AUJAS
CYBERSECURITY
An NSEIT Company

Assessing enterprise security readiness with DDoS simulations

Why modern enterprises need DDoS simulation services

DDoS simulation services enable enterprises to identify and respond to vulnerabilities in their defenses against growing DDoS threats. By simulating various attack scenarios in a controlled setting, these services strengthen security and facilitate better incident response planning.

150%
Increase in DDoS attacks globally since 2020

200%
Rise in DDoS attacks in 2023

23000
DDoS attacks occur every day

Common DDOS attack targets include

- E-commerce websites
- Financial institutions
- Government websites
- Healthcare organizations
- Social media platforms
- Cloud service providers
- Web hosting companies
- Streaming services
- IoT devices and networks

Sector-wise increase in DDoS attacks

794%	230%	177%	253%
Cloud/Saas	Finance	Government	Healthcare

$200,000
Average cost per DDoS attack without adequate cyber protection

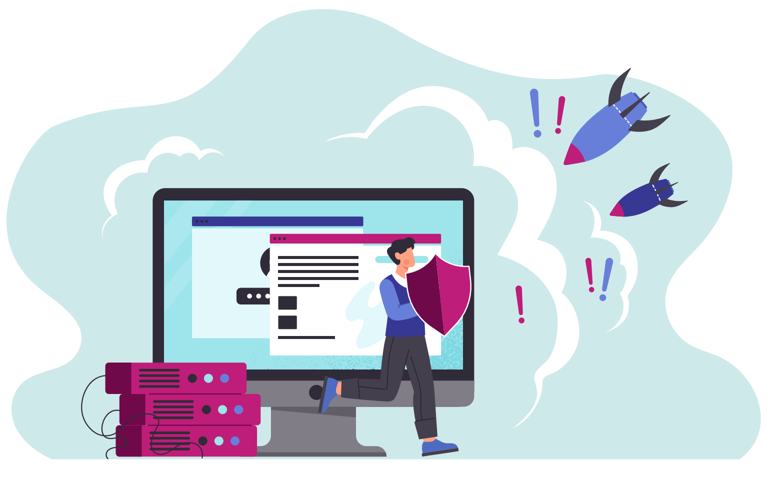
$120,000
Average cost of recovery from a DDoS attack for small businesses

29.3
Average number of attacks mitigated by organizations per day

Effects of DDoS attacks on organizations

- Ransom costs
- Loss of revenue
- Loss of productivity
- Remediation costs
- Damaged reputation
- Loss of market share

How DDoS attack simulations can help



- Evaluate DDoS defense performance
- Optimize defense system capabilities
- Assess third party vendor risk
- Enhance monitoring and instrumentation
- Improve operational incidence response

Key benefits of implementing DDoS simulations

- Improved operational monitoring
- Enhanced defense capability
- Improved incident response time
- Reduced mean time to resolution
- Preparedness against DDoS attacks

Experience the Aujas Cybersecurity benefit

- 100+ attack vectors
- 100 Gbps traffic generation capacity
- 200 agents with 10 GB bandwidth, 1 million/sec packet rate, and 4 million TCP connections
- Cloud servers (agents) in 140 global data centers
- Advance & Complex attacks including Application & Connection oriented attacks
- Real-time access to monitoring portal during attack simulation

1 Tbps

1 Tbps traffic generation capacity

150+ advanced attack vectors

Cloud servers (agents) in **140** global data centers

200 agents with 10 GB bandwidth, **1 million**/sec packet rate, and **4 million** TCP connections

Resource links

Source - Protecting Your Business From Cyber Attacks - https://go.zayo.com/zayo-ddos-protection-ebook/

Source - Protecting Your Business From Cyber Attacks - https://go.zayo.com/zayo-ddos-protection-ebook/

Source - Protecting Your Business From Cyber Attacks - https://go.zayo.com/zayo-ddos-protection-ebook/

Source - Protecting Your Business From Cyber Attacks - https://go.zayo.com/zayo-ddos-protection-ebook/

Source - Protecting Your Business From Cyber Attacks - https://go.zayo.com/zayo-ddos-protection-ebook/

Source - Protecting Your Business From Cyber Attacks - https://go.zayo.com/zayo-ddos-protection-ebook/

Source - Protecting Your Business From Cyber Attacks - https://go.zayo.com/zayo-ddos-protection-ebook/

Source - Protecting Your Business From Cyber Attacks - https://go.zayo.com/zayo-ddos-protection-ebook/

Source - Protecting Your Business From Cyber Attacks - https://go.zayo.com/zayo-ddos-protection-ebook/

Source - Radware Full Year 2022 Report: Malicious DDoS Attacks Rise 150% - https://www.radware.com/newsevents/pressreleases/2023/radware-full-year-2022-report-malicious-ddos-attacks/#:~:text=Attack%20frequency%3A%20The%20frequency%20of, at%20the%20end%20of%202021.