CybrHawk
Transforming Cybersecurity

CybrHawk Cloud SaaS

Managed Detection and Response Solution

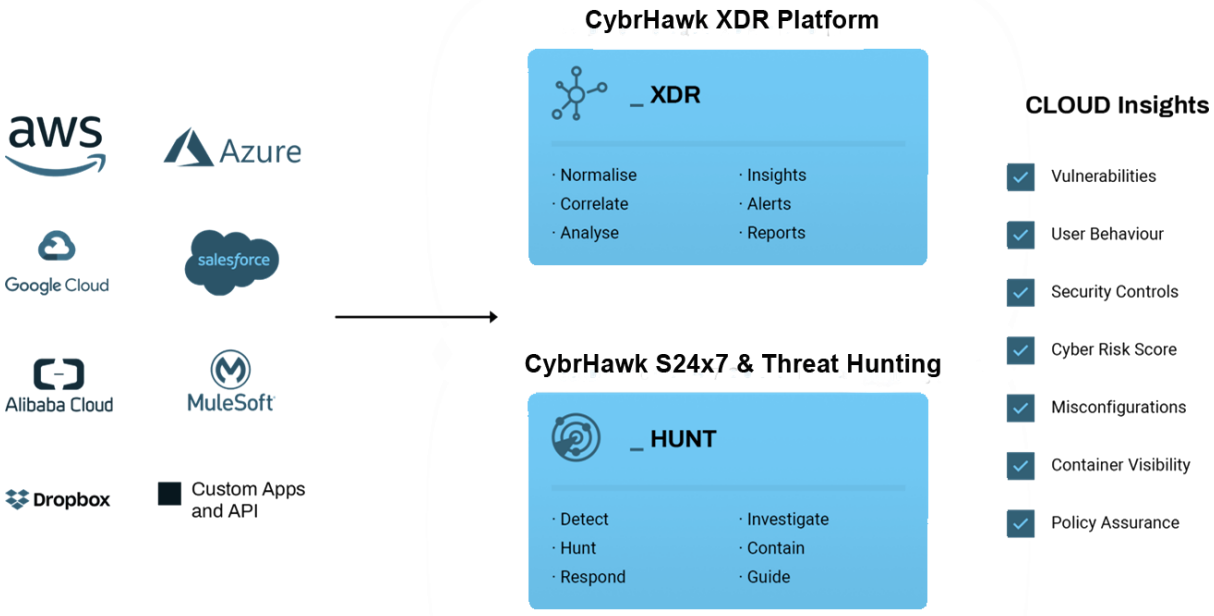
SOLUTION BRIEF

CLOUD

Managed Detection and Response for your cloud applications and infrastructure

CybrHawk Cloud Solution is a comprehensive cloud security suite, providing deep cloud visibility, security baseline and configuration management, ongoing vulnerability management, and advanced detection and response in a multi-cloud environment.

Our CybrHawk Cloud Solution solution provides ongoing assurance and delivers valuable security insights empowered by our XDR platform and our Managed Detection and Response capability. The insights communicate the risks to your business and provide ongoing assurance of the overall cyber resilience of your cloud footprint.



Cloud security risks are on the rise

Cloud security issues have always been a concern for organisations, but with billions of people now working from home due to the COVID-19 pandemic, bad actors have found ways to create even more worry. With so much work being done remotely via enterprise collaboration

tools like Microsoft Teams, Zoom, and Skype, hackers are infiltrating those legitimate services and tools to launch cyberattacks.

Highlight the quote:

"We must look beyond basic protection decisions and improve organisational resilience through innovative approaches to detection and response, and ultimately, recovery from security incidents."

Gartner Security & Risk Management Summit, 2020

Among those services under siege, Microsoft has become one of the most targeted. Indeed, according to Check Point, the brand featured in nearly a fifth of all brand phishing attacks in the third quarter of 2020. In particular, Office 365 user account takeovers are on the rise. In a user account takeover, hackers attempt to steal login credentials to access and launch attacks from within an organisation.

Some examples of recent activity include phishing campaigns targeting Office 365 users. In these attacks, malicious actors attempt to steal login credentials by claiming to notify users of a "missed chat" from Microsoft Teams or by other similar methods. With that information in hand, bad actors can pilfer sensitive data and launch ransomware and phishing attacks across corporate networks. Another approach uses OAuth2 and other token-based authorisation methods to access Office 365 accounts. With this attack, the hackers gain read-only permissions to pry into Office 365 accounts, including profiles, emails, and contacts, which they can use to steal data or intercept password reset messages from other accounts, like online banking.

With this type of nefarious activity on the rise and the ongoing necessity for employees to work-from-home, it's even more critical to implement a security solution that provides full cycle detection, investigation, and response for your infrastructure and all your cloud applications.

Understand risks. Eliminate threats. Get unprecedented visibility.

Deep Visibility

Integrate your cloud workloads into your security operations, achieving the same level of visibility across the on-premises and in-cloud

Containment Without Boundaries

Contain threats regardless of where your data and applications reside, minimising lateral movement and threat propagation

Ongoing Assurance

Get continuous visibility into your cloud vulnerabilities, security configurations, and policies, providing ongoing assurance to the business

Business Friendly Security

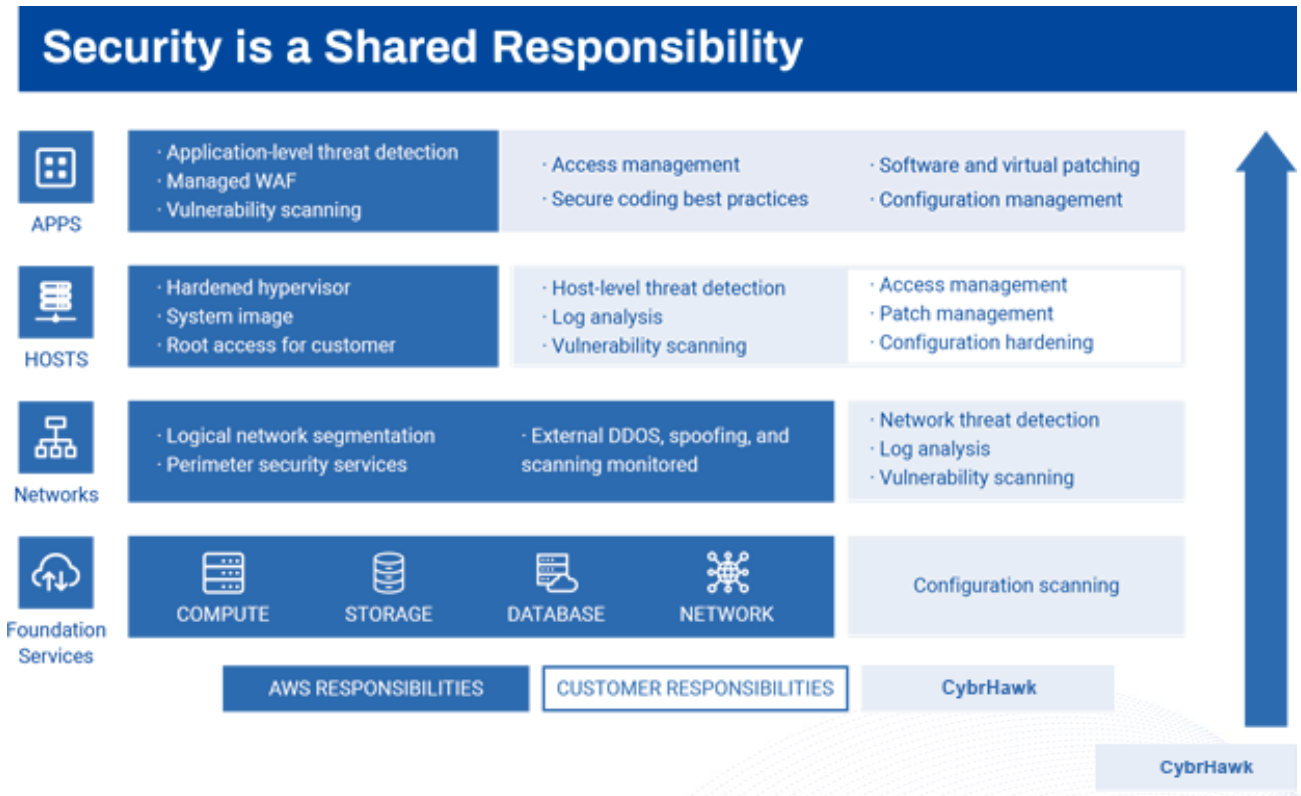
Understand the actual risks as applied to your specific environment, without the need to filter through numerous alerts and detections

Threat Hunting

Award-winning threat hunting capabilities, integration of all data from cloud, network, endpoint, and other systems in the same cyber kill chain

Extend your shared-responsibility model to include comprehensive detection and response

All public cloud providers practice some kind of a shared-responsibility model, providing basic infrastructure protection, while expecting their tenants to look after the security of their workloads. With CybrHawk, you can easily extend this model and add us into the mix, providing full cybersecurity coverage across your cloud infrastructure from day one.



Deep Cloud Visibility

Cloud Infrastructure
Visibility and detection across your Office365, Azure, AWS, and other public cloud providers

Cloud Applications and Containers
End-to-end visibility of containers, cloud services, and DevOps tools

SaaS Integrations
Integration with numerous cloud services such as ServiceNow, Salesforce, Office365, G-Suite, Okta, Mulesoft, Duo, and many others

Cloud Assets and Configuration Baselines
Rich visibility into cloud inventory and configured assets, providing end-to-end visibility and identifying shadow IT

User Behaviour
Monitor all users' activities across endpoints and cloud systems, and detect anomalies

Vulnerabilities and Misconfigurations
Identify in real time vulnerabilities and security weaknesses and misconfigurations across workloads, applications, databases, and containers using standard benchmarks like CIS

Threat Detection and Response

Automated Detection
Hundreds of detection use cases, rich correlation, and threat identification

Machine Learning
Integrated machine learning to detect threat from unexpected user behaviour, not-seen-before objects, and other anomalies

Rapid Response
Rapid root-cause analysis using the data from all sources, real-time response across the whole infrastructure footprint

Threat Hunting

Human Threat Hunters
Ongoing hunting by best-in-the-industry analysts and consultants to identify unknown threats

Threat Intelligence
Know who you are dealing with, with our quick attribution to a known threat actor, identification of methods and techniques, level advice on what to expect

MITRE ATT&ACK
Integrated mapping of adversary activities into ATT&CK techniques and behaviours

Ongoing Assurance

Security Policy Assurance
Ongoing assurance of your cloud security with continuous vulnerability management, security configuration inspection, configuration benchmarks, and real-time inventory

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

Compliance Reporting
Meet your compliance requirements with out-of-the-box comprehensive reports meeting regulatory compliance requirements of PCI DSS, HIPAA, GDPR, ISO27001, and other standards

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

Cloud Advisory
Get ongoing access to our expert cloud advisory team for an expert's advice on your cloud security maturity, security policies, and cyber resiliency capabilities

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.