Website Security for e-Commerce

What you need to know about current threats to your business and how to protect your website

prepared by Section

Section

Table of Contents

Why e-Commerce Sites Need Better Security

Now more than ever, e-commerce websites need to be aware of and protected from the wide range of cyber attacks that can compromise websites and their customers.

In the past few years it's seemed like there has been a new widespread security breach every other week. High profile incidents such as Heartbleed and WannaCry and hacks of notable entities including Sony Pictures and the Democratic National Committee have brought cybersecurity to the front of people's minds. The magnitude of Distributed Denial of Service (DDoS) attacks has risen with the increased number of devices connecting to the Internet, and as more of the population engages with these devices the risk of sensitive information being taken advantage of continues to rise.

Bank accounts, credit card information, health care data, tax returns and personal identifying information are now regularly submitted online or stored in a network that could be vulnerable. Markets on the so-called "dark web" that sell stolen information can wreak havoc by enabling others to charge money to someone's account or even steal their identity. Connected Internet of Things devices like fridges, home security systems and even cars can be taken over remotely, bringing severe consequences.

Of course, some of these examples point to the worst case situations. But they demonstrate that all Internet users need to be aware of the security of websites they visit, and websites themselves need to be increasingly aware of the security lapses they could face. In this white paper, we will focus specifically on website security in the e-commerce industry. Online retail stores are becoming more and more prevalent, with almost 400 billion dollars being spent online in the US alone. Pew Research found that 79% of American adults have used e-commerce sites to purchase books, clothes, makeup, and household essentials. Among people under the age of 30 that number is even higher: 90% have bought something online and 77% have used their mobile phone for an e-commerce purchase.

E-commerce sites of all sizes are susceptible to attack because they process credit card information, email addresses, and passwords for user accounts. If not properly secured, credit card numbers can be taken and email/password combinations can be tried on other websites. In the following sections we will go through what security issues e-commerce sites face and the tools they can use to secure their sites and reassure visitors.

Threats Posed To e-Commerce Sites

1 Known Vulnerabilities

Any software you are using, including your e-commerce platform and extensions, will have certain vulnerabilities that are known to attackers. These could include ways to access your site through a back door, inject malicious JavaScript into a form to create new administrative accounts or takeover legitimate customer accounts, or inject other code to take over your database. Some of the most common vulnerabilities found in e-commerce sites include:

Cross Site Scripting: In this form of attack, an attacker will insert a JavaScript snippet on a vulnerable web page that to a browser looks like a normal script and is therefore executed. This can then perform a number of harmful actions such as accessing a user's cookie information to impersonate them. This technique can also give attackers access to other information on the user's computer and leave them vulnerable to phishing attempts or malware installation. Although this form of attack may not be \ targeting the website itself, it is targeting your website's users which can still impact your business. In 2016, one attack of this type impacted over 6,000 e-commerce websites by stealing customer credit card data. Even when those websites use a 3rd party payment processor or HTTPS encryption they were still vulnerable, and some did not patch the issue for months.

SQL Injection: SQL injection can affect any website or web application using a SQL database, which includes e-commerce platforms such as Magento. In this type of attack a hacker can insert malicious SQL statements in a payload which will be included as part of a legitimate-seeming SQL inquiry. If the attacker gains access to the database they can create an administrative account for themselves, delete database entries, or view sensitive information.

2 Phishing Attempts

Phishing scams are often in the form of emails that look legitimate or like they come from someone you know, although phishing through phone calls also occurs. These scams usually include a link or direction to a page that if accessed will take over an email account or install malware on your computer that can steal personal information, access your microphone and camera, or log keystrokes. Targeted phishing attacks can be very convincing, and if a company employee falls for one they could inadvertently give an attacker access to their administrative account and other information that poses a risk to your website and company.

3 Distributed Denial of Service (DDoS) Attacks

A Denial of Service (DoS) or Distributed Denial of Service (DDoS) attack aims to take down your site by overwhelming servers with requests. In its distributed form, the attack will come from hundreds or thousands of IP addresses which usually have been compromised themselves and tricked into requesting your website over and over again. This attack type overloads your servers, slowing them down significantly or taking your site temporarily offline, preventing legitimate users from accessing your site or completing orders.

DDoS attacks are difficult to stop by simple IP blocking since they come from many sources, and those sources often look similar to your legitimate traffic. As more devices are connected to the Internet, DDoS attacks have grown both in prevalence and strength, meaning even websites with a large number of powerful servers are unable to withstand them. High-profile e-commerce sites are susceptible to this type of attack, and smaller e-commerce sites may also be vulnerable if their web host or DNS provider is targeted: For example, in October 2016 DNS provider Dyn was targeted by a DDoS attack and thousands of websites were taken offline as a result.

4 Bad Bots

Bots are prevalent all over the Internet, and can be both good and bad. "Good" bots are used by search engine sites such as Google and Bing to crawl and index your site for their search results. You want your site to be visible to these bots so that when someone searches for keywords related to your site it will show up in the results. However, there are also malicious bots which gather information from your website such as pricing data, hold products in carts without intending on buying them, buy up your inventory of a limited release to resell it at a higher price, or take over real accounts by guessing the passwords. Some bad bots can also access your database and gather a list of user account logins that can be resold later.

A report by Distil networks found that 97% of sites are hit with some sort of bad bots. For e-commerce sites, bad bots account for an average of 15.6% of a website's traffic, with good bots accounting for 9.3% of traffic. Bots can be programmed to perform a wide range of activities, but here are the most common for e-commerce sites:

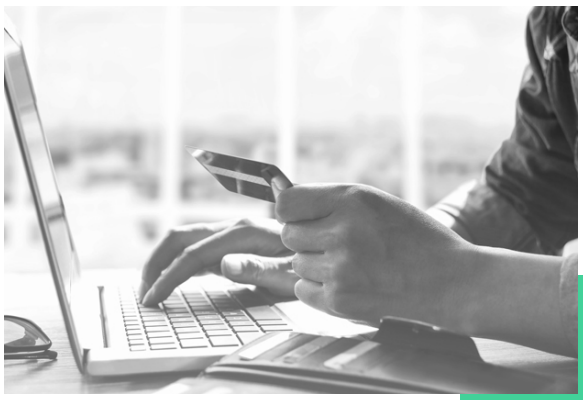
Price Scraping: If your site has unique pricing and product information, the chances are extremely high (around 97% according to Distil) that you will be hit by scraping bots. These bots collect pricing and product data and send it back to the bot-maker, who could be a competitor, so they can lower their prices and take sales away from you. Scraping can also hurt SEO and the likelihood that potential customers find your product, as the scrapers may create duplicate content which search engine then take into account when ranking websites. This type of bot can be extremely hurtful if you are selling the same product as other websites and trying to price competitively.

Login Fraud: Bots can attempt to login using one of your real user's credentials by guessing the password by rapidly going through a dictionary of words and number combinations (a brute-force approach), or by testing known credentials that have been leaked elsewhere. If bots are successful at logging in, they may not use the account information immediately, but sell the information to a third party. If a purchase is made using a stolen account and stored credit card information it will compromise the trust your users have in your site and result in a loss of money if an order ships and you need to refund the customer. If admin accounts are compromised using these same tactics, you could be unwittingly giving away a larger list of account logins.

Bots can also create new accounts in order to test stolen credit card numbers. If bots are able to access an account by guessing the login, they can guess the expiration date and CVV number of stored credit cards and make a fraudulent purchase.

Holding Items: Because bots can act more quickly than human browsers, they are able to refresh pages many times over to check for sales or limited-release products. Bots can add items to a cart, limiting inventory for actual users who came to your site looking for a specific product. If the product has a high resale value, bots may purchase it and resell it at a higher price on a third party website such as eBay. Even if bots do not ultimately purchase the product, your actual visitors may abandon your site if it appears an item is out of stock, and when the bot releases the product, your cart abandonment rate will go up.

Incorrect Analysis: A secondary effect of bad bot traffic is that it can significantly impact the analytics you track. Over 50% of bots can load JavaScript, which is the mechanism most analytics tools use to measure page views, bounce rate, conversion rate, and more. Since bots are imitating human behavior, they will be included in your analytics and can do harm to these important metrics, lowering your average conversion rate or convincing you to spend more money on advertising. Bots can also make it falsely appear that one advertising campaign is working better than another, or in other ways encourage you to target specific keywords or interests which are unlikely to have good a good click through rate.



5 Man In The Middle Attacks

A man in the middle attack is when an attacker listens in on a user's communication with your website. This could happen because a user is connected to an unsecure public wifi network, has been tricked into connecting into a vulnerable network, or because a hacker has targeted a specific network and gained unauthorized access to it. If the connection between the user and website is not encrypted, a man in the middle attack could see all of the pages a user is visiting, view emails they are sending, and intercept usernames, passwords, and credit card numbers.

Even if a website has a SSL/TLS certificate to encrypt data with the HTTPS protocol, there are a number of ways hackers can trick the user's browser and gain access to unencrypted data. In addition, websites who only use HTTPS on certain pages (for example on the payment or login pages) are leaving their users more susceptible to this type of attack, as attackers could steal session cookies or other sensitive information when users browse an unsecured page on the same website after they have logged in.

6 Malware

Malware is the malicious software that attackers insert into your web files or pages once they have gained access to your site. Malware may be found on an individual's computer if they have themselves fallen victim to a phishing attack or otherwise been compromised, or it may be inserted directly onto your website after a successful SQL injection or if administrative account access has been granted to a harmful entity. Malware can also be installed on your site if you are on a server with other compromised websites in a cross-site contamination incident. Popular e-commerce platforms like Magento are particularly susceptible to widespread malware infections due to their prevalence in the market.

As with software, malware can perform an extremely wide range of activities, from turning your computer into a botnet that can be part of a DDoS attack, to stealing credit card and account information from your website users. One type of malware that targeted Magento sites was able to take credit card information and store it in images so that the attacker could easily access it without flags being raised. Malware can also perform spam activities by linking to websites selling pharmaceutical or other goods, redirecting pages to other sites, inserting pop-up ads onto your site, or adding tags into the metadata of your site.

Protecting Your e-Commerce Sites From Attack

Understanding the threats posed to your e-commerce site is only half the battle: to be effective in protecting your website and customers you must stay on top of patches and deploy more advanced protective measures.

Now that you know what major security issues you want to protect your e-commerce website from, the question is what measures should you take to secure your site? The truth is website security will be slightly different for every site. Some large e-commerce sites may need an internal security team in place to juggle the various security tools being utilized, while smaller to mid-size sites can manage without a dedicated security team.

This is due to the complexit y of larger sites, but also because the bigger a site the more attacks it will face: Distil's 2017 Bad Bot Report found that large sites (defined as Alexa rank 1 - 10,000) get 57.9% bad bots compared to 42.1% good bots, whereas the smallest sites (defined as Alexa rank 150,000+) get a ratio of 28.6 % bad bots to 71. 4% good bots. A similar trend is likely seen with other types of attacks, as the bigger the site the more sensitive information they have access to.

Although it does take some developer effort to coordinate and manage security for any size website, there is a trend towards out-of-the-box security solutions for blocking threats which don't require as much tuning to be effective, as we discuss in more detail below.

To get started with improving your website security, you should take the following steps, which we have broken down into two sections:

1. Quick Fixes that you can start doing right away, and
2. Big Wins that give you more protection in the long run.

Quick Fixes To Start Improving Security

The below security tips are standards that any e-commerce site should be adhering to. While they may not protect your site from particularly large or sophisticated attacks (see the Big Wins section for those solutions), these will ensure you are taking regular steps to protect your site and your customers.

Scan your Website for Vulnerabilities: The first thing you should do when examining your website security is to do an audit of where you currently stand. There are many tools that will scan your website for malware and known vulnerabilities from platforms including Wordpress, Magento, Joomla and Drupal. Some popular free tools include Sucuri and Quttera. Once you know what your vulnerabilities are, you can start patching them and evaluating what additional tools your site needs to block threats.

Another way you can examine your site for potential threats is to look at your logs. If you use a log management tool or ELK stack logs (a combination of ElasticSearch, LogStash, and Kibana) you can search logs to see where requests come from and identify if your site is getting unusual requests. For example, if you sell exclusively in the US and get a lot of suspicious traffic from other countries, you could see that and try to block that traffic from accessing your site.

Use SSL/TLS Encryption for All Pages: The majority of e-commerce sites use the HTTP S encryption protocol on t heir payment pages through the payment gateway t he y use, however having HTTPS only on some pages of your website could still leave you vulnerable to attack and your users' browsing information open to be taken. Browsers including Google Chrome (which has an 59% market share on desktop) will label your site as insecure in the URL bar if it is not on HTTPS throughout the site. In addition, Google search has started ranking HTTPS-only sites higher in search results, and having HTTPS implemented on all pages will allow you to use the newer HTTP/2 protocol, which offers better website performance and can also improve SEO.

We also highly recommend using the Qualys SSL Labs tool to evaluate the quality of your SSL configuration. You should aim for an A+ rating which indicates the certificate itself is valid, and that the protocol support, key exchange, and cipher strength are also strong. Just having an SSL/TLS certificate isn't enough, as there are weaknesses in the way some SSL certificates are deployed and if your certificate is expired it could also expose you to attacks and harm your reputation with customers.

Stay on Top of Security Patches: 44% of attacks are because of known vulnerabilities in the platforms websites use. Some bots will scan your website regularly for vulnerabilities so that an attacker can take advantage of those found without manually searching. Always stay up to date on patches for these issues, which will be in a developer or security section on the platform's website or in their portal.

Doing regular scans of your website yourself will also help pick up these security risks. If you use an open-source Web Application Firewall, as discussed in more detail below, it's also crucial that you are regularly updating that against new security risks.

Use Strong Passwords and 2-Factor Authentication for Admin Accounts: Administrator accounts are particularly vulnerable to hacking attempts by bots or individual attackers. You should regularly audit the people who have administrator access to your website or database to check that no one has created an unauthorized administrator account, and make sure that your authorized users are strongly protected against hacking attempts. Requiring them to use a strong, randomly generated password that is unique from any other logins is important. A password manager such as LastPass is useful in generating and storing strong passwords.

If you can enable 2-factor authentication for logins that will go a step further in protecting your administrator accounts. In addition, there may be platform-specific steps you can take to protect your self from login fraud. Wordpress by default does not limit login attempts, meaning bots can continue to try login combinations. To protect yourself from this, you can enable brute-force protection.

Be PCI Compliant: E-commerce websites of all sizes that accept credit card payments are required to be PCI compliant. The Payment Card Industry Data Security Standard (PCI DSS) are security standards to protect your customers when they are submitting payment details online. There are several levels of verification depending on the number of transactions you process each year, ranging from a full network-level assessment to a self-assessment for smaller merchants.

Using an e-commerce platforms such as Magento or Shopify will not directly make you PCI compliant because they don't directly process transactions. You will need to make sure your server network, Content Delivery Network (CDN), and payment gateway (such as Stripe or Authorize.net) are PCI compliant before performing your assessment.

Use Trusted Extensions, Platforms, and Themes: As mentioned previously, it is crucial that you stay on top of updates for the platforms that you are using. In addition, you should use trusted platforms, extensions, and themes as these can open you up to vulnerabilities: Last year, e-commerce platform Magento found that several third party extensions were at risk of SQL injection attacks. Wordpress has also found vulnerabilities in their numerous plugins and themes, with 52% of known Wordpress vulnerabilities coming from plugins and 11% coming from themes.

To find trusted themes and plugins that are less likely to have vulnerabilities, download directly from the platform's marketplace and be wary of free tools which seem too good to be true. You can also check how many other extensions a company has created, the number of downloads or reviews each extension has, and the length of time they have been creating extensions as a good indicator of if they are a trustworthy business.

Big Wins To Protect Your Site Top To Bottom

Mid-size to large e-commerce sites who are being regularly targeted by bots and other attacks should strongly consider getting more protection through a WAF or Bot Blocking solution, or a combination of the two. While Content Delivery Networks are often thought of as website performance tools, CDNs provide network-layer security and many have additional tools such as WAFs available, although not all are as robust as they could be. Below we lay out the different types of advanced website security available to ecommerc e websites, and how you should go about choosing between solutions.

Web Application Firewalls: Web Application Firewalls or WAFs inspect HTTP traffic going to specific websites, rather than traffic between servers which traditional firewalls inspect. WAFs were first deployed in data centers, but are now often deployed in the cloud as a reverse proxy. This means the WAF is placed between a website's origin server and a visitor's browser, and acts as a proxy for the website origin server so that it can inspect traffic and either block it or pass it through to the origin. WAFs aim to protect against web application-specific attacks including Cross Site Scripting, SQL Injections, Cookie Poisoning, known platform vulnerabilities and more. They prevent websites and apps from unknowingly letting hackers into their system or sharing user data.

The majority of WAFs do this by employing a set of rules and using those rules to inspect traffic before it is let through to the website origin. The open-source WAF ModSecurity and many others base their initial rule-sets off of the Open Web Application Security Project (OWASP) Top 10 list, which has published a list of the top website attacks since 2003. Below we go into how these rules-based WAFs work and what other solutions have arisen in the WAF marketplace in recent years.

How Firewall Rules Block Threats: Rules-based WAFs deployed as reverse proxies inspect all traffic that attempts to connect to a website's origin server against a list of rules and either blocks the traffic or lets it through. Whether these rules block or allow traffic in by default depends on if the WAF is set up with a negative model or positive model.

Negative and Positive Security Models: Negative security models, which have traditionally been the default WAF configuration, allow all traffic except that which meets rules showing it is a known threat. This configuration protects legitimate traffic from being incorrectly labeled as an attack, but also requires the use of a large database of rules and signatures of attack types to scan against. This type of configuration is a good solution for those looking to block known attack types and system vulnerabilities with less setup, as many WAFs come with automatic deployment of the OWASP Top 10 rule-set along with other databases of rule-sets.

A positive security model takes a different approach by blocking all incoming traffic unless it meets requirements that show it is not a malicious entity - for example location or browser type. This type of security requires less rules because it blocks traffic by default, but also requires websites to have an intimate knowledge of their visitor profile so that legitimate users are not blocked.

Negative security rule-sets operate on the guideline that the majority of attackers are using known vulnerabilities to exploit websites that do not have protection. While this may be the case, these WAFs require constant maintaining to ensure the new attack types discovered each day are included in that WAF instance's rule-set. If a WAF is irregularly updated to include new attack types or vulnerability patches, that website becomes just as vulnerable to new attack types as it would be without a WAF.

Positive security models more strictly limit the routes an attacker can take to gain access to a website, and because of this block against both known and unknown attack types and vulnerabilities. When first deployed, positive models may block a good amount of legitimate traffic in so-called "false positive" events, however by white listing visitor characteristics over a few rounds of rules editing the positive model will (when configured correctly) successfully allow in real visitors while blocking a wider range of malicious activity than negative models.

Rules-based vs Next Generation Firewalls: WAFs have operated on a rules-based approach that lets visitors in or blocks them since their inception, but more modern solutions have recently started to question this method due to some downsides of this approach.

Rules-based WAFs can be inexpensive, relatively easy to install, and if updated and monitored regularly will block most attacks. Companies such as CloudFlare offer WAF services with protection against th e OWASP Top 10 attacks starting at just $ 20/month, and provide additional rule-sets at an upcharge. These basic WAFs are an attractive option for those looking for protection against some attacks at a low cost, but the true cost comes in the developer time it takes to maintain the rules that form the core of the protection.

Rules-based WAFs need to be constantly updated, and a developer must inspect logs to set initial rules and continue to adjust them according to traffic patterns they see. This takes time and means that many rules-based WAF deployments will remain in "detect" mode where they are not blocking threats.

Next-generation WAFs take away some of the developer pain by using heuristics and intelligent technology to learn a specific site's threat profile and monitor and block threats automatically based on contextual information such as location, device, time, and on-site behavior. By removing the rule-sets that traditional solutions use, modern systems can stay one step ahead of attackers as they do not know what rules are being used against them. In addition, legitimate traffic that might set off one rule in a rules-based traffic is let through.

Rules-based WAFs include ModSecurity, which can be deployed on your own if your development team has the necessary skills, and the WAFs found in CloudFlare, Akamai, and Fastly. Examples of next-generation WAFs include Signal Sciences and Threat X, both offered with Section's Edge Compute Platform.

Bot Blocking: Although most WAFs will block a decent percentage of bots as well as individual attacks, some e-commerce sites who are particularly hard hit by bad bots will want to deploy a bot blocking solution in addition to or instead of a WAF. Websites can block individual bots by looking at logs and blacklisting certain IP addresses or IP ranges, but it takes a significant amount of effort to manually update blacklists.

Websites can also add a CAPTCHA to any vulnerable pages on their website which will force users to prove they are human by solving a problem or typing out a word. Although this is effective at keeping out bots, it can also lead to a decrease in conversion rate. Newer solutions like Google's reCAPTCHA make it easier for legitimate users to pass through a verification without being frustrated by a CAPTCHA form.

There are other basic bot blocking tools available for specific e-commerce platforms , often deployed as extensions, which will make it easier to manage bad bots while allowing in the good bots from search engines. While these may seem like quick solutions for a small bot problem, they may not block advanced bots: As with WAFs, traditional bot blocking solutions use rules to determine if a user is real or a bot, which can block legitimate traffic while at the same time failing to catch newer types of bot attacks.

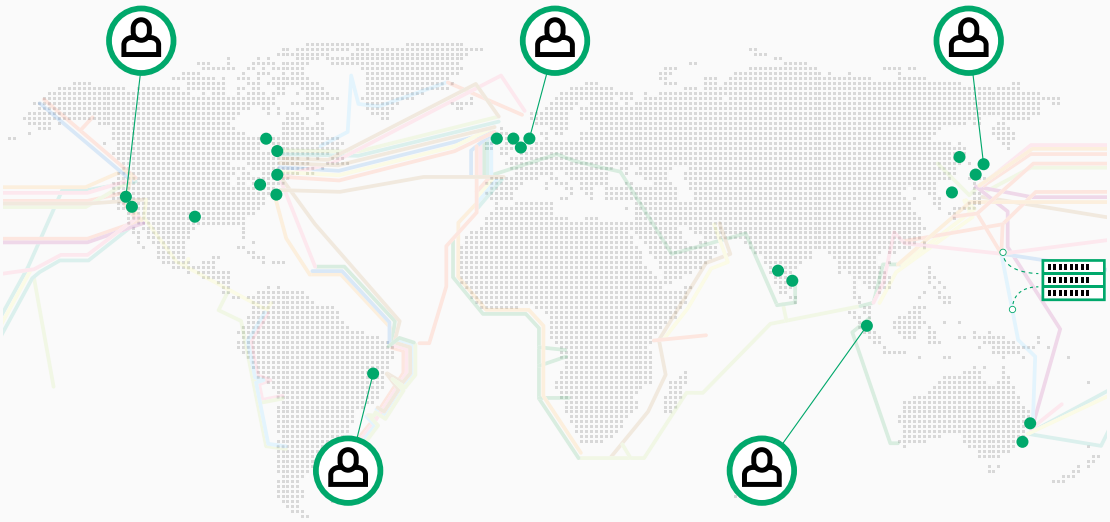
On example of a more advanced solution is Perimeter X, which blocks bots while protecting real shoppers by giving each visitor a "Risk Score." This score is based on behavioral analysis that includes factors such as mouse and click movement and timing, unusual web application requests, and hidden clicks. These techniques are able to defend against even the most sophisticated bots that use real browsers to take over accounts and can slip past older security methods.

Distil Networks is another popular bot mitigation tool which uses machine learning to defend against bots without you having to manage rules manually. They look for anomalies in your site's traffic to indicate a visitor is not legitimate and block them.

Content Delivery Networks: CDNs are popular tools for both website performance and security. CDNs have two layers: A DNS layer that routes your traffic to the closest in their global server network, and a reverse proxy layer. The reverse proxy layer intercepts traffic and acts on behalf of your origin server while using software that speeds up your site and blocks threats. Reverse proxy software can cache content, block bots, act as a Web Application Firewall, optimize images, and much more. By deploying a CDN for your e-commerce website you'll get several security benefits:

Network Protection: Since Content Delivery Networks intercept traffic before it hits your origin server, you're getting added protection from network-layer DDoS attacks. Depending on the CDN you use, this DDoS protection may be backed by industry leaders like Amazon and Microsoft through their server networks. Some CDNs will also allow you to block specific traffic (such as one IP address or a range of IP addresses) through their platform even if you have not deployed a specific security solution such as a Web Application Firewall.

By caching as much content as possible through the CDN, you're also reducing the load on your origin server which again protects your origin from large-scale attacks. Because the security of your website is linked t o how much content you are a ble to cache , we strongly recommend using a solution which caches both static objects like images and dynamic content like your HTML document. Modern CDNs including Section make this simpler than older CDNs like Akamai, and Section has the added benefit of a local development environment so developers can test if their dynamic content caching is working as expected before pushing the configurations to production.



■ CDNs add network layer security and can deploy Web Application Firewalls and Bot blockers.

CDN Security Solutions: Many CDNs offer tools including WAFs and Bot Blockers that are deployed within the CDN as reverse proxies. Using a Content Delivery Network for network-player protection along with another security tool can be beneficial as it brings your performance and security into one platform. This can save you cost compared to having separate CDN and security solutions, and will also make it easier for your developers to manage.

If you choose to set up a WAF or Bot Blocking tool within a CDN is imperative that the Content Delivery Network you choose includes the tools necessary to view traffic and quickly adjust security settings when needed. To properly manage security for an ecommerce site, you should have access to detailed, searchable logs, real-time metrics, and the ability to fully tune your solution without engaging professional services. With these tools available you will be able to quickly view malicious traffic, update security rules, and see how your new configurations are impacting traffic to ensure you aren't blocking customers.

This will also enable your team to quickly identify, troubleshoot, and resolve any problems that arise using a DevOps workflow. Unfortunately, many Content Delivery Networks do not provide this level of detail or integration with DevOps and Agile principles. When choosing a CDN you should look for one which provides ELK stack logs for all reverse proxies deployed within the network, detailed metrics and monitoring, code-level configuration control, and a local testing environment. Although modern CDNs provide some of these features, Section's Edge Compute Platform is the only solution to provide all of the above including a virtual machine so developers can tune their security and test configurations before pushing them to production.

In addition, we recommend using a CDN that is open and flexible in the security solutions that are deployed. You may try a Bot Blocker only to discover a WAF would be the more appropriate solution for your websites, or decide you want to upgrade from a rules-based to an intelligent WAF. Your CDN should be open about the tools they offer and allow you to switch security solutions when necessary. Section offers a library of edge modules for both security and performance and allow customers to add or change modules.

Conclusion

Retailers often dedicate many resources to the look and feel of their e-commerce websites, designing an attractive layout, using high quality images, and making pages load fast so customers can quickly go through the checkout flow. However, website security is just as important as the speed and design of your website, as the consequences to an insecure website can be more impactful to your business. An attack that takes your website offline for any period of time will result in a loss of sales, and attacks that spread malicious code, steal customer data, or insert spam into your site will result in reduced customer trust. In addition, dealing with the fallout of an attack that has used stolen customer data to place orders will cause a loss of both funds and merchandise. If you need to reset all customer passwords, there is a strong likelihood some customers will choose not to reset their account.

A vulnerable website also has less obvious impacts on your finances. Bots that scrape price and product data for competitor sites will drive your customers to buy elsewhere, and bots can also have a huge impact on the legitimacy of your analytics and marketing spend, tricking you into spending more on advertisements which falsely seem to be working. False analytics can also hurt your business when it comes time to report on metrics including page views, bounce rate, and conversion rate.

Luckily, there are many solutions available for e-commerce websites to improve their security and decrease the chance of being compromised by an attack. The quick fixes we have outlined above will get you started on the path to a more secure website, but we strongly recommend implementing a stronger defense mechanism such as a Web Application Firewall. Once you add more security measures to your website, make sure your development team is regularly updating them to ensure all known threats are being blocked. If you follow these steps, your business will be safer and customers will continue to trust you while making online purchase decisions.

Get the best in website security and performance with Section

Need help implementing the tips above? Section is an Edge Compute Platform which gives users a choice of website performance and security tools to speed up and protect their website. Section provides a range of solutions for e-commerce sites, including Varnish Cache for caching, PageSpeed for front-end optimizations, Signal Sciences and ThreatX for intelligent threat blocking and ModSecurity for an open source rules-based WAF, and ShieldSquare and PerimeterX for bot blocking.

In addition, Section provides many core features, including SSL certificates, real time metrics, ELK stack logs, real time metrics, real user and synthetic monitoring, and a local development environment, all included at no extra cost.

Contact Section at www.section.io/contact-us/ to discuss your specific security needs.

Additional Reference

http://www.cmswire.com/information-management/e-commerce-security-threats-5-trends-online-businesses-need-to-know/
http://www.cio.com/article/2384809/e-commerce/15-ways-to-protect-your-e-commerce-site-from-hacking-and-fraud.html
https://www.godaddy.com/garage/webpro/security/10-ways-to-keep-hackers-hands-off-your-e-commerce-website/
https://resources.distilnetworks.com/all-blog-posts/e-commerce-conversion-rate-is-off/
https://www.incapsula.com/web-application-security/man-in-the-middle-mitm.html
http://www.csoonline.com/article/3157377/application-development/report-attacks-based-on-open-source-vulnerabilities-will-rise20-percent-this-year.html
http://www.beyondsecurity.com/web-security-and-web-scanning.html
https://ithemes.com/wordpress-security-issues/