Key insights

41%

Percentage of API attacks in the healthcare ecosystem that targeted payer organizations

API attacks are growing steadily in the healthcare ecosystem, particularly attacks on payer organizations and insurance companies due to the wealth of information they hold: protected health information (PHI), claims data, and financial information.

API sprawl poses significant risks, like unauthorized access to data

API sprawl, or the unregulated proliferation of APIs within organizations, can create significant security gaps via a lack of visibility and their emergence outside of security controls. As a result, API sprawl expands an organization's attack surface and ushers in risks such as unauthorized access to sensitive data.

88%

Percentage of Layer 7 DDoS attacks against pharmaceutical organizations in EMEA

Pharmaceutical companies in the EMEA region experienced the highest volume of Layer 7 DDoS attacks, followed by North America and Asia-Pacific and Japan (APJ). A closer examination of H1 2024 data reveals that the number of attacks against EMEA and North America are on track to exceed the total for each region in 2023.

21 MILLION

Monthly average of web application and API attacks against healthcare providers

The push for data interoperability and other compliance requirements fueled the growth in web application and API use, which in turn created security risks for both providers and patients.

415 MILLION

Monthly average of Layer 7 DDoS attacks against healthcare providers

The healthcare industry is experiencing a surge in DDoS attacks, driven by hacktivism and the current geopolitical climate. These attacks can cause outages and disruptions that threaten patient outcomes. In 2023, Killnet launched a large-scale DDoS campaign that primarily impacted provider organizations.