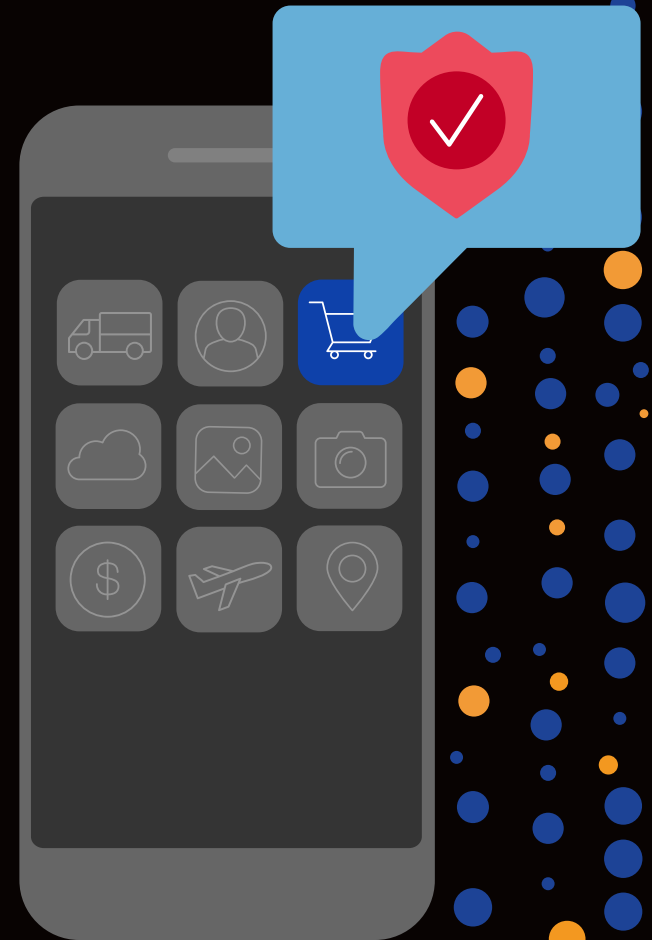


Secure eCommerce Apps with F5 and AWS

Mitigate cyber threats and deliver exceptional retail experiences.



Contents

3	The Rise of eCommerce
4	A New Wave of Threats
5	F5 and AWS for Retail
6	Modernize and Secure Apps
7	Protect Critical APIs
8	Prevent Malicious Bots
9	Safeguard Consumers
10	Secure eCommerce with F5 and AWS

The Rise of eCommerce

Consumers have changed the way they shop. While physical brick-and-mortar stores continue to play a vital role, eCommerce has revolutionized consumer expectations, offering unprecedented convenience, speed, and flexibility. With over 26 million eCommerce sites globally, online shopping has become ubiquitous, reshaping how people transact and make purchases worldwide.¹

However, as eCommerce becomes a cornerstone for today's businesses, security concerns are on the rise. Retail remains one of the most targeted industries for cyber attack² with bad actors aiming to exploit consumer likeness and interfere with

daily transactions. From service outage to consumer fraud, advanced threats are compromising user experiences and depleting bottom-line revenues. In fact, in 2023 alone, losses from eCommerce fraud alone exceeded almost \$50 billion globally.³

To succeed in today's ultra-competitive market, retailers need proven solutions that keep eCommerce apps secure and resilient—while delivering the frictionless buying experiences consumers expect.



A New Wave of Threats

In the digital marketplace, buyer expectations couldn't be clearer: provide seamless 24x7 access to goods and services. With eCommerce portals, apps, and APIs serving as the backbone for customer transactions, cyber breaches don't just threaten

immediate revenue streams; they have the potential to damage customer perceptions for years to come. Without robust security defenses in place, businesses are left vulnerable, posing significant risks to both retailers and consumers alike.



Customer Impact

From impersonating legitimate users to stealing sensitive data, cyber criminals are exploiting customer likeness for fraudulent purposes.



Identity Theft

Stealing sensitive Personal Identifiable Information (PII).



Credit Card Fraud

Using stolen or counterfeit credit card information.



Account Takeover

Gaining illegitimate access to users' online account.



Retailer Impact

Using advanced tactics, bad actors aim to disrupt critical business functions and undermine buyer perception.



Operational Disruption

Inability to manage inventory, fulfill orders, or support customers.



Revenue Loss

Unexpected downtime that suspends retail transactions and payment processing.




Brand Reputation

Poor application performance and degraded customer experiences.

F5 and AWS for Retail


Today’s businesses need proven solutions that safeguard their digital buying experiences from new forms of automated, persistent, and advanced cyber threats. Together, AWS and F5 ensure application security and performance—without

disrupting customer journeys. Now, retailers can mitigate threats, minimize financial losses, and safeguard their reputations while delivering the frictionless and reliable experiences customers expect.



Modernize eCommerce apps with confidence.

Improve IT efficiency, boost eCommerce productivity, automate supply chains, and drive continuous innovation.	Deliver consistent brand experiences across customer touchpoints, including payment, shipping, and search.	Build next-generation intelligence and insights to differentiate your brand, influence customer actions, and increase revenue.
---	--	--



Enhance security for AWS-hosted apps.

Protect apps everywhere with centralized security and uniform policy enforcement across AWS and non-AWS workloads.	Safeguard online transactions, preserve retail operations, and continuously adapt to block attackers without inconveniencing customers.	Prevent user fraud, secure customer privacy, and deliver reliable eCommerce experiences.
--	---	--





+



Distributed Cloud Services

Modernize and Secure Apps

From core to cloud to edge, applications can live in a multitude of locations—which all need adequate protection and management. As cyber risks mount and in-house resources dwindle, today's businesses need seamless security and performance across apps.

Using AWS, retailers can modernize their app footprint, enhance their digital services, and streamline operations. With Amazon CloudFront Content Delivery Network (CDN) businesses benefit from a network architecture designed to meet the demands of consumers. Low latency and high transfer speeds enable retailers to rapidly innovate, deliver personalized buying experiences in the cloud, and stay ahead of competitors in today's dynamic landscape.

Combined with F5® Distributed Cloud Web App and API Protection (WAAP), businesses can safeguard AWS apps alongside existing solutions and services—wherever they run. With industry-leading web application firewalls (WAF) and DDoS protection built in, F5 enhances native AWS security controls while delivering consistent threat defenses broadly across heterogeneous application environments.



>200M

F5 powers more than half of the world's applications, protects over 1 billion transactions daily from application attacks, and ensures the safety of more than 200 million legitimate human transactions every day.⁴



Modernize apps while accelerating and protecting dynamic and static content.



Protect against OWASP Top 10 threats, DDoS attacks, and zero-day exploits.



Standardize and centralize security in a single, SaaS-based platform.

Protect Critical APIs

Retailers have adopted APIs in droves to accelerate new innovations and drastically improve the speed and scale of their applications. From in-app search engines and product catalogs to inventory management and fulfillment operations, APIs have become a mainstay in modern eCommerce applications and play a critical role in underlying functions and app-to-app communications. Yet, as API use increases, so do risk profiles. A top target for cyber exploits, unmanaged, ungoverned, or exposed APIs provide a direct pathway for bad actors to compromise businesses and their consumers.

Amazon API Gateway secures businesses with fine-grained and certificate-based authorization for AWS-hosted applications while F5® Distributed Cloud API Security extends protections in AWS and other environments—keeping critical retail operations and services resilient from attack.



Identify known and unknown APIs and safeguard unmanaged or decentralized interfaces.



Safeguard against sophisticated attacks and block any dangerous or unwanted connections.



Configure, standardize, and enforce consistent security policies across new and legacy APIs.

Top Five API Use Cases in Retail⁵



App Development



IoT Integration



Inventory Management



Procurement



Customer Insights

Prevent Malicious Bots

While bots can automate repetitive tasks, raise brand awareness, and engage users to accelerate digital buying journeys, they can also be used to extort users or inflict damage. With bad bots making up 30% of all internet traffic,⁶ apps and APIs are at risk of exploit. This includes credential stuffing, account takeover (ATO), inventory hoarding, scraping, and gift card cracking. To counteract malicious bots and keep eCommerce operations resilient, businesses need proven detection solutions that adapt to attackers' tactics as they evolve.

F5® and Amazon help organizations deliver engaging and secure customer experiences. With F5 Distributed Cloud Bot Defense Connector for Amazon CloudFront, businesses get AI-powered protection from bots and automated attacks, seamlessly integrated with AWS' scalable and globally distributed architecture.



F5 Distributed Cloud Bot Defense enabled a Fortune 500 retailer to eliminate tens of millions of dollars in fraudulent transactions and chargeback fees.⁷



Prevent credential stuffing attacks that result in account takeover fraud.



Safeguard eCommerce apps from attacks emulating human behavior.



Remove unwanted automation traffic to prevent fraud and reduce costs.

Safeguard Consumers

From initial login through purchasing, businesses need multilayered security that mitigates threats and guarantees trusted user access and transactions. However, as consumers prioritize convenience, added security measures that introduce complexity or slow down the purchasing processes can lead to abandoned sales and harm the perception of the brand. In fact, over half of customers would switch to a company's competitor after just one bad experience.⁸

With F5 and AWS, you can create a secure shopping experience while seamlessly ensuring the simple, fast, and effortless transactions that buyers demand with:

- **Frictionless Access and Authorization**

Improve application authentication and access while delivering a frictionless zero-trust user experience. With simple, secure, and context-aware access for apps, consumers can easily and securely use digital services—mitigating unwanted access and fraud risks.

- **Data and Privacy Protection**

Monitor and mitigate browser-based attacks in real-time. This enables retailers to fill the gap in existing security to protect against critical risks.

F5 helped a multinational shoe retailer mitigate account takeovers and gift card cracking to **save \$500k** in the first month alone.⁹



Defend against Magecart, formjacking, skimming, PII harvesting, credential stuffing, and other client-side attacks.



Gain visibility and control of third-party JavaScript libraries to keep customers' personal and financial data safe.



Track third-party scripts running on sites to detect suspicious activity and stop stealthy supply chain attacks.

Secure eCommerce with F5 and AWS

F5 offers a robust portfolio that works across the entire hybrid cloud estate to help accelerate cloud migrations, secure cloud applications, and improve user experience with AWS cloud services. The long-standing partnership between F5 and AWS means you can expect solutions that work together seamlessly to help you slash fraud losses, improve customer experiences, and maximize operational efficiencies.

Ensure your clouds, apps, and services are always:



Secure



Available



Fast

The F5 and AWS Partnership:

- 10+ years of collaboration
- Over 1,000 joint customers
- Competencies for containers, networking, and security
- Service validations for AWS WAF, Amazon CloudFront, AWS Outposts, and Linux
- Over 20 AWS certifications

¹ Markinblog, [Study: How Many eCommerce Sites Are There?](#), Sep 2023

² Orange, [Security Navigator 2024](#), Nov 2023

³ Mastercard, [Ecommerce Fraud Trends and Statistics Merchants Need to Know in 2024](#), 2023

⁴ F5, [Automated Gift Card Fraud](#)

⁵ AIMultiple Research, [Top 5 Use Cases of API in Retail With Examples in 2024](#), Jan 2024

⁶ Barracuda, [Threat Spotlight: How Bad Bot Traffic Is Changing](#), 2023

⁷ F5, [Automated Gift Card Fraud](#)

⁸ Zendesk, [CX Trends 2023](#), May 2023

⁹ F5, [Retailer Solves Shoe-Bot Spikes: Fixes Fraud, Friction, and Fake](#)

ABOUT F5

BRINGING A BETTER DIGITAL WORLD TO LIFE

F5 is a multi-cloud application services and security company committed to bringing a better digital world to life. F5 partners with the world's largest, most advanced organizations to secure and optimize apps and APIs anywhere—on premises, in the cloud, or at the edge. F5 enables organizations to provide exceptional, secure digital experiences for their customers and continuously stay ahead of threats.

For more information, go to f5.com. (NASDAQ: FFIV).

Learn more about F5 solutions for AWS at f5.com/aws

