CybrHawk Network Solution

NETWORK

Managed Network Detection and Response for your datacentre, virtual, WAN, and branch networks

24x7 Inspection

Ongoing, real-time monitoring and detection via advanced analytics and machine learning

Detect the Most Elusive Threats

Advanced detection capabilities and rich threat intelligence leave no opportunities for attackers

Threat Hunt Like a Pro

Get data from all sources in a single view, and follow attackers as they move laterally, visualising the entire extent of the attack

Consolidated Response

When a threat is detected, we activate our investigation and response capabilities across all parts of the environment, would it be network, endpoint, or cloud

CybrHawk Network Solution is a real-time managed network detection and response solution which can be deployed to monitor inline network traffic on-premises or in-cloud, inspecting both horizontal and vertical traffic flows in physical and virtual networks.

CybrHawk Network Solution brings automated and integrated threat intelligence and expert human security-analyst threat hunting to your network to provide superior threat detection and response capabilities, leaving no threat undetected.

CybrHawk Network Solution detects even the most concealed activities and utilises our machine learning technologies to identify unknown threats, lateral movement, and malicious insider behaviour.

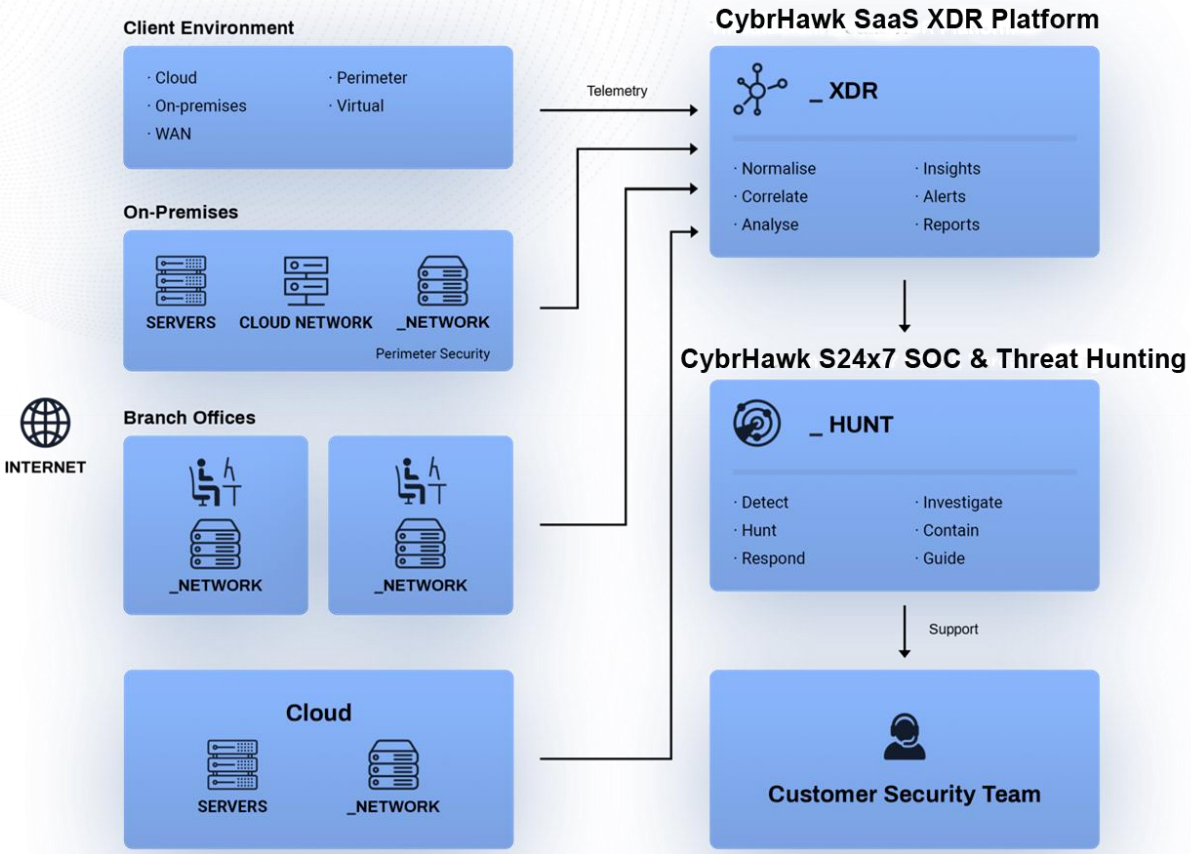
The collected data is transitioned to our XDR platform and correlated with other information collected from endpoints, applications, system logs, and public cloud instances. Within our rich threat intelligence ecosystem, threat indicators are transformed into the full attack kill chain and all attack stages as seen in various parts of the environment are identified.

CybrHawk Network Solution brings full forensic investigation capability into your environment and supports full packet capture for advanced investigation and evidence collection.

HOW IT WORKS

CybrHawk Network Solution integrated out-of-band into your network segments and inspects both inbound and outbound traffic in your environment in real time. The sensor appliances can tap into your branch offices, WAN segments, and cloud networks.

All data is integrated into our XDR platform where threats are detected and blocked on the network perimeter and within the network in real time.



- Lateral movement
- Command & Control traffic
- Backdoors and tunnels
- Malware and botnet connections
- Internal port scanning and reconnaissance
- Password brute forcing
- Insider threats
- Impersonation and spoofing attacks
- Exploitation attempts
- Unauthorised remote access tools
- Rogue devices

Immediate visibility. Detect the most elusive attackers. Threat hunt like a pro.

Deep Network Visibility

Forensic Captures
Detailed recording of network metadata and full packet-level communications for investigations and forensic evidence gathering

User Behaviour
CybrHawk Network Solution analyses user and machine behaviour and provides insights based on detected deviations and anomalies

Network Baseline
Get full visibility into your network and see who is talking to what to create a complete baseline for all internal and external connections

Threat Detection and Response

24x7 Detection and Response
Automated and human-powered detection, threat hunting, and immediate threat response

Threat Intelligence
Detection is supported by our threat intelligence data, distributed to all CybrHawk Network Solution sensors in real time

Automated Response
The detected threats can be immediately disrupted, at the network perimeter level or as a tactical within-the-network containment measure

Ongoing Assurance

Security Policy Assurance
Ongoing assurance of your security posture with continuous network inspection and detection, identifying policy violations such as the use of unencrypted services, plain-text passwords, and shadow IT assets

Risk Identification
All collected data is translated into an organisation-level risk report, with a detailed security scorecard for all components of your environment

Real-Time Visualisations
Access real-time reporting and visualisations in your Customer Portal instance, constructing the whole enterprise scorecard in one click

FULL ENTERPRISE ATTACK SURFACE COVERAGE

Our XDR platform provides full enterprise coverage, integrating all the security data you can possibly reach into, including data that directly resides within your network and on your endpoints, as well as the external data such as cloud workloads, SaaS applications, Dark Web breaches, compromised credentials, external vulnerabilities, and weaknesses and exposures related to third-party organisations in your supply chain.

_ENDPOINT — Advanced endpoint visibility, forensic analysis of endpoint telemetry, detection and response

_NETWORK — Detect insider threat and lateral movement with network-based intrusion detection and packet analysis

_CLOUD — Multi-cloud security insights, cloud workload vulnerability management, and continuous risk assessment

_OSINT — Continuously integrated Open Source Intelligence, including indicators from Dark Web, social media, and third-party vulnerabilities

_ANYTHING — Any standard or custom application or log source, completely integrated into the platform

ABOUT CYBRHAWK

CybrHawk provides innovative MDR, SOC-as-a-Service, and proactive cyber defence solutions to MSPs and Enterprises. Our Adaptive XDR Platform was created to help companies of any size to deploy a world-class detection and response, embracing all information that businesses can reach to, would it be within their network, on the Dark Web, or hiding deep into their supply chain. We believe in open ecosystems and connect you to any and all threat intelligence feeds and log sources, instantaneously providing you with actionable security insights. For more information, visit www.cybrhawk.com.