FACT SHEET

SD-WAN

Windstream Enterprise SD-WAN HIPAA Safeguards

Windstream Enterprise SD-WAN is an overlay network, which meets the conduit exception to the HIPAA Final Omnibus Rule, same with any Windstream Enterprise network and connectivity solution. SD-WAN is a means of transport of data and does not store, nor have access to, the ePHI data. The only information that's stored within SD-WAN is the network configuration and monitoring that lists the type of traffic flows. Below you will find a detailed description of the HIPAA safeguards that we apply to our next-generation SD-WAN solution.

Windstream Enterprise SD-WAN HIPAA Safeguards

The Windstream Enterprise SD-WAN solution is encrypted via IPSec from the customer premises until it reaches the Windstream Enterprise private core. Furthermore, we provision our SD-WAN solution with virtual separation between each customer's instance, and we can virtually separate various types of traffic, as required.

Finally, Windstream Enterprise's SD-WAN uses geo-diverse gateways that are scattered throughout the Windstream Enterprise footprint, in order to provide diversity and resiliency. The access to those physical areas is limited to Windstream Enterprise support staff. That access is logged and tracked.

For more information, enclosed is a checklist that summarizes how Windstream Enterprise's SD-WAN solution addresses different security criteria.

SD-WAN Security Checklist

CRITERIA	YES	NO	COMMENTS
Does the product modify and/or access electronic Protected Health Information (ePHI)?		x	
Is the product software-based?	+		
Is the product website-based?	+		It is managed via a web portal.
Is the product hardware-based?	+		
If yes, can the hardware be locked in place?	+		Equipment should be secured in telco rack or telco closet.
Does the hardware have protections against tampering?		x	
Does the product use cloud-based technology?	+		
Does our organization have the following:			
Business Continuity Plan?	+		
Disaster Recovery Plan?	+		
Security Incident Response Plan?	+		
Data Destruction Policy?	+		
Data Retention Policy?	+		Only SD-WAN configuration and monitoring data — 12 months.
Access Control Policy?	+		
Does our organization own the data used by the product?		x	The application data is owned by our end customer.
Does our end customer own the data used by the product?	+		
Is the product at a minimum FIPS 140-2 certified?		x	VeloCloud, as the underlying SD-WAN vendor is still seeking this certification.
Are redundancies in place to prevent possible downtime?	+		The product allows for access, gateway and orchestrator redundancy.
Does the product use unique IDs?	+		
Does the product use passwords?		x	It uses RSA token keys.
If Yes, do passwords require the following: - At least 8 characters? - Uppercase? - Numbers? - Symbols?			RSA token keys do not use passwords, but 2-factor authentication that randomly generates keys that refresh every 30 seconds.
Does the product have auto-login capabilities?		x	
Does the product have auto-logoff capabilities?	+		
Does the product have timeout capabilities?	+		
Does the product use two-factor authentication?	+		
Are there administrative capabilities?	+		
Does the product have Access Controls for our end customer to utilize?	+		
Are there audit reports that the end customer can review for HIPAA and/or other security procedures?	+		
Is the data at rest encrypted? If Yes, please indicate the encryption standard you are using.			No data at rest within provider equipment. This solution does not handle resting data/storage.
Does anyone other than Windstream Enterprise and the end customer have access to the stored data?		x	Windstream Enterprise SD-WAN solution is an encrypted solution over public or private underlay.
Where is the data physically stored?			N/A – We do not store ePHI data.
Is the data stored by a Third Party? If Yes, please indicate the Third Party.			This solution does not handle resting data/storage.
Is the data in motion encrypted? If Yes, please indicate the encryption standard being used. If No, please indicate how the data is being protected.	+		All data in motion is encrypted via IPSec and then onboarded onto Windstream Enterprise's private core for transport. AES-256 and SHA-256 are used to encrypt the data in transport.
Is there any latency/lag with the transmission of data?	+		All latency is within parameters required for real-time communications.

WINDSTREAM
ENTERPRISE