DATA SHEET

StreamPlus: on-premises data lake for network metadata

Overview

Organizations around the globe continue to defend against breaches while ensuring data privacy. While many have turned to cloud offerings to store data, it may not be possible due to lack of offerings or compliance requirements, and can be cost prohibitive.

For organizations looking to store network data locally, Vectra's StreamPlus provides on-premises data lake to collect, store, and search important network metadata. This drastically reduces the cost of storing full network packets that will never be used, while providing salient information that will be needed for investigations and risk mitigation in the future.

Delivered in open-source Zeek format, you get an on-premises data lake without the management overhead, cost burden, or scale limitations that accompany open-source Zeek.

KEY BENEFITS

1. Meet privacy and compliance requirements mandated by government and corporate regulations
2. Expose gaps in your security posture with proactive investigation and threat hunting
3. Reduce costs by storing curated network metadata instead of full packets

An on-premises data lake for privacy, compliance, and security without the headache

Vectra is the global leader in AI-driven network detection and response. Vectra is revolutionizing network security with the Cognito® platform that replaces legacy technology which fails to solve today's detection and response challenges across zero trust networks including data center, enterprise networks, IoT devices, as well as public and private cloud environments.

With StreamPlus, security teams are provided rich network metadata necessary to perform detailed threat hunting, investigation, response, and ensure policy compliance. Delivered in open-source Zeek format, you get an on-premises data lake without the management overhead, cost burden, or scale limitations that accompany open-source Zeek.

Software sensors send network metadata to Vectra Cognito where it deduplicates and runs host identification and enrichment using machine learning algorithms. StreamPlus normalizes the metadata into Zeek-format and it is presented in a series of standard and customizable dashboard where it is fully searchable.

The metadata from Cognito Stream is enriched with host identity, enabling investigations based on device names rather than just IP addresses. This eliminates the need to search DHCP logs in parallel to find the device using an IP address at specific times, and to track the changes in the device's IP address for the period of time relevant to an investigation.

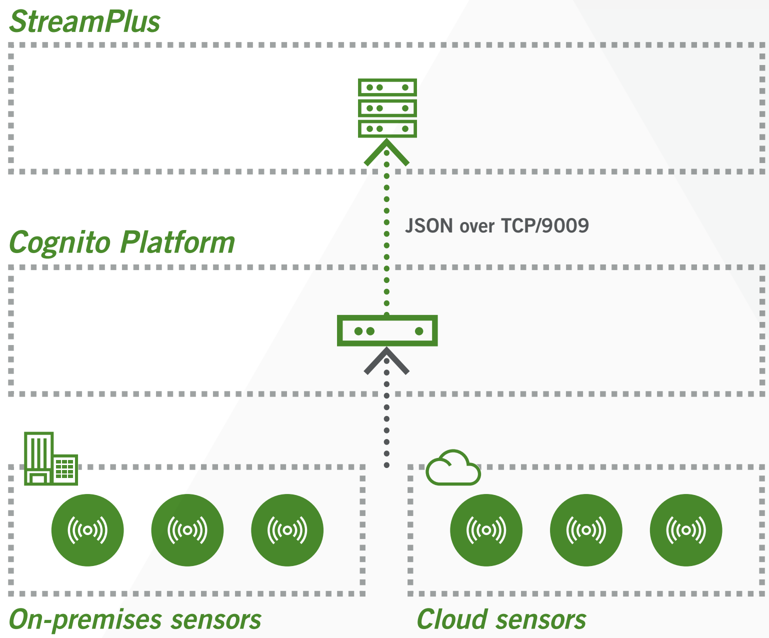
Searching by device name saves time when speed is crucial. Security insights embedded in the metadata provide threat hunters with intelligence for investigations and proactive threat hunting efforts.

How it works:

StreamPlus: This is the data lake built on your choice of hardware, whether a virtual machine, or Vectra provided hardware. This component includes the dashboards, and exports the network metadata.

Cognito: All deployed sensors are connected to the Vectra Cognito platform. This is the user interface, and where all configuration takes place.

Sensors: Physical, Virtual or Cloud-based sensors collect network traffic at strategic location across the infrastructure using passive (SPAN or TAP/vTAP) technology.



Specifications

StreamPlus Server Hardware Specifications	
CPU	AMD 48 CPU Cores @2.3 Ghz
Memory	128 Gb
Storage	1x 480Gb Solid State (SSD) 6x 1.92Tb Solid State (SSD) (RAID 10)
Network Interface	Intel X710 Dual Port 10GbE SFP+ OCP NIC 3.0 with SR Optic 10GbE 850nm
Operating System	X64 Ubuntu 20.04
Physical Dimensions	
Rack Units	1U Rack Units
Height	44.45mm (1.75”)
Width	434.0mm (17.1”)
Depth	736.54mm (29”)
Weight	21.8kg (48.1lbs)
Input Power @ 100% CPU	528 Watts; 1802.6 BTU/h
PSU Capacity	1400 Watts; 4777 BTU/h
Airflow	35.5 CFM; 16.8 l/s

For more information please contact a service representative at info@vectra.ai.

Email info@vectra.ai vectra.ai

Version: **020921**