PROACTIVE RISK



PATIENT TRUST MEETS CYBER THREAT

What Healthcare Leaders Need to Know

Today's healthcare providers don't just protect patient health, they also safeguard sensitive data, critical infrastructure, and constant uptime. Unfortunately, threat actors know this. That's why healthcare remains one of the most frequently targeted industries for ransomware, credential theft, and cloud compromise.

KNOW THE STATISTICS:

Healthcare remains one of the top targeted industries

$1M median ransom demand across sectors

Identity-based attacks involving MFA bypass and stolen session tokens are rising fast

Here's why Hackers Target Healthcare

Healthcare providers face a perfect storm of cyber risk: legacy systems, complex vendor ecosystems, high-stakes operations, and compliance pressure.

Attackers exploit the fact that you can't afford downtime, and that makes you a high-value target.

HOW THE ATTACKS HAPPEN

- Identity-based intrusions using stolen credentials and session hijacking
- Ransomware groups deploying tools like Lumma Stealer, Rclone, and remote desktop software
- Cloud environments compromised via weak MFA or misconfigured APIs

The Bigger Picture:

A single breach can mean patient safety concerns, regulatory penalties, insurance challenges, and irreparable damage to trust.

Security isn't just about preventing attacks, it's about preserving care, continuity, and credibility.

HOW WE PROTECT HEALTHCARE BUSINESSES

- Team of expert security analysts monitoring and responding to any sign of attack
- 24/7/365 attack surface protection; endpoint, cloud and identity, enabling secure remote and hybrid work
- Identity protection and response

Let's talk about building a modern security approach that keeps your systems secure, your team focused, and your patients safe. Schedule a 15-minute consultation to review your security gaps and how we close them, no pressure.

Operate securely. Care confidently.

www.proactiverisk.com

Sources:
Blackpoint Cyber Mid Year Threat Report 2025