

How to Secure Your E-commerce Apps

Cybercriminals target e-commerce companies with a diverse array of attacks that exploit various vulnerabilities.

Threat Landscape Overview

Expected growth of global e-commerce by 2026

\$8.1 Trillion



H1 2023 attacks that targeted retail

35.5%

Companies reporting at least one cyber incident or breach in 2022

9 out of 10



Share of all website traffic with intent to harm your applications

25%

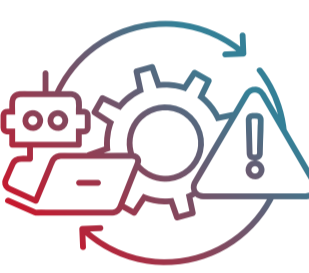
Key Threats Retailers Need to Look Out For



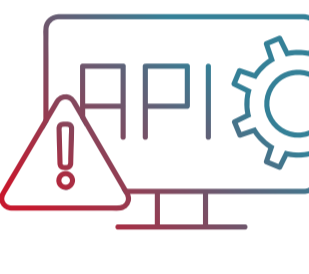
Availability Threats



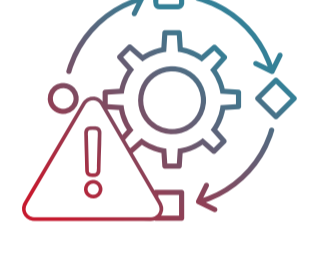
Web App Vulnerability Exploits



Bots & Automated Threats



API & Data Threats



Supply Chain Attacks

Radware's Comprehensive Cloud Application Protection Services

Web DDoS Protection

- Industry-leading DDoS defense
- Behavioral-based real-time protection against L7 DDoS rising Web Tsunami attacks



Cloud WAF

- Negative and positive security model, real-time defense
- Deep coverage of the OWASP Top 10 and zero-day attacks



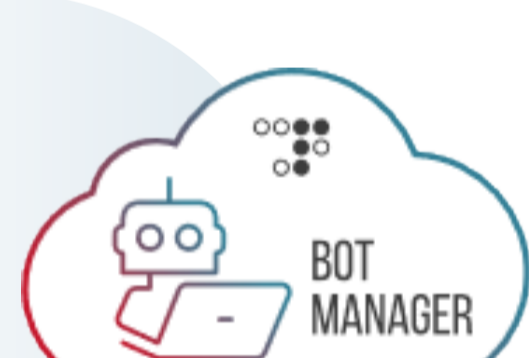
Client-Side Protection

- Protection against supply-chain attacks
- Continuous discovery of third-party services in your supply chain



Bot Manager

- Identification and mitigation of malicious bot traffic
- Browser-based challenges, mobile device attestation



API Protection

- Protection against API threats
- Automated API Discovery



Benefits to Retailers

Comprehensive Protection:

One-stop-shop protection against all types of http layer attacks



State-of-the-Art Security:

AI-based behavioral algorithms for robust protection



Flexible Deployment:

Seamless adaptation to evolving infrastructures



Unified View:

Simplified monitoring



360°

Application Protection

Radware offers a 360-degree, fully managed protection strategy for e-commerce companies.

Learn more at [radware.com](https://www.radware.com)