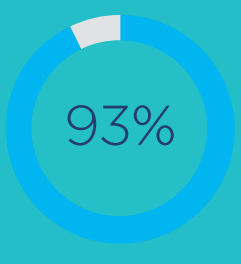
INFOGRAPHIC

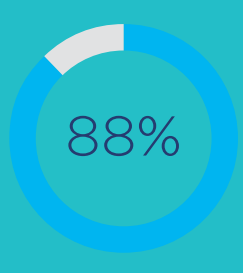
How to protect your healthcare network from evolving threats

Keeping patient data secure across multiple locations, networks and devices is a critical challenge for healthcare organization (HCO) IT leaders.



of healthcare organizations have experienced a data breach over the past three years.[1]

more healthcare data breaches were reported in 2020 vs. 2019.[2]



of providers cite budget constraints is a major obstacle to properly securing and protecting health information.[3]

Keep your network and sensitive patient data safe by doing the following:

Understand why the healthcare industry is at risk

Attackers are drawn to the sector because of the high-value, high-impact of a breach and vast amount of protected health information (PHI).

29 million+ patient records were breached in 2020 — this is the third worst year on record.[4]

The impact is more than just money

While $9.2 million is the average cost of a healthcare data breach, the harm isn't just financial.[5] It can also effect:

Productivity

Patient care

Reputation

Data loss

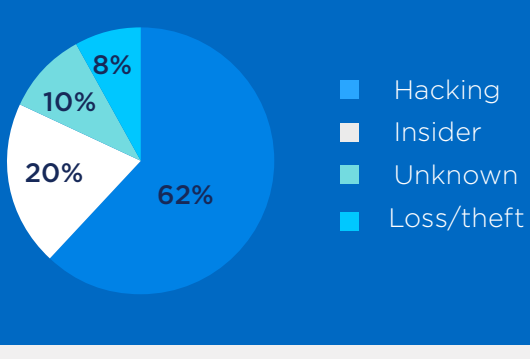
Track the evolving threat profile

The types of cyberthreats in healthcare are constantly changing and come from a wide range of attack vectors. The top data breach threats in healthcare organizations include:

- **DDoS:** Distributed denial of service (DDoS) attacks have increased in size, duration, sophistication and frequency during the Covid pandemic. There were nearly 5.4 million DDoS attacks worldwide in the first half of 2021 alone, up 11 percent year-over-year. The average attack duration was 50 minutes, up 31 percent.[6] Since 2020 the healthcare sector has suffered some of the largest attacks, with average attack size of more than 60,000 megabits per second; other industries suffered attacks of 10,000 mbps or less.[7]
- **Ransomware:** Today's advanced strains of ransomware encrypt data on a network and often lock users out of their devices. Ransomware was the leading cause of healthcare data breaches in 2020, accounting for nearly 55% of incidents.[8]
- **Business email compromises:** Email compromise, a category that includes phishing attacks, was identified as the root cause of 21% of healthcare data breaches in 2020. It was the third most-common attack type that year.[9]
- **Insider threats:** An insider threat refers to incidents caused by someone within or close to an organization, such as an employee, a former employee, a contractor or a business partner, who misuses his or her authorized access in a way that negatively impacts the organization. Insider threats accounted for 7% of data breaches in the healthcare sector during 2020.[10]

Know your vulnerabilities

Types of incidents that led to healthcare data breaches in 2020:[11]



Find comprehensive coverage and support

Widespread, coordinated network protection can keep you one step ahead of evolving and growing healthcare network threats. Learn how to protect your organization and what to look for in a network security provider in our healthcare cybersecurity guide.

Get the guide

Sources

1. "The 2020 Healthcare Cybersecurity Report." Special Report from the Editors at Cybersecurity Ventures Sponsored by Herjavec Group. 2020.
2. "Healthcare Breach Report 2021: Hacking and IT Incidents on the Rise." Bitglass. February 17, 2021.
3. "State of the Healthcare Cybersecurity Industry." Black Book Market Research LLC. October 2020.
4. "2020 Healthcare Data Breach Report: 25% Increase in Breaches in 2020." HIPAA Journal. Jan. 19, 2021.
5. "2021 Cost of a Data Breach Report." IBM and Ponemon Institute. July 28, 2021.
6. "Netscout Threat Intelligence Report. Issue 7: Findings from 1H 2021." 2021.
7. "DDoS Attack Trends for 2021." David Warburton. May 7, 2021.
8. "Healthcare Security: Ransomware Plays a Prominent Role in COVID-19 Era Breaches." Rody Quinlan. Tenable. March 10, 2021.
9. Ibid.
10. Ibid.
11. "2021 Breach Barometer." Protenus. March 15, 2021.

SE-HC-IG008_v2

Spectrum ENTERPRISE