INFOGRAPHIC

Protect your network from cyberthreats

Cybercrime grows more disruptive every year. Attacks are relentless and becoming more sophisticated, forcing IT leaders to confront massive business risks as they manage increasingly complex networks. The threat underlines a growing need for comprehensive, up-to-date protection for users, networks and data.

Attacks are becoming more frequent and more damaging

Cybercriminals are taking advantage of a rapidly expanding threat surface. Hybrid networks, cloud applications, AI adoption and proliferating endpoints from the Internet of Things all add to the potential for vulnerabilities. Risks include outdated software, unprotected data and distributed denial of service (DDoS) attacks that overwhelm critical services.

2,850
Number of data breaches reported in the United States in 2024.[1]

549%
Increase in the number of web DDoS attacks from 2023 to 2024.[2]

$4.44M
Average cost of a data breach as of 2025.[3]

Understand the risk

More than half of all data breaches involve customers' personally identifiable information (PII) — incidents that can have long-lasting effects on brand reputation and consumer trust.[4]

Among enterprises that experienced a breach in customer and employee data:[5]

30% dealt with cyber insurance repercussions.

19% had greater difficulty attracting new customers.

15% lost business partners.

66% of tech leaders say mitigating cybersecurity risks is one of their highest priorities.[6]

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. Nearly half of organizations worldwide consider the advance of adversarial capabilities to be the biggest security concern surrounding AI.[7]

☑ **Ransomware and other malware**
Attackers increasingly use malware that encrypts critical data to bring operations to a standstill before extorting payments. In 2024, at least 195.4 million records were breached in ransomware attacks worldwide.[8]

☑ **DDoS attacks**
Volumetric attacks can be executed with tools purchased on the dark web for as little as $30 per month, making them a frequent threat.[9] On average, businesses lose $6,130 per minute from an application-layer DDoS attack.[10]

☑ **Data breaches**
Unauthorized access to or use of confidential data remains a risk. The global average cost of a data breach reached $4.44 million as of 2025.[11]

Know where you're vulnerable

IT decision-makers must address a wide range of potential vulnerabilities to keep their networks secure. Some of the most urgent include:

Weak user authentication

The most common passwords in 2025 were **123456**, **123456789**, **qwerty** and **password**.[12] This vulnerability can be even more severe when organizations fail to use multi-factor authentication (MFA).

Legacy systems

Older infrastructure can be more difficult to secure, and 71% of organizations say they have network assets that are aging or obsolete.[13]

Limited expertise

For many organizations, IT resources haven't kept up with the expanding threat environment. Only 14% of executives are confident their organization has the cybersecurity talent needed today.[14]

Insecure cloud applications

Between 2024 and 2025, 30% of breaches involved data distributed across multiple environments, more than public clouds, private clouds or on-premises experienced on their own.[15]

Find comprehensive coverage and support

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

Learn more

[1] "Identity Theft Resource Center 2024 Data Breach Report," Identity Theft Resource Center, January 28, 2025.
[2] "2025 Global Threat Analysis Report," Radware, 2025.
[3] "Cost of a Data Breach Report 2025: The AI Oversight Gap," Ponemon Institute and IBM Security, July 2025.
[4] Ibid.
[5] Heidi Shey, Amy DeMartine, Danielle Chittem et al., "The State of Data Security, 2025," Forrester, October 22, 2025.
[6] "Bridging the Gaps to Cyber Resilience: The C-Suite Playbook," PwC, 2024.
[7] "Global Cybersecurity Outlook 2025," World Economic Forum, January 13, 2025.
[8] Rebecca Moody, "Ransomware Roundup: 2024 End-of-Year Report," Comparitech, January 9, 2025.
[9] Michael Hill, "DDoS Attack-for-Hire Services Thriving on Dark Web and Cyber Criminal Forums," Cyber Security Hub, December 4, 2023.
[10] "Application Security in a Multi-Cloud World 2023," Radware, November 8, 2023.
[11] "Cost of a Data Breach Report 2025."
[12] Paulius Masiliauskas, "Most Common Passwords: Latest 2025 Statistics," Cybernews, April 18, 2025.
[13] "2024 Infrastructure Lifecycle Management Report," NTT Data, 2024.
[14] "Global Cybersecurity Outlook 2025."
[15] "Cost of a Data Breach Report 2025."