WEBSCALE

The Global Ecommerce Security Report 2022

Insights and Learnings from a
Blockbuster Year for Commerce

Table of Contents

01 | 2021 Holiday Shopping: Share of Online Drops

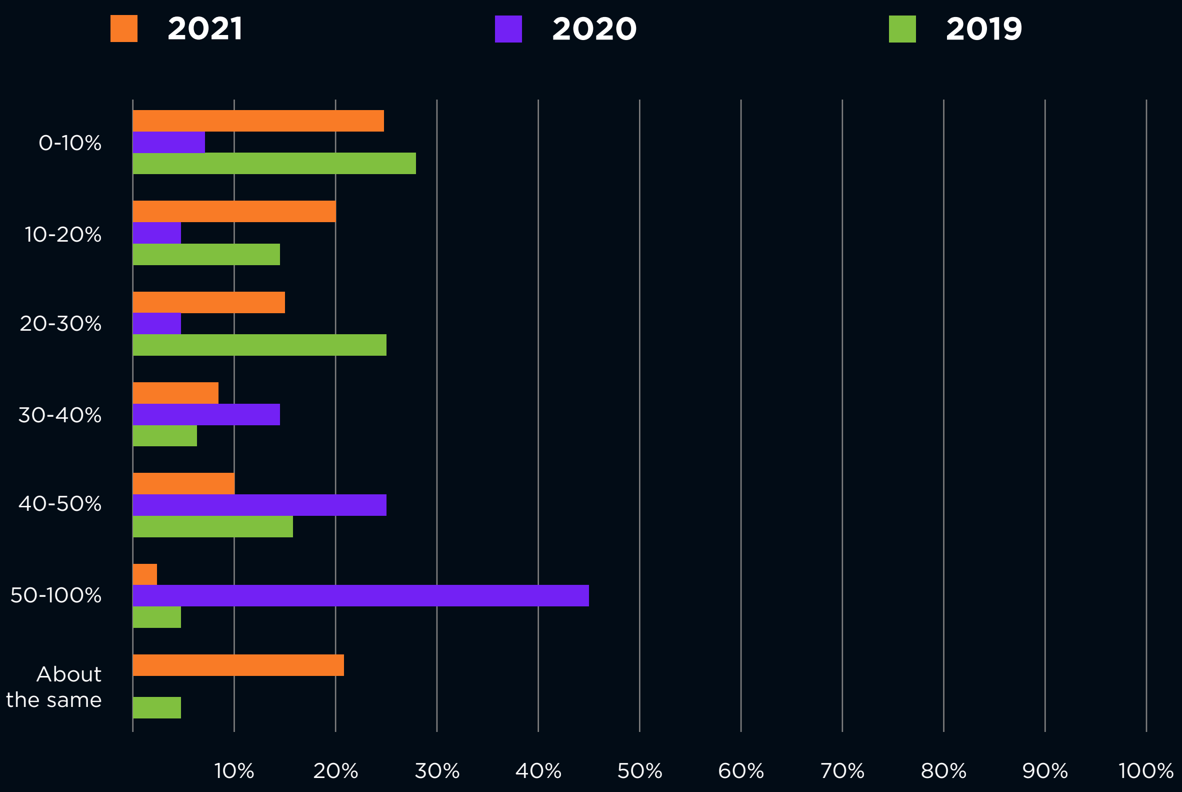
With supply chain-related challenges due to COVID-19 plaguing virtually every industry throughout 2021, nearly 50% of consumers, according to the National Retail Federation (NRF), began their holiday shopping earlier than Thanksgiving. More than 55% of merchants surveyed by Digital Commerce 360 kicked off sales events before November, some as early as August 2021.

U.S. consumers spent $33.90 billion online during the Cyber 5 weekend, a 1.4% year-over-year (YoY) decline from the $34.36 billion in ecommerce revenue during the same weekend in 2020, according to Adobe's Digital Economy Index.

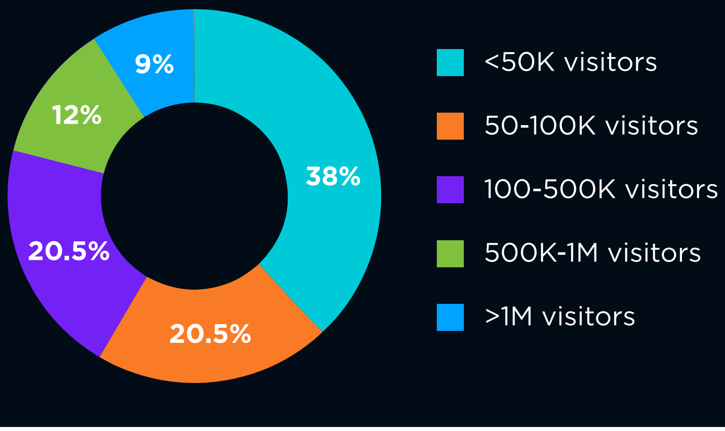
From $9.03 billion in 2020, Black Friday 2021 sales were down marginally by 1.4% to $8.9 billion — its first-ever YoY dip. Cyber Monday sales also slumped 1.4% YoY to $10.7 billion. Online sales on Thanksgiving Day stayed flat at $5.1 billion.

21% of merchants Webscale surveyed reported more than 30% growth in sales during the Cyber 5 weekend; for 20.5% of the businesses, sales remained flat compared to the previous year.

% growth in sales on Black Friday/Cyber Monday



Total site traffic in November 2021

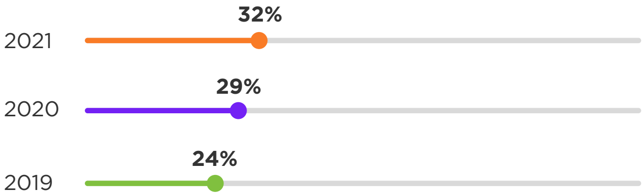


02 | Availability Woes Continue

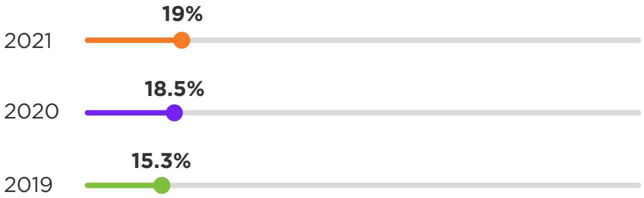
Office Depot went down for hours on Cyber Monday. Other major retailers, including Walmart, GameStop, Boohoo Group PLC's fashion brand PrettyLittleThing, Bass Pro Shops and its Cabela's brand site, also suffered website outages and other performance issues during Cyber 5. As a result, Office Depot had to extend its Cyber Monday sale through Tuesday; so did many others.

Average downtime on Black Friday/Cyber Monday

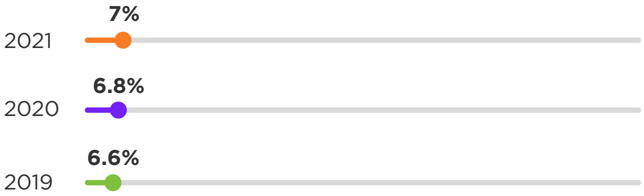
Merchants who experienced outages in excess of 5 min



Merchants who experienced outages in excess of 10 min



Merchants who experienced outages in excess of 30 min



Webscale's patented predictive auto-scaling and high availability (HA) architecture delivered 100% uptime for thousands of B2C and B2B storefronts on our SaaS platform while reporting more than 15 billion traffic requests and processing 7.2 million checkouts just through November.

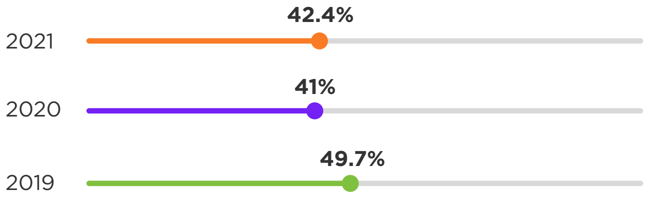
03 | High Performance is Table Stakes

Merchants need to focus more on getting performance right, now more than ever. More than 80% of the world's websites fail Google's Core Web Vitals, its new ranking algorithm designed to evaluate the user experience of a website.

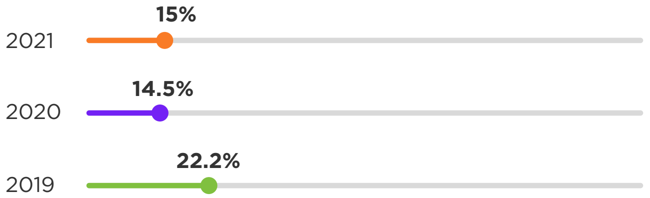
Just 12% of ecommerce merchants Webscale surveyed think poor Core Web Vitals is a critical business challenge.

Average page load time on Black Friday/Cyber Monday

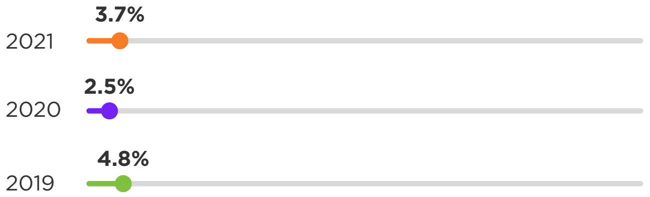
Merchants who faced page loads times in excess of 3 sec



Merchants who faced page loads times in excess of 5 sec



Merchants who faced page loads times in excess of 10 sec



During the 2021 holiday season, merchants on the Webscale SaaS platform reported improvements in mobile performance by an average of 20+ points and desktop performance by 50+ points in Core Web Vitals. Ecommerce businesses with PWA storefronts saw improvements in excess of 200% in mobile performance.

04 | State of Ecommerce Security

The 2021 ecommerce security report card is disappointing and disturbing. And, by all accounts, 2022 is on its way to becoming yet another banner year for cybercrime targeting online storefronts.

As this report was getting drafted, news broke of over 500 ecommerce sites being hit by a Magecart attack compromising payment information. In January, the ecommerce website of Segway, the manufacturer of single-rider vehicles was impacted by the same attack, as were over 4151 small business websites in November, according to the UK's National Cyber Security Centre (NCSC).

> Phishing, carding, identity theft, ransomware, chargeback fraud, 'silent' fraud, account takeovers, and pharming are major threats for online shoppers and merchants.

Phishing attacks, carding attacks, identity theft, ransomware, chargeback fraud, 'silent' fraud, account takeovers (ATO), and pharming are major threats for online shoppers and merchants.

The U.S. Federal Trade Commission (FTC) has said that financial advisory services, romance, and ecommerce, combined, accounted for 70% of all social media scams in 2021.

Smart hackers are upping the game, and data is increasingly being exfiltrated as well as encrypted, a process known as double extortion. Ransomware as a Service (RaaS) and double extortion ransomware are expected to explode in 2022.

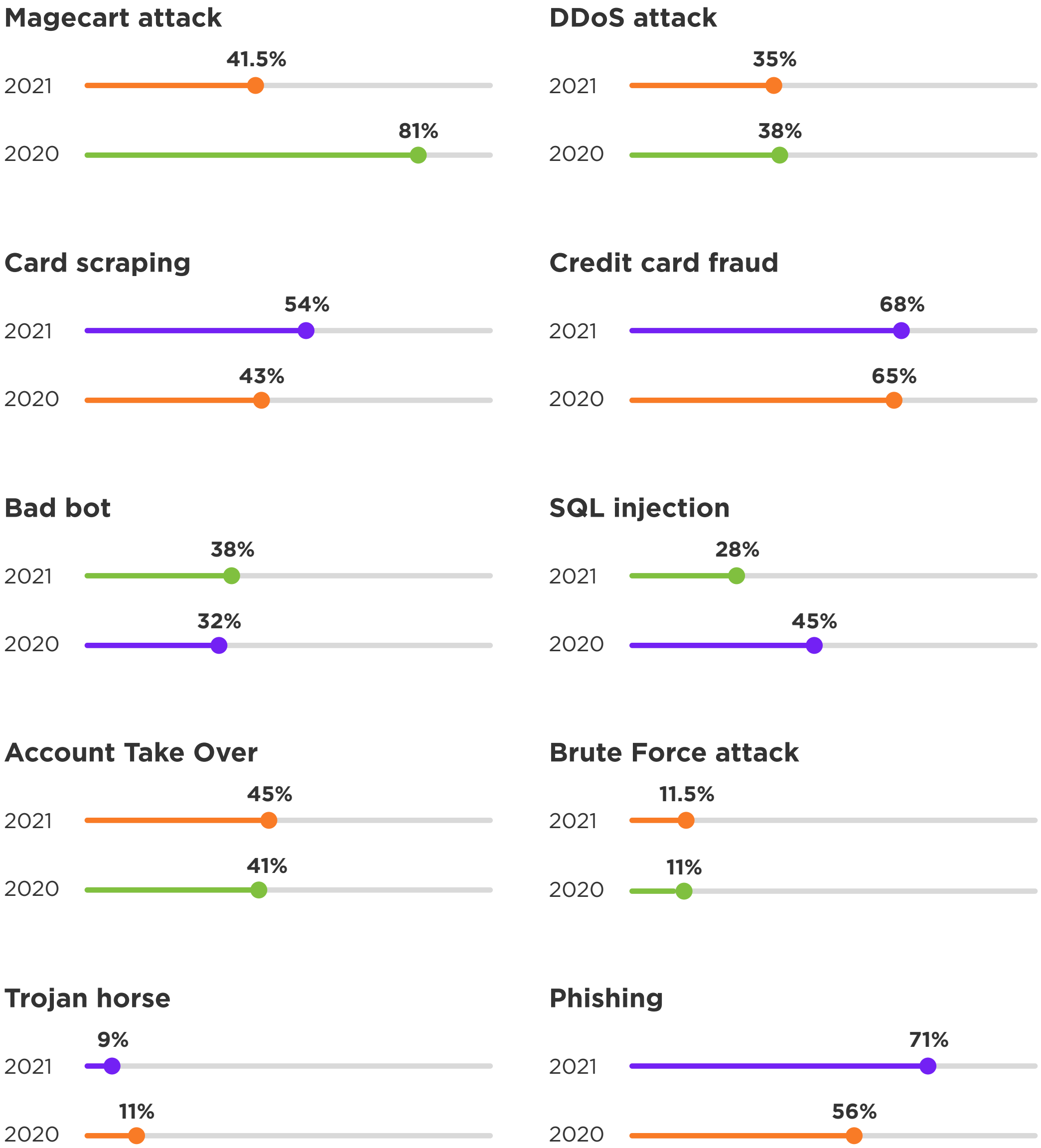
More and more businesses are today maintaining secure backups to avoid having to pay a ransom to unlock encrypted data. Frustrated cybercriminals are now threatening to expose sensitive data publicly. With the fallout from such a breach impacting customers, partners, and service providers, businesses face significant risk, in the form of loss of revenue and reputation, litigation costs, and penalties.

Did you experience any security-related incidents on Black Friday/Cyber Monday?

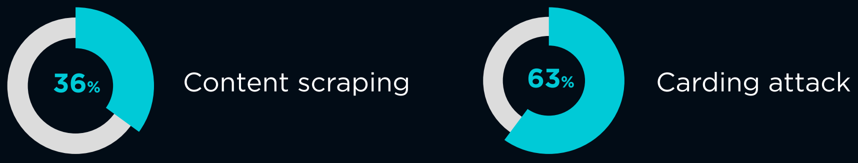
2021	2020	2019
82.5% ✓	78% ✓	32.6% ✓
✗ 17.5%	✗ 22%	✗ 67.4%

Cyberattacks continue to rise

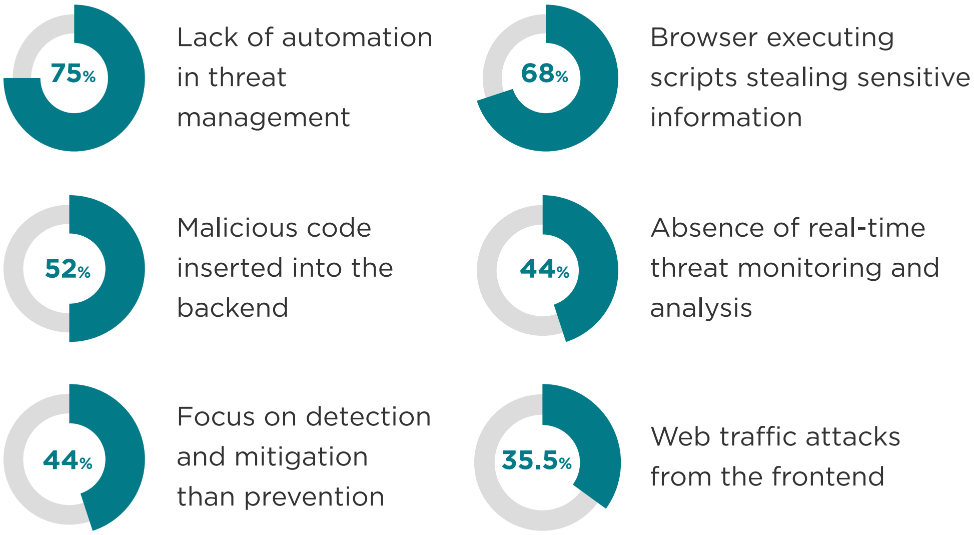
Holiday season 2021 saw increases in the number and types of attacks (compared to 2020)



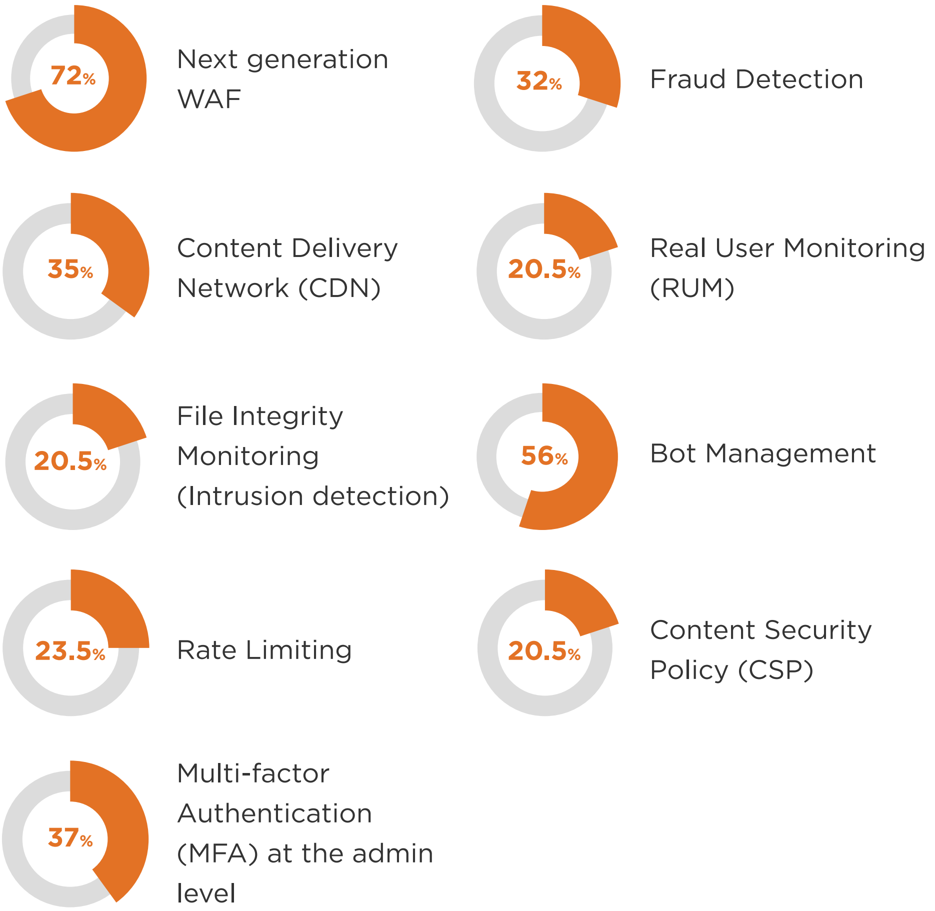
New attack types included this year



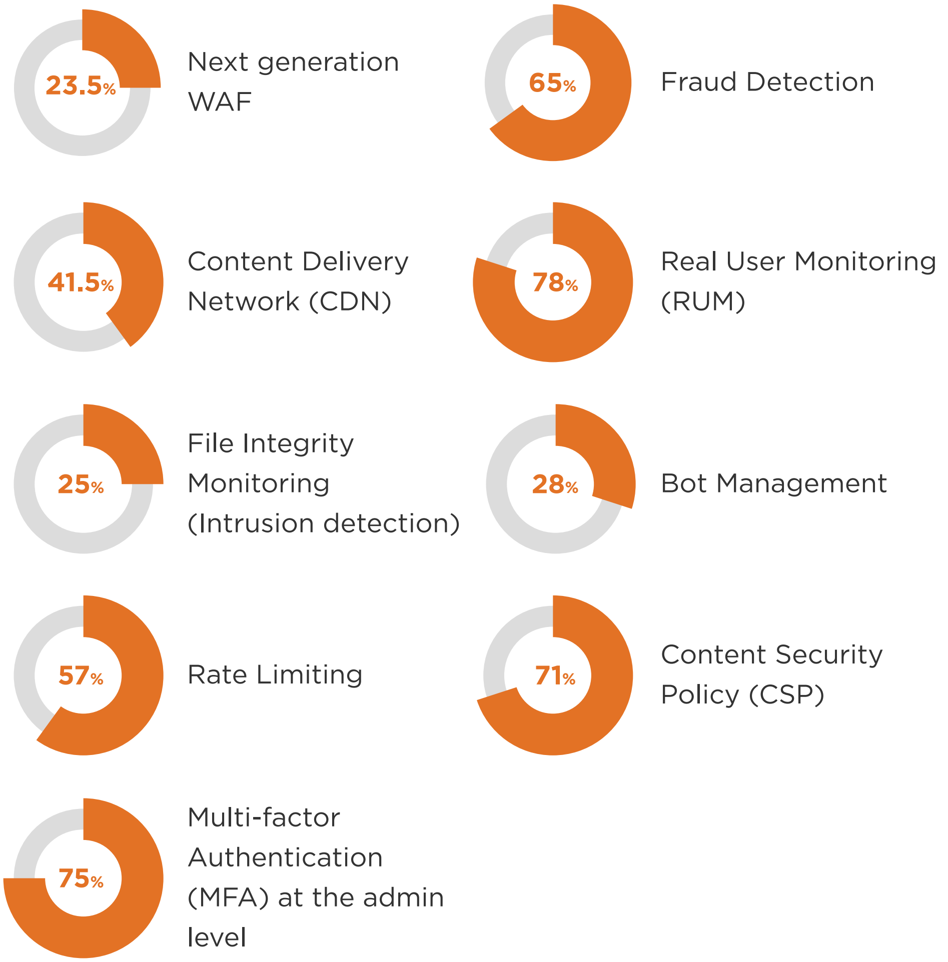
Major security challenges merchants faced in 2021



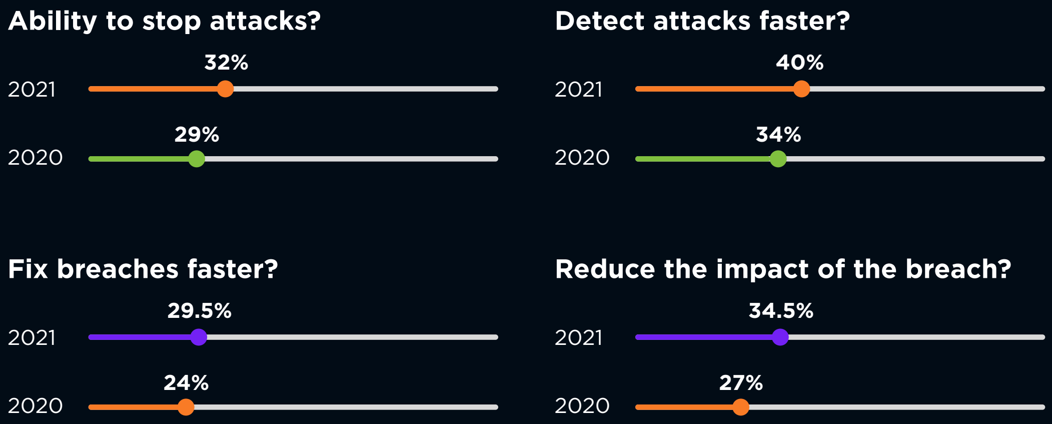
Security technologies merchants are already employing as part of their hosting infrastructure



Security technologies merchants are considering investing (in the next 3 years) to enhance their security posture



Security readiness of merchants in 2021



According to multiple reports, more than half of all cyberattacks on ecommerce websites in 2021 were carried out by bots, including sophisticated bad bots that can mimic human behavior. With many ecommerce platforms bundling just a traditional WAF (web application firewall) as the only line of defense against bot attacks, sophisticated bots are triggering fraud and account takeovers (ATO) with ease.

September 2021 recorded an unprecedented rise in Distributed Denial of Service (DDoS) attacks across ecommerce platforms, attributed by the ecommerce security community to the “Meris” bot. Cybersecurity experts say that the DDoS attacks from this network are capable of disrupting ecommerce platforms by flooding them with bot traffic and rendering them useless for genuine customers.

More than half of all cyberattacks on ecommerce websites in 2021 were carried out by bots.

DDoS attacks spiked on Black Friday and Cyber Monday, with some reports stating the YoY increase in 2021 was over 200%.

In a study conducted by the US-based Aberdeen Strategy and Research, it was estimated that 75-80% of ecommerce operational costs (including the cost of website hosting infrastructure, website marketing spend, cost of checkout fraud) — are negatively impacted by malicious bots, which equates to between 18-23% of net revenue across the six popular ecommerce categories (consumer electronics; fashion and beauty; food and beverage; furniture, appliances and home improvement; general merchandise; and health and leisure) that were evaluated.

An advanced bot management solution that includes proactive detection and rapid mitigation, can cut this impact in half, even more at times of peak bad bot traffic, safeguarding the bottom line.

However, 44% of merchants Webscale surveyed do not have a bot management solution in place.

Top 5 Attack Types of 2021

Phishing

Phishing is a social engineering attack used to steal data, including user credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.

Multi-factor authentication (MFA) can easily secure web applications from the aftermath of a successful phishing attack.

In our survey, merchants reported that phishing grew 71% in 2021 over the previous year. But only 37% of merchants have deployed MFA.

Card scraping

Through successful phishing campaigns, bad actors gain access to admin sites, installing card scrapers designed to extract credit card information. A trojan horse that comes in through a phishing attack can kick start card scraping or when a weak password is broken by the intruder. If multi-factor authentication (MFA) has been implemented for the admin site, the trojan horse cannot fully break in.

A card scraper can also be surreptitiously included in any 3rd party JavaScript tool a developer downloads for use on an ecommerce site and any page that references the tool will get compromised. Real-time CSP (content security policy) protection can help mitigate this threat.

Merchants responding to our survey said they saw a 54% spike in card scraping in 2021 over the previous year. But only 20.5% of merchants have implemented real-time CSP protection.

Carding

Once credit card information is stolen, they need to be validated to make them viable for sale on the dark web, or for use in credit card fraud. Numerous API calls are made during a carding attack. If the website has robust bot management in place, such nefarious traffic and IP sources can be identified quickly, moved to a block list and rate limiting can be activated on the check-out process to defend against the attack. An intelligent visibility tool that monitors online traffic and user behavior can easily detect such anomalous activity.

In 2021, a 63% jump in carding attacks was reported by merchants in our survey when compared to 2020. But only 20.5% of merchants have real user monitoring (RUM) and file intrusion detection implemented while just 23.5% of the merchants can activate rate limiting.

Credit card fraud

Bad actors who procure stolen and validated credit cards use them to commit credit card fraud. An intelligent fraud management solution can detect anomalies, like contact and shipping addresses, country of origin, IP, or others, and flag suspicious transactions.

2021 saw a 68% YoY growth in credit card fraud according to our survey. But only 32% of ecommerce merchants have a fraud detection solution in place, rendering the sites of a vast majority a sitting duck.

Ransomware

In 2021, ransomware attacks became rampant, destabilizing not just ecommerce businesses but even public utilities. Ransomware is a type of malicious software that infects a computer system and the perpetrator demands a sum of money be paid in order to mitigate the attack. The most common types of ransomware include Maze, Crypto malware, Doxware, Lockers, RaaS (ransomware as a service), Scareware, and others. Some of the popular ransomware attacks include TeslaCrypt, Cryptolocker, Bad Rabbit, and Petya, among others.

05 Recommendations

However comprehensive and fail-proof your security solution is, the adage ‘prevention is better than cure’ applies. Here are five simple steps to ensure your data is safe:

- Ensure your software is routinely patched and always the latest version
- Employ strong multi-factor authentication (MFA)
- Train staff, partners, and third-party service providers regularly on security best practices
- Have a daily backup protocol
- Establish an incident response plan; test and update it regularly

Tackle zero-day threats: Bad actors continue to exploit zero-day threats in web APIs and popular ecommerce platforms, especially Magento 1.x. One of the most effective ways to prevent zero-day exploits is deploying a web application firewall (WAF) on the network edge. Ensuring security patches are up to date always is critical too. Since the Magento 1 end of life announcement, Webscale has released 56 patches.

Avoid point solutions: Ecommerce businesses must not rely on point solutions with limited coverage that may not effectively integrate with your entire infrastructure, leaving vulnerabilities exposed. An enterprise-grade security solution that includes measures to block malware delivery infrastructure and payloads, limitations on internet-accessible services, and multi-factor authentication (MFA) is par for the course.

Invest in deep observability: An intelligent tool and established protocols that enable rapid and accurate identification of suspicious activity within an ecommerce environment can flip the well-scripted journey of any attacker. The swiftness of detection and response leveraging automation and machine learning can grant an ecommerce business the potent power to arrest an attack before it gets to exfiltration and encryption.

Go beyond the perimeter: In our view, perimeter-only defenses will no longer be enough. In 2021, we have seen numerous cyberattacks breaching perimeter defenses. Network owners must assume that perimeter defenses will be compromised, and that means they must defend the internal/core network as if each node is a perimeter node. There has to be a zero-tolerance policy towards not implementing a zero-trust architecture.

06 | How can Webscale Help?

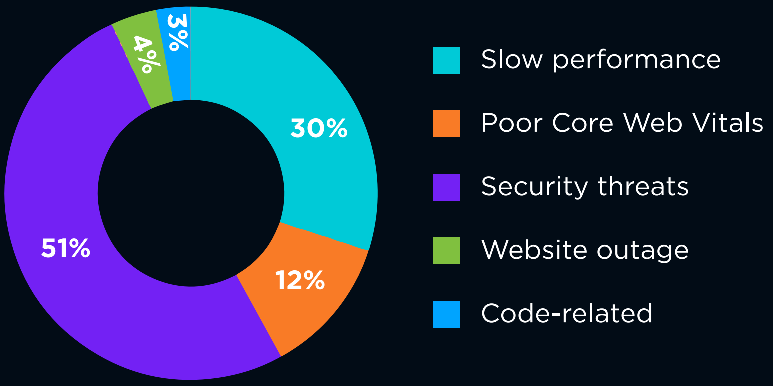
Bot attacks accounted for 68% of all attacks on Webscale customers in November 2021. During the 2021 holiday season, Webscale defended against malicious bots with more than 76 million denial or redirect responses. No Webscale customers were impacted in any way during their busiest, and a most lucrative quarter.

In Webscale's survey, for 51% of merchants, security remains their number one business challenge. With cyberattacks and insurance payouts becoming more frequent, the cost of cyber insurance has also climbed significantly in the last few years. Reports suggest that prices rose 96% in the US and 73% in the UK for Q3 2021 compared to the same quarter in 2020. This upward trend is expected to continue in 2022.

Going forward, insurance providers will insist on the insured merchants deploying stringent security protocols that substantially reduce the risk of an attack - payouts will not anymore be the norm but the exception. Hence, merchants should never treat the insurance policy as their only protection against bad actors.

Bot attacks accounted for 68% of all attacks on Webscale customers in November 2021.

The #1 challenge merchants faced on Black Friday/Cyber Monday related to their hosting environment



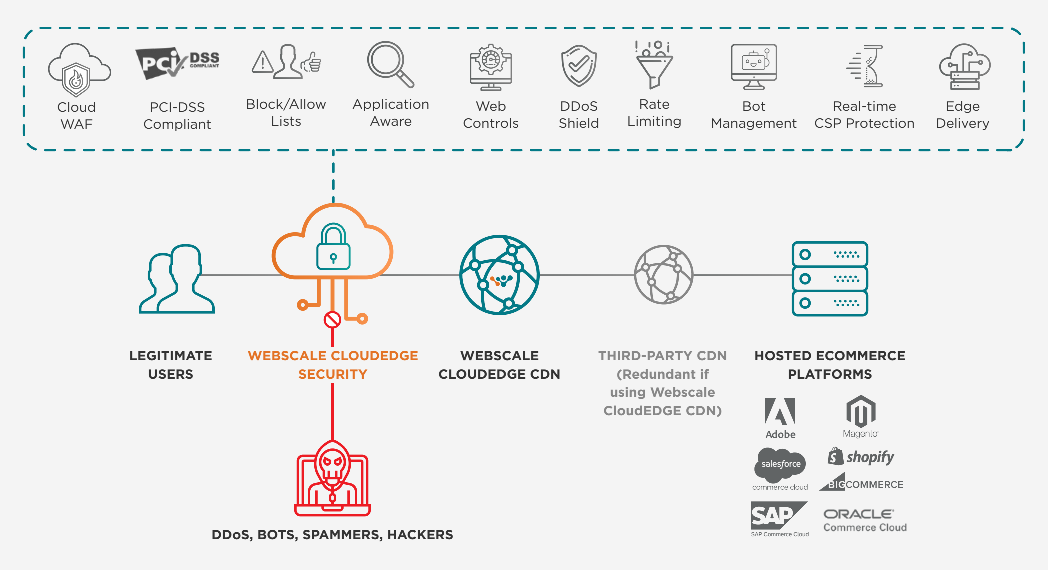
In Webscale's latest survey, 75% of merchants have stated they intend to invest in multi-factor authentication (MFA), 71% in real-time CSP (content security policy) protection, and 78% want to deploy real user monitoring (RUM). 75% of merchants (up from 68% in 2021), demand automation in their security management solution.

Webscale CloudEDGE Security

Webscale CloudEDGE Security is an award-winning ecommerce security platform, deployed at the traffic edge, alongside or as a replacement for traditional CDNs and WAFs. CloudEDGE Security sits in any cloud and atop any ecommerce platform, using automation and analytics to proactively identify and protect web applications from the front end through web traffic, malicious code, or from browsers executing scripts to steal sensitive information.

> CloudEDGE Security sits in any cloud and atop any ecommerce platform, using automation and analytics to proactively identify and protect web applications.

Websites protected by CloudEDGE Security have always-on, 360° security with application-aware, customized rules to protect against sophisticated attacks. In addition to a managed WAF, CloudEDGE Security includes a range of features that allow for real-time application monitoring and analysis through machine learning, detection, automated mitigation, and ongoing protection. CloudEDGE Security is available as an add-on to all Webscale Cloud Delivery plans, or as a stand-alone product for merchants and developers struggling with inadequate protection on hosted ecommerce platforms. Unlike current products that leave remediation to the merchant or the developer, Webscale's DevSecOps team works alongside to help detect and protect.



Webscale CloudEDGE Security includes:

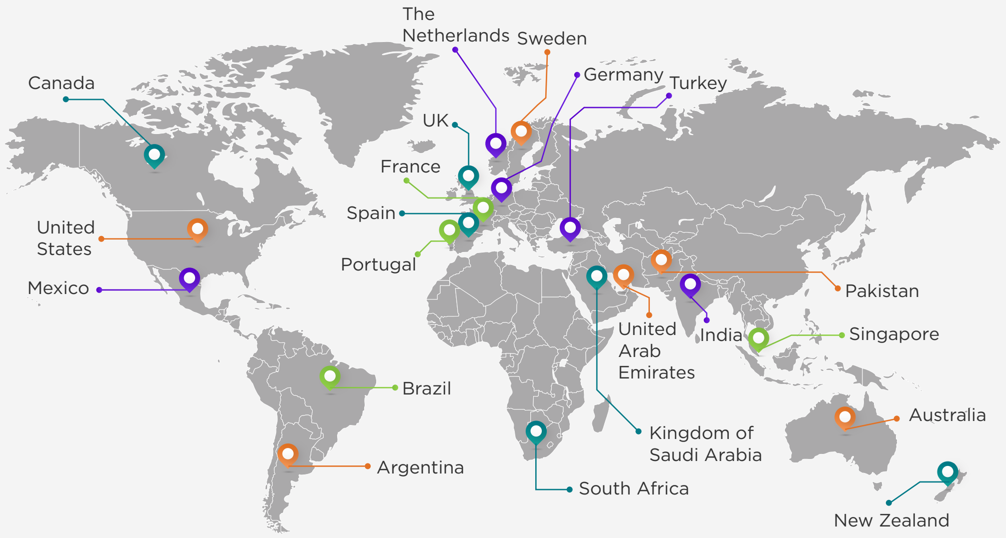
- A managed, application-aware programmable **WAF**
- **Bot Management** for allow/block of good/bad bots powered by machine learning
- **Web/Edge Controls –** a unique, DIY policy and rules engine that allows users of any skill set, to create (or use existing) security rules to ensure enterprise-grade security
- **Real-time Content Security Policy (CSP)** protection prevents XSS attacks by enhancing trust between browser and application server. It prevents card scrapers from being installed inadvertently
- Programmable **CloudEDGE workers** that can be deployed to address any emerging threat, such as carding attacks by activating measures including advanced **Rate Limiting** for request rate throttling
- **DDoS Shield Mode** for single-click protection
- **Secure Access –** enterprise-grade security for **multi-factor authentication (MFA),** ensuring only real admins can get to the admin page, even before credentials are entered. It's the best bet against phishing attacks

Request a Demo

07 | About the Report

Demographics of Respondents

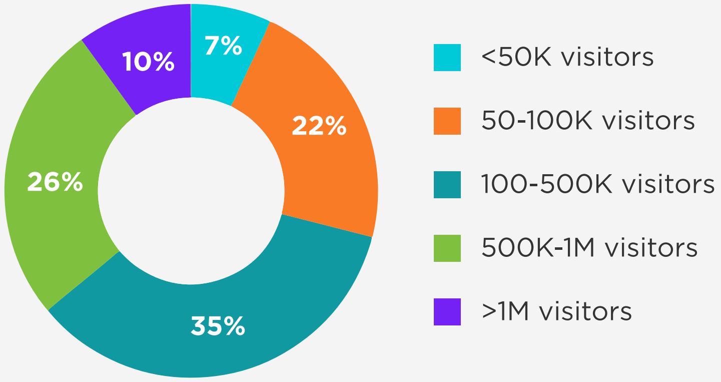
21 countries



22 Industries

- Fashion and Lifestyle
- Medical and Pharmaceuticals
- Health, Sports and Fitness
- Home and Gardens
- Banking, Financial Services and Insurance
- Food and Drink
- Industrial and Hi-tech
- Technology and Computing
- Travel and Hospitality
- Media and Publishing
- Consumer Packaged Goods
- Energy and Utilities
- Education and Career
- Telecom
- Automotive
- Arts and Entertainment
- Family and Parenting
- Electrical and Electronics
- Hobbies and Interests
- Real Estate
- Religion and Spirituality
- Business Services

Website Traffic of Respondents

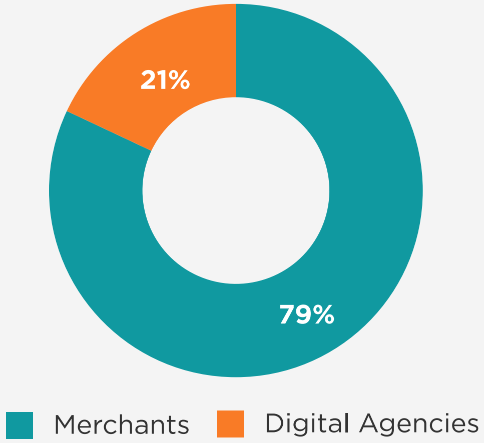


Number of Respondents

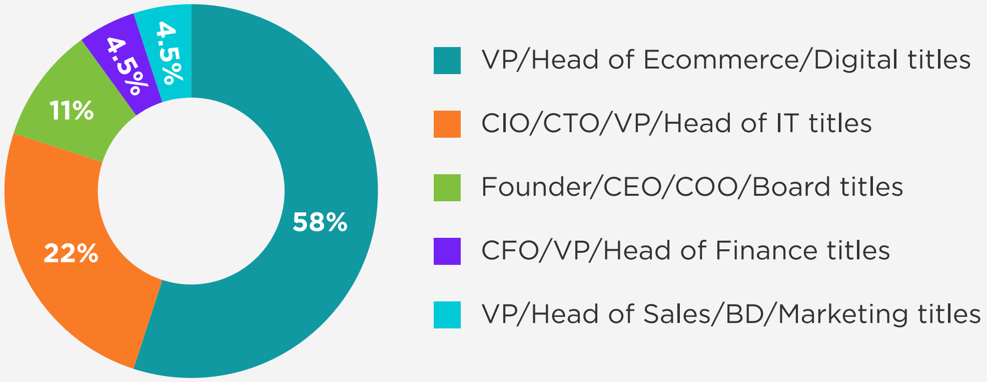
1890

Executives

Type of Business of Respondents



Role of Respondents



Sources

Hackers rigged hundreds of ecommerce sites to steal payment info

US ecommerce grows 14.2% in 2021

Online holiday sales grow a more muted 10% in 2021

Cyber Monday ecommerce sales drop 1.4% YoY

ATO attacks increased 307% between 2019 and 2021

Magecart attacks hit thousands of UK SMBs ahead of Black Friday

Number of DDoS attacks per one organization tripled from January to September 2021

Applying mitigation is longer working since the cyberattacks toll is increasing

Social media a gold mine for scammers in 2021

As Ransomware costs balloon, it's last call for legacy security

Omnichannel ecommerce growth increases API security risk

Cost of a data breach: Retail costs, risks and more to know

How shopping bots can compromise retail cybersecurity

Cybercrime, fraud, and digital scams reach an all-time high in 2022

Magecart attackers ride into Segway's ecommerce website

Data breaches reach an all-time high in 2021

Holiday ecommerce sales surge (but not on Cyber Monday), fraudsters looking for bigger scores

Website outages, slowdowns hit dozens of retailers during Cyber 5

The Global Ecommerce Security Report 2022

Published in March 2022 by Webscale Networks, Inc.

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.

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

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

WEBSCALE

www.webscale.com