2022 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

> *"The fact that...five benefits were cited by at least 30 percent of the respondents indicates that a unified platform for application and data security is one of those areas in cybersecurity where integration and single-vendor sourcing just make sense."*
>
> *– 2022 CDR*

CyberEdge Group's ninth 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 2021, 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

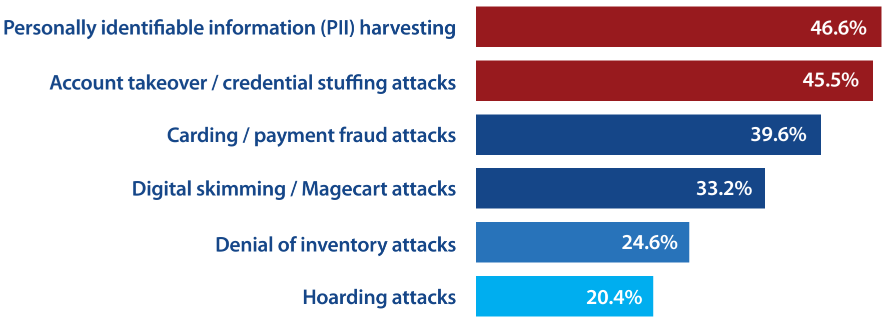
- **Concern about ATO attacks is surging.** The concern level about account takeover (ATO) and credential stuffing attacks soared in the past year; of all threats tracked by the survey it is now second only to malware.
- **Other web attacks also stand out.** Survey respondents highlighted PII harvesting, carding and payment fraud attacks, and digital skimming attacks such as Magecart.
- **API protection and WAF are mainstays.** More than 60% of organizations have installed API protection and web application firewall (WAF) technology.
- **Unifying application and data security technologies pays off.** Benefits include an improved cloud security posture, enhanced incident investigations, and better customer support experiences.

The Attacks That Keep Security Professionals up at Night

The network-based attacks that IT security professionals worry about most included ATO and credential stuffing attacks (rated 3.97 on a scale of 1 to 5), denial of service attacks (rated 3.85), and web application attacks such as SQL-injection and XSS attacks (rated 3.83).

When asked to indicate their three most-concerning web and mobile application attacks, 46.6% of the respondents listed PII harvesting, 45.5% cited ATO and credential stuffing attacks, 39.6% selected carding and payment fraud attacks, and 33.2% mentioned digital skimming and Magecart attacks.

Most-concerning web and mobile application attacks



Essential and Emerging Technologies for Application and Data Security

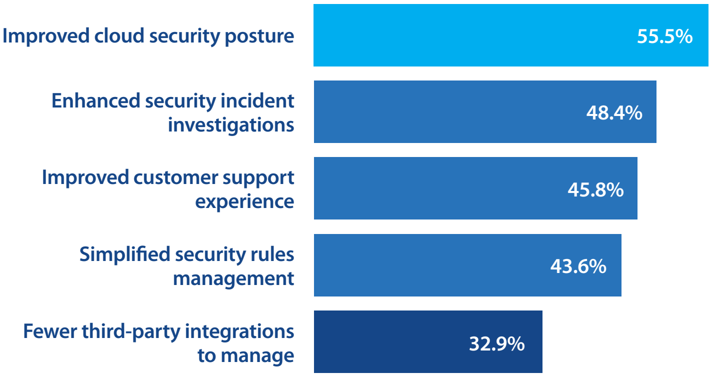
API protection products, web application firewalls (WAFs), and database firewalls are being used by at least six out of ten of the organizations surveyed, indicating that they are considered essential technologies for application and data security. The most popular emerging technologies (i.e., those most often planned for acquisition in 2022), included bot management, advanced security analytics, and database activity monitoring (DAM).

Advantages of Unifying Application and Data Security Technologies

When it comes to sourcing related technologies, security professionals are often faced with a choice between a multiple-source approach and a single-source, integrated solution. The latter reduces the costs of integrating multiple products and hassles related to working with incompatible management and reporting tools and working with multiple vendors.

But what are the specific benefits achieved by unifying application and data security defenses? More than half of the survey respondents (55.5%) highlighted the ability to improve their organization's cloud security posture. Almost as many (48.4%) pointed to enhanced security incident investigations. Other high-level advantages include improved customer support (45.8%), simplified security rules management (43.6%), and fewer third-party integrations to manage (32.9%).

Benefits achieved by unifying application and data security defenses



Application and data security technologies in use and planned for acquisition

	Currently in use	Planned for acquisition	No plans
API gateway / protection	64.1%	28.6%	7.3%
Web application firewall (WAF)	61.1%	29.9%	9.0%
Database firewall	59.5%	30.5%	10.0%
Application container security tools/platform	54.3%	36.5%	9.2%
Cloud access security broker (CASB)	53.3%	33.2%	13.5%
Database activity monitoring (DAM)	53.1%	35.9%	11.0%
Application delivery controller (ADC)	52.2%	33.6%	14.2%
Runtime application self-protection (RASP)	50.4%	35.1%	14.5%
File integrity / activity monitoring (FIM/FAM)	50.2%	37.8%	12.0%
Advanced security analytics (e.g., with machine learning, AI)	50.2%	39.7%	10.1%
Static/dynamic/interactive application security testing (SAST/DAST/IAST)	48.0%	38.2%	13.8%
Bot management	42.6%	39.8%	17.6%

Complimentary Report

Download a copy of the full 2022 Cyberthreat Defense Report at: www.imperva.com/cdr2022

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 GROUP

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.