2023 Cyberthreat Defense Report

Executive Brief

Platinum Sponsor

imperva

Survey Demographics

- Responses from 1,200 qualified IT security decision makers and practitioners
- All from organizations with more than 500 employees
- Representing 17 countries across North America, Europe, Asia Pacific, the Middle East, Latin America, and Africa
- Representing 19 industries

"API gateway/protection is the application and data security solution installed in the largest percentage of organizations (60.6%), and is the leader for the fourth year running... security teams need tools to detect and respond to attacks targeting APIs."

– 2023 CDR

CyberEdge Group's tenth annual Cyberthreat Defense Report provides a penetrating look at how IT security professionals perceive cyberthreats and plan to defend against them. Based on a survey of 1,200 IT security decision makers and practitioners conducted in November 2022, the report delivers countless insights IT security teams can use to better understand how their perceptions, priorities, and security postures stack up against those of their peers.

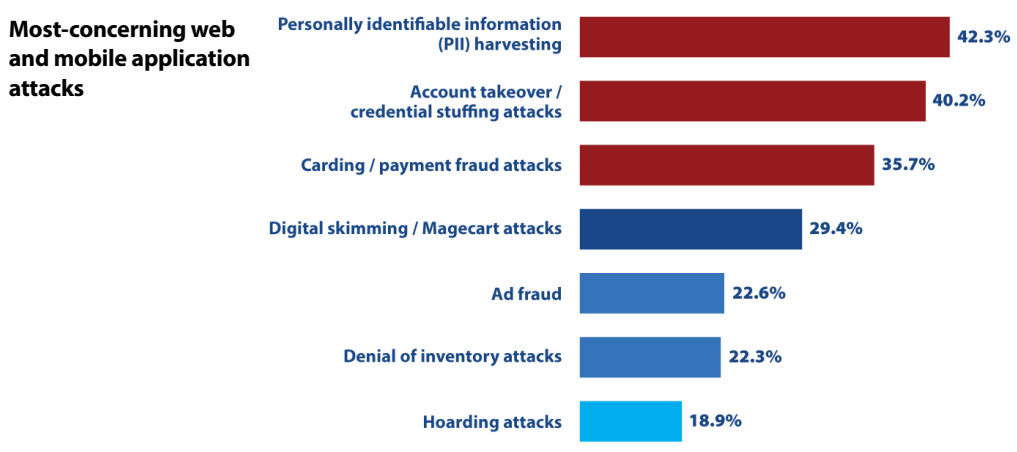
Notable Findings

- **Web and mobile attacks are major concerns.** The top threats in this category are PII harvesting, account takeover (ATO), and carding and payment fraud attacks.
- **Bot management is hot.** Among application and data security technologies, bot management is the most frequently planned for acquisition.
- **API protection is now a top issue.** As organizations move to cloud applications, more than 60% have installed API gateways or API protection solutions.
- **Many benefits of unifying application and data security technologies.** Advantages include an improved cloud security posture, enhanced incident investigations, and simplified security rules management.

Network-based Attacks That Most Concern Security Professionals

Any organization that does business through websites and mobile apps needs to protect against attacks on their web and mobile applications. Those that worry IT security professionals the most include ATO and credential stuffing attacks (rated 3.95 on a scale of 1 to 5), web application attacks such as SQL-injection and XSS attacks (rated 3.81), and denial of service attacks (rated 3.77).

When asked to indicate their three most-concerning web and mobile application attacks, respondents highlighted PII harvesting (42.3%), ATO and credential stuffing attacks (40.2%), carding and payment fraud attacks (35.7%), and digital skimming and Magecart attacks (29.4%).



Innovation Technologies for Application and Data Security

"Must have" application and data security technologies are led by API protection products, database firewalls, and web application firewalls (WAFs), which are currently in use at 60.6%, 60.1%, and 55.4% or organizations, respectively. API protection solutions have been the leader in this category for four years running. They enforce authorization and encryption policies, limit the impact of DDoS attacks, and uncover rogue APIs, among other capabilities.

The application and data security technologies that organizations most often plan to acquire in 2023 include bot management, application security testing, and database activity monitoring (DAM). Bot management is in demand because it controls traffic from bots used in ransomware, spam, DDoS attacks, and other threats.

Application and data security technologies in use and planned for acquisition

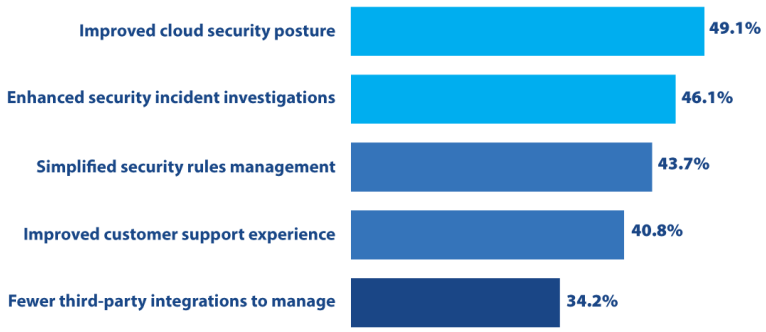
	Currently in use	Planned for acquisition	No plans
API gateway / protection	60.6%	30.9%	8.5%
Database firewall	60.1%	29.0%	10.9%
Web application firewall (WAF)	55.4%	35.8%	8.8%
Database activity monitoring (DAM)	51.7%	36.1%	12.2%
Application container security tools/platform	50.8%	40.1%	9.1%
Cloud access security broker (CASB)	50.2%	35.4%	14.4%
Application delivery controller (ADC)	50.2%	33.7%	16.1%
Runtime application self-protection (RASP)	49.3%	35.8%	14.9%
File integrity / activity monitoring (FIM/FAM)	46.4%	39.9%	13.7%
Third party code analysis	45.1%	35.3%	19.6%
Static/dynamic/interactive application security testing (SAST/DAST/IAST)	44.6%	41.2%	14.2%
Bot management	35.9%	43.6%	20.5%

Benefits When Application and Data Security Technologies Work Together

Everyone has a sense that integrating security technologies together in a single platform is a good thing. But what specifically are the benefits of integrating application and data secuity defenses like web application firewalls (WAFs), DDoS protection, RASP, API security, data risk analytics, and database security?

Survey respondents highlighted the ability to improve their organization's cloud security posture (49.1%), enhanced security incident investigations (46.1%), and simplified security rules management (43.7%). They also mention improved customer support (40.8%) and fewer third-party integrations to manage (34.2%).

Benefits achieved by unifying application and data security defenses



Complimentary Report

Download a copy of the full 2023 Cyberthreat Defense Report at: www.imperva.com/cdr2023

About Imperva

Imperva is a cybersecurity leader with a mission to protect data and all paths to it. We protect the data of over 6,000 global customers from cyber attacks through all stages of their digital transformation. Our products are informed by the Imperva Research Lab, a global threat intelligence community, that feeds the latest security and compliance expertise into our solutions.

CYBEREDGE

About CyberEdge Group

CyberEdge Group is an award-winning research, marketing, and publishing firm serving the needs of information security vendors and service providers. Our expert consultants give our clients the edge they need to increase revenue, defeat the competition, and shorten sales cycles. For information, connect to our website at www.cyber-edge.com.