Active Application Security and Fraud

IDC's *Active Application Security and Fraud* covers the tools and technologies that protect custom-built applications and infrastructure. Applications and APIs provide businesses with the ability to deliver an engaging online user experience across mobile and web to key audiences. These applications face a specialized set of threats and technical requirements, which has led to a diverse marketplace of security solutions. However, IT buyers are shifting from traditional piecemeal or siloed application security practices to a holistic and unified view of application security considerations, requirements, and best practices. Furthermore, this CIS provides insights into the emerging technologies and strategies that businesses rely on to defend applications and APIs.

MARKETS AND SUBJECTS ANALYZED

- Web application firewall (WAF)
- API security
- Bot management
- DDoS mitigation
- Client-side security
- Web fraud and abuse prevention
- Web application and API protection (WAAP)
- SaaS security posture management (SSPM)

CORE RESEARCH

- Application protection and availability IT buyer survey insights
- Active Application Security Market Share
- Web Application Firewall (WAF) Market Forecast
- Online Fraud and Integrity Market Forecast
- Pervasive Application Edge Defense Market Perspective
- DDoS Mitigation Market Forecast
- Bot Management Market Forecast
- API Security Market Forecast
- Web Application and API Protection (WAAP) IDC MarketScape
- Client-Side WAF Market Forecast

In addition to the insight provided in this service, IDC may conduct research on specific topics or emerging market segments via research offerings that require additional IDC funding and client investment. To learn more about the analysts and published research, please visit: Active Application Security and Fraud.

KEY QUESTIONS ANSWERED

1. What is the outlook for the application security market?
2. How is security adapting to emerging technologies such as WebAssembly and WebSockets?
3. What does fraud prevention mean for web and mobile channels?
4. What is the business risk of DDoS?
5. What is the future of API security?

COMPANIES ANALYZED

This service reviews the strategies, market positioning, and future direction of several providers in the active application security and fraud market, including:

Akamai, Alibaba Group, Amazon Web Services, Array Networks, Baidu, Barracuda, Broadcom, China Telecom, Citrix, Cloudflare, DBAPP Security, EF5 Networks, Fastly, Fortinet, Google, Help/Systems, Huawei, Imperva, Ivanti, Microsoft, NetScout, NSFOCUS, OpenText, Penta Security Systems, Qualys, Radware, RaonSecure, Rapid7, RSA, SAP, SGA, SonicWall, and Tencent.