# 2024 Cyberthreat Defense Report

# Executive Brief

Platinum Sponsor

imperva
a Thales company

### 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

*"[Among application and data security technologies,] bot management is... the leader in planned acquisitions, at 43.7%. Controlling traffic from bots is a priority because of their use in ransomware, spam, DDoS attacks, and other threats."*

*– 2024 CDR*

**CyberEdge Group's tenth anniversary edition 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 2023, 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

- **We'll be hearing a lot about AI this year.** Cybersecurity professionals predict that AI will increase the productivity of security teams – and the effectiveness of threat actors.
- **Bot management is a priority.** 44 percent of the organizations surveyed are planning to strengthen bot management in 2024. It is viewed as a defense against ransomware, spam, DDoS attacks and other threats.
- **Web and mobile attacks menace everyone.** 90% of organizations say they are affected. The top three threats web and mobile threats are account takeover (ATO), PII harvesting, and carding and payment fraud attacks.
- **API protection is a "must have."** More than 60% of organizations have installed API gateways or API protection. They have become an essential part of cloud security.

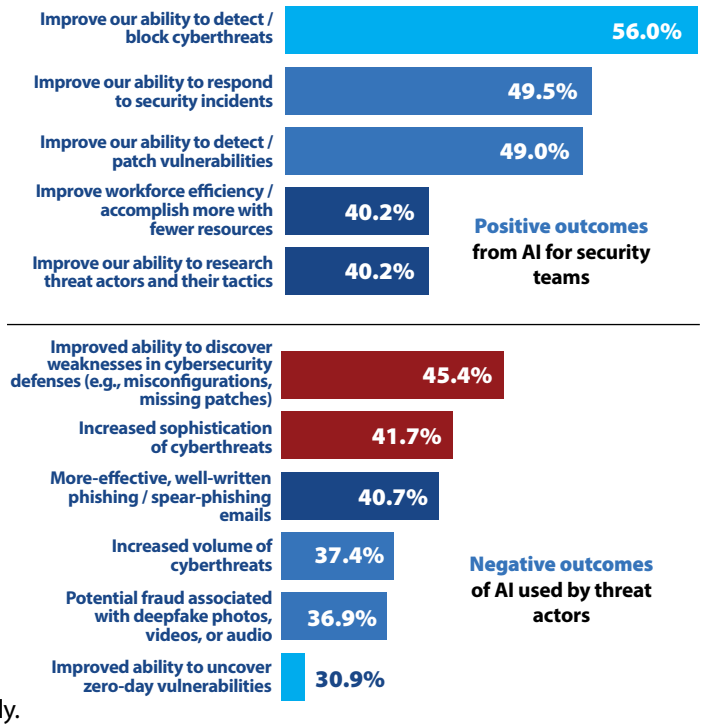
## AI Boosts Cybersecurity Teams – And Adversaries

Artificial intelligence technologies are being incorporated into a very wide range of security solutions – and being used to defeat them.

Security teams expect that AI help them detect and block threats, respond faster to incidents, and generally make them more productive and effective.

But survey respondents also expect theat actors to employ AI to find vulnerabilities, develop more sophisticated threats, and create well-written phishing messages.

Who will be helped more? Most respondents said with IT security teams would benefit more or that both sides would benefit about equally.

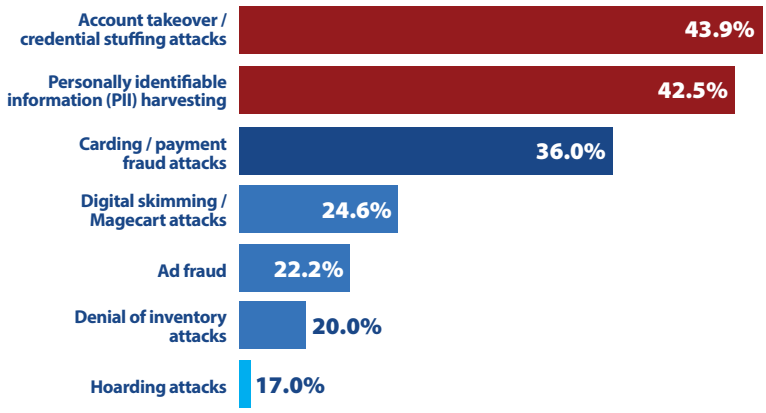


## Web and Mobile Application Attacks Causing Anxiety

Web and mobile application attacks affect every organization that handles customer, client, and constituent data. Threat actors steal credentials and personal information which they use to impersonate victims to carry out data breaches, identity theft, and other crimes.

Which ones cause the most anxiety? The most often cited are account takeover and credential stuffing attacks (selected as one of the top three by 44% or respondents), PII harvesting (43%), carding and payment fraud attacks (36%), and digital skimming and Magecart attacks (25%).

**Most-concerning web and mobile application attacks**




## Application and Data Security Technologies – Essentials and Rising Stars

Six out of ten organizations are currently using database firewalls, web application firewalls (WAFs), and API protection products. These are clearly considered essential technologies for application and data security.

Which technologies are the rising stars in application and data security, most often planned for acquisition in 2024? Leaders by that criterion include bot management, third-party code analysis, file integrity and activity monitoring (FIM/FAM), and runtime application self-protection (RASP).

Rising stars in the security management and operations deployment sector include advanced security analytics, full-packet capture and analysis, and threat intelligence platforms and services.

**Application and data security technologies in use and planned for acquisition**

| | Currently in use | Planned for acquisition | No plans |
|---|---|---|---|
| Database firewall | 62.8% | 25.7% | 11.5% |
| Web application firewall (WAF) | 60.8% | 29.8% | 9.4% |
| API gateway / protection | 60.0% | 32.9% | 7.1% |
| Database activity monitoring (DAM) | 55.6% | 33.4% | 11.0% |
| Application container security tools/platform | 54.3% | 35.7% | 10.0% |
| Cloud access security broker (CASB) | 50.8% | 35.1% | 14.1% |
| Application delivery controller (ADC) | 48.3% | 36.6% | 15.1% |
| File integrity / activity monitoring (FIM/FAM) | 46.9% | 39.5% | 13.6% |
| Runtime application self-protection (RASP) | 45.2% | 37.9% | 16.9% |
| Static/dynamic/interactive application security testing (SAST/DAST/IAST) | 44.8% | 39.3% | 15.9% |
| Third party code analysis | 41.4% | 39.6% | 19.0% |
| Bot Management | 36.0% | 43.7% | 20.3% |

## Complimentary Report

Download a copy of the full 2024 Cyberthreat Defense Report at: www.imperva.com/cdr2024.

## About Imperva

Imperva, a leading global cybersecurity company, protects and provides secure, data-driven insights to businesses worldwide. Imperva's advanced technology defends critical systems from cyber threats, ensuring the safety of business operations. Imperva's solutions offer robust protection for applications and APIs anywhere, delivering unparalleled security without compromising operational efficiency. With a commitment to innovation and customer-centric service, Imperva empowers businesses to thrive in an increasingly digital world.

CYBEREDGE GROUP℠

## About CyberEdge Group

CyberEdge Group is an award-winning research and marketing consulting firm serving the diverse needs of information security vendors and service providers. Headquartered in Annapolis, Maryland, with 40+ consultants based across North America, CyberEdge works with approximately one in every five IT security vendors and service providers. For more information, visit www.cyber-edge.com.