WEBSCALE

SOLUTION BRIEF

Securing Ecommerce Storefronts for the Holidays

Protect your online store from bad guys to safeguard revenue and reputation

The world of commerce is moving from tracking customer acquisition to customer retention as their success metric. Security is critical to achieve that. When the World Economic Forum asked respondents in a recent study which dangers will pose the largest threat to the world over the next two years, cybersecurity failure made it to the top four. After all, when cybersecurity vendors get hacked (FireEye – SolarWinds), it’s a moment of reckoning for the industry.

The “Securing Ecommerce Study” commissioned by PYMNTS.com in May 2021, revealed that **65% of shoppers would desert an ecommerce merchant** after a single data breach incident, further reiterating the importance of keeping transactions and data safe.

Retail continues to be a prime target for cyberattacks, making up 20% of all reported incidents in the first half of 2021. In the National Retail Federation’s 2021 Retail Security Survey, 76% of merchants responded saying cybersecurity incidents have become more of a priority in the last 5 years.

Despite warnings and recommendations, malicious actors continue to exploit zero-day threats in web APIs and popular ecommerce platforms. Best practices around end-to-end security, automation and real-time visibility are critical for every ecommerce business.

Best Practices for Ecommerce Security

Incident response strategy

Educate teams and establish outage repair and response strategies before attacks hit. Ensure your cloud delivery provider and ecommerce security vendor have support SLAs.

Security update plan

Code freeze your storefront at least 2 weeks prior to the holidays, but not your security. Patch your site for any vulnerabilities and ensure they are up-to-date.

Compliance first

While meeting cybersecurity compliance standards does not necessarily mean your storefront is fully secure, non-compliance can have legal and financial implications.

PCI DSS

Ensure Level 1 PCI DSS 3.1 compliance, and let customers know that you treat their credit card and personal data as seriously as you protect your own content from scrapers.

SOC2 compliance

Investing in ensuring your systems and processes and those of your business partners meet SOC2 requirements is crucial to build a 360-degree security barrier.

HIPAA compliance

If your business has any access to patient data, make sure your network is secure and compliant and all your partners have signed your business associate agreement (BAA).

Multi-Factor Authentication

Deploy MFA on all remote access points into your network and to access your admin servers online and offline. Focus on securing or disabling remote desktop protocol (RDP) access, a vulnerable entry point for attackers.

Proxy protection

Take your storefront off the internet! Going behind a proxy layer or a protective shield to the outside world can save your storefront from malicious traffic in the event of an attack.

SSL for HTTPS

Utilize SSL to authenticate and encrypt links between networks. With an SSL certificate for your ecommerce site, you can move from HTTP to HTTPS, which serves as a trust signal to customers.

Security Action Plan for the Holidays

The holiday season is, unfortunately, a time you can expect higher volumes of attempted fraud and cybercrime. Here are some things you can do to ensure your website stays secure through the holidays:

1

Perform a pre-holiday security check

Perform exhaustive application testing covering code, traffic, infrastructure, 3rd party software, and access privileges. Running tests to mimic attacks enable you to gauge your current security posture, assess ongoing risks and find flaws in your defense. Availability of backup files can help a business recover quickly from a cyberattack. Using an alternate location or cloud region is key.

2

Deploy comprehensive edge security

The traditional WAF is not enough to fight modern cybercrime. Boost your storefront's security with multiple defense layers – rate limiting, MFA, bot monitoring, malware scanner, traffic viewer, CSP protection, DDoS shield, intrusion detection, and edge security closer to the end user.

3

Leverage automation, not people power

Leverage automation and analytics to proactively identify and protect your web applications from the front end through web traffic, malicious code inserted into the back end, or from browsers executing scripts to steal sensitive information.

4

Improve bot management

A fully-featured bot management solution ensures the good bots allow valid traffic to find your site, while keeping out the bad guys more interested in scraping your pricing and data. Traditional hosting providers are "black boxes" offering little observability into infrastructure, traffic, and threats. A "single pane of glass" helps merchants stay ahead of these threats and be proactive towards security.

5

Enhance fraud protection

An intelligent fraud detection and mitigation solution can detect anomalies, like contact and shipping addresses, country of origin, IP, or others, to flag suspicious transactions and prevent credit card fraud.

6

Evaluate and optimize 3rd party risk

From POS systems and mobile apps to supply chain tracking solutions and loyalty programs, 3rd party applications expand the attack surface. Adopt a zero-trust approach that prevents 3rd party applications from becoming single points of failure.

Conclusion

To protect revenue and reputation at every point of your infrastructure, merchants need a security technology stack that is custom built for ecommerce.

Webscale CloudEDGE Security is an award-winning 360-degree security solution that provides the ecommerce industry's most robust protection for storefronts. Websites protected by CloudEDGE Security have always-on, end-to-end security with application-aware, customized rules to defend against sophisticated attacks. CloudEDGE Security is deployed at the traffic edge, alongside 3rd party CDNs and WAFs, and on top of any fully hosted commerce cloud, headless/PWA deployment or on-premise application.

Need urgent help to secure your storefront before a major sales event? Reach our global security team at **secure@webscale.com**

About Webscale

Webscale is powering modern commerce by layering software for performance, security, availability and compliance, over a distributed global network that leverages the cloud, automation, machine learning, and DevOps protocols to address the needs of growing brands. With use cases across a variety of ecommerce platforms and architectures, Webscale simplifies the deployment and day-to-day management of storefronts, including headless and progressive web application infrastructure, and across any self-hosted or fully hosted commerce cloud. Deployed in multi-cloud environments, including Amazon Web Services, Google Cloud Platform, and Microsoft Azure, Webscale powers Fortune 1000 brands including Dollar General, Unilever, Swarovski, Olympus, Regal Cinemas, and thousands of other B2C, B2B, and B2E ecommerce storefronts across 12 countries. Webscale has offices in Santa Clara, CA, Boulder, CO, San Antonio, TX, Bangalore, India, and London, UK.