G-Cloud 15 Service Definition

Huntress - Managed Threat Detection and Response

HTG
SECURE CLOUD EXPERTS

Service Name	Huntress Managed Threat Detection and Response
Service Type	Software as a Service (SaaS)
Supplier	Howell Technology Group Limited
Framework	G-Cloud 15

Service Summary

Huntress Managed Threat Detection and Response provides 24/7 managed security operations combining automated threat detection with human-led security analysis to identify and remediate advanced threats that bypass traditional antivirus solutions. The service specialises in persistent footholds detection, ransomware monitoring, and proactive threat hunting, providing organisations with enterprise-grade security operations centre (SOC) capabilities without the complexity and cost of building internal security teams.

Service Description

Traditional antivirus and endpoint detection and response (EDR) solutions focus primarily on preventing initial compromise, yet sophisticated threat actors increasingly employ techniques specifically designed to evade these defences. Once attackers gain initial access, they establish persistent footholds, escalate privileges, and move laterally through environments, often remaining undetected for weeks or months whilst exfiltrating data or preparing ransomware deployment.

Huntress addresses this critical security gap by focusing on what happens after the initial compromise—detecting the persistent mechanisms, credentials abuse, and lateral movement that indicate an active breach. The platform combines automated detection technology with expert human threat hunters who investigate suspicious activities, eliminate false positives, and provide actionable remediation guidance.

The service operates as a managed security offering where Huntress's 24/7 Security Operations Centre monitors your environment continuously, investigates alerts, confirms genuine threats, and works with your IT team to remediate incidents. This model provides enterprise-grade security capabilities to organisations of all sizes, delivering the expertise of seasoned security professionals without requiring recruitment, training, or retention of specialised security staff.

Huntress agents deployed to Windows, macOS, and Linux endpoints continuously monitor for indicators of compromise including unauthorised scheduled tasks, registry modifications, suspicious PowerShell activity, unauthorised remote access tools, credential dumping attempts, and malicious service installations. When threats are detected, the Huntress SOC team investigates, confirms the threat, assesses impact, and provides step-by-step remediation instructions or, with customer approval, performs automated remediation.

The platform integrates with existing security tools including Microsoft Defender, CrowdStrike, SentinelOne, and traditional antivirus solutions, providing complementary detection capabilities that identify threats these tools miss. Huntress also monitors for vulnerabilities, misconfigurations, and security weaknesses that could be exploited by attackers.

Service Benefits

Advanced Threat Detection

- Identify persistent threats that bypass traditional antivirus
- Detect Living-off-the-Land (LotL) attacks using legitimate tools maliciously
- Identify ransomware precursor activities before encryption begins
- Detect credential theft and abuse before data exfiltration
- Early warning of active breaches enabling rapid response

24/7 Managed Security Operations

- Continuous monitoring by expert security analysts
- Human verification eliminates false positives requiring IT investigation
- Proactive threat hunting identifies dormant threats
- Incident response guidance from experienced SOC analysts
- Escalation to senior threat hunters for complex incidents

Rapid Incident Response

- Automated containment of confirmed threats
- Step-by-step remediation guidance from SOC analysts
- Remote remediation capabilities with customer approval
- Incident reports detailing threat activities and remediation steps
- Post-incident analysis and recommendations

Reduced Security Operations Burden

- Eliminate need to recruit and retain security specialists
- Reduce alert fatigue through human-verified threat notifications
- Free IT teams from security monitoring and triage
- Leverage external expertise for complex security incidents
- Predictable costs compared to building internal SOC

Compliance and Risk Management

- Demonstrate due diligence in threat detection
- Audit trail of security incidents and responses
- Meet cyber insurance requirements for monitoring
- Support Cyber Essentials Plus and ISO 27001 requirements
- Documented incident response capabilities for compliance audits

Cost-Effective Security

- Enterprise-grade security at SME-friendly pricing
- Eliminate costs of building internal SOC team
- Reduce breach costs through early detection
- Lower cyber insurance premiums through demonstrable security controls
- Predictable monthly subscription costs

Service Features

Persistent Threat Detection

- Unauthorised scheduled tasks and persistence mechanisms
- Registry key modifications indicating persistence
- Suspicious PowerShell scripts and fileless malware
- Unauthorised Windows services installations
- Malicious browser extensions and plugins
- Rootkit and bootkit detection
- Suspicious driver installations

Ransomware Protection

- Ransomware precursor activity detection
- Encryption behaviour monitoring
- Shadow copy deletion detection
- Volume Shadow Service (VSS) manipulation detection
- Suspicious file encryption patterns
- Known ransomware group IOC monitoring

Credential Protection

- Credential dumping detection (Mimikatz, ProcDump)
- LSASS memory access monitoring
- Kerberos ticket theft detection
- Pass-the-Hash attack detection
- Golden Ticket attack identification
- Credential stuffing and brute force detection

Network and Lateral Movement Detection

- Unauthorised remote access tools (TeamViewer, AnyDesk, etc.)
- RDP activity monitoring and alerting
- SMB lateral movement detection
- Suspicious network reconnaissance
- Port scanning and enumeration detection
- Command and control (C2) communication detection

Account Compromise Detection

- Suspicious authentication patterns
- Off-hours access from unusual locations
- Privilege escalation attempts
- Unauthorised administrative access
- Service account abuse
- Dormant account activation

Vulnerability and Exposure Management

- Critical vulnerability identification
- Missing security patches detection
- Security misconfiguration identification
- Exploitable software versions
- Unnecessary service exposure
- Weak authentication configurations

Managed Detection and Response

- 24/7/365 SOC monitoring by security experts
- Human investigation of all alerts before notification
- Threat confirmation and false positive elimination
- Severity assessment and impact analysis
- Actionable remediation guidance
- Automated remediation with customer approval

Threat Intelligence Integration

- Real-time threat intelligence feeds
- Indicators of Compromise (IOC) monitoring
- Threat actor Tactics, Techniques, and Procedures (TTPs)
- Zero-day vulnerability monitoring
- Ransomware group activity tracking

- Industry-specific threat intelligence

Reporting and Analytics

- Real-time security dashboard
- Incident reports with detailed analysis
- Trend analysis and threat landscape reports
- Vulnerability exposure reports
- Compliance reports for audits
- Executive summary reporting

Integration Capabilities

- Microsoft Defender integration
- RMM platform integration (ConnectWise, Datto, NinjaOne)
- SIEM integration via API and webhooks
- PSA ticketing integration
- Slack and Microsoft Teams notifications
- Email alerting and reporting

How the Service is Delivered

Initial Assessment and Planning

HTG conducts a comprehensive security assessment to understand your environment, existing security controls, threat landscape, and compliance requirements. This assessment informs deployment strategy, integration requirements, and ongoing monitoring priorities.

Agent Deployment

Huntress agents are lightweight software components deployed to endpoints requiring monitoring:

Windows Endpoints: Agent deployment via MSI installer, supports deployment through RMM tools, Microsoft Intune, Group Policy, or manual installation. Typical deployment completes within 1-2 days for organisations up to 500 endpoints.

macOS Endpoints: Agent deployment via PKG installer, supports deployment through MDM solutions or manual installation.

Linux Servers: Agent deployment via package managers (apt, yum, dnf), supports cloud-based and on-premises Linux systems.

Agents are configured with appropriate monitoring policies based on asset criticality, data sensitivity, and risk profile. High-value targets such as domain controllers, file servers, and workstations with access to sensitive data receive enhanced monitoring.

Integration Configuration

HTG configures Huntress integration with your existing security and management tools:

- Microsoft Defender integration for enhanced context
- RMM platform integration for automated remediation
- ITSM ticketing system integration for incident tracking
- Communication platform integration (Slack, Teams) for real-time notifications
- SIEM integration for centralised logging where applicable

Baseline Establishment

Following deployment, Huntress establishes behavioural baselines for your environment over 7-14 days, learning normal patterns of activity to improve detection accuracy and reduce false positives. The HTG security team reviews initial findings, validates configurations, and fine-tunes policies.

Ongoing Monitoring and Management

24/7 Monitoring: Huntress SOC continuously monitors your environment for threats, investigating alerts and confirming genuine security incidents before notification.

Threat Investigation: When suspicious activity is detected, Huntress security analysts investigate to determine legitimacy, assess severity, understand impact scope, and develop remediation plan.

Incident Notification: Confirmed threats are communicated to your IT team through your preferred notification channel with incident details, severity assessment, affected systems, and recommended actions.

Remediation Support: Huntress provides step-by-step remediation guidance, automated remediation scripts where appropriate, verification of remediation success, and post-incident recommendations.

HTG Oversight: HTG security engineers provide additional layer of oversight, reviewing high-severity incidents, coordinating complex remediation efforts, providing strategic security guidance, and conducting quarterly security reviews.

Service Management Options

Standard Monitoring: Huntress SOC performs threat detection and investigation with your IT team executing remediation based on provided guidance. HTG provides technical support and advisory services.

Enhanced Managed Response: HTG security engineers work alongside Huntress SOC to coordinate response, execute complex remediation activities, and provide strategic incident response guidance. Includes monthly security reviews and vulnerability assessments.

Full Security Operations: HTG assumes primary responsibility for security incident response, including remediation execution, security tool management, vulnerability management, security policy development, and executive security reporting.

Service Management

Service Desk and Support

- UK-based security team available during business hours (08:00-18:00 GMT)
- 24/7 emergency security incident support
- Email, telephone, and web portal support
- Ticket tracking through HTG's service management platform
- Direct access to Huntress SOC team for confirmed threats
- Dedicated security account manager

Incident Management

- Priority-based incident classification and response
- P1 (Critical - active breach): 15-minute response time, 24/7
- P2 (High - confirmed threat): 30-minute response time, 24/7
- P3 (Medium - suspicious activity): 2-hour response time, business hours
- P4 (Low - vulnerability notification): 1 business day response

- Proactive threat hunting activities daily

Escalation Procedures

- Automated escalation for high-severity threats
- Executive notification for critical incidents
- Senior threat hunter engagement for complex investigations
- Third-party forensics engagement if required
- Law enforcement coordination support for reportable incidents

Service Reporting

- Daily security dashboard updates
- Weekly threat summary reports
- Monthly security operations reports
- Quarterly strategic security reviews
- Annual threat landscape analysis
- Compliance reports for audits

Onboarding and Offboarding

Onboarding Process

Typical onboarding completes within 1-2 weeks:

1. **Security Assessment (Days 1-2):** Environment documentation, security maturity assessment, threat landscape analysis, compliance requirements

2. **Deployment Planning (Days 3-4):** Agent deployment strategy, integration requirements, monitoring policy design, notification preferences

3. **Agent Deployment (Days 5-7):** Phased agent rollout, integration configuration, baseline establishment, testing

4. **Training and Handover (Days 8-10):** IT team training, notification procedures, incident response processes, platform familiarisation, go-live

Offboarding Process

Should you choose to discontinue the service:

1. **Notice Period:** 30 days' notice required for service termination

2. **Final Security Review:** Comprehensive security posture assessment

3. **Knowledge Transfer:** Incident history and threat intelligence documentation

4. **Agent Removal:** Coordinated uninstallation of Huntress agents

5. **Data Export:** Complete export of security logs and incident reports

No penalties for service termination. Historical security data provided for your records.

Service Constraints and Dependencies

Prerequisites

- Windows 7 or later, Windows Server 2008 R2 or later
- macOS 10.12 Sierra or later
- Modern Linux distributions (Ubuntu, CentOS, Red Hat, Debian)
- Internet connectivity for agent communication

- Administrative credentials for agent deployment
- Endpoint protection exemptions for Huntress agent

Technical Constraints

- Agent requires outbound HTTPS connectivity (TCP 443)
- Minimum 100MB RAM per agent
- Minimum 500MB disk space per endpoint
- Administrative/root access required for deployment
- Some security tools may conflict without proper exclusions
- Virtual desktop infrastructure may require special configuration

Monitoring Limitations

- Linux agent provides limited functionality compared to Windows
- macOS ransomware canary functionality limited
- Network-based threats require network monitoring tools
- Cloud infrastructure monitoring requires cloud-specific agents
- Physical security events not monitored
- Application-layer attacks may require additional tools

Response Limitations

- Automated remediation requires customer approval
- Remote access dependent on existing RMM tools
- Some threats may require endpoint re-imaging
- Zero-day threats may not have immediate remediation
- Containment may require network segmentation capabilities
- Legacy systems may have limited remediation options

Supported Environments

- On-premises Windows domains
- Azure AD-joined endpoints
- Hybrid identity environments
- Cloud-hosted virtual machines
- Remote worker endpoints
- Unmanaged BYOD devices (with limitations)

Excluded from Monitoring

- Network appliances and IoT devices
- Mobile phones and tablets
- Industrial control systems (ICS/SCADA)
- Embedded systems
- Legacy operating systems (Windows XP, Server 2003)

Pricing Information

Licensing Model

Huntress is licensed on a per-endpoint, per-month basis. Pricing includes:

- 24/7 SOC monitoring by Huntress security analysts
- Unlimited threat investigations
- Automated and guided remediation
- Access to threat intelligence feeds
- Regular platform updates and new detection capabilities
- Standard technical support

HTG Managed Services

HTG's security oversight and management services are priced separately based on service level:

- Standard Monitoring: Basic oversight and technical support
- Enhanced Managed Response: Active incident response coordination
- Full Security Operations: Comprehensive security management

Professional services including deployment, training, and security assessments are quoted separately based on environment complexity.

Pricing Transparency

Detailed pricing is available through HTG's G-Cloud 15 pricing document. Pricing is based on:

- Number of monitored endpoints (Windows, macOS, Linux)
- HTG service level selected
- Implementation and professional services requirements
- Contract term and volume discounts

No Hidden Costs

- No additional fees for threat investigations
- No charges for remediation guidance
- No fees for technical support within service hours
- No incident response charges for standard incidents
- No termination or exit fees

Data Security and Protection

Data Location and Sovereignty

- Huntress platform hosted in Amazon AWS (US-East region)
- Telemetry data processed in United States
- No storage of business documents or email content
- Security logs retained for 365 days
- European data processing under review for future implementation

Data Collection and Processing

- Endpoint telemetry: process execution, file system changes, registry modifications, network connections
- Security logs: authentication events, security tool alerts, system events
- No collection of: business documents, email content, personal files, web browsing history (except malicious sites)
- Data encrypted in transit and at rest
- Access restricted to authorised SOC analysts only

Data Security Measures

- TLS 1.2 encryption for all data transmission
- AES-256 encryption at rest
- Multi-factor authentication for platform access
- Role-based access control for SOC analysts
- Comprehensive audit logging
- Regular security assessments and penetration testing

Compliance and Certifications

- SOC 2 Type II certified
- ISO 27001 aligned security practices
- GDPR compliant data processing
- UK Data Protection Act 2018 compliance
- HTG Cyber Essentials Plus certified
- Regular third-party security audits

Privacy Protection

- Data Processing Agreement provided
- Privacy policy clearly defines data use
- No sale or sharing of customer data
- GDPR rights honoured
- Right to erasure upon service termination
- Transparent data retention policies

Incident Data Handling

- Incident reports contain only security-relevant information
- Personal data minimised in reporting
- Sensitive findings communicated via secure channels
- Incident data access restricted by role
- Automatic redaction of credentials and PII where possible

Service Level Agreement (SLA)

Platform Availability

- 99.9% uptime guarantee for Huntress platform
- Measured monthly excluding planned maintenance
- Service credits available for SLA breaches
- Redundant infrastructure for high availability

Detection Performance

- Threat detection within 5 minutes of activity
- Human investigation initiated within 15 minutes for critical threats
- SOC analyst review within 1 hour for high-priority alerts
- Threat notification within 30 minutes of confirmation

Response Times

- P1 (Critical - active breach): 15 minutes, 24/7
- P2 (High - confirmed threat): 30 minutes, 24/7
- P3 (Medium - suspicious activity): 2 hours, business hours
- P4 (Low - vulnerability): 1 business day

False Positive Rate

- <1% false positive rate for confirmed threats
- Human verification eliminates alert fatigue
- Continuous tuning improves accuracy
- Customer feedback incorporated into detection tuning

Terms and Conditions

Service provision is governed by HTG's G-Cloud 15 Call-Off Terms and Conditions. Key terms include:

Contract Duration

- Minimum initial term: 12 months
- Monthly renewal thereafter
- 30 days' notice required for termination
- No penalties for termination after minimum term

Service Changes

- HTG reserves right to update service features
- Material changes communicated 30 days in advance
- Pricing changes on 90 days' notice
- Customer right to terminate if changes unacceptable

Liability

- Liability terms as per G-Cloud framework
- Professional indemnity insurance: £5,000,000
- Public liability insurance: £5,000,000
- Cyber liability insurance: £5,000,000

Incident Response

- Best efforts to detect and remediate threats
- No guarantee of breach prevention
- Customer responsible for accepting remediation recommendations
- HTG not liable for threat actor actions
- Customer maintains ultimate security responsibility

Additional Information

Environmental and Social Value

- Cloud-based delivery minimises environmental impact
- Remote security operations reduce travel requirements
- Paperless security operations and reporting
- Security awareness training for community organisations
- Apprenticeship programmes in cybersecurity

Supplier Information

- Company Name: Howell Technology Group Limited
- Microsoft Solutions Partner status
- Huntress Certified Partner
- ISO 27001 certified
- Cyber Essentials Plus certified
- CREST registered consultants available

Document Version: 1.0

Last Updated: January 2026

Framework: G-Cloud 15