is one of HubSpot's primary considerations. As described in our Privacy Policy, we never sell your personal data to any third parties. The protections described in this document and other protections that we have implemented are designed to ensure that your data stays private and unaltered. The HubSpot products are designed with privacy first and built with customer needs in mind . Our privacy program incorporates best practices, customers' and their contacts' needs, as well as regulatory requirements.

Data Retention and Data Deletion

Customer data is retained for as long as you remain an active customer. The HubSpot platform provides active customers with the tools to delete their data (see the 'Deletion or Return of Personal Data' section outlined in our DPA), or export their data (see the KB article on how to export your content and data).

Former customers' data is removed from live databases upon a customer's written request or after an established period following the termination of all customer agreements. Freemium customers' data is purged when the portal is no longer actively used, and former paying customers' data is purged 90 days after all customer relationships are terminated.

Information stored in replicas, snapshots, and backups is not actively purged but instead naturally ages itself from the repositories as the data lifecycle occurs. HubSpot retains certain data like logs and related metadata in order to address security, compliance, or statutory needs.

HubSpot does not currently provide customers with the ability to define custom data retention policies.

Privacy Program Management

HubSpot's Legal, Security, and Privacy teams collaborate to ensure an effective and consistently implemented privacy program. Information about our commitment to the privacy of your data is described in greater detail in our:

- Privacy Policy
- Data Processing Agreement

Breach Response

You can find our breach reporting policies, process, and obligations outlined in our SOC Report under our "Incident Response" section.

HubSpot will notify customers without undue delay after it becomes aware of any Personal Data Breach and will provide timely information relating to the Personal Data Breach as it becomes known or reasonably requested by the customer. We further outline our obligations regarding personal data breaches in our DPA.

GDPR

The HubSpot platform has a number of features that enable our customers to easily achieve and maintain their GDPR compliance requirements, including the ability to perform a GDPR delete in response to a data subject access requests (DSARs) (see the KB article here). Please refer to our GDPR page for more information. While use of the HubSpot product can enable your GDPR compliance efforts, use of the HubSpot product alone does not make you GDPR compliant.

Document Scope and Use

HubSpot values transparency in the ways we provide solutions to our customers. This document is designed with that transparency in mind. We are continuously improving the protections that have been implemented and, along those lines, the information and data

in this document (including any related communications) are not intended to create a binding or contractual obligation between HubSpot and any parties, or to amend, alter or revise any existing agreements between the parties.