INFOGRAPHIC

Is your healthcare organization's network safe from DDoS attacks?

A distributed denial of service (DDoS) attack can cause significant disruption to the network, applications or services your healthcare organization relies on. This can adversely affect your operational and patient care capabilities, in addition to being potentially costly and impacting your reputation.

Healthcare entities are popular hacker targets

Healthcare was second only to financial services in the number of times the industry was compromised in 2024, marking the first year since 2017 that it did not occupy the top spot.[1]

82%
of healthcare organizations reported significant security incidents in 2024.[2]

2,210
The number of weekly cyberattacks experienced by the average healthcare organization.[3]

DDoS threats are expanding

Today's large-scale DDoS attacks are designed to flood and overwhelm your internet connectivity, preventing access to online resources for clinicians, staff and patients. Cybercriminals exploit practices with limited cybersecurity budgets, a shortage of dedicated cybersecurity staff and outdated security technologies.

512,000
The number of DDoS attacks registered worldwide in Q4 2024.[4]

92%
of healthcare organizations experienced a cyberattack in 2024.[5]

Goals of attacks on healthcare networks

- Extort organizations for a ransom to stop the attack.
- Interrupt time-sensitive scientific research data collection.
- Disrupt scheduled activities or cause chaos.
- Overload a network to prevent access to patient records and interrupt care.
- Hinder online collaboration among clinicians and other medical professionals.
- Prove it can be done, which is easy when a practice's network lacks protection.

$6,130 Average cost of an application-layer DDoS attack per minute.[6]

Reasons DDoS attacks are on the rise in healthcare

Practices may be more inclined to pay ransom demands to avoid disrupting care.

Interruptions in critical services attract widespread news coverage and provide desired notoriety for attackers.

The proliferation of Internet of Things (IoT) devices has expanded healthcare's attack surface.

Inadequate resources complicate a practice's ability to fend off attacks.

Easy access to affordable DDoS tools and instructions online simplifies attacks.

$30 a month
The cost of a subscription for DDoS attack-for-hire tools on the dark web.[7]

174%
The increase, noted by one platform in a single month in 2024, in the use of botnets, a key component of many DDoS attacks.[8]

Implement a security strategy that includes DDoS protection

To prevent disruptions to your network and safeguard your healthcare organization, DDoS mitigation measures need to thwart attackers and prevent downtime. An ideal solution will:

Monitor and evaluate
Offer intelligent monitoring and comprehensive traffic evaluation that uses advanced analytics to identify anomalies.

Provide fast resolution
Quickly and proactively detect, redirect and mitigate malicious traffic, minimizing the impact of attacks.

Scale with needs
Easily and seamlessly expand the solution as the demands of your practice change.

Offer continuous support
Provide always-available network and security expertise for swift issue resolution.

Only 14% of healthcare IT leaders say that their organizations' IT security teams are fully staffed.[9]

Be prepared and don't go it alone. A network service provider is uniquely positioned to provide the DDoS protection you need.

Discover how DDoS Protection from Spectrum Business® can help protect your network.

Learn more

1. "Identity Theft Resource Center 2024 Data Breach Report," Identity Theft Resource Center, January 28, 2025.
2. "2024 HIMSS Healthcare Cybersecurity Survey," HIMSS, 2025
3. "The State of Cyber Security 2025," Check Point Research, 2025.
4. Ani Petrosyan, "Number of DDoS Attacks Worldwide from 1st Quarter 2023 to 4th Quarter 2024," Statista, February 24, 2025.
5. "2024 Ponemon Healthcare Cybersecurity Report," Proofpoint, 2024.
6. "Application Security in a Multi-Cloud World 2023," Radware, November 8, 2023.
7. Michael Hill, "DDoS Attack-for-Hire Services Thriving on Dark Web and Cyber Criminal Forums," Cyber Security Hub, December 4, 2023.
8. "Cyber Threat Trends Report: From Trojan Takeovers to Ransomware Roulette," Cisco, June 2024.
9. Jordan Scott, "New CDW Research Report: Shortages Impact Healthcare Cybersecurity Strategies," June 10, 2024.

SE-MSHC-IG004