NETWITNESS

NetWitness Incident Response Retainer Packages

Silver | Gold | Platinum

Service Overview

Organizations and agencies in every vertical across the globe require guaranteed response times, structured escalation, and predictable investigative capacity during high-impact cyber events. NetWitness Incident Response (IR) Retainers provide pre-authorized access to senior incident responders, forensic analysts, and investigative tooling under defined service levels.

Each IR Retainer tier includes formal activation, committed SLAs for triage and preliminary analysis, and a fixed annual pool of effort hours. The Platinum tier extends this capability through proactive incident discovery using network and endpoint telemetry.

Service Purpose

The NetWitness Incident Response Retainer establishes operational readiness before an incident occurs and ensures rapid engagement when one does. The primary objectives are to:

- Eliminate onboarding and procurement delays during an incident
- Establish access controls, escalation paths, and communication workflows
- Reduce time to triage and time to investigative clarity
- Provide defensible forensic reporting for executive, legal, and regulatory stakeholders
- Deliver predictable response capacity within a defined 12-month service window

This retainer represents a structured operational capability rather than ad-hoc consulting support.

Retainer Activation Framework (All Tiers)

Prior to any incident, NetWitness conducts a structured activation process to ensure readiness:

- Identification of potential response locations
- Review of mission-critical assets and data sensitivity
- Validation of approved security and forensic tools
- Verification of secure remote access for IR analysts
- Definition of roles, responsibilities, and escalation contacts
- Review of incident handling procedures and breach disclosure requirements
- Delivery and walkthrough of the retainer welcome packet

Completing activation significantly reduces coordination delays when an incident is formally declared.

Incident Engagement Model (All Tiers)

Once activated during a live incident, the engagement proceeds through structured phases:

Phase 1 - Initial Triage

- Assessment of the current situation and impact
- Review of actions already taken
- Coordination with legal, compliance, finance, and executive stakeholders
- Identification of additional data requirements, including logs, packet captures, forensic images, memory dumps, and malware artifacts

Phase 2 - Preliminary Analysis

- Host-based forensic examination
- Network-based forensic analysis
- Malware assessment if necessary
- Open-source intelligence research
- Initial derivation of Indicators of Compromise (IOCs)

Phase 3 - Strategic Guidance

- Containment recommendations
- Direction on additional investigative steps
- Guidance on enterprise-class NetWitness tool deployment
- Escalation planning under a separate statement of work if required

Phase 4 - Reporting

- Delivery of a preliminary analysis report summarizing findings, impact assessment, investigative scope, and recommended next actions.

Retainer Tier Comparison

Capability	Silver	Gold	Platinum
Annual Effort Pool	Up to 60 hours	Up to 120 hours	Up to 240 hours
Initial Triage SLA	≤ 6 hours	≤ 3 hours	≤ 3 hours
Remote Preliminary Analysis	≤ 24 hours	≤ 12 hours	≤ 12 hours
On-Site Mobilization	≤ 48 hours	≤ 24 hours	≤ 24 hours
Preliminary Analysis Report	Yes	Yes	Yes
Repurpose Unused Hours	No	Yes	Yes
Proactive Incident Discovery	No	No	Yes
Tool Deployment as Needed	No	No	Yes
Incident Discovery Findings Report	No	No	Yes

All tiers operate within a 12-month Service Period. Effort hours must be consumed within that period. Unused hours in Gold and Platinum may be applied to approved proactive incident response services, subject to service terms.

Silver Retainer

Effort Allocation: Up to 60 hours
Response Profile: Foundational rapid-response capacity
Silver provides structured IR readiness and guaranteed response times for organizations requiring surge IR support.

Key Characteristics:

- Six-hour triage SLA
- Remote preliminary analysis within 24 hours
- On-site mobilization within 48 hours
- Delivery of a preliminary analysis report

Investigative Focus Areas Include:

- Host compromise validation
- Malware presence identification
- Log and artifact review
- Initial network activity review when available
- Identification of indicators of compromise

Additional Forensic Services May Include:

- Host forensic artifact review
- Malware sample evaluation
- IOC derivation and validation
- Evidence preservation guidance

Ideal Organizations

Silver is appropriate for organizations maintaining internal SOC teams that require external escalation support during complex incidents.

Gold Retainer

Effort Allocation: Up to 120 hours
Response Profile: Accelerated engagement with expanded investigative capacity

Key Characteristics:

- Three-hour triage SLA
- Remote preliminary analysis within 12 hours
- On-site mobilization within 24 hours
- Increased investigative bandwidth for complex or multi-system compromises

Investigative Focus Areas Include:

- Host-level compromise investigation
- Malware persistence analysis
- Network activity review for lateral movement
- Command-and-control communication detection
- Expanded IOC development

Additional Forensic Services May Include:

- Memory dump analysis
- Malware capability assessment
- Network artifact review
- Timeline reconstruction across affected systems
- Strategic containment guidance

Ideal Organizations

Gold is well suited for regulated industries and enterprises managing sensitive data that require faster response and deeper forensic investigation.

Platinum Retainer

Effort Allocation: Up to 240 hours
Response Profile: Integrated response combined with proactive compromise discovery
Platinum incorporates all Gold capabilities and adds a proactive incident discovery workstream.

Incident Discovery Capabilities (Platinum Only)

Platinum includes:

- Deployment of a NetWitness network appliance if required
- Deployment of endpoint telemetry using a customer-provided server
- Monitoring of inbound, outbound, and lateral network activity
- Host telemetry collection and analysis

Investigative Focus Areas Include:

- Active malware presence
- Beaconing activity
- Lateral movement
- Command-and-control communications
- Data exposure or exfiltration attempts

Additional Forensic Services May Include:

- Forensic imaging of live or offline systems
- Malware capability analysis and IOC derivation
- Secure data wipe procedures upon request
- Executive briefings outlining threat posture and remediation strategy

Deliverables:

- Preliminary analysis report
- Incident discovery findings report

Ideal Organizations

Platinum is designed for large enterprises, critical infrastructure operators, and organizations requiring both rapid response and proactive compromise discovery.

Commercial and Operational Model

Across all tiers:

- Services are primarily delivered remotely
- On-site engagements exclude travel costs
- Service period is 12 months from booking
- Multi-year retainers are invoiced annually
- Effort hours do not roll over beyond the service period

Expanded remediation and long-term recovery activities require a separate statement of Work.

Strategic Outcomes

The NetWitness IR Retainer provides measurable operational benefits:

- Reduced time to triage
- Faster investigative clarity
- Defensible forensic reporting
- Defined escalation workflows
- Controlled response costs through pre-allocated effort

Platinum additionally enables:

- Proactive threat identification
- Visibility across network and endpoint environments
- Detection of persistent attacker activity

Summary

NetWitness Incident Response Retainer moves incident response from reactive procurement to operational preparedness.

Silver delivers essential rapid-response capability.
Gold accelerates engagement and expands investigative capacity.
Platinum integrates proactive discovery with extended forensic visibility.

For organizations operating in high-risk or regulated environments, securing incident response capacity in advance is not optional. It is a fundamental security control.

See the Full Response Flow

Explore how NetWitness delivers structured triage, forensic investigation, and rapid escalation under real incident conditions.

Request a Demo

NETWITNESS