Last Update: October 2021

Security Overview

HubSpot

Table of Contents

HubSpot Security Overview

Our Company and Products

HubSpot is the world's leading inbound marketing, sales, services, content management, and operations platform. Since 2006, HubSpot has been on a mission to make the world more inbound. Today, over 100,000 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, application programming interfaces (APIs), and email plugins.

HubSpot Security and Risk Focus

HubSpot's primary security focus is to safeguard our customers' data. This is the reason that HubSpot has invested in the appropriate resources and controls to protect and service our customers. This investment includes the implementation of dedicated Corporate Security and Product Security teams. These teams are responsible for HubSpot's comprehensive security program and the governance process. We are focused on defining new and refining existing controls, implementing and managing the HubSpot security framework as well as providing a support structure to facilitate effective risk management. Our Chief Information Security Officer oversees the implementation of security safeguards across HubSpot and its products.

Our Security and Risk Management Objectives

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

- Customer Trust and Protection – consistently deliver superior product and service to our customers while protecting the privacy and confidentiality of their information.
- Availability and Continuity of Service – ensure ongoing availability of the service and data to all authorized individuals and proactively minimize the security risks threatening service continuity.
- Information and Service Integrity – ensure that customer information is never corrupted or altered inappropriately.
- Compliance with Standards – we design our corporate security program around the industry cybersecurity best practice guidelines including the Center for Internet Security (CIS) Critical Security Controls. Our controls governing the availability, confidentiality, and security of customer data are also designed to be SOC 2 compliant with the 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 security controls throughout our organization. The following sections describe a subset of our most frequently asked about controls.

HubSpot Product Infrastructure

Cloud Infrastructure Security

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

HubSpot outsources hosting of its product infrastructure to leading cloud infrastructure provider, Amazon Web Services (AWS). Our hosting provider guarantees between 99.95% and 100% service availability ensuring redundancy to all power, network, and HVAC services.

HubSpot's AWS product infrastructure resides in the US east region or in the Germany region. AWS maintains an audited security program, as well as physical, environmental, and infrastructure security protections. Business continuity and disaster recovery plans have been independently validated as part of their SOC 2 Type 2 and ISO 27001 certifications.

Compliance documentation is publicly available at the AWS Cloud Compliance Page.

HubSpot also maintains a Knowledge Base (KB) article with frequently asked questions regarding our Cloud Infrastructure: here.

Network Security and Perimeter Protection

The HubSpot product infrastructure enforces multiple layers of filtering and inspection of all connections throughout the platform.

Network-level access control lists are implemented to prevent unauthorized network access to our internal product infrastructure. Firewalls are configured to deny network connections that are not explicitly authorized by default, and traffic monitoring is in place for detection of anomalous activity.

Changes to our network security 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. The product infrastructure is a highly automated environment that expands capacity and capability as needed. 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 configuration within 30 minutes.

All server type configurations are embedded in images and configuration files. Server-level configuration management is handled using these images and configuration scripts when the server is built. Changes to the configuration and standard images are managed through a controlled change management process. Each instance type includes its own hardened configuration, depending on the deployment of the instance.

Patch management is handled using automated configuration management tools or by removing server instances that are no longer compliant with the expected baseline and provisioning a replacement instance in its place. Rigorous and automated configuration management is baked into our day-to-day infrastructure processing.

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 and alerts to the appropriate teams for response, investigation, and correction. As unexpected or malicious activities occur, automated systems bring in the right people to ensure that the issue is rapidly addressed.

Many automated triggers are also designed into the system to immediately respond to unforeseen situations. Traffic blocking, quarantine, process termination, and similar

functions kick in at predefined thresholds to ensure that the HubSpot platform can protect itself against a wide variety of undesirable situations.

Application Protection

Web Application Defenses

All customer content hosted on the platform is protected by a Web Application Firewall (WAF). The WAF is configured with a combination of industry standard and custom rules that are capable of automatically enabling and disabling appropriate controls to best protect our customers. These tools actively monitor real-time traffic at the application layer with ability to alert or deny malicious behavior based on behavior type and 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 available continuously.

Development and Release Management

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

New code is proposed, approved, merged and deployed thousands of times daily. Code reviews, testing (where applicable), and merge approval is performed before deployment. Approval is controlled by designated repository owners. Once approved, code is automatically submitted to HubSpot's continuous integration environment where compilation, packaging and unit testing occur.

All code deployments create archives of existing production-grade code in case failures are detected by post-deploy hooks. The deploying team manages notifications regarding the health of their applications. If a failure occurs, roll-back is 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.

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

Vulnerability Scanning, Penetration Testing, and Bug Bounties

The HubSpot Security team manages a multi-layered approach to vulnerability scanning, using a variety of industry-recognized tools to ensure comprehensive coverage of our technology stack.

Vulnerability scans are configured to scan for exploitable vulnerabilities on a daily basis. Continually running scans, using adaptive scanning inclusion lists, and continuously updating vulnerability detection signatures helps HubSpot stay ahead of many security threats.

We also bring in industry-recognized third parties to perform annual penetration tests. The goal of these programs is to iteratively identify flaws that present security risk and rapidly address any issues. Penetration tests are performed against the application layers and network layers of the HubSpot technology stack.

In addition to internal vulnerability scanning and third party penetration testing, HubSpot manages a bug bounty program where Independent security researchers are invited to participate in identifying security flaws in the HubSpot products. Security community members and HubSpot customers are welcome to perform security testing against trial portals. Information about HubSpot's bounty program is available at https://bugcrowd.com/hubspot.

Customer Data Protection

Logical Tenant Separation

HubSpot provides a highly scalable, multi-tenant SaaS solution. The HubSpot user interface and APIs restrict access to authorized content exclusively. HubSpot logically segments the data using portal IDs and associates that unique ID with all data and objects specific to a customer. Information is made available via the user interface or APIs to be produced for a specific HubSpot portal, without the risk of cross-portal access or data pollution.

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.

Confidential Information

The HubSpot products are an integrated marketing, sales, services, content management, and operations experience. The information collected in our products is data gathered through lead or customer interaction, public directories, and reputable third party sources.

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 capture only appropriate information to support their marketing, sales, services, content management, and operations processes. The HubSpot products should not be used to collect or capture sensitive data such as credit or debit card numbers, personal financial account information, Social Security numbers, passport numbers, driver's license numbers employment, financial or health information.

Further detail on the classification of data used and supported by the HubSpot system can be found within the Data Classification table in our SOC 2 report.

Encryption In-Transit and At-Rest

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.

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. Certain email features work by providing an additional level of both at-rest and in-transit encryption.

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 a frequency that's dependent upon the sensitivity of the data they're encrypting. 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 details.

Additionally, we provide real-time updates and historical data on system status and security 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 a disaster recovery plan that is tested annually as a part of our SOC 2 controls. Please refer to our SOC 2 report (downloadable at hubspot.com/security) 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 their 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 on HubSpot product infrastructure networks and access control lists on the file systems storing the backup files.

CUSTOMER BACKUP OPTIONS

For customers who would additionally like to back up their data, the HubSpot platform provides many ways of making sure you have what you need. Many of the features within

your HubSpot portal contain export features, and the HubSpot library of public APIs can be used to synchronize your data with other systems. For the details about backing up your data, please check out 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 users of their portals and assign the privileges that are appropriate for their accounts and limit access to their data features.

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 built-in HubSpot login, "Sign in with Google" login, or Single Sign On (SSO). The built-in 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 built-in login cannot change the default password policy.

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

Customers who use an SSO provider can set up SSO-based login for their users. 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 with their Google accounts.

Customers who use HubSpot's built-in login are also encouraged to set up two-factor authentication for their HubSpot accounts, and portal administrators can configure their HubSpot portals to ensure that all users have two-factor authentication enabled.

Product API Authorization

Application programming interface (API) access is enabled through either API key or Oauth (version 2) authorization. Customers have the ability to generate API keys for their portals. The keys are intended to be used to rapidly prototype custom integrations. HubSpot's Oauth implementation is a stronger approach to authenticating and authorizing API requests. Additionally, Oauth is required of all featured integrations. Authorization for Oauth enabled requests is established through defined scopes. For more information about API use, please see the Developers portal at HubSpot.com.

Production Infrastructure Access

Access to HubSpot's systems is strictly controlled and follows the principle of least privilege. HubSpot employees are granted access using a role based access control (RBAC) model.

Day to day access is minimized to only the individuals whose jobs require it. For emergency access (e.g. alerts responses/troubleshooting) and access to administrative functions, HubSpot's system uses a Just-In-Time-Access (JITA) model in which users can request access to privileged functions for a limited duration. Each JITA request is logged, and logs are continuously monitored for anomalous requests. After the configured session limit, access to the account expires and is automatically revoked.

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.

Employee access to both corporate and production resources is subject to daily automated review and at least semi-annual manual recertification.

HubSpot Employee Access to Customer Portals

Customer Support, Services, and other customer engagement staff may request JITA to customer portals on a time limited basis. Requests for access are limited to their work responsibilities associated with supporting and servicing our customers. The requests are

limited to a specific customer's portal for a maximum 24-hour period. All access requests, logins, queries, page views and similar information are logged.

Corporate Authentication and Authorization

Access to the Corporate network, both remotely and while in office, requires multi factor authentication (MFA), and any SaaS applications in use by HubSpot require SSO with MFA in order to facilitate centralized access control.

Password policies follow industry best practices for required length, complexity, and rotation frequency.

We built an extensive set of support systems to streamline and automate our security management and compliance activities. In addition to many other functions, the system sweeps our product and corporate infrastructure several times daily to ensure that permission grants are appropriate, to manage employee events, to revoke accounts and access where needed, to compile logs of access requests, and to capture compliance evidence for each of our technology security controls. These internal systems sweep the infrastructure validating that it meets approved configurations on a 24-hours basis.

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 define employee's security responsibilities in protecting company assets/data (including, but not limited to protecting mobile devices, and securing corporate equipment).

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 - the policy covers data handling requirements, privacy considerations, and responses to violations, among many other topics.

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 well trained for their roles. Security awareness training that covers general security best practices is offered to all new HubSpot employees upon hire, and on an annual basis. In addition to awareness training, HubSpot keeps employees aware of recent security news or initiatives with internal knowledge articles.

After initial training, more specialized content is available based on an employee's role or resulting access. For example HubSpot has a Security Advocates program, where developers on the product teams have opportunities for additional training on security development, common risk, threats, and issues.

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 via a ticketing system 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 at hubspot.com/security).

Vendor Management

We leverage a number of third party service providers who augment the HubSpot products' ability to meet your marketing, sales, services, content management, and operations needs. 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, 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 guards are employed 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 many other protective measures are implemented across HubSpot offices.

Corporate Network Protections

Centrally managed application firewalls are deployed for High Availability at HubSpot Corporate offices. Our guest networks are separate from our corporate network, and are serviced by separate firewalls. Firewalls are set up to filter unauthorized inbound traffic from the Internet and are configured to deny inbound network connections that are not explicitly authorized by a rule.

HubSpot enforces system compliance checks prior to authorizing a device's connection to the Corporate network. Unauthorized devices are disconnected immediately or moved to containment VLANs.

Endpoint Protection and Antivirus/Malware Protection

HubSpot leverages Endpoint Detection and Response (EDR) capabilities to protect its systems. This enables us to have extensive visibility into anomalous system behavior as well as to rapidly investigate and take appropriate action through either automated event triggers or manual containment of a system. Our EDR platform is integrated with other tools in our security stack so as to create an optimized, multi-tooled ecosystem to effectively defend our business.

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. Pre-defined 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.

In responding to any incident, we first determine the exposure of the information and determine the source of the security problem, if possible. We provide periodic updates as needed to ensure appropriate resolution of the incident.

Our Chief Information Security Officer 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.

In addition to our SOC, HubSpot also has an internal Threat Hunter team that works to systematically discover any vulnerabilities and ensure best practices are in place to secure our product.

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 here on our Investor Relations page here: https://ir.hubspot.com/

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 as they map to Trust Service Principles (TSPs) established by the American Institute of Certified Public Accountants (AICPA). We are proud of the excellence of our controls and invite you to obtain a copy of our SOC 2 Type 2 report by contacting your HubSpot representative. Our SOC 3 is available for public download from the HubSpot Security page (hubspot.com/security).

Sensitive Data Processing and Storing

Please see our Terms of Service (legal.hubspot.com/terms-of-service) for details about prohibited data types. The HubSpot products should not be used to collect or capture sensitive data such as credit or debit card numbers, personal financial account information, Social Security numbers, passport numbers, driver's license numbers or similar identifiers, or employment, financial or health information.

Many healthcare customers utilize HubSpot for their front-office needs without incorporating sensitive healthcare information. However, 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 and built with customer needs and privacy considerations in the forefront. Our privacy program incorporates best practices, customers' and their contacts' needs, as well as regulatory requirements.

Data Retention / 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 several other 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
- Product 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.

We also 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: here.

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.