WEBSCALE

The Global Ecommerce Security Report 2021

Critical Insights and Key Learnings
from the Year that Broke all Records

Foreword

Welcome to the 2021 Global Ecommerce Security Report, our annual review of the preparedness, trends, technologies, sentiments, investments, performance, and business impact of security on the ecommerce industry. The assessments and opinions are based on our observations managing thousands of B2B, B2C, and B2E ecommerce storefronts on the public cloud as well as inputs shared by our customers, partners, and prospects from around the world participating in the survey, which was launched in December 2020.

During what was an unprecedented year for ecommerce, threat actors also upped their game and sophistication. As a provider of managed hosting and security solutions to the ecommerce segment, we wanted to look back at 2020 for key learnings that will better prepare us for the next decade of growth, as well as ensure that we are accurate in our recommendations to merchants wanting to enhance their security as their businesses scale.

2020 saw a huge, 50% spike in Magecart-type attacks targeting storefronts, according to some reports, and the industry's growth due to the pandemic has offered an increasingly fertile hunting ground for cyber attackers.

While some of this year's findings are in line with expectations, others, like the degree of complacency that still exists when it comes to securing storefronts, were surprising. The Marriott International data breach, for example, highlighted the absence of basic security hygiene, namely two-factor authentication and user account activity monitoring.

However, the good news is that a majority of merchants view security as their number one challenge and have plans to invest in 2021 to protect their storefronts better. Cyber resilience is improving year over year, and organizations are getting better at thwarting direct attacks, especially those through the frontend via web traffic. But, bad actors are becoming smarter and are now increasingly targeting the "less-monitored" backend application.

As ecommerce grew quarter over quarter, experiencing a decade's worth of growth in the space of a few months, so did cyber threats. The CPG (Consumer Packaged Goods) industry, especially, became a prime target for malicious actors, a clear indicator that CPG brands need to be taking a serious look at their security posture in the coming year. Rather than relying solely on yearly compliance reviews, continuous assessment of threats and vulnerabilities is needed.

2020 saw a huge, 50% spike in Magecart-type attacks targeting storefronts.

We are not alone in strongly recommending a much deeper dialogue among security leaders in the ecommerce industry. Every online business faces very similar threats and risks, and in this sense, none are competitors. However, security still plays only a supporting role when one looks at the topics of the most popular ecommerce conferences. Merchants need to share insights more often, collaborate around threat intelligence, share best practices on how to detect and respond to attacks, and fortify the ecommerce industry from those seeking only to take advantage of it.

We hope the information contained in this report will provide valuable insights into the ever-evolving threat landscape; indicators as to how the industry as a whole is mobilizing to address these challenges; and how to further enhance your storefront's protection, so that security becomes a highlight of your 2021 strategy, and not a headline.

Andrew Humber
VP Marketing

Table of Contents

The opinions, statements, and assessments in this report are subjective and do not constitute legal advice.

Chapter 01

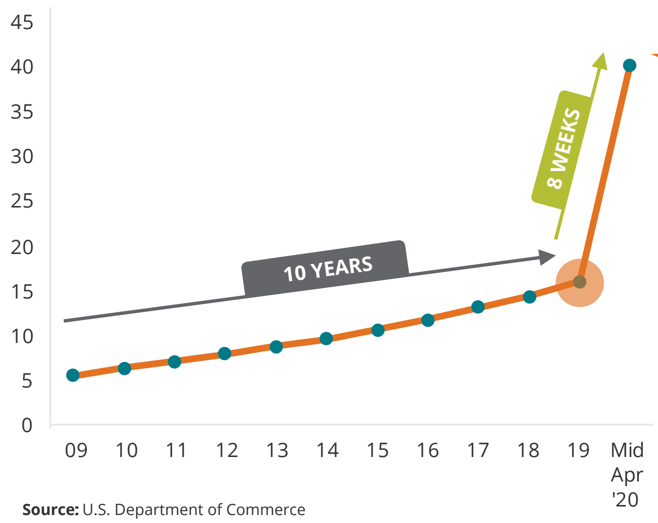
Navigating the Dynamic World of Ecommerce Security

Navigating the Dynamic World of Ecommerce Security

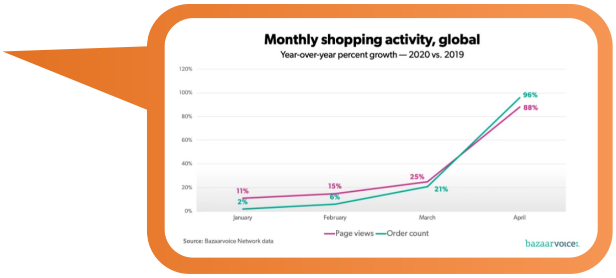
In the last twelve months, the ecommerce industry registered a decade's worth of growth, as COVID-19 forced consumers all around the world to shelter in place, and rely heavily on ecommerce for just about every need.

This meteoric rise in traffic, and revenue, has led to cyber criminals increasingly targeting online storefronts and executing a wide range of attacks.

Ecommerce as a Percentage of Total Retail Sales (USA)



Source: U.S. Department of Commerce



COVID-19 took share in Q2 to

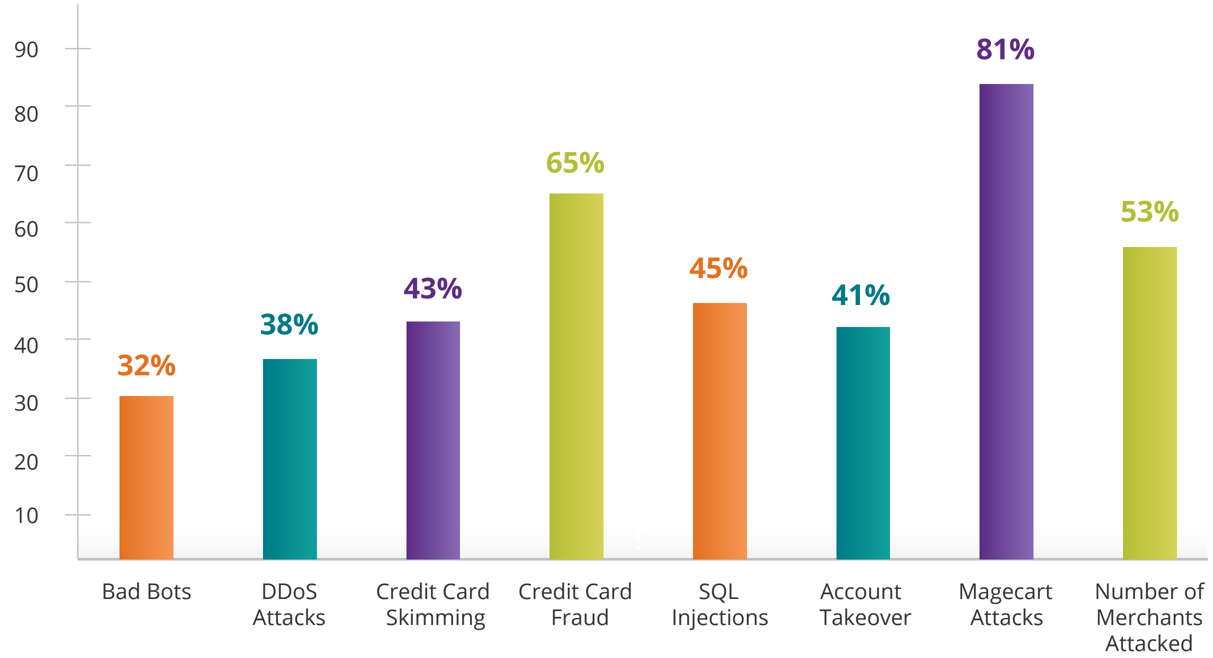
40%

CPG was the most impacted industry, while sectors like Fashion and Lifestyle, Health and Fitness, Banking and Financial Services, Sports and Outdoor, and Food and Drink were also targeted. Our survey's respondents reported that it was their number one business challenge during peak sales events. Bad bots, SQL injections, Cross Site Scripting (XSS) attacks, DDoS attacks, and Magecart attacks upset the plans of many merchants. According to our research, For a vast majority of businesses, the financial impact of such security incidents was significant, ranging on average from $100K-250K.

The holiday season in 2020 saw large increases in the total number of bad bots (**32%** more than 2019), DDoS attacks (**38%** more than 2019), Credit Card Skimming (**43%** more than 2019), Credit Card Fraud (**65%** more than 2019), SQL injections (**45%** more than 2019), Account Takeover (ATO) attacks (**41%** more than 2019), Magecart attacks (**81%** more than 2019) and the number of merchants attacked (up **53%** from 2019). During the November - December period, Webscale prevented over **520M cyber attacks** including malicious bots, credit card skimmers, brute force login attempts, and scrapers.

Cyber Attacks on the Rise

Holiday season 2020 saw large increases in the number of attacks (compared to 2019)



Source: Webscale Global Ecommerce Security Report 2021

This aligns with national data released by the FBI in August 2020 that reported a 400% increase in cyber crimes. Overall, security incidents in ecommerce grew by an alarming **20%** in 2020 for **69%** of the businesses we surveyed.

Magecart attacks were a recurring headache last year, and the Magento 1 ecommerce platform was the most sought after target, thanks to its known vulnerabilities after it went end of life (EOL) in June. More than 2000 merchants fell victim to the largest attack to date that saw the Magento "downloader" used to inject JavaScript code into ill-prepared storefronts. (We're proud to report that not a single web application hosted with Webscale was impacted.)

According to data gathered, we can predict a massive uptake in security solutions in the next 36 months. Ecommerce businesses are committing a **15-20%** increase in their security spending in the next **3 years**. When asked more specifically about which security areas would see the most investment, bot management, CSP (Content Security Policy) protection, fraud detection, and real user monitoring (RUM) top the lists. Merchants are also exploring automated threat intelligence and management solutions to remain ahead of bad actors.

We are also witnessing a problematic gap in the readiness and capability of ecommerce businesses to identify, defend and protect their web applications from sophisticated attacks. Automation leaves a lot to be desired across many available security solutions, with many businesses continuing the concerning trend of "throwing people at the problem."

Security incidents in ecommerce grew by an alarming **20%** in 2020 for **69%** of the businesses we surveyed.

Ecommerce businesses are committing a **15-20%** increase in their security spending in the next **3 years**.

Notable Findings – Security

72%

of businesses stated that "Security" is their number one business challenge

78%

of organizations surveyed reported at least one cyber security incident

70%

of organizations have already invested in WAF

54%

of organizations have already invested in bot management

79%

of businesses intend to invest in CSP Protection

64%

of businesses intend to invest in Fraud Detection

72%

of businesses intend to invest in RUM

68%

of merchants want "Automation" in their security management solution

67%

of storefronts commit to enhance security spending by 15-20%

62%

of businesses lost between 100-250K due to a cyber attack

In spite of a significant increase in the number of attacks targeting ecommerce storefronts, our findings seem to suggest that many merchants continue to take security lightly. We also asked respondents to evaluate their readiness and capability across 4 vectors:

Prevent more breaches

29%

of merchants have improved their ability to stop attacks compared to two years ago.

Identify attacks sooner

34%

of merchants are able to detect attacks faster compared to two years ago.

Fix attacks quicker

24%

of merchants now have the ability to fix breaches faster compared to two years ago.

Limit the impact of the attack

27%

of merchants are able to reduce the impact of the breach compared to two years ago.

Source: Webscale Global Ecommerce Security Report 2021

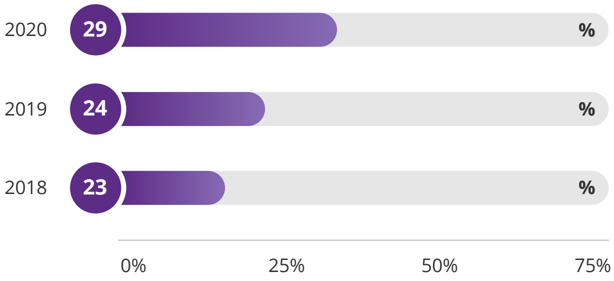
Availability and Performance

While security remains the number one concern for merchants we surveyed, the report also asked them to share any valuable insights related to two other equally important vectors for a successful ecommerce business – availability and performance.

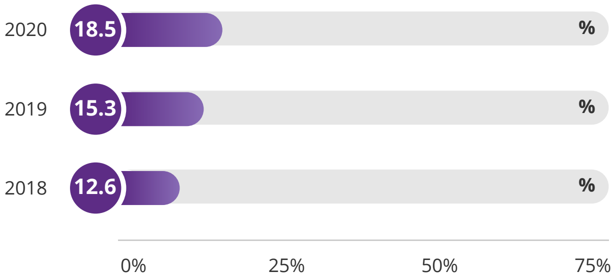
While leading brands like Costco, Nordstrom Rack and Home Depot avoided 2019's well-publicized downtime during the 2020 Black Friday-Cyber Monday weekend, several global brands, including Currys, Etsy, Ulta Beauty, and Naked Wines, fell victim to outages due to demand in 2020.

Availability

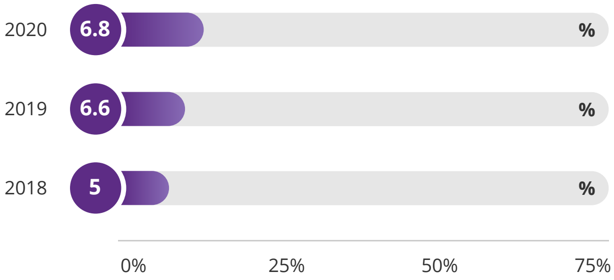
Merchants who experienced outages in excess of 5 mins on Black Friday/Cyber Monday



Merchants who experienced outages in excess of 10 mins on Black Friday/Cyber Monday

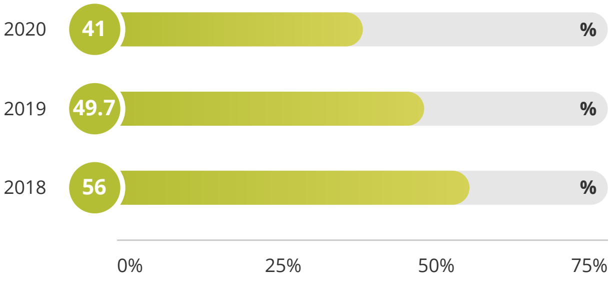


Merchants who experienced outages in excess of 30 mins on Black Friday/Cyber Monday

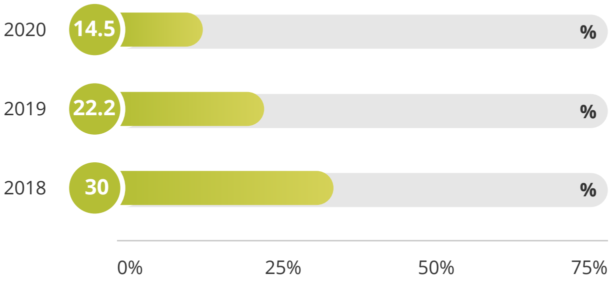


Performance

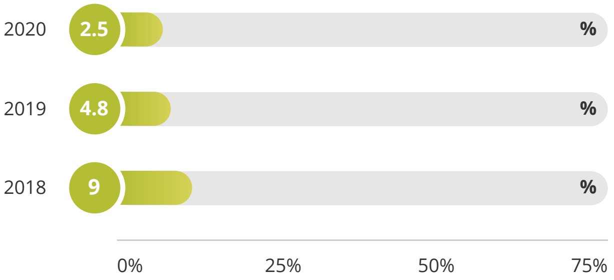
Merchants who faced page loads times in excess of 3 secs during Black Friday/Cyber Monday



Merchants who faced page loads times in excess of 5 secs during Black Friday/Cyber Monday



Merchants who faced page loads times in excess of 10 secs during Black Friday/Cyber Monday



Source: Webscale Global Ecommerce Security Report 2021

Chapter 02

The State of Ecommerce Security

The State of Ecommerce Security

In early January 2021, the Biden administration announced that it would, for the first time in U.S. history, appoint a Deputy National Security Advisor (NSA) focused exclusively on cyber security, as part of the National Security Council. The Trump administration's proposed Budget of the U.S. Government Fiscal Year 2021, had earmarked about $18.8 billion towards spending on federal cyber security programs and initiatives.

International Data Corporation's (IDC) Worldwide Semi-annual Security Spending Guide indicates that global spending on security products and services is expected to touch $151.2 billion by 2023, at a CAGR of 9.4% over that period – considerably higher than their estimated spending of $106.6 billion in 2019. According to the report, the banking industry, discrete manufacturing industry, and federal/central governments are projected to be the largest spenders worldwide in terms of security tools and solutions over this forecast period; industries like retail, which includes ecommerce, are lagging far behind in projected security spending.

With more consumers shopping online than ever before and cyber attacks increasing in line, businesses of all sizes scrambled to procure web application firewalls (WAF) and basic bot management solutions. However, traditional edge security solutions are proving ineffective as application backends become exposed as a result of increasingly sophisticated attack vectors, perpetrated by similarly sophisticated hackers.

According to Gartner, spending on cloud security is predicted to increase by 33%, making it a $585M market this year. Security services are forecast to drive $64.2B in worldwide revenue this year, comprising 51.9% of the total market. Data security will grow by 7.2%, becoming a $2.8B market this year.

While IT spending declined in 2020, security and risk management (cyber security) has grown, albeit by a lesser extent than initial predictions. Industry reports suggest that spending on security services, infrastructure protection, network security equipment, identity access management, and consumer security software together accounted for the majority of all investments in security and risk management in 2020.

Of the eight to ten cyber security segments growing more than the average, cloud security is the fastest. In 2019, it was the smallest, fastest-growing cyber security segment with a market size of $439M. Its projected 33% growth in 2020 was a function of its small initial market size, and organizations' preference for cloud-based cyber security solutions.

Cloud-based delivery models represent 48% of all cyber security deployments in the ecommerce industry. Merchants are finding it easier to pilot cloud-based cyber security applications with remote IT teams, which is a significant advantage cloud delivery models have over traditional on-premise deployments. Cloud-based cyber security platforms are providing the much-needed analytics and reporting that help to prove their business case, driving further investment.

> Of the eight to ten cyber security segments growing more than the average, cloud security is the fastest.

In 2020, major retailers extended their Black Friday sales periods to compensate for the drop in foot traffic through their brick and mortar stores. Sales events began in mid-October with the onset of Amazon's Prime Day, which was quickly followed by Walmart and Target also announcing their events. Prime Day usually occurs in July, which gave October an added boost compared to 2019. For the three months of October through December, retail non-store sales (mostly online) were up 24.1% and up 23.4% for the season (February through December). The five highest traffic days in 2020 (ranked highest to lowest) were Black Friday, Super Saturday, Boxing Day (the day after Christmas), December 12th (Saturday), and December 23rd (Wednesday). As a result, the October - December period saw cyber attacks grow by a significant 10x compared to 2019.

The economic impact of cyber attacks on ecommerce applications in 2020 is difficult to ascertain accurately. Cyber crime as a whole was estimated to harm the global economy to the tune of $2.7 trillion in 2020. A recent survey reported that some companies are losing more than $5 million in stolen data and many others have suffered losses over $100 million, not to mention the millions of consumers that have had their credit card and bank account details compromised.

The massive spike in security breaches in 2020 reflects a new normal and a clear indication that the mandate of organizations, like Webscale, in defending and securing ecommerce applications and building a safe transaction environment for customers, is only growing more complex as we navigate the ever-expanding threat landscape.

The October - December 2020 period saw cyber attacks grow by a significant 10x compared to 2019.

Chapter 03

Major Ecommerce Security Incidents in 2020

JAN

Leading currency dealer and travel money services provider, Travelex, was hit by the “Sodinokibi” ransomware attack on New Year’s Eve, impacting services across 1200 locations in 70 countries. Sales and reloading of travel credit cards had to be stopped. Third-party exchange services that rely on Travelex to provide currency, including Tesco Bank, HSBC, Sainsbury's Bank, and Virgin Money – all had their operations impacted by the attack.

250 million Microsoft customer records, spanning 14 years, were discovered online without password protection due to misconfigured servers. The information included customer email addresses, IP addresses, geographical locations, descriptions of the customer service and support claims and cases, Microsoft support agent emails, case numbers and resolutions, and internal notes marked as confidential.

The attackers got into an application that Marriott hotels use to provide services to guests, by compromising and using login credentials of two employees at a franchise property. Contact details and loyalty account information of some 5.2 million guests were compromised.

FEB

Customer data obtained during a malware attack against convenience store chain Wawa, appeared on Joker's Stash, a marketplace on the Dark Web for stolen credit card information. 30 million debit and credit card records from U.S. customers across 850 stores in 40 states were on sale.

The independent owners and operators of several Quaker Steak & Lube casual dining restaurants disclosed that customer payment card data was sent to an unauthorized source due to malware infecting the stores' retail point-of-sale (POS) terminals over weeks to months.

ESTĒE LAUDER

Security researcher Jeremiah Fowler discovered a non-password protected middleware database containing more than 440 million records. After further review, it was determined to be connected to New York-based cosmetics giant Estée Lauder.

MGM RESORTS INTERNATIONAL™

The personal information of more than 10.6 million guests who stayed at MGM Resorts leaked on a hacking forum. Among the guests who were impacted included celebrities like Justin Bieber and Twitter founder, Jack Dorsey.

MAR

Virgin media

A Virgin Media database containing the personal details of 900,000 people was left unsecured and accessible online for 10 months, the company admitted. The data was accessed at least by one unknown person and investigations are ongoing.

Nintendo®

The Japanese gaming giant said that 160,000 Nintendo accounts were compromised, exposing personal information. In an updated statement in June, the company said another 140,000 Nintendo accounts had been compromised.

MAY

tokopedia

Hacker group ShinyHunters initially leaked 15 million user records online, for free, of Tokopedia's customers, Indonesia's largest online store. They later put the company's entire database of 91 million user records on sale for $5,000.

ShinyHunters

Spurred by the success of Tokopedia, this hacker group went on to release 73 million user records from 10 companies on the dark web for sale. This includes user databases allegedly stolen from organizations such as online dating app, Zoosk (30 million user records); food delivery service, Home Chef (8 million user records); online marketplace, Minted (5 million user records); and U.S. newspaper StarTribune (1 million user records).

JUN

claire's

Jewelry and accessories retailer Claire's informed that hackers using Magecart tactics stole their customers' payment card data. The investigation identified the unauthorized insertion of code to its ecommerce platform, hosted on Salesforce Commerce Cloud, which was designed to obtain payment card data entered by customers during the checkout process.

JUL

Keeper Magecart Group

It was revealed that the Keeper group, a faction of the Magecart umbrella, targeted at least 570 ecommerce stores in 55 countries over a period of three years. Information on more than 184,000 stolen credit cards generated over $7 million in illegal transactions. 85% of the victim sites operated on the Magento CMS.

AUG

GARMIN

Hackers deployed the ransomware tool WastedLocker, encrypting key data on Garmin's digital infrastructure, and demanded $10 million. Garmin was forced to close its call centers, websites, mobile app and online services after the cyber attack.

Carnival

The world's biggest cruise operator which employs more than 150,000 staff and normally welcomes 13 million people on board its ships every year, announced that it fell victim to a ransomware attack which accessed and encrypted a portion of one of its brand's IT systems – and the personal data of both its customers and staff may be at risk.

Canon

Canon services suffered an outage caused by a maze ransomware attack, affecting internal applications, email servers, Microsoft Teams, and the USA website. The maze ransomware attack affected users of the 10GB free storage service.

SEP

Tesla was notified by an internal employee who had been approached with an unusual offer – for $500,000, the employee was to install ransomware on the company's network. The FBI worked with Tesla and the employee to set up a sting operation which led to the arrest of 27 year-old, Egor Igorevich Kriuchkov.

Shopify supports over one million registered merchants in 175 countries, including brands like Tesla and Sephora. An internal data breach compromised the personally identifiable information (PII) of about 200 users (storefronts). Shopify summarized the breach as the work of two rogue employees.

OCT

Singapore-based online grocery platform RedMart, which is owned by Alibaba, suffered a data breach that compromised the personal data of 1.1 million accounts. The compromised data contained personal information such as names, phone numbers, encrypted passwords, and partial credit card numbers.

NOV

The popular online game for 9- to 11-year-olds notified parents that 46 million records had been stolen via a cyber breach. Stolen records date as far back as 10 years; billing names and addresses accounted for only 0.02% of the breached records.

Disclaimer: Information gathered from The Cyber Security Hub (CS Hub), The SSL Store and other public sources. Webscale does not guarantee the veracity of these incidents.

Chapter 04

Ecommerce Security Trends in 2020

Ecommerce Security Trends in 2020

While there is clear evidence proving the relentless growth of cyber crime in 2020, four types of attacks have stood out due to their frequency and dramatic economic impact. These are Magecart attacks, carding attacks, ransomware, and credit card fraud, and they have destroyed millions of ecommerce dollars and thousands of jobs.

Magecart-type attacks – the second pandemic

Ecommerce security analysts unanimously agreed that Magecart-type attacks were the biggest threat to ecommerce in 2020 and beyond. Magento is the most abused platform by this attack, hence the name, however, OpenCart has also become a prime target. It is the umbrella term for 13 different cyber criminal groups who practice digital skimming or form jacking to hack their way into customer PII (personally identifiable information), especially credit card details, and sell them on the dark web. There were more than 2.5 million digital skimming incidents in 2020 compromising over 25,000 websites – major retail and travel brands like Macy's and Delta fell victim. By mid-2020, when the pandemic was in full force, and online shopping peaked, Magecart-type attacks became a frequent occurrence for ecommerce businesses. Magecart-type attacks have ranged from a simple dynamic injection of malicious code using a criminally hosted domain to leveraging Google Cloud or GitHub storage services and using steganography to embed malicious payment card-stealing code into an active domain's logos and images.

> There were more than 2.5 million digital skimming incidents in 2020 compromising over 25,000 websites.

The first high profile Magecart-type attack success was in late 2016 at Ticketmaster UK when about 40,000 customers fell victim to a scam. Their chatbot vendor Ibenta Technologies was the source, highlighting the risk that third-parties pose when it comes to Magecart-vulnerable blindspots for online merchants. One of the biggest Magecart-type attacks was on British Airways in September 2018, where the airline was fined $230M and remains exposed to millions more in liabilities.

Third-party vendors and open source libraries are used by retail websites now to deliver a rich customer experience. Unfortunately, these scripts introduce risks to the brand and business. While the attacks are difficult to detect early, there are few approaches that can work.

- **Inspect code thoroughly** as part of CI/CD process and do it early before going into production. Malicious codes that executes only in production can cause a challenge, so it's critical that site admins have the mechanisms in place to detect malicious code changes and JS anomalies.
- **Content Security Policies (CSP).** Developed by the W3C in response to XSS attacks. Real-time CSP protection enhances trust between the browser and application server, validating trusted domains and preventing blocked domains from executing scripts.
- **External scanner.** Continuous monitoring using a bot is highly advisable. This is an alert only solution, and since Magecart-type attacks are often a slow load process, the external scanner may not always detect a malicious code insertion.
    - Continuously monitor software/library versions.
- **Multi-factor Authentication (MFA)** locks down the admin to only authorized users, a critical first step in security, preventing bad actors from getting access to the backend.

Security solutions offering full visibility and control for real-time monitoring and early detection are critical to combat Magecart-type attacks. With customers increasingly unwilling to return to websites that have had a data breach, the risk of loss, both revenue and brand reputation, should be enough to push merchants to take appropriate measures to protect themselves and their customers.

Carding attacks – The silent killer

Once credit card information is stolen, cyber criminals have to validate the cards to sell them on the dark web, or use them for committing credit card fraud. Ecommerce websites are used to validate cards by attempting low-value transactions. Numerous API calls are made in the process. If the website has robust security in place, such nefarious traffic can be identified quickly and rate limiting can be activated on the check out process to defend against the attack.

Credit Card Fraud – The end game

Bad actors who procure stolen and validated credit cards use them to commit credit card fraud. In our survey, we found that many ecommerce merchants have not subscribed to a fraud detection solution. Without one in place, the site is a prime target. 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.

Ransomware attacks – The perfect storm

In 2020, ransomware attacks became one of the most common cyber attacks among organizations. Ransomware is a kind of malicious software that infects a computer system and demands a sum of money be paid in order to mitigate the issue. The most common types of ransomware include Maze, Crypto malware, Doxware, Lockers, RaaS, Scareware, and others. Some of the popular ransomware attacks include TeslaCrypt, Cryptolocker, Bad Rabbit, Petya, among others.

IBM Security X-Force has reported that ransom demands are increasing exponentially, some touching $40 million. Sodinokibi (also known as REvil) ransomware attacks account for one in three ransomware incidents IBM Security X-Force has responded to in 2020 so far. 41% of all ransomware attacks IBM Security X-Force analyzed in 2020 targeted organizations with operational technology (OT) networks.

In August, the world's largest cruise line operator, Carnival Corporation fell victim to a ransomware attack. The unauthorized third party had gained access to personal information relating to guests, employees, and crew for three of the corporation's brands, namely Carnival Cruise Line, Holland America Line and Seabourn, as well as casino operations.

Ransomware attack tactics increased in their severity in 2020. Threat actors now steal sensitive information before encrypting it, and if the victim chooses not to pay for a decryption key, attackers threaten to release stolen information publicly. Even if the victim can restore encrypted files from backup, they will likely suffer a data breach, a loss of data and customer records, and have to pay regulatory fines, not to mention the loss of customer confidence.

> Ransomware attack tactics increased in their severity in 2020.

The FBI does not support paying a ransom. Ransom payments encourage attackers to continue their malicious activity, validate their business model, and incentivize other cyber criminals. Yet, even in these difficult situations, companies can take actions that can help mitigate risks and minimize damage.

- **Maintain offline backups.** Availability of backup files can help a business recover quickly from a ransomware attack.
- **Implement a data theft prevention strategy.** This is critical as businesses today upload large amounts of data to cloud storage platforms that bad actors can misuse.
- **Monitor user account behavior.** Monitor and analyze user behavior to identify potential security risks. Quickly act on suspected abuse.
- **Deploy multi-factor authentication (MFA)** on all remote access points into an enterprise network. Focus on securing or disabling remote desktop protocol (RDP) access, a vulnerable entry point into a network for attackers.
- **Conduct penetration testing** to identify weak points in enterprise networks and vulnerabilities like CVE-2019-19781 that should be prioritized for patching.

Chapter 05

Ecommerce Threat Intelligence

Ecommerce Threat Intelligence

The omnichannel experience, where consumers can enjoy the same consistent user experience across any connected device, encourages the increasing use of third party software, analytics engines, digital payment systems, AI-powered search, marketing automation, and more – all stacked up, a potent cocktail for cyber attack success. While these innovations place the “customer first,” they can create a vast attack surface for cyber criminals to exploit and expose merchants to an increasingly sophisticated threat landscape.

The breadth of cyber risks that retailers now face is significantly broader and attacks themselves more frequently than ever. Webscale’s deep understanding of global attacker behavior is informed by monitoring and mitigating cyber risk for thousands of B2C, B2B, and B2E customers, 24x7x365, over the last eight years.

Since the volume and frequency of attacks are increasing, it is important to have a threat intelligence solution that can see through the noise and make the right decisions at the right time. When serious threats can be identified early enough, the business and the information security team, in particular, can focus on them and take appropriate action before it’s too late.

A robust threat intelligence solution will help:

- **Understand threat actors,** malware, and vulnerability trends and define a SecOps team that will be responsible for monitoring the latest security feeds
- **Proactively build defenses** against potential threats targeting the organization
- **Have a plan** to accelerate threat response times and ensure business continuity

Ecommerce businesses store large amounts of invaluable customer data, which means that cyber security cannot be an afterthought. It has to be part of the core business strategy. Any complacency can carry a severe cost, in the form of compliance penalties and loss of customer credibility, perhaps the most fragile and valuable commodity of them all.

Continuous threat monitoring and real-time fraud detection through robust threat intelligence should be more than a checkbox. They should be baked into the DNA of all online businesses, tightly coupled with established processes for continued cyber education and hygiene around your application and network infrastructure.

> While technology innovations place the “customer first,” they also create a vast attack surface for cyber criminals to exploit.

Chapter 06

Global Ecommerce Platform Vulnerabilities

Global Ecommerce Platform Vulnerabilities

Magento

M1 EOL in June 2020.

Magento is a favorite of Magecart groups looking to exploit flaws before patches are applied– SQL injections and XSS bugs usually. In 2020, Magento had 38 security vulnerabilities published.

(Webscale supports the Magento 1 platform for both, Community and Enterprise versions and has released patches and taken actions to counter all known vulnerabilities through our extensive M1 support initiative.)

Woo COMMERCE

In 2020, WooCommerce had 2 security vulnerabilities published.

WordPress

In 2020, WordPress had 21 security vulnerabilities published.

SAP
SAP Commerce Cloud

In 2020, SAP Commerce Cloud had 7 security vulnerabilities published.

HCL Commerce

IBM Websphere (now HCL Commerce) had 22 security vulnerabilities published last year.

php

In 2020, PHP had 12 security vulnerabilities published.

ORACLE
COMMERCE

Oracle Commerce did not have any security vulnerabilities published last year.

jQuery
write less, do more.

In 2020, JQuery had 3 security vulnerabilities published.

A

In 2020, Angular JS had 2 security vulnerabilities published.

BIGCOMMERCE

BigCommerce did not have any security vulnerabilities published last year.

shopify

Shopify did not have any security vulnerabilities published last year.

Disclaimer: Information gathered from stack.watch. Webscale does not guarantee the veracity of this information.

Chapter 07

Technologies to Consider

Technologies to Consider

AI/ML-led Automation

Artifical intelligence (AI) and Machine Learning (ML) are changing the game for cyber security, analyzing massive amounts of risk data to deliver instant insights and real-time alerts to accelerate response times and increase the output of commonly under-staffed security teams. For many years now, malware attack responses have been automated, with good results. This involves moving infected files into quarantine before disruption is caused.

Increasingly, ecommerce merchants evaluating security solutions are demanding AI and ML to expand the scope and impact of their investments. Traditional security systems are programmed, rule-based and playing catchup when threats are constantly evolving. Also, as ecommerce businesses grow, unencumbered by geographical boundaries, traditional security solutions cannot scale. Next-generation cloud security systems will leverage AI, ML, and NLP (Natural Language Processing) to scale faster, learn quickly and respond to threats sooner.

AI in cyber security automates the consumption of security information from threat intelligence feeds, security events, and related data, as well as sources like research papers, security blogs, websites and advisories. The resulting knowledge base can then be used to gather insights and create smarter response plans.

> Next-generation cloud security systems will leverage AI, ML, and NLP to scale faster, learn quickly and respond to threats sooner.

Like many surveys reveal, including ours, even though cyber attacks have the power to bring an ecommerce business to its knees, cyber security remains an area that does not receive the attention it deserves. Cyber security teams are grossly understaffed even in large successful ecommerce organizations. It is here that AI can help augment critical capability.

For example, in the case of threat hunting, which is largely a manual affair, AI can pour through large volumes of data to quickly identify bad actors. In tandem, ML can be leveraged to reduce false positives when looking for potential security vulnerabilities in source code, or detect changes in user behavior.

The goal is to be better informed, even if you don't have the staff to do it, prevent attacks before they happen and if they do, eliminate or minimize their effects as soon as possible.

Real-time CSP Protection

Ecommerce websites use dynamic JavaScript codes on the client-side browser to offer customers a compelling digital experience. Services like chatbots, analytics, and payments are typically third-party JS components. In fact, more than 50% of scripts on a website are third-party. Even first-party scripts extensively use open source libraries to deliver specific functionalities. Magecart and other digital skimming attacks thrive on the vulnerable client-side. The W3C consortium formulated CSP to tackle XSS. In an XSS attack, a piece of malicious JS code on a web page loads a script from a malicious domain. CSPs prevent such unauthorized code injections.

However, implementing CSP protocols is challenging in ecommerce websites that are dynamic with CI/CD methodologies. Maintaining allow lists when there are so many third-party vendors involved is cumbersome. Lack of visibility to third-party applications on a client's browser is another reason why CSP protection may not always be effective. However, real-time CSP protection enhances trust between the browser and application server by validating "trusted" domains executing scripts, and prevents or reports any block-listed domains from executing scripts on the browser.

While CSP is not a 100% fail-proof strategy against Magecart and other digital skimming attacks, not implementing CSP on the client-side is effectively turning a blind eye to potential attacks.

Fraud Detection

In a year that saw ecommerce and online payments skyrocket, the focus on fraud detection and prevention is nothing but timely. Chargebacks, credential stuffing, and account takeover (ATO) attacks are eating away into the profits of ecommerce merchants.

Identifying genuine transactions and minimizing false positives is as important as detecting suspicious anomalies and fraudulent transactions.

As Strong Customer Authentication (SCA) under PSD2 comes into effect in Europe soon, it will lead to wider use of two-factor authentication – mostly in the form of 3-D Secure. This will certainly lead to sales disruption for many merchants.

Identifying genuine transactions and minimizing false positives is as important as detecting suspicious anomalies and fraudulent transactions. To reduce friction for genuine customers, merchants have been working on planning and agreeing their SCA exemptions strategy with their acquirer. They also continue to monitor transactions for fraud themselves, to ensure fraud rates are kept low so as to qualify for these exemptions.

A comprehensive fraud detection solution, consisting of AI/ML, positive profiling, and smart use of third-party intelligence via an orchestration engine combined with a team of specialized fraud analysts, will offer merchants the best chance of achieving the right balance between fraud prevention and maximizing the revenue from genuine customers. Beware of misleading advertising by some fraud detection solutions in the market with high price tags that do nothing more than score to prevent a portion of charge backs.

Real User Monitoring (RUM)

In the “always-on” world of ecommerce, compelling and personalized user experiences are delivered by a complex multi-tier application ecosystem. It is this very complexity that is hindering optimal performance across devices, services, and applications. APM (Application Performance Management) professionals increasingly demand real-time visibility into the application landscape to monitor and detect vectors impacting customer journeys.

Synthetic monitoring for years has helped webmasters test applications before they go into production. However, more traditional synthetic monitoring has fallen out of favor with merchants seeking real-time visibility and insights into the end-user experience of their storefront.

RUM gathers data from the frontend and backend and delivers accurate, real-time transactions – actual site log-ins, site hits, clicks, requests for data, and other server transactions, and detection information – page load times, traffic bottlenecks, global DNS resolution delays. With RUM, merchants can monitor the end-user experience and prioritize issues based on end-user impact, thereby ensuring customer satisfaction.

In most businesses, especially ecommerce, the “build it, and they will come” approach is unlikely to succeed without application uptime monitoring. RUM puts the website visitor at the center of the universe, tracks their evolving needs, and allows merchants to make decisions that directly impact customer engagement.

Chapter 08

The Road Ahead

The Road Ahead

A message from Webscale's CEO, Sonal Puri

2020 was a challenging year for the world, one of tremendous growth and opportunity for the ecommerce segment, and sadly one of the best years for cyber crime startups. Far from the lone wolf, hooded hacker image we have become accustomed to, today's cyber criminal networks are funded, organized, and highly capable.

While these groups are scaling their operations and widening their reach, we, as a community, have gotten much better at predicting their attack vectors and developing solutions that can monitor, identify and defend against a myriad of threats.

Cloud security solutions that incorporate automation led by AI and ML can analyze massive quantities of data, recognize patterns, and predict imminent threats. The ecommerce businesses we surveyed for this report indicate genuine intent to invest in such solutions this year, to build their defense against malicious attacks. While this spending is often the hardest to do, because "if it's not broken, why fix it," PwC's latest Global Economic Crime and Fraud Survey says it best: "When it comes to preventing and tackling fraud, our research shows that a dollar invested now is worth twice as much when a fraud hits."

The International Data Corporation (IDC), in its Worldwide Security Spending Guide, had projected worldwide spending on security-related hardware, software, and services at $125.2 billion in 2020, an increase of 6.0% over 2019. As the global economy recovers from the impact of COVID-19, IDC expects worldwide security spending to reach $174.7 billion in 2024 with a CAGR of 8.1% over the 2020-2024 forecast period. Security services will be the largest and fastest-growing segment of the security market, accounting for roughly half of all spending. Managed security services – single-tenant solutions operated by third-party providers and residing on customers' premises – is the largest category of security services spending, followed by integration services and consulting services. Software will be the second largest segment of the security market, led by endpoint security and security analytics, intelligence, response, and orchestration software.

While businesses are bullish about investing in cyber security tools, another area of concern is the grossly inadequate pool of trained cyber security professionals globally. Research by the International Information System Security Certification Consortium (ISC)² says that, in the US alone, the cyber security workforce will need to grow by 62%, and globally by 145%, to meet the demands of the business. This is another reason why investing in the right cyber security solution with a high level of automation and from the right vendor, whose pool of experts can become your extended team, are both critical.

In our experience, we can outline a straightforward 4-step plan to get ahead of cyber crime.

- **Evaluate the security vulnerabilities of your business** and the economic value of a data breach (compliance fines, customer litigations)
- **Create a cyber threat strategy** that covers your business' complete ecosystem – customers, partners, vendors, and employees.
- **Invest in automated, comprehensive cyber security solutions** that offer full visibility into infrastructure, traffic, and assets, and an expert team (internal or external) that understands cloud and ecommerce.
- **Enforce a zero-trust strategy.** Educate employees about cyber security best practices, the company's data policy, and the cost of non-compliance.

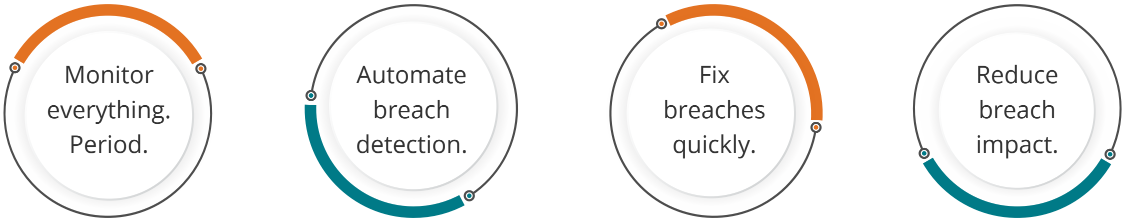
Be Smart.
Be Secure.

Chapter 09

How can Webscale help?

Enterprise-grade Security and Automation

Webscale is the world's safest cloud hosting platform for ecommerce. Thousands of B2C, B2B, and B2E storefronts rely on Webscale to deliver a fast, flawless, and secure shopping experience for their millions of customers. Webscale follows a four-point charter to address cyber security for ecommerce businesses:



Monitor everything. Period.

Automate breach detection.

Fix breaches quickly.

Reduce breach impact.

- **Monitor everything. Period.** Going beyond a simple WAF, Webscale throws a security blanket around the business covering the frontend (web traffic), backend (malicious code insertion), and browser (bad scripts), and we monitor everything in and out.
- **Automate breach detection.** Relying on manual intervention to fight cyber crime is impossible as the threat landscape is vast and evolving, and bad actors are sophisticated. Webscale's ML-led automation scans the landscape for gathering vital threat intelligence and aids in Intrusion Detection even before an attack can be executed.
- **Fix breaches quickly.** In the unfortunate event of a security incident, time is of the essence. Webscale's Application Shield and real-time CSP Protection cordon off the attack surface and secure the application and infrastructure. Our team of cloud security specialists work closely with the merchant to fix the breach.
- **Reduce breach impact.** A successful cyber attack always comes with an economic impact for the business, be it lost sales, compliance fines and/or customer litigations. Webscale's security team is focused on reducing the impact of the breach by adopting insights and best practices gathered from 8 years of defending storefronts from vicious attacks.

During the 2020 holiday season, Webscale mitigated over 520 million threats, and no customers were impacted in any way during their busiest, and most lucrative quarter.

What is 360° Security?

Webscale has developed the ecommerce segment's most complete security technology stack, offered as part of our hosting plans and services, and designed to protect your users from the myriad of evolving threats.

Focus your Site Experience on Actual Shoppers
Website traffic can arrive any time from different geos, networks, and devices, some of which you may not even serve. With Web Controls, Rate Limiting, and Access Control, you can block threats, limit requests or allow only valid users to access your storefront, reducing security risk, providing a rich user experience to actual shoppers, and maximizing cart conversions.

Protection Against Account Takeovers
Username and password lists are regularly sold to hackers who use them to take over unsuspecting user accounts—an attack known as credential stuffing. Once access is gained to a single site, hackers can disrupt the entire digital life of that user. Allowing your customers to be exposed in this way destroys the hard-earned trust of your customers and can have a significant, long-term impact on revenue. Together, Webscale's real-time Traffic Viewer, which provides deep visibility into login pages, tracking both successful and failed logins, and Rate Limiting, make it easier to detect brute force attacks or repeated failed logins, shutting down, or limiting access, to login pages.

Magecart Attacks
Magecart attacks are now very common in ecommerce. They insert malicious code into the ecommerce application in order to skim sensitive information such as credit card data and social security numbers. They can go undetected for long periods of time, so consistent monitoring is essential. Webscale's CSP protection identifies, in real-time, any script violation from a pre-established policy and reports (or prevents) the malicious script so that administrators can take immediate action to protect the website.

Serve Real Customers, not Bots
Bots can account for up to 50% of your storefront's traffic, consuming capacity and impacting user experience. You can easily identify legitimate bots (Google, Bing) using pre-configured Address Sets and serve them from Webscale Dynamic Site Cache without using up infrastructure capacity. In addition, Webscale Cloud Bot Manager allows you to block access to unwanted bots through a dynamically maintained database of known bad bots, refreshed every five minutes.

Price and Content Scraping
Price and content scraping techniques are unfair, often illegal means by which competitors or hackers use botnets to obtain real-time information about your products and prices. Typically, products are bought and sold at lower price points to gain a competitive advantage. Through Webscale Cloud Bot Manager's machine learning, Anomaly Detection helps detect these sophisticated bots from actual human users, protecting your business from outside threats.

The World's Safest Cloud Hosting for Ecommerce.

Smarter Security for Smarter Hackers
Hackers will frequently use bots that pose as humans and avoid obvious attack vectors such as a flood of traffic. Instead, they may insert malicious code on the backend and execute this code through seemingly normal web traffic requests. Unlike other security vendors (firewalls, CDNs) that only have access to traffic, Webscale's deep application visibility, Intrusion Detection, and inbuilt Elastic WAF can detect spurious infrastructure changes, quarantine the infected servers, self-heal the backend, and block any requester trying to execute the malicious code—all before a single request can adversely affect your website.

The Edge is Not Enough
If a hacker is able to circumvent the firewall layer, and attack the application infrastructure directly, all the security you have at the edge is redundant. With App Shield, your application will only respond to traffic that is being served directly from the Webscale platform, which is always enabled with the latest enterprise-grade security protocols.

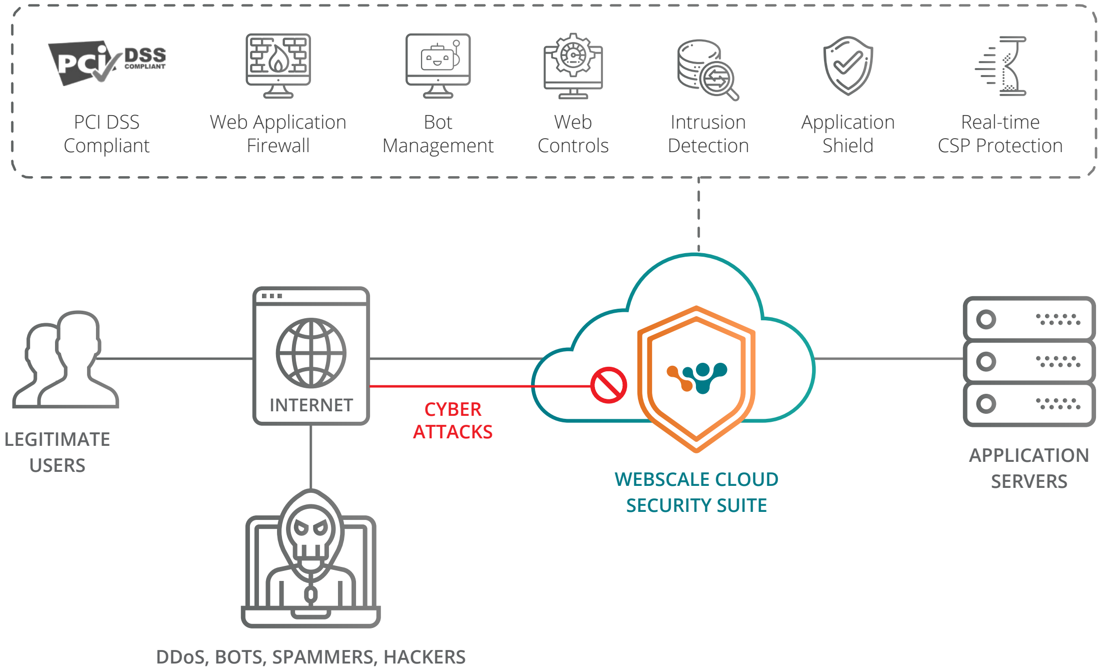
Webscale Security Solutions

Whether you are hosted with Webscale, or on a hosted platform such as Magento Commerce Cloud or SAP Commerce Cloud, Webscale has a security solution to address your need.

Webscale Cloud Security Suite

Webscale Cloud Security Suite is a 360° security solution that provides the ecommerce industry's most robust protection against attacks from the frontend through web traffic, malicious code inserted into the backend, or browsers executing scripts stealing sensitive information. Websites protected by Cloud Security Suite have comprehensive, always-on security with application-aware, customized rules to protect against sophisticated attacks. In addition to a managed WAF, Cloud Security Suite includes a range of features that allow for real-time application monitoring and analysis through machine learning, detection, automated mitigation, and ongoing protection. Cloud Security Suite is available as an add-on to all Webscale Cloud Hosting plans.

- A comprehensive security solution that goes beyond a traditional WAF to address bot management, application shielding, intrusion detection, and real-time CSP protection.
- A 360-degree security solution that provides robust protection against attacks from the frontend through web traffic, malicious code inserted into the backend, or browsers executing scripts stealing sensitive information.
- Enables threat analysis through machine learning, early detection and automated mitigation.
- Offers unmatched visibility and control with Webscale Web Controls, a DIY policy and rules engine.

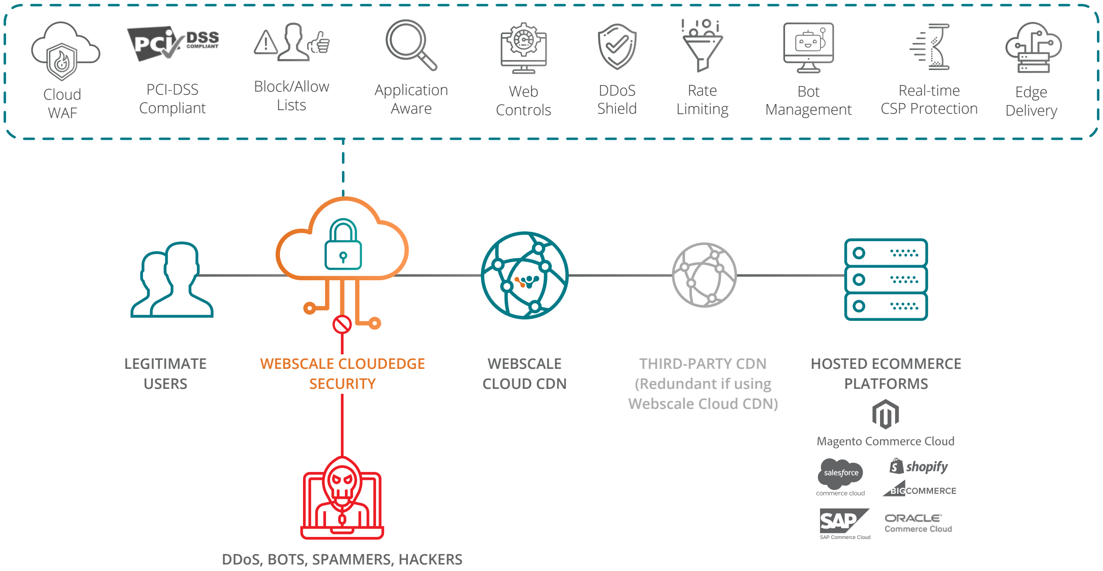


DOWNLOAD THE DATASHEET

Webscale CloudEDGE Security

Webscale CloudEDGE Security is a comprehensive security solution deployed on the traffic edge to fortify storefronts on hosted platforms like Magento Commerce Cloud, BigCommerce, Shopify, SAP Commerce Cloud and Salesforce Commerce Cloud or within a site deployed with a headless frontend and fully hosted backend. Combining the best of Webscale security and support, CloudEDGE Security offers merchants demanding more than the bundled basic CDN and WAF solutions offered by their provider and frustrated by their poor support, a scalable, responsive, and cost-effective security solution. Websites protected by CloudEDGE Security have unmatched visibility and insights into their application infrastructure through Webscale's Customer Portal and Web Controls, a DIY security policy engine, in addition to power-packed security features like rate limiting, real-time CSP protection, and bot management.

- Enterprise-grade security for any hosted ecommerce platform.
- Sits alongside Webscale CDN or any 3rd party provider; supports all hosted ecommerce platforms.
- Fills "product gaps" inherent in bundled security solutions, reducing security risk and exposure for merchants
- A comprehensive security solution that addresses application shielding, bot management, and real-time CSP protection.
- Enables threat analysis through machine learning, early detection and automated mitigation.
- Offers unmatched visibility and control with Webscale Web Controls, a DIY policy and rules engine.



DOWNLOAD THE DATASHEET

Q&A with Jay Smith

Webscale's Founder and CTO

What are your top 3 observations on the state of ecommerce security in 2020?

Last year, while ecommerce businesses were growing unhindered as a result of the pandemic, they also became extremely vulnerable to three types of security threats – Magecart-type attacks, carding attacks, and credit card fraud.

- Magecart-type Attacks
- Carding Attacks
- Credit Card Fraud

These are all a value chain progression from a cyber criminal's standpoint. First, credit card information is stolen, then the cards are validated to see if they are active or not, and finally, they are used to commit fraud.

Ecommerce websites are seen as the easiest platform through which to commit these three types of crime, so merchants need to double down on security, more so now than ever before.

This industry is set to grow even more this year, attracting more traffic and revenue, and that's only going to make it more attractive for cyber criminals.

What 3 things should merchants do, today, to improve their security posture in 2021?

To start with, lock down your site admin. MFA (multi-factor authentication) is the best way to do this as it's easily managed.

At Webscale, we have our DIY policy engine, Web Controls, to do this, and even non-technical staff can create these security rules with a few clicks. When in doubt, err on the side of being over restrictive.

Secondly, rate limit the checkout process the moment you witness an abnormally large number of API calls or requests, especially if they originate from a geography you deem suspicious. This way, you can avoid a carding attack.

And thirdly, subscribe now to a good fraud detection service if your charge backs are high enough to warrant the spend. Credit card companies give you some protection but fraud attacks are on the rise, and you certainly don't want to be at the receiving end.

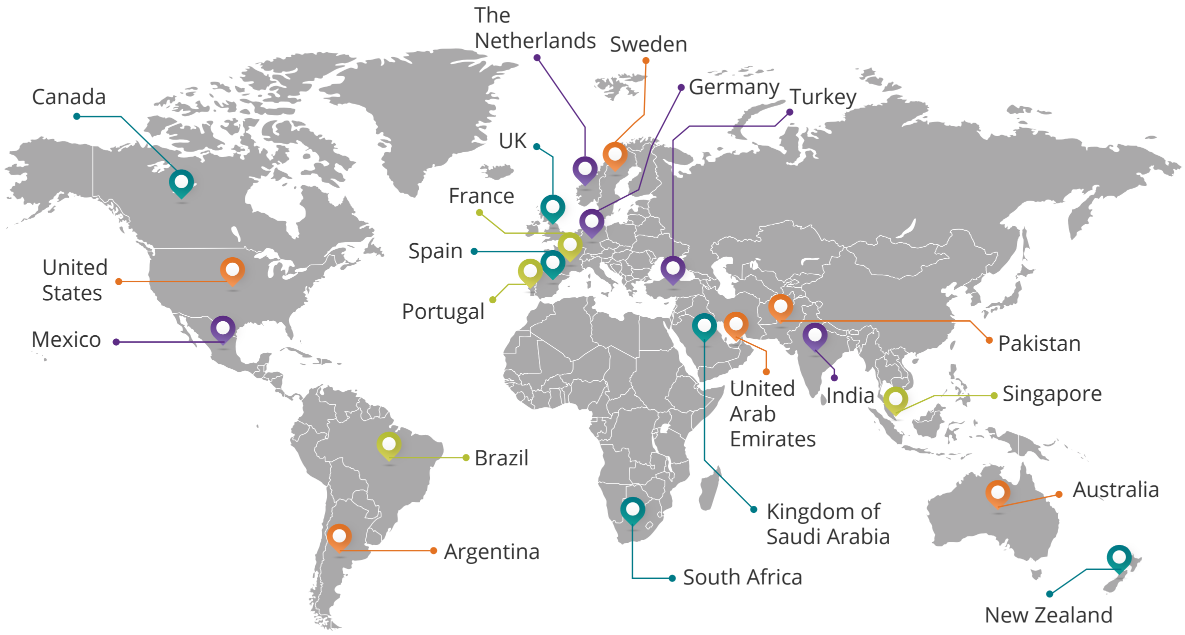
- MFA (Multi-Factor Authentication)
- Rate Limiting
- Fraud Detection Service

Chapter 10

About the Report

Demographics of Respondents

21 Countries



18 Industries

Fashion and Lifestyle

Health and Fitness

Home and Gardens

Banking and Financial Services

Food and Drink

Industrial and Hi-tech

Technology and Computing

Travel and Hospitality

Media and Publishing

Consumer Packaged Goods

Energy and Utilities

Chemicals

Telecom

Automotive

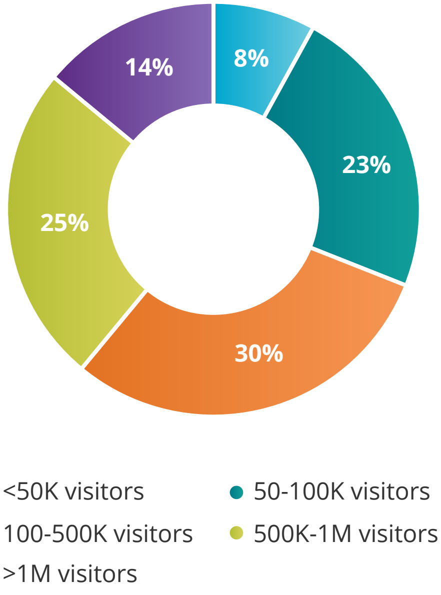
Arts and Entertainment

Family and Parenting

Electrical and Electronics

Hobbies and Interests

Website Traffic of Respondents

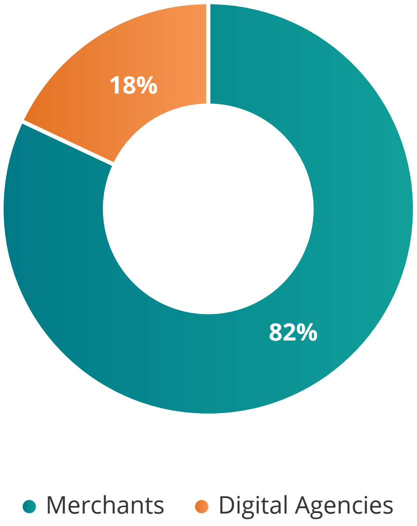


Number of Respondents

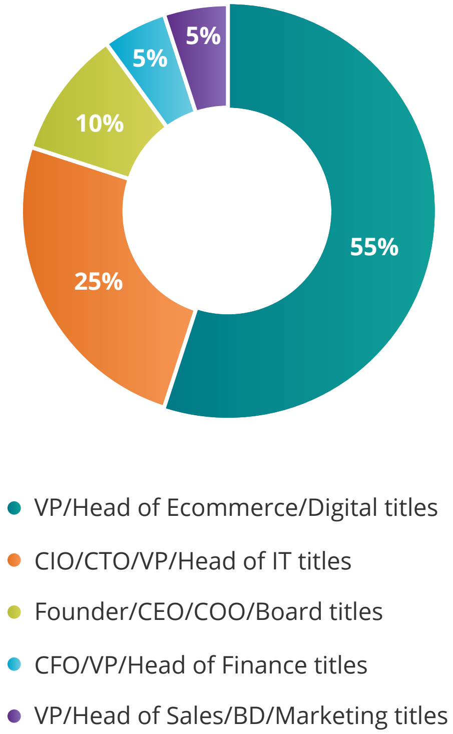
1572

Executives

Nature of Respondent’s Business



Role of Respondents



Sources

The Effect of Cyber Crime on Online Shopping

Cyber Crime Costs Projected to Reach $2 Trillion by 2019

Cybersecurity Spending to Reach $123B In 2020

Holiday Sales Hit $876 Billion: by the Numbers

Cyber Security Statistics Guide for 2020

PwC's Global Economic Crime and Fraud Survey 2020

2020 Top Breaches

Top 10 Cybersecurity Incidents in 2020

Ransomware 2020: Attack Trends Affecting Organizations Worldwide

Hackers Break into 570 Ecommerce Stores

Follow Security Vulnerabilities in your Favorite Software Stacks

Ongoing Demand Will Drive Solid Growth for Security Products and Services, According to New IDC Spending Guide

The Definitive Cyber Security Statistics Guide for 2020

(ISC)² Finds the Cybersecurity Workforce Needs to Grow 145% to Close Skills Gap and Better Defend Organizations Worldwide

The Global Ecommerce Security Report 2021

Published in February 2021 by Webscale Networks, Inc.

About Webscale

Webscale is the world's safest cloud automation, management and hosting provider focused exclusively on ecommerce challenges. Offering enterprise-grade security, predictive scalability and blazing-fast performance, the Webscale SaaS platform leverages automation and DevOps protocols to simplify the deployment, management and maintenance of infrastructure. The platform supports omnichannel use cases across a variety of ecommerce platforms and architectures, including headless, progressive web applications, self-hosted and fully hosted commerce clouds. Webscale can be deployed immediately in 75 countries in multi-cloud environments, including Amazon Web Services, Google Cloud Platform, and Microsoft Azure. Webscale powers thousands of B2C, B2B, and B2E ecommerce storefronts in ten countries and seven of the Fortune 1000 businesses and has offices in Santa Clara, CA, Boulder, CO, San Antonio, TX, Bangalore, India and London, UK.

Webscale Global Headquarters
5201 Great America Parkway, Suite 232
Santa Clara, CA, 95054

Need urgent help?
Reach our global security response team
at **secure@webscale.com**

WEBSCALE

www.webscale.com