



Stay open for
business —
but closed to
cyberthreats

E-commerce relies on always-on connectivity to customers whenever they want to access services. Your store must offer the same high level of service however customers want to access it and on whatever sort of device.

Retail security must be frictionless. If you frustrate customers with unnecessary checks or slow access to the products — for instance with a CAPTCHA — they will go elsewhere. A full [52% of merchants think friction in the checkout process](#) is a top driver of shopping cart abandonment.

Even so, e-commerce must also be secure. Dealing with customer details and card details makes retailers a tempting target for the bad guys.

[Verizon's 2021 Data Breach Investigations Report](#) looked at 725 retail incidents that led to 165 confirmed breaches. Of those, 20% were web application attacks.

The attacks were almost entirely financially motivated, with just 1% due to espionage, and criminals were after payment details (42%), personal details (41%), and credentials (33%).

Running e-commerce systems also means complying with a variety of regulations. Failure to do so will lead to reputational damage, lost business, and potentially punishment from payment providers who may increase charges or even withdraw services entirely.

And while retailers need to take security seriously, they also need systems that will not impact website or e-commerce performance or negatively affect customer experience.

E-commerce provides some unique challenges. It changes rapidly — mobile sales now make up the majority of most retailers' online turnover, compared to a small fraction just a few years ago. In addition, these systems must also be able to scale quickly and securely as demand changes rapidly due to sale and discount events, as well as normal seasonal changes.

The vast majority of e-commerce sites now rely on a complex mix of third-party vendors and software providers. These will likely include performance measurement, business intelligence, load balancing, recommendation engines, and dozens of other [services](#) all relying on APIs. Keeping these applications and APIs secure from malicious actors is yet another challenge for retailers.

What is the threat from cybercriminals?

Back in the day there were barriers to even committing e-commerce fraud. You needed skills, knowledge of your targets, and infrastructure to mount attacks.

Today, you can deploy bots that do this work for you. Bots automate the complex and manual tasks of performing various e-commerce attacks, making it easy to run large volumes of attacks with limited resources.

Bots make up two-thirds of internet traffic, both “good” and “bad” bots. Retailers rely on “good bots” for keeping their services running profitably, while they want to minimize the impact of bots such as price aggregators and completely block bots that are scanning for weaknesses. This makes filtering good traffic from bad traffic even more difficult.

Traditional tools like IP address blocking and CAPTCHA barriers are no match for modern attacks using IP hijacking and sophisticated bots.

Once the bot has found a way into your system, attackers can now go after sensitive customer data and payment details, or attempt to steal data during transactions. They can use credential stuffing to breach customer accounts and set up fraudulent purchases, threaten you with ransomware, or simply take you offline. Bots are also used by scalpers to buy up concert tickets, hot gaming consoles, newly dropped shoes, and more to sell for a profit later. All of these attacks cause significant issues — some of which are problematic enough that both the U.S. and UK governments have introduced or talked about introducing legislation to stop these hacks.

E-commerce fraud has adopted many of the practices and techniques of mainstream software development. This has allowed rapid growth, taking advantage of new technologies, and moved attacks to a service-based model. Fraud losses are growing at double digit rates, meaning the ROI or return on investment for bad actors continues to improve.



First steps to safety

Barracuda was an innovator in application protection well before today's rapid-fire attacks, and our early adoption of the cloud has allowed our Web Application Firewall (WAF) and WAF-as-a-Service to play a key role in helping retailers cope with these ever-evolving challenges.

Barracuda Web Application Firewall solutions provide you with air cover and protect your web applications and APIs against known and unknown (zero-day) attacks.

Reverse proxy WAFs like the Barracuda solution also provide identity and access controls for your users, i.e. the protection is bidirectional. You can use Barracuda Web Application Firewall to enforce specific logins and even integrate application logins with systems like Google or Facebook and enforce multifactor authentication with ease.

Barracuda Web Application Firewall sits between the internet and your web servers and scans both inbound and outbound traffic. It understands HTTP and HTTPS better than a traditional firewall, allowing it to inspect traffic for targeted application-layer attacks.

While Barracuda Web Application Firewall comes preconfigured with templates to provide instant

security, it is also automatically updated as new attack types appear. The Active Threat Intelligence cloud layer provides near-real time threat intelligence to stop emerging attacks as they start. It defends against bot attacks both through the use of a list of known bot attack networks as well as cloud-based machine learning (Advanced Bot Protection) to identify new attack types. Advanced Bot Protection detects and blocks hidden almost-human bot attacks with machine learning. It secures your online data, analytics, and inventory against advanced bots while ensuring improved user experience and security.

Barracuda Web Application Firewall can secure all applications, whether they are provided on-premises, hosted in the cloud, or running as mobile apps. It can be deployed in your own data center, on a virtual machine, or hosted in the cloud — or it can be consumed as software-as-a-service (Barracuda WAF-as-a-Service). It is easy to integrate with other security tools such as scanners and security information and event management solutions.

It also automates report creation and audit logs, further reducing workloads for administrators and managers.

Staying ahead of the game

There is no reason to think that retail will not remain a top target for cybercriminals. E-commerce managers will have to continue to balance the conflicting pressures of maintaining easy access for customers and good bots and working to keep bad bots and other threats out of crucial systems.

Increasing use of mobile applications and devices and automated shopping assistants will all make this job even harder. Online consumers are not getting easier to satisfy either — they're demanding faster and more frictionless transactions. But the push to reduce abandoned carts or sign-up processes must be balanced against maintaining security.

Retailers represent some of the world's most valued brands, and that value relies on consumer trust. Maintaining that trust requires the best e-commerce and web security systems to protect your customers' data and with it your reputation.

Secure your e-commerce operations, everywhere.

Barracuda's [application security solutions](#) offer a perfect way for retailers to keep e-commerce websites, applications, and customers protected from cyberattacks.

About Barracuda

At Barracuda we strive to make the world a safer place. We believe every business deserves access to cloud-first, enterprise-grade security solutions that are easy to buy, deploy, and use. We protect email, networks, data, and applications with innovative solutions that grow and adapt with our customers' journey. More than 200,000 organisations worldwide trust Barracuda to protect them — in ways they may not even know they are at risk — so they can focus on taking their business to the next level. For more information, visit barracuda.com.



Contact us for further information on how to secure your [e-commerce operations](#).