Vectra AI Premium Support Proactive System Health Monitoring and Remediation Service

Premium service offering delivers 24/7/365 health monitoring for Vectra AI solutions.

For Vectra AI customers with Premium Support, the Proactive System Health Monitoring and Remediation Service ensures that the health of their solution is monitored 24/7/365. Should an issue arise, the support team will immediately investigate and work to remediate it accordingly. Customers have the option to choose if they prefer the issue to be proactively and remotely resolved by the Vectra AI support team (when applicable) or if they want to be contacted before any changes are made.

Key Benefits

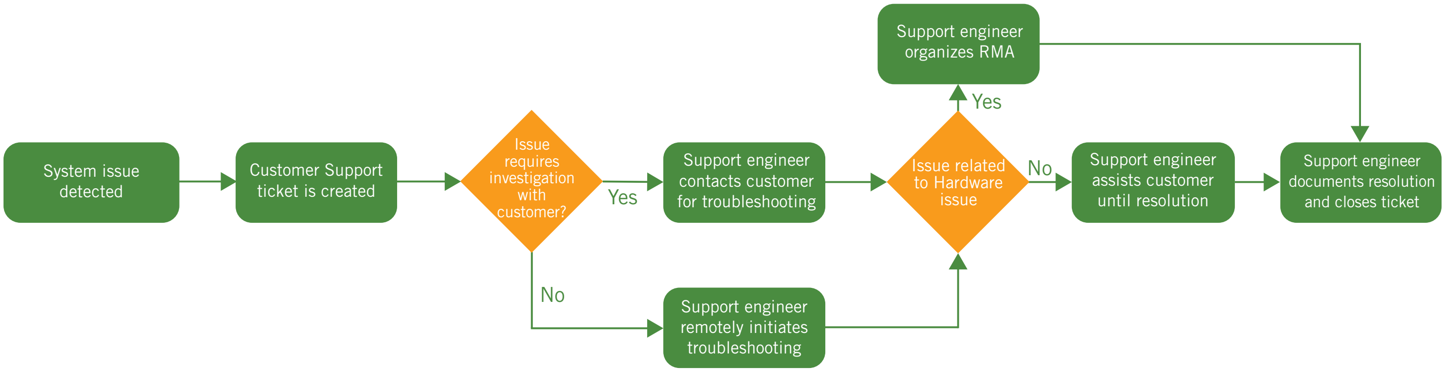
- 24/7/365 solution monitoring
- Immediately investigate platform issues
- Fast remediation turnaround
- Flexible resolution options
- Augments your IT OPS team

Value

Regardless of if or when attackers decide to target an organization, the Vectra AI Premium Support Proactive Monitoring and Remediation Service allows customers to ensure their Vectra AI Platform is fully functional and ready to keep pace with the speed and scale of today's sophisticated attacks.

How it works

The Vectra AI support team follows the following process when a system issue is found:


System issue detected
Customer Support ticket is created
Issue requires investigation with customer?
Yes
No
Support engineer contacts customer for troubleshooting
Support engineer remotely initiates troubleshooting
Issue related to Hardware issue
Yes
Support engineer organizes RMA
No
Support engineer assists customer until resolution
Support engineer documents resolution and closes ticket

1. As the issue is detected, a support ticket is automatically created, and a support engineer is assigned to investigate it.
2. Depending on support remote access being enabled, a support engineer will initiate investigation and troubleshoot independently or with the customer.
3. If the issue is hardware related, a support engineer will initiate a replacement as necessary.
4. If the issue is software or network related, a support engineer will work on investigating and remediating it as diligently as possible.
5. Throughout the steps, a support engineer will document in the ticket any actions taken.
6. Once the issue has been fully resolved, the support engineer will document the resolution in the ticket and close it.

Key Requirements

Service Requirements

Active service requires that customers allow a cloud connection between their on-premises solution and Vectra AI. Additionally, if customers choose to allow proactive remote remediation, remote support access will need to be enabled.

Required connectivity for system checks monitoring:

- Source: Brain
- Destination: api.vectranetworks.com (54.200.5.9)
- Port: TCP/443 (HTTPS)
- Source: Brain
- Destination: update2.vectranetworks.com (54.200.156.238)
- Port: TCP/443 (HTTPS)

Requirements for remote support access:

- Source: Brain
- Destination: rs.vectranetworks.com (74.201.86.229)
- Port: TCP/443 or UDP/9970

Please note that following IP ranges will conflict with remote support capability: 192.168.72.0/21 and 192.168.80.0/21

The full list of product connectivity requirements can be found here:

https://support.vectra.ai/s/article/KB-VS-1011

https://support.vectra.ai/s/article/KB-VS-1045

What's covered?

Vectra Network Detection and Response, Vectra Respond UX, Vectra Recall and Vectra Stream provide system checks on services running to the Vectra AI cloud.

The system checks below are reported to support when an issue is detected:

- Hardware alerts:
  - Brain/Sensor faulty hardware
  - Brain/Sensor hardware down/not communicating.
- Software alerts:
  - Critical services down
  - Database issues
  - Recall/Stream data ingestion issue
  - Remote support tunnel down

System checks receive ongoing updates as new products and updates are added.

Your Vectra AI Platform is Ready to go 24/7/365

Whether to ensure your platform is running at peak performance or to augment your IT team with 24/7/365 monitoring, Vectra AI Premium Support will make sure your organization remains resilient against today's most sophisticated attacks.

About Vectra AI

Vectra® is the leader in hybrid cloud threat detection and response. Vectra AI's patented Attack Signal Intelligence detects and prioritizes threats across public cloud, SaaS, identity, and networks in a single platform. Vectra's Attack Signal Intelligence goes beyond simple anomaly detection to analyze and understand attacker behavior. The resulting high-fidelity signal and deep context enables security operations teams to prioritize, investigate and respond to cyber-attacks in progress sooner and faster. Organizations worldwide rely on the Vectra platform and MDR services to stay ahead of modern cyber-attacks. Visit www.vectra.ai.

For more information please contact us:
Email: info@vectra.ai | vectra.ai

Version: **101923**