WHITEPAPER

Securing Today's Networks

PRESENTED BY:

Spectrum ENTERPRISE

PUBLISHED BY:

FIERCE Telecom

SECURING TODAY'S NETWORKS

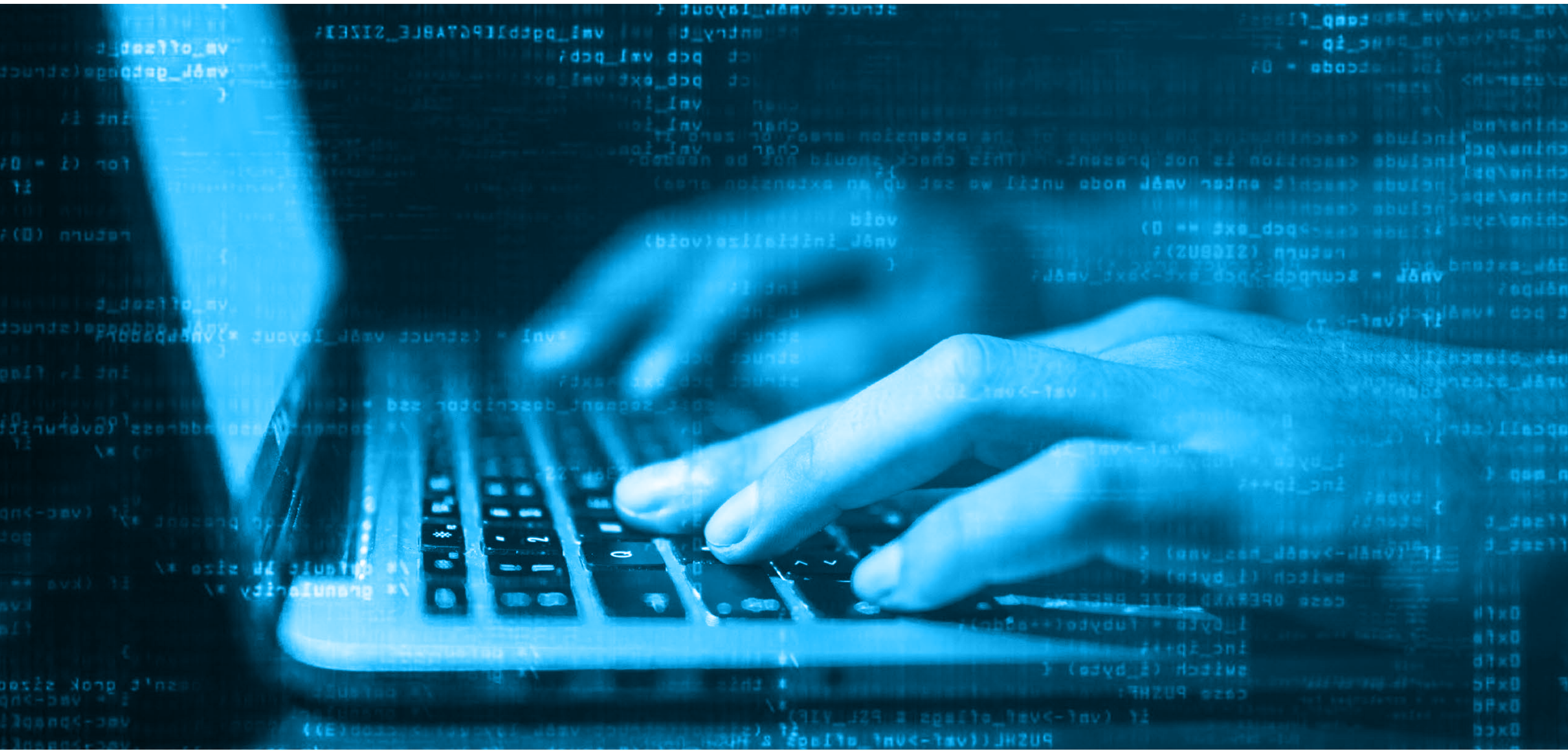
Transitioning to a more modern network architecture often leaves IT leaders asking: Will modernizing my network make maintaining security measures easier and help with evolving threats, or will it create more complexity to manage?

Cyber threats like ransomware, DDoS attacks and security vulnerabilities that allow attackers to access networks and steal information are on the rise:

- Ninety percent of IT professionals lack confidence that their networks are secured against attacks or breaches.
- Ransomware attacks have grown more than tenfold over the past 12 months.
- A survey by Cybereason found that eight in 10 organizations that paid ransomware demands were exposed to a second attack.

Even if organizations transition to a more simplified modern network, the security included typically protects the on-premises or core network, but other critical elements such as connectivity and the network edge must also be protected.

In this white paper, we'll explain the current security risks to your network across the three key areas of the network: the core, the connectivity, and the edge. We'll also outline best practices for proactive prevention, as well as how managed security solutions can make comprehensive and strategic security easier to implement and maintain.



ENSURING CORE NETWORK SECURITY VIA FIREWALLS

Firewall security is part of a multifaceted approach to protecting any enterprise organization. A high-level firewall can monitor inbound and outbound network traffic to identify and block suspicious activity. From external threats like hacking attempts and malware to internal threats like malicious insiders or data leaks, the enterprise firewall is highly effective at mitigating a significant number of risks and vulnerabilities.

However, managing and optimizing a firewall can be resource intensive. From deploying, integrating and configuring firewall technology to monitoring traffic, performing upgrades and ensuring that the enterprise firewall is aligned with security policies, the effort of continuous firewall management can easily fall short as IT staff work to keep up with other high-priority, strategic network initiatives.

A managed firewall service can help to better protect the enterprise by offloading these routine-but-critical tasks to a team of highly qualified firewall specialists. With a managed firewall security service, IT teams can:

- Improve data protection through automatic updates to the firewall that help to mitigate known risks and vulnerabilities.
- Eliminate network threats more easily with a fully managed and optimized firewall.
- Provide remote security that allows remote users to connect through secure VPN connections.
- Comply with regulatory mandates such as HIPAA and CIPA.
- Minimize the burden on IT staff by offloading tasks to a team of dedicated specialists.
- Provide expert support from certified technicians through 24/7/365 phone and online support.

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 offer unified threat management (UTM) with capabilities for intrusion prevention, content filtering, DNS and antivirus protection. Some vendors offer this protection as part of a comprehensive all-in-one network solution while others may require the need to buy security features as an added service.

PROTECTING THE NETWORK AGAINST DDOS THREATS

Cyberattacks are becoming more frequent and complex, particularly Distributed Denial of Service (DDoS) attacks. In the first half of 2021, cybercriminals launched approximately 5.4 million DDoS attacks, increasing 11% over 1H 2020 figures. Additionally, data projections point to 2021 as another record-setting year on track to surpass 11 million global DDoS attacks.

DDoS attacks flood connectivity to a network, application, or service so that the intended users cannot access their resources. They are initiated with the goal of halting network operations, potentially causing damage to an organization's reputation, loss in revenue, or both.

The current DDoS threat has:

- **High costs:** A typical attack could cost $2.3 million to $4 million.
- **Longer duration:** The median downtime of a DDoS attack lasts between 7 and 12 hours.
- **More points of origin:** There will be an estimated 30.9 billion connected IoT devices by 2025.

For every defense that is put in place, hackers will eventually adapt and come up with a different way to compromise networks. This is why it's so important for firewalls, DDoS protection services and other security measures to be constantly updated with new attack signatures, which are traffic patterns used to identify attacks.

In the first half of 2021, cybercriminals launched approximately ***5.4 million DDoS*** *attacks, increasing 11% over 1H 2020 figures. Additionally, data projections point to 2021 as another record-setting year on track to* ***surpass 11 million*** *global DDoS attacks.*

Many companies struggle with the constant evolution of attacks and required updates but using a managed DDoS service where all connections are continuously monitored for malicious traffic can help tremendously. With this in mind, there are still proactive and protective steps you can take to safeguard your network:

- **Create a plan** that ensures fast, comprehensive response to DDoS attacks, including:
  - » Specific support for volumetric/flood attacks.
  - » Visibility into current and past attacks to maintain compliance.
- **Work with your service provider** to design a customized detection and mitigation strategy that can:
  - » Notify you of network threats.
  - » Reroute and scrub traffic at the IP address level, so you can continue to operate.
  - » Gain 24/7/365 automatic protection, via smart algorithms, to redirect and mitigate malicious traffic.
- **Implement a system** to support staff and ease DDoS protection management via:
  - » Managed services that provide an always-available, single point of contact to security experts for swift issue resolution.
  - » Managed services that help you avoid hiring additional onsite security experts and buying new equipment.

SECURING THE EDGE: NEVER TRUST, ALWAYS VERIFY

The edge of the enterprise network is an increasing focal point of IT investments. This is where many organizations are aiming to bolster data storage in the cloud, processing, and analytics capabilities to generate business insights from data gathered from connected devices and systems.

The network edge is also becoming an increasing focus for cyberattacks. According to Jaikumar Vijayan, computer security and privacy writer for CSO magazine, "With more devices performing compute actions, and more devices with internet connectivity, attackers have a lot more targets with potentially more sensitive data and access to other systems, to go after. Issues like physical access and product security assume greater significance as well."

Below are best practices for better protection at the network edge:

- **Build a comprehensive strategy –** Edge security shouldn't be considered a "nice to have" but a critical aspect of any cyber security strategy. IT should also require all remote employees to use a VPN in order to access corporate resources to help mitigate security concerns.
- **Never trust, always verify (Zero Trust) –** Security at the edge must not only check each device every time it accesses the network, but also see if the device is trying to access areas of the network it doesn't normally utilize. This zero trust effort ensures that compromised devices don't gain access to a network to capture important data.

> *"With more devices performing compute actions, and more devices with internet connectivity, attackers have a lot more targets with potentially more sensitive data and access to other systems, to go after. Issues like physical access and product security assume greater significance as well."*
>
> **— Jaikumar Vijayan, computer security and privacy writer for CSO magazine**

WHY MANAGED SECURITY SERVICES?

Organizations must safeguard against online threats while protecting their network operations. But maintaining the proper security requirements to make this happen can strain internal IT teams. 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. This takes the guesswork out of network security and also free up your IT team to focus on other business-critical initiatives.

When it's time to evaluate a provider and its services, ask the following questions to help you find the best protection possible:

- How can you safeguard us against malware, phishing and other common cyberattacks?
- How do you identify and mitigate network threats? Can you scan our network for attacks and drain suspicious traffic?
- What protection do you provide against volumetric DDoS attacks?
- Do you have a means of letting us continue to work productively after a DDoS attack on the parts of the network that were not affected?
- Do you provide UTM? What protection does that provide?
- Can your firewall protect traffic between our various sites as well?
- Is a next-generation firewall part of what you offer? What protection does it provide?
- Do you have an integrated solution that includes firewall, UTM and internet service to simplify protection?
- Threats are evolving, and our network is always changing and growing. Can you support us and our investment as the environment and our needs change?
- How can you offload day-to-day administration work from our IT team during and after implementation?
- What types of teams and experts will we have access to for service?
- Are they available 24/7/365?

IN CONCLUSION

Studies show that global losses from cybercrime topped $1 trillion in 2020, and they are expected to skyrocket to more than $6 trillion in 2021. Being proactive has never been more critical. Security threats can derail an organization but adopting modern security measures can be easier than it looks.

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.

By working with an experienced and trusted service provider, you can ensure consistent protection with automated updates built into your network at every level. Managed services can reduce the complexity of network modernization, which is critical to improving reliability and security for your users and network .

Learn More

Spectrum ENTERPRISE

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.

©2022 Charter Communications. All rights reserved.
SE-MS-WP003