2022 Cyberthreat Defense Report

Executive Brief

PLATINUM SPONSOR

THREATX

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.

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

"In the area of application and data security, the most popular offering continues to be API gateway and protection products. Usage of these technologies has soared over the last few years, rising from 45.1% in our 2018 report to 64.1% today... We think API protection will become an even bigger area of focus in coming years."

– 2022 CDR

Notable Findings

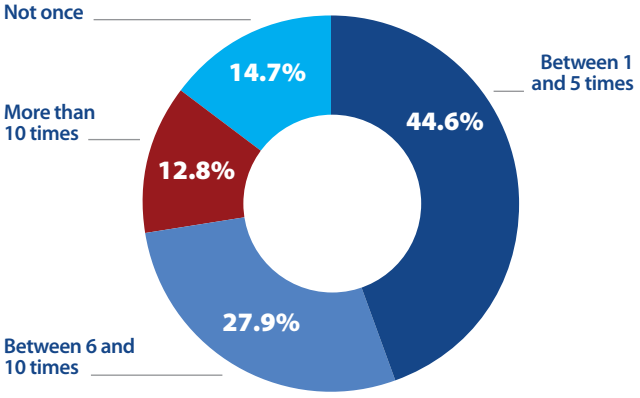
- **Nobody is immune from cyberattacks.** Eighty-five percent of organizations were victimized by cyberattacks last year, and 76% expect to be compromised this year.
- **ATO attacks are now top-of-mind.** Account takeover (ATO) and credential stuffing attacks are a growing concern, now second only to malware among major threats.
- **Security teams are most worried about mobile devices, ICS, IoT, and APIs.** Among IT domains, security professionals are least confident about their ability to protect mobile devices, industrial control systems (ICS), Internet of Things (IoT) devices, and APIs.
- **Use of API protection technology is soaring.** API gateway and protection tools are now the most-installed products in the application and data security technology category.

No Let-Up in Pressure on Security Teams

The number of organizations that experienced a successful cyberattack last year hovered at a near-record 85.3%, while the percentage victimized by six or more attacks increased to a new high of 40.7%. Also not reassuring: the number of respondents who think it likely that their organization will be successfully attacked in the coming year reached a record 76.1%.

What threats are the greatest concerns? Malware is still #1, with an average concern rating of 4.01 (on a scale of 1 to 5). But account takeover (ATO) and credential abuse attacks increased the most of any of the 12 categories of major threats on our list, moving from fourth place last year to second place now (3.97 rating). Ransomware retained third place (3.96), and phishing and spear-phishing were fourth (3.93). These were followed by attacks on brand and reputation (3.86), and APTs and denial of service attacks (both 3.85).

Frequency of successful cyberattacks in the last 12 months



Security Teams are More Confident About Protecting Some Areas than Others

The survey asked security professionals about their ability to defend against cyberthreats across different types of systems, technologies, and environments. They are most comfortable about their security posture for software as a service (SaaS) applications, physical and virtual servers, datastores such as file servers, databases, and SANs, and laptop and notebook computers. However, security teams are least confident about their ability to protect mobile devices, industrial control systems (ICS), Internet of Things (IoT) devices, and application programming interfaces (APIs).

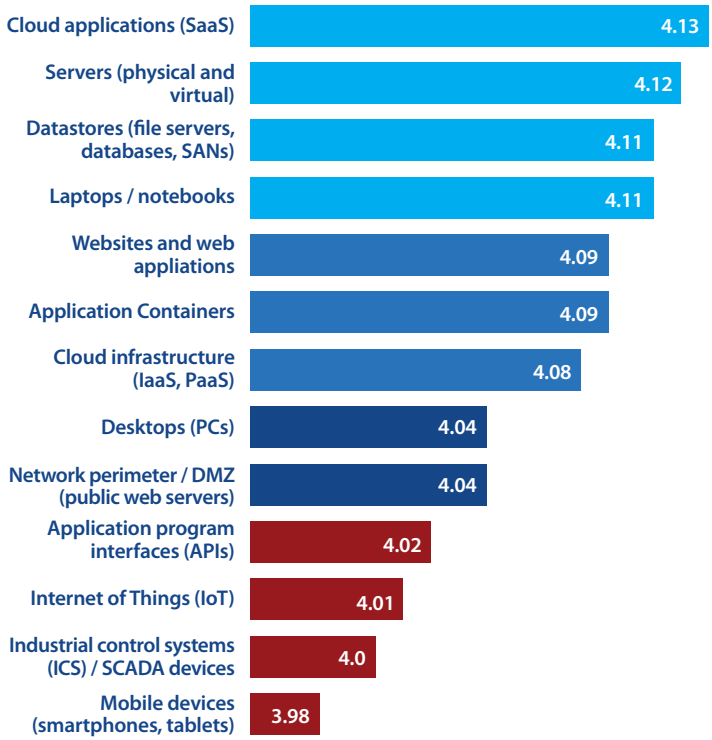
API Protection and Bot Management are in the Spotlight

Respondents were asked about technologies currently in use and planned for acquisition in five technology categories.

In the field of application and data security technologies, API gateway and protection products, web application firewalls (WAFs), and database firewalls were in the "must-have category," being used in roughly six out of ten of the organizations surveyed. API protection technologies in particular have taken off, rising from 45.1% of organizations to 64.1% over the past four years.

The application and data security technologies most widely planned for acquisition this year are bot management, advanced security analytics, and application security testing.

Perceived security posture by IT domain



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.threatx.com/cdr2022.

About ThreatX

ThreatX's API protection platform makes the world safer by protecting APIs from all threats, including DDoS attempts, BOT attacks, API abuse, exploitations of known vulnerabilities, and zero-day attacks. Its multi-layered detection capabilities accurately identify malicious actors and dynamically initiate appropriate action. ThreatX effectively and efficiently protects APIs for companies in every industry across the globe.

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.