INFOGRAPHIC

Protect your hotel network from cyberthreats

The pressure to modernize and meet guest expectations makes hospitality a dynamic industry — and a vulnerable target for cyberattacks.

Hoteliers continue to adopt new technology to gain efficiencies, reduce costs and improve the guest experience. These include biometrics to speed up check-in, smartphone apps that simplify room access, smart HVAC systems that save energy, occupancy sensors to assist housekeeping and many other connected technologies. However, the more devices added to a network, the more difficult it becomes to protect.

Attacks are becoming more frequent and more damaging

1,270

The average number of cyberattacks experienced weekly by organizations in hospitality, travel and recreation.[1]

33%

Increase in the average number of weekly attacks reported by hospitality organizations from 2023 to 2024.[2]

$4.03M

Average cost of a data breach in the hospitality sector as of 2025.[3]

Understand why the hospitality industry is at risk

Multiple factors put hotels at high risk for cyberattacks. Security challenges faced by organizations in the hospitality industry include:

Valuable data

Hotels are a frequent target because they collect personally identifiable information (PII) — like addresses, birth dates, driver's license information and passport numbers — that can be sold on the dark web for identity theft.

Legacy systems

Older networks are harder to protect, and 40% of hotel IT and cybersecurity leaders say outdated or insufficient technology is increasing their risk of cyberattacks.[4]

Limited resources

As IT teams protect their organizations from a growing number of increasingly sophisticated threats, more than half of hoteliers say a lack of skilled expertise is a top technology challenge.[5]

Track the evolving threat profile

Attackers constantly search for new workarounds to gain entry into systems and bypass security measures. Some of their most effective tactics include:

- **Social engineering**

  Phishing attacks have become widespread, with attackers often impersonating legitimate entities to steal data or plant malware through malicious files or downloads.

- **AI-powered cyberthreats**

  AI is being used to create automated attacks that are harder to detect and thwart. More than 90% of security experts expect a significant rise in AI-driven threats.[6]

- **Ransomware and other malware**

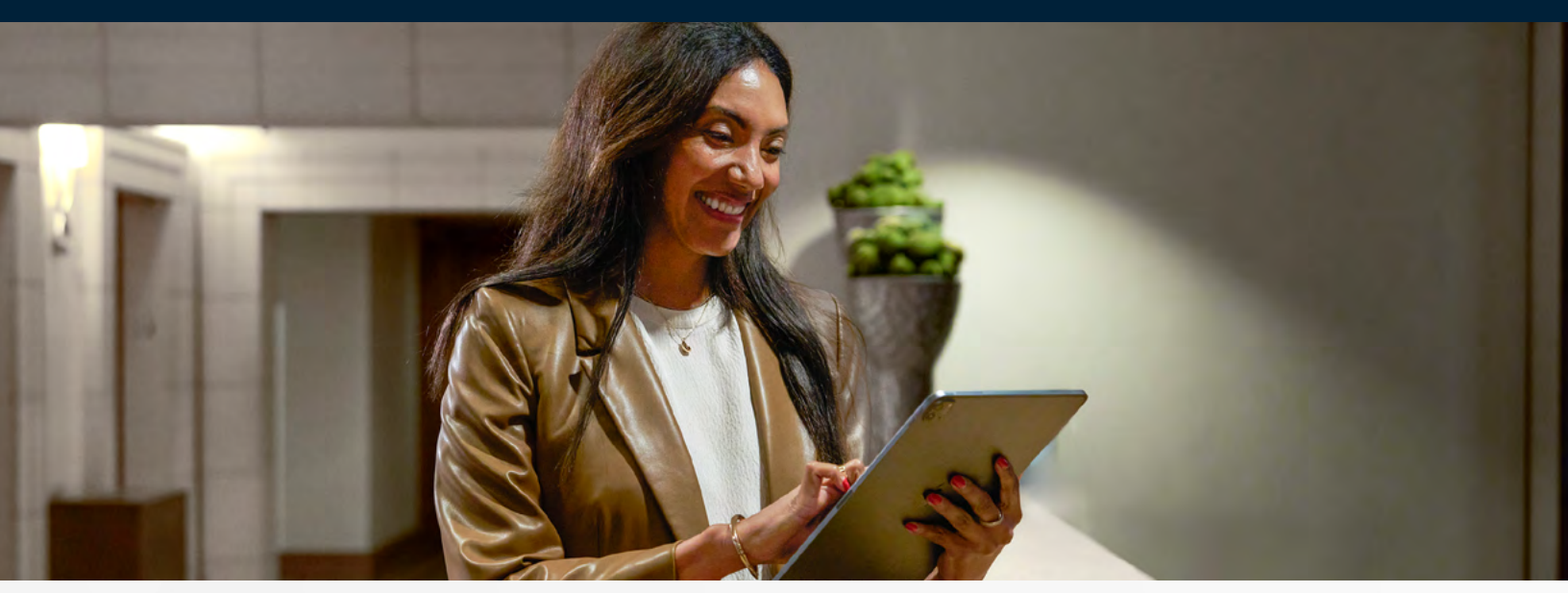
  Attackers increasingly use malware that encrypts critical data to bring operations to a standstill before extorting payments. Disrupting revenue at a critical time of the year, cyberattacks successfully hit 82% of North American hotels in summer 2024.[7]

- **Distributed denial of service (DDoS) attacks**

  Hotel networks, websites and cloud applications can be overwhelmed by malicious traffic. Volumetric DDoS attacks can be executed with tools purchased on the dark web for as little as $30 per month, making them a common threat.[8]

- **Data breaches**

  Unauthorized access to or use of confidential data remains a risk in the hospitality industry. As of 2024, there were 95,040 identified vulnerabilities in publicly exposed hospitality systems.[9]



Know where you're vulnerable

When hospitality IT and cybersecurity leaders were surveyed about risks to their organizations, the most frequently cited areas of vulnerability were:[10]

1. Payments and point-of-sale systems (72%).
2. Guest WiFi (56%).
3. Front desk systems (34%).
4. Internet of Things room devices (22%).
5. Booking engines or websites (16%).

Find comprehensive coverage and support

Widespread, coordinated network protection can help keep you one step ahead of growing hospitality network threats. Spectrum Business® offers a complete set of managed services that can help protect your hotel and guests while simplifying cybersecurity.

Learn more

1. "The State of Cyber Security 2025," Check Point Research, 2025.
2. Ibid.
3. "Cost of a Data Breach Report 2025: The AI Oversight Gap," Ponemon Institute and IBM Security, July 2025.
4. "Peak Season, Peak Risk: The 2025 State of Hospitality Cyber Report," VikingCloud, July 2025.
5. "2024 Lodging Technology Study: Digital Transformation & ROI," Hospitality Technology, 2024.
6. "Cybercrime Trends 2025," SoSafe, 2025.
7. "Peak Season, Peak Risk."
8. Michael Hill, "DDoS Attack-for-Hire Services Thriving on Dark Web and Cyber Criminal Forums," Cyber Security Hub, December 4, 2023.
9. "2025 Trustwave Risk Radar Report: Hospitality Sector," Trustwave, 2025.
10. "Peak Season, Peak Risk."

©2025 Charter Communications. All rights reserved. Spectrum Business is a registered trademark of Charter Communications. All other logos, marks, designs, and otherwise are the trademarks and intellectual property of their respective third-party owners. Not all products, pricing and services are available in all areas. Pricing and actual speeds may vary. Restrictions may apply. Subject to change without notice.

SE-HO-IG003_v3