BIGCOMMERCE

BigCommerce Infrastructure and Platform Security Guide

2020

Introduction

Your business is everything. At BigCommerce we know that to meet the demands of a large organization you have greater requirements for availability, scalability, reliability, performance and security, etc. Thus, choosing the right platform to power your online presence requires careful deliberation and diligence.

This guide lays out top concerns and requirements of technology leaders, and demonstrates how BigCommerce is specifically designed to power current and future merchant success.

Infrastructure

BigCommerce is a multi-tenant SaaS ecommerce platform that helps to lower your total cost of ownership; your organization is not responsible for maintaining servers, installing updates or patching the servers when security vulnerabilities are discovered. With SaaS, your staff can be reallocated to spend more time on innovation and less time on tactical maintenance.

Data centers

The BigCommerce platform is hosted within Google Cloud Data Centers in the United States. We use the Google Cloud Platform because it is the industry's fastest, most flexible and secure cloud hosting infrastructure.

Backed by a rigorous system of independent verifications that certify the platform's security, privacy and compliance controls, Google Cloud provides additional protection for BigCommerce merchants via its multi-layered approach to security, global infrastructure and round-the-clock monitoring, resulting in unprecedented resilience against DDoS attacks and other malicious behavior.

Some ancillary services not integral to running the BigCommerce platform are hosted on Amazon Web Services.

For production traffic, we utilize Google Cloud's U.S. Central region as our primary data storage location. Across this region, the BigCommerce infrastructure is replicated across multiple availability zones. Cardholder Data Environments are logically separated from non-Cardholder Data Environments.

Through these data centers and our strict adherence to PCI DSS standards, each BigCommerce store is protected by multiple layers of security to prevent unauthorized access. This includes perimeter and server-specific firewalls, file integrity scanners, intrusion detection software, web application firewalls and 24/7 monitoring. You can read more about this in the PCI DSS section. Google Cloud makes their SOC2 reports available upon request.

Content delivery network (CDN)

Many online services use a content delivery network (CDN) to deliver photos and other web content and files more efficiently. This improves site speed, which is used by Google and other search engines as a ranking signal for search results. The CDN simultaneously hosts copies of commonly used files at several data centers (nodes) around the world. Files are delivered by the node closest to the shopper, decreasing the distance data has to travel enabling the site to load faster. At no additional charge, BigCommerce's ecommerce hosting includes the industry-leading CDN, Akamai and the Akamai Image Manager, an automated image optimizer to help sites load faster no matter a browser's origin.

Software as a Service (SaaS) methodology

Because we are a SaaS platform, BigCommerce can place new code into production at any time to deliver value to merchants or correct issues that have arisen. The Engineering team at BigCommerce pushes code to the production environment at least three times a day. When releasing this often, it is essential that new features, bug fixes and other improvements do not disrupt the merchants that rely on our platform. All code released to production undergoes rigorous review before release, and performance testing tools are triggered automatically during QA testing. Additionally, our Information Security team reviews all payment-sensitive code before release. More information about development practices concerning payment data and personally identifiable information can be found in the Platform Security section. The BigCommerce core application is written in PHP, Ruby and Scala.

Uptime, traffic spikes and load balancing

You can't sell if you're offline. Whether it's the malicious traffic of a DDoS attack or the high-volume traffic associated with holiday shopping, BigCommerce has the stability to keep you selling. Our platform's uptime is markedly higher than the industry average at 99.99%. This means with BigCommerce the potential for store downtime would only be a few minutes annually compared to nearly two days with other commerce providers.

The BigCommerce platform undergoes regular load and performance testing to maintain this uptime. We have an internal model that tells us how many requests per second we can serve with acceptable performance and can scale linearly by adding more application servers. We always carry a minimum of twice our peak load in server capacity, scaling up or down when necessary.

BigCommerce engineers use many internal and external tools and services to monitor our platform. For external performance and availability monitoring, trending and alerting, we use AlertSite and Uptime Cloud Monitor. We also use third-party cloud services for Nagios monitoring, as well as our own internal Nagios servers. For more specific application-based metrics, we utilize Graphite, Grafana and New Relic. We also have an extensive internal log analysis system built using Elasticsearch, Logstash and Kibana.

Distributed Denial of Service (DDoS) attack protection

BigCommerce uses Google Cloud DDoS mitigation services. Our Technical Operations team, which is on call 24/7/365, ensures mitigation occurs instantly. All DDoS protection is provided at no extra cost to all BigCommerce customers.

High availability infrastructure

BigCommerce operates on a High Availability (HA) durable infrastructure that allows us to ensure better uptime, resiliency and performance for our merchants. This environment provides cost-effective failover protection against hardware and operating system outage where stores are not assigned to a single server which eliminates any single points of failure. The HA environment allows us to increase capacity for all stores just by adding new servers in the appropriate spot. We can provision more servers to handle higher traffic, and all stores will see the benefits.

HTTPS, SSL and TLS

BigCommerce knows trust is a huge factor in closing the deal in any transaction. Our platform enables HTTPS, the secure version of HTTP, which increases site security and shopper trust while improving your site's search ranking.

BigCommerce supports TLS v1.2, and all merchants have a shared TLS certificate by default which is used on a .mybigcommerce.com domain. Once a merchant applies a custom domain name to their store, BigCommerce will automatically provision a free private SSL via Encryption Everywhere. Additionally, merchants can choose to use a third-party TLS certificate or purchase a True BusinessID w/ EV certificate for extended verification.

Platform security

Security is the utmost concern of any technology leader. Every part of the BigCommerce platform is built with security top of mind.

ISO/IEC 27001:2013

BigCommerce is certified as ISO/IEC 27001 compliant, which ensures a comprehensive and continually improving model for security management. ISO/IEC 27001 outlines and provides the requirements for an information security management system (ISMS), specifies a set of best practices, and details the security controls that can help manage information risks, ensuring a secure e-commerce platform for our customers.

Data security

Payment Card Industry Data Security Standard (PCI DSS)

The main governing document for security in the payments industry is the Payment Card Industry Data Security Standard (PCI DSS). BigCommerce is certified as a PCI DSS 3.2 Level 1 Service Provider, which protects against credit card data breaches and eliminates the massive cost and hassle of handling compliance yourself. The standards include rules on access approvals, restriction of access based on the principle of least privilege, patching and incident response, to name a few. There is an extensive security policy and procedure governing PCI Compliance.

The BigCommerce Cybersecurity team:

- Audits our environment daily by reviewing logs from our Intrusion Detection and File Integrity Monitoring systems
- Review sections of code that are sensitive to PCI concerns when changes are proposed
- Performs Internal/External Penetration Testing regularly
- Hires an external PCI compliance vendor to audit our environment annually and certify our compliance at Level 1
- Hires both internal and external ISO/IEC ISO27001 auditors annually to certify our information security management system.
- Is organized around, and aligned with NIST 800-53 controls
- Conducts continuous vulnerability scanning
- Adheres to jurisdictional privacy requirements, such as GDPR, CCPA and Australian Privacy Act

Additionally, with BigCommerce:

- Security updates are automated
- Sensitive payments data (including PAN, CVV2 and expiration date) are encrypted in transit and are not allowed to come to rest on BigCommerce infrastructure
- All employees are trained on secure practices to comply with PCI DSS based on the following documentation:
- Secure Coding Practices section to **learn more about our secure coding and business practices.**
- **BigCommerce's PCI DSS Attestation of Compliance.**
- Our merchants are provided with tools to manage the security and privacy of their store.
- Our merchants are provided with their own database in which to store their customer information.

Secure infrastructure

All systems are kept on Debian Linux Long Term Support (LTS) and patches are applied at least weekly. Highly critical security patches (such as Heartbleed and POODLE) are applied automatically without downtime, freeing up your technology resources. Firewall logs are monitored daily for security policy violations and intrusion attempts. We perform penetration testing annually and employ several different technologies for guarding against malware and spam.

Secure coding and business practices

BigCommerce follows both ISO27001 and PCI DSS 3.2.1 requirements for secure development practices and training for our developers. We follow best practices from NIST, OWASP and CIS. We have a secure product development framework in place that includes continuous integration and deployment, integrated static and dynamic code analysis, open source code analysis and regular manual penetration testing. We partner application security engineers with each development team. All of our employees undergo Information Security training during onboarding, and again annually. All developers must take a day-long Secure Development Training before being given access to the codebase and they must update their training annually or their access is revoked. Finally, we conduct security scans of our production infrastructure after each code release.

Data backup and disaster recovery

All BigCommerce stores have their data replicated and are active in four data centers for greater redundancy and availability. These data centers are spatially separated to mitigate any potential failure. Production servers are backed up once per day to remote backup servers. Remote storage of backups ensures that merchant customer data captured via the backup process will survive a disaster impacting all production data centers, and will be available for restoration on alternative servers.

Summary and further resources

BigCommerce has made significant investments in its platform security and infrastructure to ensure you feel confident choosing us to host your ecommerce store. For more back-end information on the BigCommerce platform, read:

- The Current and Future State of Ecommerce Security
- Securing Your Ecommerce Site Against Cyber Threats
- Site-Wide HTTPS on BigCommerce
- SSL Certificate Overview