Q&A missing link

| Hardware | Cloud | **Cyber Security** | Software | Support | Disaster Recovery | Monitoring | Networks | Remote & Communication | Pricing |

Why do I need a new firewall, what's up with the one I have?

Firewalls are an essential component of network security as they help protect your computer or network from unauthorised access and potential threats. If you already have a firewall in place, it's important to evaluate its effectiveness and determine whether upgrading to a new firewall is necessary. Here are a few reasons why you might need a new firewall.

Outdated technology:
If your current firewall is outdated, it may not be equipped to handle the latest threats and security vulnerabilities. Hackers and malicious actors are constantly evolving their techniques, and newer firewalls often come with updated features and enhanced protection mechanisms.

Insufficient performance:
As your network grows and more devices are connected, your existing firewall may struggle to handle the increased traffic. This can lead to performance issues, such as slow internet speeds or network congestion. Upgrading to a more powerful firewall can help ensure that your network operates smoothly and efficiently.

Advanced threat detection:
Newer firewalls often incorporate advanced threat detection mechanisms, such as intrusion prevention systems (IPS), deep packet inspection (DPI), or behavior-based analysis. These features can identify and block sophisticated threats like malware, ransomware, or zero-day attacks more effectively than older firewall models.

Enhanced security features:
Modern firewalls may offer additional security features that can provide better protection for your network. For example, they might include application control, content filtering, virtual private network (VPN) support, or secure remote access capabilities. Assess your specific security requirements to determine if these features would be beneficial for your network.

Compliance requirements:
If you operate in an industry that has specific compliance regulations, such as healthcare (HIPAA) or finance (PCI DSS), you may need a firewall that meets those requirements. Upgrading to a new firewall that is compliant with the necessary regulations can help ensure that you adhere to the industry standards.

Conclusion

It's important to note that while firewalls are a crucial part of network security, they are just one component. A comprehensive security strategy may also involve other measures like antivirus software, regular security updates, user education, and network monitoring. Assessing your network's specific needs and consulting with a Missing Link specialist can help you determine whether a new firewall is necessary and which features would best suit your requirements.

Missing Link Q&A Information Sheet
Subject: Hardware
Topic: The Evolving Role of Servers: Do I Still Need One?

Date: August 2023
Version: 1