CHECKLIST

MANAGED NETWORK SECURITY

7 must-have security tools for IT leaders

1 Distributed Denial-of-Service (DDoS) mitigation

DDoS attacks account for 40% of security incidents,[1] so look for a DDoS managed service that continuously monitors your network, offloads the burden of the attack on a separate infrastructure and automatically begins mitigation at the first signs of trouble.

2 Firewall

Firewall maintenance is even more important than installation. Keep up to date with patches, updates and automatic threat identification intelligence to ensure it's protecting your company for both incoming and outgoing Internet traffic.

3 Web and application filters

These important filters identify and restrict content that users access on the Internet based on customizable rules and categories via a Unified Threat Management (UTM) system (also referred to as a UTM Firewall). This capability is essential for preventing users from accessing potentially liable websites.

4 Compliance

If your enterprise is subject to PCI, GDPR, HIPAA or any similar regulation, your network and/or security provider may be able to help. Businesses that process cardholder data can partner with a service provider that meets the standards for network-level compliance in alignment with the PCI DSS Version 3.2 Compliance, and then leverage that provider's Attestation of Compliance (AOC) to help meet its PCI merchant requirements for securing payment card data during transport.

5 Password protection and authentication

Complex passphrases rather than passwords provide more protection for your users and networks, as does two-factor or multi-factored authentication. Encourage your users to leverage the "something you know, something you have and something you are" method to further secure their identity and access management. This is especially important if you use remote access Virtual Private Network (VPN) technologies.

6 Security Information and Event Management (SIEM)

Guarding your network against malicious attacks is a full-time job. A SIEM solution that is correctly installed and configured on your networks and servers can provide much-needed, rapid detection and remediation of threats and potential risks. This self-learning tool automates the real-time collection and analysis of security events logged by firewalls, network hardware and servers.

7 Secure Access Service Edge (SASE)

With the rise in remote working, it's becoming increasingly difficult for traditional security solutions to provide protection anywhere, anytime, via any device. Built on a solid foundation of SD-WAN technology, SASE dynamically extends the edge of a private network right up to multiple clouds that are hosting Software as a Service (SaaS) applications and other business services like Microsoft 365 and Salesforce. In doing so, SASE transforms network edges into virtual private on-ramps to the cloud, delivering the most flexible and reliable security against cyber threats.

For a thorough review of your current security strengths and vulnerabilities, reach out to Windstream Enterprise to get help evaluating your environment and to learn how to protect your business with Managed Network Security.

1. Verizon 2020 Data Breach Investigations Report Securelist by Kaspersky, DDoS Attacks in Q4 2020

About Windstream Enterprise

Windstream Enterprise collaborates with businesses across the U.S. to drive digital transformation by delivering solutions that solve today's most complex networking and communication challenges.

To learn more about network solutions, visit windstreamenterprise.com

WINDSTREAM ENTERPRISE

CONNECT. TRANSFORM. ELEVATE.