EXECUTIVE BRIEF

SECURING A MODERN NETWORK

Tips to protect your network from ransomware and DDoS attacks

Cyber threats like ransomware, DDoS attacks and security vulnerabilities that allow attackers to access networks and steal information are on the rise. Don't think your organization will fall victim? Think again.

Over $1 billion in ransomware payments were made in 2023 worldwide.[1] Sixty-six percent of 1,700 IT and cybersecurity professionals surveyed reported to falling victim to ransomware.[2] Most likely, organizations will experience recurring attacks in the future, too. As an example, a survey by Cybereason found that 78% of organizations that paid ransomware demands were exposed to a second attack.[3]

Evolving security threats often leave IT leaders with more questions than answers, including: Will modernizing my network make maintaining security measures easier and help with evolving threats, or will it create more complexity to manage? In this executive brief, we'll explain the current security risks to your organization, steps you can take before an attack hits and some of the comprehensive security solutions available for a modern network that make it easier to maintain.

Same challenges, new threats

Critical business systems and applications that have not been updated are more susceptible to data breaches. In 2023, 26,447 vulnerabilities were disclosed by Common Vulnerabilities and Exposures (CVE), 1,500 more than in 2022.[4] Most organizations, including those with IT-developed departments, have a limited amount of time to work through the steady churn of updates to critical systems. This has been a constant in IT security for years. What has changed, though, are the threats to an organization's network.

Critical business systems and applications that have not been updated are more susceptible to data breaches.

Ransomware's rising cost

One of the most popular threats today is ransomware. Expenditures related to mitigating a ransomware incident can go far beyond the asking price to unlock data encrypted by attackers. These costs can include the ransom, network downtime, employee time, equipment costs, network costs, lost opportunities and other financial losses. Excluding ransoms, the average cost for organizations to recover from a ransomware attack is nearly $3 million, an increase of almost $1 million since 2023.[5] To top it off, 84% of victims paid the ransom, but only 47% got their data and services back uncorrupted.[6]

$3 million

was the average cost for organizations to recover from a ransomware attack in 2022.[7]

Few sectors of the economy have been spared from cybercrime. While ransomware impacts all industries, there's been a recent surge in attacks on shipping and supply chain businesses as more people shop online. Cybereason found that 41% of ransomware attacks breached organizations via supply chain partners.[8]

For municipalities, the Center of Internet Security (CIS) found that cyberattacks on state and local governments increased during first eight months of 2022 and 2023 based on a survey of 3,600 state, local, tribal and territorial government organizations.[9] According to CIS, malware attacks increased by 148%; ransomware incidents were 51% more prominent; and there was a 313% rise in endpoint security services incidents, such as data breaches, unauthorized access and insider threats.[10]

New twists on DDoS attacks

Distributed denial of service (DDoS) attacks are designed to flood a network, application or service with traffic to block legitimate access to resources. DDoS attacks are not new, but they are evolving and even showing seasonality in sectors like education — peaking in May and September to coincide with standardized testing.

Another new twist on DDoS attacks is the addition of ransom requests before an attack occurs. A triple extortion attack is a good example. In a triple extortion attack, bad actors use a three-pronged approach to extort money from victims by:

- Targeting business systems with ransomware to encrypt sensitive information.
- Extracting this sensitive customer data and encrypting it with ransomware followed by threatening the business with leaking or selling data online.
- Threatening to disrupt business operations with a DDoS attack which pressures the victim to pay the ransom fee by a specific date.[11]

Even if a DDoS attack doesn't involve extortion, it can still be used to distract IT teams from other attempts to breach the network at the same time. For example, bad actors will sometimes launch a small scale DDoS attack to keep IT professionals busy. The thieves then hack the network and steal data while no one is looking. Tactics like these demonstrate that DDoS incidents can be multi-faceted and are not something that organizations can wait out.

Steps to take now to protect your organization

Backup your data off site

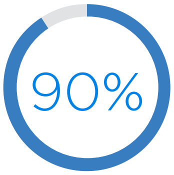
Leaving your network vulnerable to external threats can impact your bottom line. The good news is that there are simple precautions you can take to help protect your network on your own or with the help of security solutions from a trusted provider. One of the most important steps to take right now is to conduct regular backups of data that are stored off site or on hardware that does not have a permanent connection to your network. Many IT teams make the mistake of storing backups on systems interconnected with the rest of the organization. This renders them useless as an attack spreads as they can be infected along with the rest of the network.

Know the details of your connectivity

You should also know who supplies your network connections and what kind of connections you have for your organization. Keep the phone number of your internet provider within reach in case your network is not available to search for contact information during an attack. On a similar note, keep an updated list of your IP address blocks stored offline. Giving that information to a DDoS protection provider can help them resolve attacks faster.

Train your staff to identify threats

Many of the most destructive attacks begin with a single click in an employee's email. In 2022, 81% of cyberattacks were in the form of phishing, password and malware attacks.[13] One report found there were 255 million phishing attempts in 2022, a 61% jump from 2021.[14] Worse yet, more than 70% of those emails were opened by the recipient.[15] Organizations can help protect themselves by training staff to identify common phishing tactics and by regularly testing the team with emails that simulate an attempt to breach your network.



of corporate security breaches are the result of phishing.[12]

A comprehensive approach to security

Securing your network

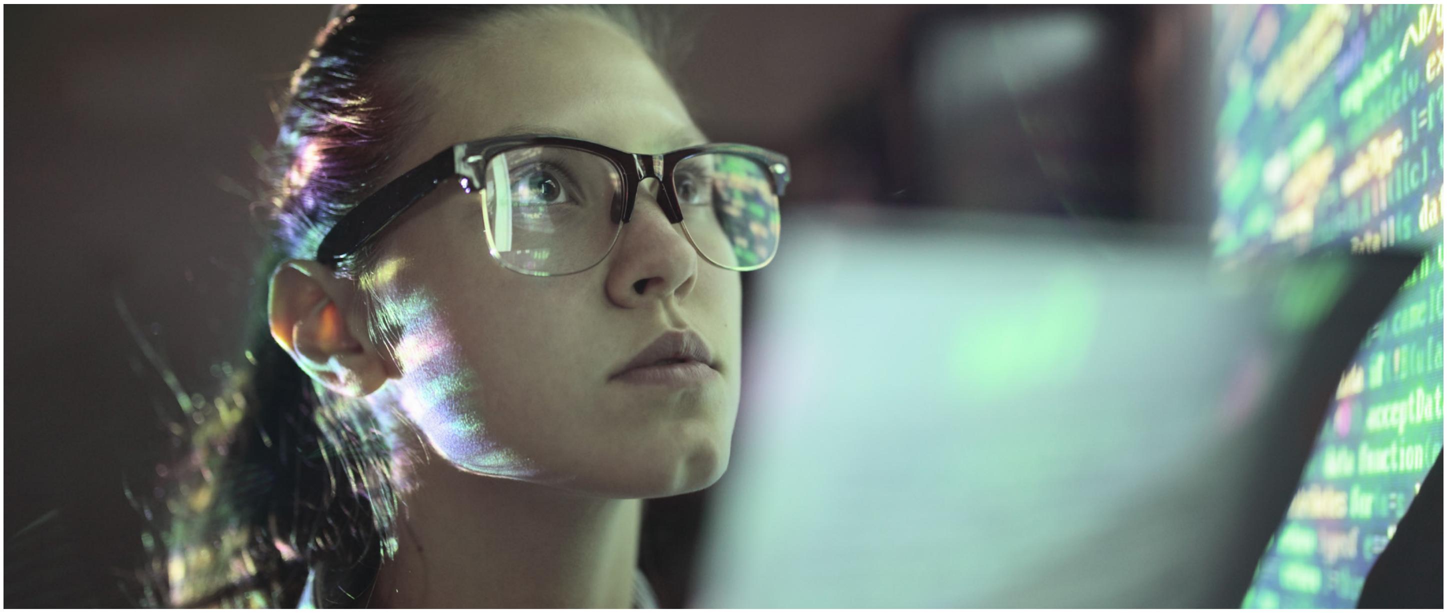
Organizations can better protect their networks by investing in a managed security service from a provider with technology that can safeguard network operations and ensure security measures are always up-to-date. Managed services take the guesswork out of network security and also free up your IT team to focus on other business-critical initiatives.

When evaluating solutions, look for an option that provides a fully integrated firewall and comes with end-to-end system design, installation and support. The best solutions also offer unified threat management (UTM) with capabilities for intrusion prevention, content filtering, DNS protection and antivirus. Some vendors offer this protection as part of a comprehensive, all-in-one network solution while others may need to buy security features as an added service.

Securing your connectivity

No matter what modern network solution your organization chooses, DDoS protection from a nationwide connectivity partner can further protect your network with 24/7/365 threat detection and mitigation, ensuring the availability of your network assets. The best solutions for modern networks use cloud-based intelligence to evaluate your network activity and identify threats before they reach your IP addresses.

Automated attack mitigation and traffic rerouting will help keep your network resources available while malicious traffic is rerouted and scrubbed clean by your provider. Read the terms of service contracts carefully as some charge an added fee for every incident. That can get costly. DDoS protection that has a flat-rate, subscription-based service lets you avoid unexpected expenses in the event of multiple attacks.



Keep your data safe with a partner you can trust

Proactive prevention is the best defense. Waiting until your organization is under attack is not the time to figure out who to call. Instead, plan ahead and have solutions in place before you need them.

Security threats can derail an organization, but adopting modern security measures can be easier than it looks. By working with an experienced and trusted service provider, you can ensure consistent protection with automated updates built into your network at every level.

Discover how Managed Network Edge, delivered over the Cisco Meraki platform, can quickly and easily strengthen your network security posture.

Learn more
https://enterprise.spectrum.com/ManagedNetworkEdge

1. "2024 MSP Threat Report," ConnectWise, April 2024.
2. "The State of Email Security Report," Mimecast, 2023.
3. Greg Day, "Ransomware: True Cost to Business 2024," Cybereason, 2024.
4. Saeed Abbasi, "2023 Threat Landscape Year in Review: If Everything Is Critical, Nothing Is," The Research Unit, Qualys, Jan. 4, 2024.
5. "Ransomware Payments Increase 500% In the Last Year, Finds Sophos State of Ransomware Report," Sophos, April 30, 2024.
6. Greg Day, "Ransomware: True Cost to Business 2024," Cybereason, 2024.
7. "Ransomware Payments Increase 500% In the Last Year, Finds Sophos State of Ransomware Report," Sophos, April 30, 2024.
8. Greg Day, "Ransomware: True Cost to Business 2024," Cybereason, 2024.
9. Sophia Fox-Sowell, "Cyberattacks on state and local governments rose in 2023, says CIS report," StateScoop, Jan. 30, 2024.
10. Ibid.
11. "Defeating Triple Extortion Ransomware: The Potent Combo of Ransomware and DDoS Attacks," Akamai, March 21, 2023.
12. "The State of Email Security Report," Mimecast, 2023.
13. "2023 Cybersecurity Skills Gap Global Research Report," Fortinet, March 2023.
14. "The State of Phishing Report," SlashNext, 2022.
15. "The State of Email Security Report," Mimecast, 2023.

About Spectrum Enterprise

Spectrum Enterprise, a part of Charter Communications, Inc., is a national provider of scalable, fiber technology solutions serving many of America's largest businesses and communications service providers. The broad Spectrum Enterprise portfolio includes networking and managed services solutions: Internet access, Ethernet access and networks, Voice and TV solutions. The Spectrum Enterprise team of experts works closely with clients to achieve greater business success by providing solutions designed to meet their evolving needs. For more information, visit enterprise.spectrum.com.

©2024 Charter Communications. All rights reserved. Spectrum Enterprise 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.