Active Application Security and Fraud

AN IDC CONTINUOUS INTELLIGENCE SERVICE

IDC's *Active Application Security and Fraud* covers the tools and technologies that protect custom-built applications and infrastructure. Applications 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. Further, the CIS provides an overview of key technologies used to secure applications, including DDoS mitigation, web application firewalls (WAFs), API security, and bot management.

Markets and Subjects Analyzed

Active Application Security and Fraud examines the technologies and tools that keep our digitally transformed applications and related systems operating at all times, and secure. Unfortunately, as businesses adopt more varied and more powerful application functionality, cybercriminals have taken notice. Web application front ends and APIs represent a useful target for fraud, business logic abuse, and data theft. These applications are also gaining recognition as a viable foothold for malware and other cyberthreats, targeting more sensitive data and IT systems. However, security is just the beginning as we look to mature our applications with integrated trust, a strategy to promote granular, application-specific access controls and proactive, predictive protections. Today's applications incorporate many of these concepts via a holistic view of applications, user identity context, access control methods, application infrastructure protection, and application integrity assurance.

Core Research

- Active Application Security Market Share
- Web Application Firewall Market Forecast
- Online Fraud and Integrity Market Glance
- Pervasive Application Edge Defense Market Perspective
- DDoS Mitigation Market Forecast
- Bot Management Market Forecast
- API Security 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 size of the application security market?
2. Who is the market share leader in application security?
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, F5 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.