Central Networks & Technologies Ltd.
Bryon House, Green Lane
Heywood
OL1 02DY

Central Networks & Technologies Ltd - Huntress

Crown Commercial Service

Prepared by: Vicki Coleman
Date: 15/01/2026

info@centralnetworks.co.uk
+44 (0)1706 747474
www.centralnetworks.co.uk

Contents

Central Networks and Technologies Ltd (Central)

Founded in September 1991 by Christopher Mycock. In the earlier years Central was responsible for running the core ICT systems for many of the UK Magistrates Courts Services, which involved moving and hosting the mainframes and employing staff via TUPE. We also have a focus in the Housing Association and not-for-profit sector. In the last 10 years we have migrated many of our customers to cloud or partial cloud provision.

Our customer base is diverse in terms of size, geography, skills, business requirements and objectives. We have recognised this and created a solutions and services portfolio that can be tailored to meet the individual requirements of all our customers. Some of our customers have large ICT teams and only look for assistance where they have investigated and exhausted every avenue. Others are far smaller, where finance officers often take on ICT responsibility and need additional help and assistance. Central provides a bespoke service to each of our customers, providing best value for money and an ICT service which matches their requirements which assists them in delivering their objectives.

Huntress Managed Detection & Response – Service Description

Huntress is a fully managed 24/7 threat-hunting and response platform that provides continuous protection across endpoints and Microsoft 365 identities. Built for real-world attacks rather than theoretical risks, the service combines lightweight endpoint telemetry with human-led SOC analysis to identify, investigate, and remediate malicious activity that traditional security tools often miss. The platform is operated by a global Huntress Security Operations Centre, giving organisations round-the-clock coverage without the cost or complexity of running an internal SOC.

1. Endpoint Detection & Response (EDR)

Huntress continuously monitors all protected endpoints by collecting telemetry through the Huntress Agent, including process behaviour, autorun entries and Microsoft Defender signals. This enables the SOC to detect:

- Persistent footholds
- Privilege escalation attempts
- Malicious scripts and tools
- Ransomware precursors and execution attempts

When suspicious activity is detected, Huntress analysts manually investigate signals to determine whether the behaviour indicates an active threat. Confirmed incidents generate actionable Incident Reports with clear remediation steps, or automated response actions where appropriate.

2. Ransomware Canary Early Warning System

Huntress deploys "Ransomware Canaries" across endpoints — monitored decoy files designed to trigger an immediate alert upon modification. This enables early detection of ransomware activity before widespread encryption occurs. The SOC confirms findings and escalates incidents rapidly for isolation and remediation.

3. Managed Antivirus (Microsoft Defender)

Huntress integrates directly with Microsoft Defender to centralise and enhance antivirus visibility. Defender detections are ingested as additional threat telemetry, allowing Huntress analysts to correlate behavioural and AV findings and identify adversary techniques such as LOLBins or attacker tool deployment.

4. Managed Identity Threat Detection & Response (ITDR)

Huntress ITDR monitors Microsoft 365 tenants to identify suspicious authentication patterns, impossible travel, MFA bypass attempts, malicious inbox rules and risky session activity.
The SOC investigates and validates identity threats such as:

- Compromised accounts
- Unauthorised access from foreign locations (e.g., Spain escalation noted in reports)
- Malicious OAuth applications

Critical identity incidents support automated containment actions, including account disablement for hybrid identities.

5. SOC-Driven Incident Response

Every meaningful alert is reviewed by Huntress SOC analysts before escalation, drastically reducing noise and false positives. Monthly customer reports show:

- Events analysed
- Signals detected
- Signals manually investigated
- Confirmed incidents

Incident reports contain root-cause context, attacker behaviour, affected hosts, and step-by-step remediation guidance. For critical identity incidents, partners may request a direct callback from SOC support.

6. Automated & Assisted Remediation

Huntress can automatically remediate low-severity threats such as unwanted software or benign footholds, reducing operational overhead while keeping engineers focused on high-value tasks.

High-severity incidents include mandatory host isolation unless exceptions are configured, ensuring containment during active compromise.

7. Reporting & Visibility

Huntress provides clear, consistent reporting, including:

- Monthly threat reports summarising SOC activity
- Breakdown of signals, investigations and incidents
- Ransomware canary status and foothold analysis
- Agent health and unresponsive endpoints

Reports are branded and can be supplied per tenant through Central's service desk processes.

8. MSP Integration and Automation

For Central Networks, Huntress integrates into HaloPSA to automatically raise tickets for escalations and SOC-confirmed incidents. This ensures seamless operational handling and rapid response workflows.

Notification categories (Incident, Escalation, Platform Action, Account Notice) can be routed to dedicated mailboxes or automated processes.

Service Outcome

The Huntress service provides organisations with:

- Continuous monitoring of endpoints and identities
- Early detection of sophisticated attack techniques
- Human-validated threat analysis

- Clear, actionable remediation guidance
- Automatic containment and automated threat removal
- Monthly threat intelligence and SOC activity reporting
- Seamless integration into Central's support processes

This results in a high-confidence, low-noise MDR service that strengthens security posture without adding operational burden.

Confidentiality and Copyright

This document and the information set out herein is confidential and is not to be disclosed or discussed with any person or party not associated with the selection of a service provider. The information in this proposal is a suggested technical offering. We reserve the right to amend or withdraw our proposal. Any typographical, clerical or other error or omission shall be subject to correction without any liability. The copyright in this proposal and any associated information or documents that we may provide remains vested in Central Networks and Technologies Ltd.