NETWITNESS

Potential Response - Evaluation, Analysis, Containment & Triage

(PreACT)

Service Overview

Security programs evolve constantly new threats emerge, regulations change, technologies get added, teams reorganize. What worked two years ago might have gaps today. Most organizations operate with some uncertainty about whether their current security posture truly covers all the bases: Are policies keeping pace with actual operations? Do controls align with the latest frameworks? Are critical assets protected according to their real value and risk? Is the incident response capability ready for today's threat landscape, not yesterday's?

Without a systematic assessment against current standards and practices, security leaders are making decisions based on outdated snapshots rather than current reality. PreACT provides that strategic view—a comprehensive evaluation of where your security program stands today against established frameworks, regulatory requirements, and the specific threats your organization faces, revealing exactly what's covered and where attention is needed.

NetWitness Solution - PreACT Gap Analysis

PreACT (Potential Response - Evaluation, Analysis, Containment & Triage) is a comprehensive security posture assessment that maps your existing defenses against established frameworks like NIST, ISO 27001, CIS Controls, and relevant regulatory requirements. This isn't a checkbox compliance audit. NetWitness incident response experts examine your security infrastructure, policies, procedures, and critical assets through the lens of real-world attack patterns—identifying specific gaps that adversaries would exploit and providing a prioritized roadmap for improvements that reduce risk.

The assessment evaluates what you have today, benchmarks it against what works in practice, and delivers actionable recommendations organized by priority and impact.

How PreACT Works

- **Preparation & Scoping:** NetWitness works with your team to define assessment objectives, identify which frameworks and standards are most relevant (NIST, ISO 27005, CobiT, CIS, PCI-DSS, or others), and coordinate access to necessary documentation and stakeholders.
- **Data Collection & Assessment:** The NetWitness team reviews existing security policies, procedures, and controls. This includes interviews with IT and security stakeholders, examination of network architecture and system configurations, and technical assessment of deployed security technologies—firewalls, intrusion detection systems, endpoint protection, encryption, and access controls.
- **Critical Asset Identification:** The team identifies your most valuable and sensitive information assets—intellectual property, customer data, financial records, operational systems—and evaluates whether protection measures match the value and risk profile of those assets.
- **Threat Landscape Analysis:** NetWitness analyzes the specific threat environment for your industry, business operations, and geography to understand which attack vectors and adversary types pose the greatest risk to your organization.
- **Gap Identification & Benchmarking:** Your current security posture is measured against established best practices and regulatory requirements. The analysis identifies specific gaps and weaknesses—places where your defenses don't meet standards or where real-world threats would find openings.
- **Prioritized Recommendations:** NetWitness develops a prioritized list of improvements across technical controls, procedures, and organizational structure. Recommendations are ranked by risk reduction impact and implementation feasibility, not just by framework requirements.
- **Actionable Roadmap:** You receive a detailed implementation roadmap with specific steps, timelines, resource requirements, and milestones for addressing identified gaps in order of priority.

Benefits and Outcomes of PreACT

Know Your Real Security Posture

Move from assumptions to evidence. Understand exactly where your defenses are strong and where exploitable gaps exist before an attacker discovers them.

Risk-Prioritized Improvements

Get recommendations organized by actual risk reduction, not just compliance requirements. Focus resources on changes that close the most dangerous gaps first.

Framework Alignment

Benchmark your security program against industry-recognized standards (NIST, ISO, CIS) and regulatory requirements specific to your industry—with a clear view of where you meet standards and where gaps remain.

Critical Asset Protection Validation

Confirm that your most valuable assets have protection measures that match their importance and risk profile—or identify where they don't and what needs to change.

Actionable Implementation Path

Receive a practical roadmap that translates findings into specific steps your team can execute, complete with timelines and resource requirements.

Executive-Ready Reporting

Security leadership gets comprehensive documentation of current posture, identified risks, and recommended improvements—supporting informed decisions about security investments and priorities.

Proactive Risk Reduction

Address weaknesses systematically before they become breach vectors, reducing the likelihood and impact of successful attacks.

About NetWitness

NetWitness has been at the forefront of cybersecurity detection and response for over two decades. Built on technology originally developed for the intelligence community, the NetWitness platform has evolved into one of the most capable threat detection and investigation ecosystems available to enterprise security teams today. That same depth of capability underpins every professional services engagement we deliver.

The NetWitness Incident Response team brings together experienced incident responders, threat hunters, malware analysts, and forensics specialists who have worked across some of the most complex and high-stakes investigations in the industry. We do not show up with a generic playbook. Every engagement is shaped by what we find in your environment, informed by current adversary tradecraft, and driven by a genuine commitment to giving your team clarity when it matters most.

NETWITNESS