THREATX

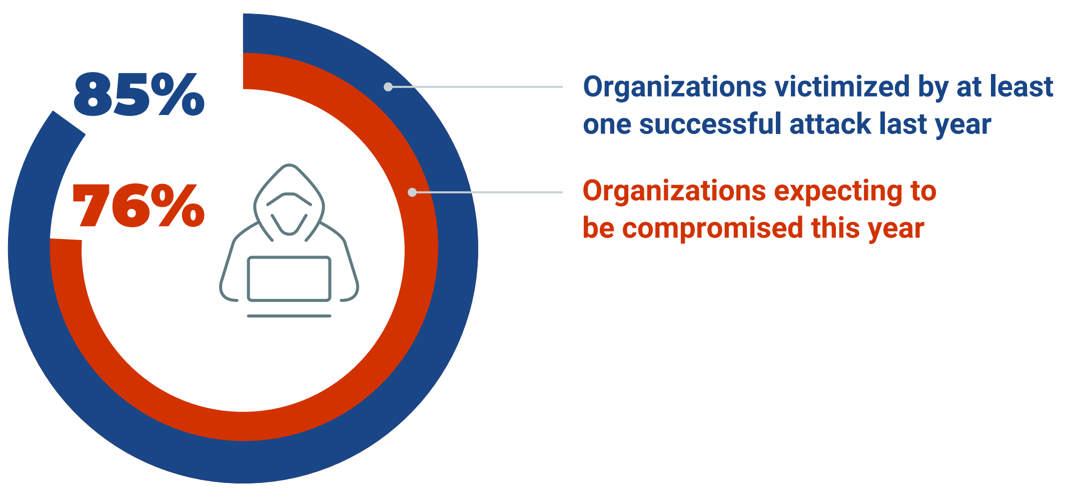
Insights from the CyberEdge Group

2022 Cyberthreat Defense Report

CyberEdge Group's ninth annual Cyberthreat Defense Report reveals how IT security professionals perceive the security posture of their organizations, the challenges they face in establishing effective cyberthreat defenses, and the plans they have to overcome those challenges. Read on to learn about some of the key findings from this year's report.

Everyone Faces Cyberattacks

Respondents at three-quarters of the organizations surveyed expect at least one successful attack this year; 85% were compromised last year



Top-of-Mind Threats

IT security professionals rated these cyberthreats as their greatest concerns. Account takeover and credential stuffing attacks rose from fourth place in the last survey to second in this one.

1. Malware
2. Account takeover / credential stuffing attacks
3. Ransomware
4. Phishing / spear-phishing attacks

Security Posture by IT Domain: Confidence Varies

Organizations are most confident about current defenses in areas like SaaS applications and servers, and least confident in domains such as mobile devices and application programming interfaces (APIs)

Rating of the organization's security posture (ability to defend against cyberthreats), on a scale of 1-5, with 5 highest

Mobile devices	3.98
Internet of Things (IoT)	4.01
Application program interfaces (APIs)	**4.02**
Desktops (PCs)	4.04
Websites and web appliations	4.09
Laptops / notebooks	4.11
Servers (physical and virtual)	4.12
Cloud applications (SaaS)	4.13

Key Application and Data Security Technologies

Must-Haves and Rising Stars

#1 API gateway / protection

#2 Web application firewall (WAF)

Most in use today

#1 Bot management

#2 Advanced security analytics

Most planned for acquisition

Managed Security Services are Increasingly Popular

IT security functions outsourced to a managed security service provider (MSSP)

Monitoring/managing SIEM platforms	41.1%
Detecting and responding to advanced cyberthreats/managed detection and response (MDR)	41.1%
Monitoring/managing web application firewalls (WAFs)	39.1%
Monitoring/managing intrusion detection/ prevention systems (IDS/IPS)	38.3%
Monitoring/managing secure web/email gateways (SWG/SEG)	37.5%
Monitoring/managing firewalls or UTMs	36.8%
Mitigating distributed denial of service (DDoS) attacks	36.6%
Managing vulnerability scans	33.3%

Download the full report at:

www.threatx.com/cdr2022

CYBEREDGE GROUP