Security Overview

Last Update: January 2021

Table of Contents

HubSpot Security Overview

1 Our Company and Products

HubSpot is the world's leading inbound marketing, sales, and services platform. Since 2006, HubSpot has been on a mission to make the world more inbound. Today, tens of thousands of customers in more than 90 countries use HubSpot's software, services, and support to transform the way they attract, engage, and delight customers. HubSpot's inbound marketing software, ranked #1 by VentureBeat, GetApp, Capterra, and G2Crowd, includes social media publishing and monitoring, blogging, SEO, website content management, email marketing, and reporting and analytics, all in one integrated platform. HubSpot Sales Hub and CRM, HubSpot's award-winning sales applications, enables sales and service teams to have more effective conversations with leads, prospects, and customers. HubSpot Service Hub is the best solution for creating frictionless and delightful customer experiences.

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.

2 HubSpot Security and Risk Governance

HubSpot's primary security focus is to safeguard our customers' and users' 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 Enterprise Security and Product Security teams. These teams are responsible for the 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 Security Officer, who reports to the Chief Operating Officer, oversees the implementation of security safeguards across HubSpot and its products.

3 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 – implement process and controls to align with current international regulatory and industry best practice guidance. We have designed our security program around best-of-breed guidelines for cloud security. In particular, we leverage standards like COBIT and Cloud Security Alliance CCM, and align our practices with ISO 27001 and NIST SP 800-53.

4 HubSpot Security Controls

In order to ensure we protect data entrusted to us, we implemented an array of security controls. HubSpot's security controls are designed to allow for a high level of employee efficiency without artificial roadblocks, while minimizing risk. The following sections describe a subset of controls. For more

information about the HubSpot security program, please check out all the details at https://www.hubspot.com/security.

4.1 HubSpot Product Infrastructure

4.1.1 Data Center Security

HubSpot outsources hosting of its product infrastructure to leading cloud infrastructure providers. Principally, the HubSpot product leverages Amazon Web Services (AWS) and Google Cloud Platform (GCP) for infrastructure hosting. These solutions provide high levels of physical and network security and well as hosting provider vendor diversity. At present, HubSpot's AWS cloud server instances reside in US locations; GCP cloud instances reside in Germany. Both providers maintain an audited security program, including SOC 2 and ISO 27001 compliance. HubSpot does not host any product systems within its corporate offices.

These world-class infrastructure providers leverage the most advanced facilities infrastructure such as power, networking, and security. Facilities uptime is guaranteed between 99.95% and 100%, and the facilities ensure a minimum of N+1 redundancy to all power, network, and HVAC services. Access to these providers' sites is highly restricted to both physical access as well as electronic access through public (internet) and private (intranet) networks in order to eliminate any unwanted interruptions in our service to our customers.

The physical, environmental, and infrastructure security protections, including continuity and recovery plans, have been independently validated as part of their SOC 2 Type II and ISO 27001 certifications. Certificates are available at the AWS compliance site and Google Cloud Platform security site.

4.1.2 Network Security & Perimeter Protection

The HubSpot product infrastructure is built with internet-scale security protections in mind. In particular, network security protections are designed to prevent unauthorized network access to and within the internal product infrastructure. These security controls include enterprise-grade routing and network access control lists (firewalling).

Network-level access control lists are implemented in AWS Virtual Private Cloud (VPC) security groups or GCP firewall rules, which applies port- and address-level protections to each of the server instances in the infrastructure. These firewalling technologies deny unintended traffic by default, and all network traffic is logged and used to inform our monitoring systems (more about that in Section 4.1.4). These network access rules allow for finely grained control of network traffic from a public network as well as between server instances on the interior of the infrastructure. Within the infrastructure, internal network restrictions allow a many-tiered approach to ensuring only the appropriate types of devices can communicate.

Changes in the network security model are actively monitored and controlled by standard change control processes. All existing rules and changes are evaluated for security risk and captured appropriately.

4.1.3 Configuration Management

Automation drives HubSpot's ability to scale with our customers' needs. The product infrastructure is a highly automated environment that flexibly expands capacity and capability as needed. Server instances are fully puppetized, meaning that any server's configuration is tightly controlled from birth through deprovisioning.

All server type configurations are embedded in images and Puppet 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 and configuration control is typically handled 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.

4.1.4 Alerting & Monitoring

Not only does HubSpot fully automate its build procedures, we invest heavily in automated monitoring, alerting and response technologies 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, 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 foreseen situations. Traffic blocking, quarantine, process termination, and similar functions kick in at pre-defined thresholds to ensure that the HubSpot platform can protect itself against a wide variety of undesirable situations.

The power behind HubSpot's ability to detect and respond to anomalies is our 24x7x365 monitoring program and extensive logging. Our systems capture and store logs that include all the technologies that comprise our products. At the application layer, all logins, page views, modifications, and other access to HubSpot portals are also logged. In the infrastructure back-end, we log authentication attempts, horizontal and vertical permission changes, infrastructure health, and requests performed. among many other commands and transactions. Logs and events are monitored in real time and events are escalated immediately at any hour of the day to developers, security professionals, and engineers to take appropriate action.

4.1.5 Infrastructure Access

Entire categories of potential security events are prevented with a stringent, consistent, and well-designed access control model. Along those lines, access to HubSpot's systems is strictly controlled. HubSpot employees are granted access to corporate services, HubSpot sales and marketing portals, and product infrastructure based on their jobs, using a role-based access control model. More information about HubSpot's RBAC model across the company is available in section 4.3.

For access to infrastructure tools, servers, and similar services, access is minimized to only the individuals whose jobs require it. For emergency access and access to administrative functions, HubSpot's system use a Just-In-Time-Access (JITA) model in which users can request access to privileged functions for a limited duration.

Users are assigned the privileges to make JITA requests by business unit and team. When non-standard, emergency access is needed, like sudo access on a Linux server, the user makes a JITA request. The JITA request is logged, and logs are continuously monitored for anomalous requests. Access to the privileged function is granted, and the person can go about his or her work.

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.

4.2 Application Protection

4.2.1 Web Application Defenses

As part of its commitment to protecting customer data and websites, HubSpot implemented an industry recognized Web Application Firewall (WAF). The WAF automatically identifies and protects against attacks aimed at the HubSpot products or customer sites hosted on the platform. HubSpot's WAF protects HubSpot platform access (e.g., the features you can access by browsing to https://app.hubspot.com or integrating with APIs available at https://api.hubapi.com). Additionally, all customer content hosted on the platform is also automatically protected. 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) in the OWASP Top 10 and similar recommendations. Protections from Distributed Denial of Service (DDoS) attacks are also incorporated, helping to ensure that customers' sites and other parts of the HubSpot products are available continuously.

The WAF is configured with a combination of industry standard and custom rules that are capable of automatically enabling and disabling of 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.

4.2.2 Development & Release Management

One of HubSpot's greatest advantages is a rapidly-advancing feature set, and we provide constantly improving products through a modern continuous delivery approach to software development. New code is proposed, approved, merged and deployed thousands of times daily. Code reviews and quality assurance are performed by specialized teams of engineers with intimate knowledge of the HubSpot platform as it is developed. 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. If all passes, the new code is deployed automatically across the application tier.

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.

As part of the continuous deployment model, we use extensive software gating and traffic management to control features based on customer preferences (private beta, public beta, full launch). Major feature changes, are communicated through in-app messages and/or product update posts.

Newly developed, built 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 and undesirable access between QA and production environments. Customer data is never used by HubSpot in the QA environment, nor does any other testing use customer data.

4.2.3 Vulnerability Scanning, Penetration Testing, & 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. We perform hundreds of vulnerability scanning and penetration testing activities against ourselves on a continuous basis. We perform vulnerability scanning continually against our internal networks, applications, and corporate infrastructure. Network-based and application-level vulnerability scans run at least daily to ensure that we detect and respond to the latest vulnerabilities. Static code analysis automatically reviews the most current code to detect potential security flaws early in the development lifecycle.

Continually running scans, adaptive scanning inclusion lists, and continuously updating vulnerability signatures help HubSpot stay ahead of many security threats. To get a second opinion about our ability to identify and respond to security risks, we bring in industry-recognized third parties to perform four 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, and penetration testers are given internal access to the HubSpot product and/or corporate networks in order to maximize the kinds of potential vectors that should be evaluated.

In addition to internal vulnerability scanning and independent penetration testing, HubSpot manages a bug bounty program. Independent security researchers are invited to participate in identifying security flaws in the HubSpot products and are rewarded for their submissions. 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.

4.3 Customer Data Protection

4.3.1 Confidential Information in the HubSpot Products

The HubSpot products are an integrated marketing, sales, and customer service experience. The information collected in our products is data gathered through lead or customer interaction, public directories, and reputable 3rd party sources. HubSpot's tools allow customers to define the type of information to be collected stored on their behalf. Per the HubSpot Terms of Service and Acceptable Use Policy, our customers ensure that they capture only appropriate information to support their marketing, sales, and service processes. The HubSpot products are not 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.

4.3.2 Credit Card Information Protection

Many HubSpot customers pay for the service by credit card. HubSpot does not store, process or collect credit card information submitted to us by customers. We leverage trusted and PCI-compliant payment vendors to ensure that customers' credit card information is processed securely and according to appropriate regulation and industry standards.

4.3.3 Encryption In-Transit & At-Rest

All sensitive interactions with the HubSpot products (e.g., API calls, login, authenticated sessions to the customer's portal, etc.) are encrypted in-transit with TLS 1.0, 1.1, 1.2, or 1.3 and 2,048 bit keys or better. Transport layer security (TLS) is also available by default for customers who host their websites on the

HubSpot platform. Please see our website setup guide for more information about configuring TLS. Customers who would like to limit the encryption protocols used for HTTPS connections may start the process by contacting Customer Support or their Customer Success Manager.

HubSpot leverages several technologies to ensure stored data is encrypted at rest. The physical and virtualized hard drives used by HubSpot product server instances as well as long-term storage solutions like AWS S3 use AES-256 encryption. Additionally, certain databases or field-level information is encrypted at rest, based on the sensitivity of the information. For instance, user passwords are hashed and certain email features work by providing an additional level of both at-rest and in-transit encryption.

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, and the frequency varies by the type of key and the sensitivity of the key and the data it protects; in general, TLS certificates expire every two years.

4.3.4 User 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. 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. Customers who use a Single Sign On (SSO) provider can set up SSO-based login for their users. Instructions for setting up SSO are available on the 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.

4.3.5 User and API Authorization

Customers can assign finely grained permissions 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.

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.

4.3.6 HubSpot Employee Access

HubSpot controls individual access to data within its production and corporate environment. A subset of HubSpot's employees are granted access to production data based on their role in the company through role based access controls (RBAC) or on an as-needed basis referred to as JITA (just in time access).

Engineers and members of Operations teams may be granted access to various production systems, as a function of their role. Common access needs include alert responses and troubleshooting, as well as to

analyze information for product investment decisions as well as product support. Access to the product infrastructure is limited by network access and user authentication and authorization controls. Access to networking functions is strictly limited to individuals whose jobs require that access, and access is reviewed on a continual basis.

Customer Support, Services, and other customer engagement staff with a need-to-know may request just in time access 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 just-in-time access to a specific customer's portal for a maximum 24 hour period. All access requests, logins, queries, page views and similar information are logged.

All employee access to both corporate and product resources is subject to daily automated review and at least semi-annual manual recertification to ensure the granted authorization is appropriate for an employee's role and job needs.

4.4 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 been 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.

Along those lines, HubSpot is certified under the EU-US and Swiss-US Privacy Shield Frameworks. More information about our certification is available on the Privacy Shield site.

4.4.1 Data Retention Policy

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, as they see fit. 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.

4.4.2 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 and Data Processing Agreement.

4.5 Business Continuity & Disaster Recovery

HubSpot maintains business continuity and disaster recovery plans focusing both on preventing outage through redundancy of telecommunications, systems and business operations, and on rapid recovery strategies in the event of an availability or performance issue. Whenever customer-impacting situations occur, HubSpot's goal is to quickly and transparently isolate and address the issue. Identified issues are published on HubSpot's status site and are subsequently updated until the issue is resolved.

4.5.1 System Reliability & Recovery

Business continuity testing is part of HubSpot normal processing. HubSpot recovery processes are validated continuously through normal maintenance and support processes. We follow continuous deployment principles, and create or destroy many server instances daily as part of our regular maintenance and growth. We also use those procedures to recover from impaired instances and other failures, allowing us to practice our recovery process every day.

HubSpot primarily relies on infrastructure redundancy, real time replication and backups. 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.

4.5.2 Backup Strategy

HubSpot ensures data is replicated and backed up in multiple durable data-stores. The retention period of backups depends on the nature of the data. Data is also replicated across availability zones and infrastructure locations in order to provide fault-tolerance as well as scalability and responsive recovery, when necessary.

- Customer (production) data is backed up leveraging multiple online replicas of data for immediate data protection. All production databases have no less than 1 primary (master) and 1 replica (slave) copy of the data live at any given point in time. Seven days worth of backups are kept for any database in a way that ensures restoration can occur easily. Snapshots are taken and stored to a secondary service no less often than daily and where practicable, real time replication is used. All production data sets are stored on a distributed file storage facility like Amazon's S3.
- Because we leverage private cloud services for hosting, backup and recovery, HubSpot does not implement physical infrastructure or physical storage media within its products. HubSpot does also 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.
- By default, all backups are protected through access control restrictions on HubSpot product infrastructure networks, access control lists on the file systems storing the backup files and/or through database security protections.
- 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 Knowledge Base article about exporting your content.

4.6 HubSpot Corporate Security

4.6.1 Employee Authentication & Authorization

HubSpot enforces an industry-standard corporate password policy. That policy requires changing passwords at least every 90 days. It also requires a minimum password length of 8 characters and complexity requirements including special characters, upper and lower case characters, and numbers. HubSpot prohibits account and password sharing by multiple employees.

Employees generally authenticate to HubSpot product infrastructure using SSH keys. Where passwords are allowed, the password policy requires 12 character passwords. Additionally, all of the tools we use to build the HubSpot products leverage multi-factor authentication or are protected by single-sign on solutions that enforce multi-factor authentication.

4.6.2 Access Management

HubSpot has regimented and automated authentication and authorization procedures for employee access to HubSpot systems, including the marketing and sales platforms. All access is logged. Most frequently, access is granted based on a role-based access control model. Just in time access is built into automated procedures around a set of rigorous authorization mechanisms.

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.

4.6.3 Background Checks

HubSpot employees undergo an extensive 3rd party background check prior to formal employment offers, wherever local regulations and employment standards allow. In particular, employment, education, and criminal checks are performed for potential employees. Reference verification is performed at the hiring manager's discretion. All employees must comply with Non-Disclosure Agreements and Acceptable Use Policy as part of access to corporate and production networks.

4.6.4 HubSpot 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.

4.6.5 Vendor Management

We leverage a small number of 3rd party service providers who augment the HubSpot products' ability to meet your marketing, sales, and service 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 team, General Counsel, and the business unit who owns each contract coordinate unique considerations for our providers as part of contract management.

4.6.6 Security Awareness & Security Policies

To help keep all our engineering, support, and other employees on the same page with regard to protecting your data, HubSpot developed and maintains a Written Information Security Policy. The policy covers data handling requirements, privacy considerations, and responses to violations, among many other topics.

With this policy and the myriad protections and standards in place, we also ensure HubSpot employees are well-trained for their roles. Multiple levels of security training are provided to HubSpot employees, based on their roles and resulting access. General security awareness training is offered to all new employees and covers HubSpot security requirements. After initial training, different training tracks are available based on an employee's role. Developer-specific training is provided by and tailored to HubSpot's engineering teams. Role-specific security awareness training for Services & Support, Sales, and many other roles is tailored for the unique considerations of the role. Recurring training is provided through regular updates, notices, and internal publications.

4.7 Incident Management

HubSpot 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 communicate back to the customer (and any other affected customers) via email or phone (if email is not sufficient). We provide periodic updates as needed to ensure appropriate resolution of the incident.

Our Chief 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.

5 Product Security Features

HubSpot's security program is designed to protect all of the HubSpot products. Each product takes advantage of common application development security best practices as well as infrastructure security and high availability configurations.

Whether our products are free or paid, feature-rich or lightweight, HubSpot works hard to maintain the privacy of data you entrust with us. Data you store in HubSpot products is yours. We put our security program in place to protect it, and use it only to provide the HubSpot service to you. We never share your data across customers and never sell it.

5.1 HubSpot Marketing Hub

About: The HubSpot marketing product is our industry-leading marketing automation solution. It provides easy-to-use and effective tools to manage your inbound marketing strategy.

Hosting: Primary Content Management System (CMS) infrastructure is hosted in Amazon Web Services and Google Cloud Platform. HubSpot's hosting strategy enables additional redundancy capabilities, architecture flexibility, and infrastructure responsiveness. Our deployment processes leverage network security, server security, and availability features, described above.

Web Application Firewall: Customer sites hosted on the HubSpot products leverage the protections of our world-class Web Application Firewall (WAF). By default, your HubSpot-hosted website, blogs, landing pages, and other online presence is protected from state-of-the-art Distributed Denial of Service (DDoS) and other web application attacks. When security events occur, HubSpot's Security Operations and DevOps teams take immediate action to ensure that your sites are protected continuously 24x7x365.

Transport Layer Security: HubSpot marketing customers have the ability to enable and configure TLS services for their sites, landing pages, and related visitor engagement. By default, TLS certificates use Subject Alternative Names and are managed through our content delivery provider. For more information about how to get started, please see this Academy article.

Encryption Options: By default, customer websites using HTTPS are configured to allow TLS 1.0, 1.1, 1.2, and 1.3. It is possible to remove support for one or more of these protocols. Customers may also opt into enabling HTTP Strict Transport Security (HSTS) for their HubSpot-hosted domain. To make these changes, please contact HubSpot Support or your Customer Success Manager.

5.2 HubSpot CRM

About: The HubSpot CRM is one of the many products your sales team will love. Sales professionals can start using CRM for no cost and with no headaches. Getting started with HubSpot CRM takes minutes at HubSpot's CRM product page.

Secure by default: CRM takes advantage of the same sophisticated security measures that help protect all other HubSpot products. We leverage the advanced secure software development processes, infrastructure management, and alerting methodologies that we have honed in our years of product development.

Email Integrations & Connected Inbox: As a CRM user, you have the ability to connect your Gmail, Office365, or IMAP-enabled email inbox. Gmail and Office365 integrations are authorized by and protected by the native integration capabilities in those platforms. IMAP integration allows your connected inbox to synchronize mail into your CRM from other mail services. When a user sets up an

IMAP integration, the HubSpot products act as an IMAP client. The services that support IMAP integrations have many built-in protections: data is encrypted in transit from end-to-end; the data is encrypted at rest at the field level as well as at the database level; and access controls ensure only authorized access to the data.

Privacy: Whether our products are free or paid, HubSpot always maintains the privacy of data you entrust with us. Data you store in HubSpot products is yours. We use it only to provide service to you.

Hosting: CRM infrastructure is hosted in Amazon Web Services, taking advantage of the infrastructure redundancy and flexibility that exists throughout HubSpot's infrastructure. Our hosting strategy also helps ensure world class infrastructure and network security and availability.

Access control: The HubSpot CRM provides easy to manage and intuitive roles that give the right access to the right sales team members. Please see our Knowledge article for more information about user roles.

5.3 HubSpot Sales Hub

About: The HubSpot Sales products include HubSpot's award-winning suite of sales tools that help professionals better engage with their leads and improve conversion.

Hosting: Primary Sales backend infrastructure is hosted in Amazon Web Services. Our hosting strategy takes advantage of the infrastructure redundancy and flexibility that exists throughout HubSpot's infrastructure.

Data storage: HubSpot Sales stores email message metadata in order to provide email tracking, link wrapping, and Connections services. Data is stored in protected stores within the HubSpot infrastructure, and access to the data is tightly controlled. Access to the data stores is assigned to a limited to a small set of HubSpot employees based on their roles, and access is limited to the individuals who need it in order to respond to customer support and related requests.

Seamless updating: Sales tools are designed to help increase your productivity. One step we've taken to improve your experience is automatically updating the plugin. Instead of being interrupted by recurring notifications to update your software, the plugin handles its updating process without getting in your way.

5.4 HubSpot Service Hub

About: The HubSpot Service Hub includes all of the features needed to delight your customers. Service Hub includes the ability to seamlessly track conversations and empowers visitors with sophisticated bot technology.

Hosting: Primary Service Hub backend infrastructure is hosted in Amazon Web Services. Our hosting strategy takes advantage of the infrastructure redundancy and flexibility that exists throughout HubSpot's infrastructure.

Seamless updating: Service Hub tools are designed to help keep customers engaged in the services offered. Service Hub tools are automatically updated on a recurring basis to ensure that you have the right features for your customer service needs.

6 Compliance

HubSpot maintains compliance with the EU-US Privacy Shield. The HubSpot platform also contains features that enable our customers to easily achieve and maintain their General Data Processing Regulation (GDPR) compliance requirements. More information about privacy compliance and the HubSpot products are available in our GPDR compliance content and the HubSpot DPA.

HubSpot's products are housed with world-class cloud infrastructure providers Amazon Web Services and Google Cloud Platform. HubSpot infrastructure providers are SOC 2 Type II and ISO 27001 certified and maintain facilities secured against electronic and physical intrusion.

7 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.