NETSCOUT

Observability Protects Healthcare from Tomorrow's Threats

Healthcare Faces Challenges

Healthcare organizations are under attack from bad actors on multiple fronts.

Patient records are a prime target for insurance fraud and identity theft. In 2023 there were 725 large security breaches in healthcare records, the highest total ever.[1]

- Healthcare ransomware attacks are up, nearly doubling in 2023.[2]
- DDoS attacks by nation-states are threatening to shut down life-saving medical systems.[3]

The large attack surface of healthcare organizations makes the problem worse.

- Internet of Medical Things (IoMT) devices are multiplying—and vulnerable.
  - The number of healthcare IoT connections, estimated at 1.27 billion in 2024, will more than double to 2.88 billion in 2028.[4]
- On-premises infrastructure, cloud-based services, server-to-server communications, and remote workers create unprecedented opportunities for hackers.
- Third-party providers are a crucial part of providing patient care, but are a major risk factor that accounts for nearly half of healthcare cyberattacks.

Healthcare organizations are under pressure to improve services, prevent downtime, protect data, and control costs.

- Providers strive to eliminate life-threatening latency and downtime, and provide high-quality patient care in person and via telehealth.
- Healthcare budgets are under pressure, and bankruptcies are not uncommon. In 2023, there were 79 healthcare bankruptcy filings, the highest total ever.[5]

How to Protect Your Organization from Disruptions

Visibility is key to data protection and resiliency.

- Beyond simply monitoring a single application, product set, or data stream, proactive defense requires borderless visibility—the ability to see a hybrid cloud network end-to-end, including server-to-server. Seeing more—and seeing it deeper—enables you to get ahead of the bad actors to stop attacks before damage is done.
- Results:
  - Fast detection and response keep operations running.
  - Avoidance of costly HIPAA fines.
  - Saved lives.

NETSCOUT's Smart Data is vital to observability and resiliency

- **Smart Data.** High-quality, enriched metadata pinpoints the root causes of issues.
- **Scale.** Infinitely scalable architecture delivers observability across the world's largest networks.
- **Historical.** Continuous retention of packet decodes and metadata drives enriched analytics.
- **AI-Ready.** Curated, AI-ready data feeds from NETSCOUT power AIOps platforms so you can identify hidden behavior patterns and prevent outages.

NETSCOUT Solutions

- **nGenius Enterprise Performance Management** pinpoints the source of anomalies in your mission-critical applications, from the data center to the cloud and everywhere in between.
- **Arbor DDoS Protection** shields essential organizations from disruptive attacks.
- **Omnis Network Security** enables faster threat hunting and incident response at scale and in real-time.
- **Omnis AI Insights** powers your predictive analytics to anticipate emerging threats.

NETSCOUT observability delivers results for healthcare.

- **NETSCOUT delivers borderless visibility** that's both broad and deep to protect patient information and ensure uninterrupted operations.
- **NETSCOUT leverages smart data** to enable investigation, analysis, and response to security events, empowering healthcare organizations to avoid life-threatening latency and outages.
- **NETSCOUT integrates with complementary technologies** to build comprehensive, affordable observability and security at scale.

Let NETSCOUT empower your healthcare system to be secure and reliable.

See this Executive Insight.

NETSCOUT

1. "Security Breaches in Healthcare in 2023" by Steve Alder. The HIPAA Journal, Jan. 31, 2024.
2. Office of the Director of National Intelligence, Feb. 2024.
3. NETSCOUT blog, Michael Wetherbee, April 26, 2023.
4. Statista Market Insights, updated March 2024.
5. Gibbins Advisors, Jan. 25, 2024.