

● THREAT ALERT

# Cyberattacks Hit Healthcare Systems at Scale, Disrupting Critical Patient Services

A wave of coordinated attacks targeted digital healthcare infrastructure, overwhelming systems, exposing sensitive data, and disrupting essential operations across the platform.

● 50 Gbps Attack Volume

● 250M+ Malicious Requests

● 250M+ Malicious Requests

## 50 Gbps

Peak Attack Size  
Volumetric traffic surge

## 250M+

Requests Generated  
Malicious traffic at scale

## 0 sec

Downtime  
Services 100% operational

## Minutes

Time to Respond  
Threats identified and controlled in real time

# A Healthcare Platform Under Attack

A leading healthcare platform faced a surge of cyberattacks targeting APIs, application layers, and exposed endpoints. Systems experienced slowdowns, failed responses, and operational instability as traffic rapidly escalated.

Over 250 million malicious requests flooded the platform, consuming 50 Gbps of bandwidth. The attack disrupted workflows, increased the risk of data exposure, and put patient services under pressure.

Layer 7 Attacks

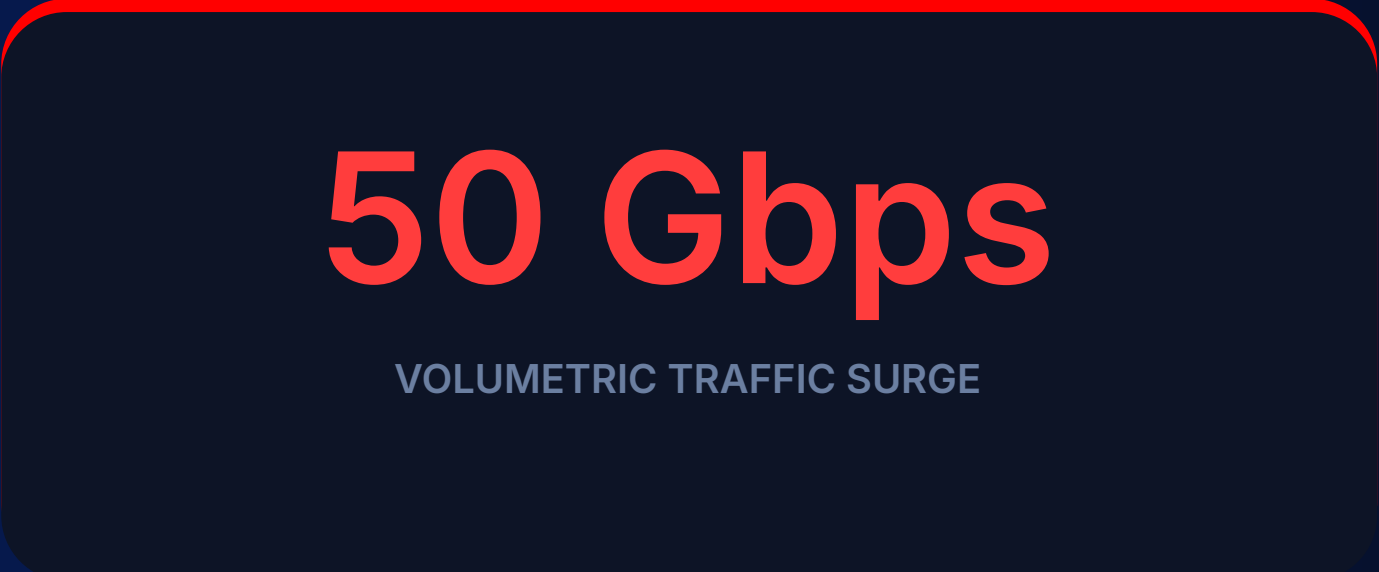
API Exploits

Bot Traffic

Credential Stuffing

Data Scraping

Zero-Day Exploits



⚠ Service Disruptions

⚠ Data Exposure Risks

⚠ Operational Instability



### Existing Defenses Couldn't Stop the Attacks

Security systems detected unusual activity but could not contain it. Traditional defenses were built for older threats, not the scale and complexity of modern attacks.



### Attack Traffic Looked Like Real Users

Bots and automated requests closely mimicked genuine patient behavior. Blocking malicious traffic risked blocking real users. There was no clear line between safe and harmful traffic.



### Security Couldn't Keep Up

Attack patterns kept changing in real time. Static rules failed to adapt. Every delay allowed the attack to push deeper into the system.



### Disruptions Impacted Critical Healthcare Services

This was not just a technical issue. Service instability affected patient access, delayed critical workflows, and weakened trust in digital healthcare systems.

# Prophaze WAAP: Built for Modern Healthcare Threats

Three coordinated capabilities that stopped what traditional tools could not.



## Stop Threats Across All Layers

- ✓ Protected APIs and application layers simultaneously
- ✓ Analyzed traffic behavior under high load
- ✓ Blocked malicious requests before impact
- ✓ No manual intervention required



## AI That Detects Hidden Threats

- ✓ Identified anomalies in user and API behavior
- ✓ Detected bot-driven and automated attacks
- ✓ Adapted instantly to evolving attack patterns
- ✓ Continuously improved detection accuracy



## Secure APIs and Critical Endpoints

- ✓ Validated and sanitized every request
- ✓ Discovered exposed and shadow APIs
- ✓ Applied rate limiting at endpoint level
- ✓ Ensured only legitimate traffic passed through

# Healthcare Systems Stabilized. Services Continued.

Here is exactly what happened and what it meant for the platform.



**Minutes**

**Attack Controlled**

Neutralized before systems faced further disruption



**0 sec**

**Zero Downtime**

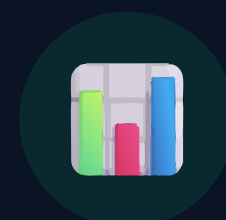
All critical healthcare services stayed live throughout the attack



**100%**

**Users Unaffected**

Patients and providers continued access without interruption



**Live**

**Full Threat Visibility**

Security teams monitored every attack pattern and response in real time



**+1**

**Stronger Security**

Every attack sharpens Prophaze's defenses. Future variants will be blocked even faster.

# What Changed When Prophase Was in Place

✘ BEFORE PROPHAZE	✔ AFTER PROPHAZE
<p>Threat Response</p> <ul style="list-style-type: none"><li>✘ Reactive systems struggled against API and bot-driven attacks</li></ul>	<p>Threat Response</p> <ul style="list-style-type: none"><li>✔ Real-time adaptive mitigation across all attack vectors</li></ul>
<p>System Stability</p> <ul style="list-style-type: none"><li>✘ Service disruptions and operational instability</li></ul>	<p>System Stability</p> <ul style="list-style-type: none"><li>✔ Stable performance under high traffic conditions</li></ul>
<p>Security Visibility</p> <ul style="list-style-type: none"><li>✘ Limited insight into attack patterns</li></ul>	<p>Security Visibility</p> <ul style="list-style-type: none"><li>✔ Real-time visibility into traffic and threats</li></ul>

*"Trusted by healthcare platforms to protect sensitive data  
and ensure uninterrupted digital care."*



Trusted by global enterprises, manufacturers, and exporters to maintain uninterrupted operations with AI-driven unified traffic management and failover protection.



**Protect Your Applications with AI-Driven  
Unified WAAP Platform in Minutes**