NETCLEAN **PROACTIVE** CLOUD

SERVICE OVERVIEW

File Threat Analysis On-Demand

www.netclean.com

NetClean.

Table of contents

Introduction

ProActive File Threat Analysis On-Demand is a service available on the NetClean ProActive Cloud Threat Intelligence Platform. It enables security teams to manually analyze file hashes – on a case-by-case basis – against NetClean's threat intelligence database, providing high-confidence, actionable detection without creating any additional noise. At present, this intelligence consists of files classified within the Child Sexual Abuse Material (CSAM) threat domain, verified by law enforcement and other trusted intelligence sources.

This service is designed for scenarios that require manual controls rather than automated analysis and is optimized for rapid processing of large volumes of hashes.
It provides high-confidence, actionable results to support investigations, incident responses, and compliance decisions – without requiring integration with other security systems. This helps organizations meet legal obligations, detect serious insider threats, and respond with confidence.

How it works

Collect: Gathering signals

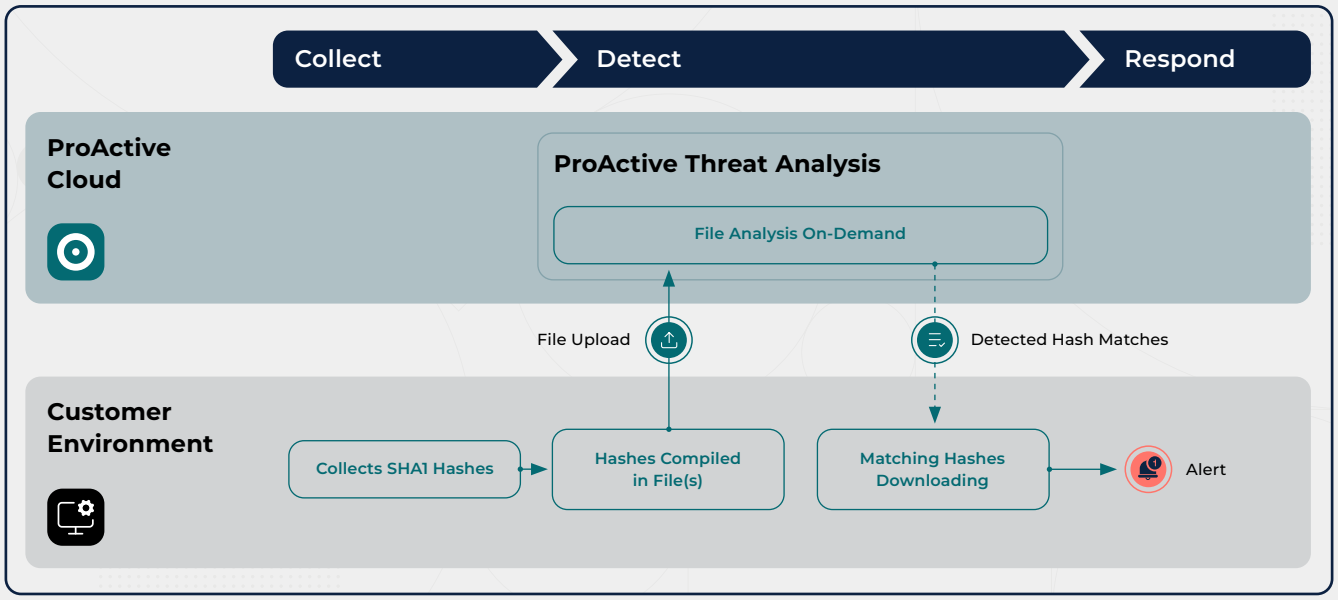
Existing security tools capable of extracting file hashes collect SHA-1 hashes from the IT environment (endpoints, DLP systems, forensic tools, cloud storage, etc.)

Detect: Identifying threats from signals

One or more files containing collected hashes are uploaded to the ProActive File Threat Analysis On-Demand service, where the hashes are checked against NetClean's threat intelligence database. If matches are detected, hashes and their verification sources are immediately delivered in a downloadable format.

Respond: Acting on threats

Security teams can use detected matches to trigger alerts, initiate investigations, log incidents, or automate response workflows.



How to access the service

Files are uploaded for analysis in the ProActive File Threat Analysis On-Demand module accessible in the ProActive Cloud portal.

Value scenarios

ProActive File Threat Analysis On-Demand is not intended to replace existing security platforms or become a standalone solution. Instead, it serves as a high-value, on-demand support tool that complements existing processes when deeper insight is needed—especially when the human insider risk dimension is critical.

This means ProActive fits naturally into existing workflows, helping SOC teams expand investigations, validate assumptions, and strengthen decision-making.

- **Incident Response & Insider Risk Investigations**
  ProActive gives Incident Response and Forensic teams fast, reliable file-level analysis during active incidents, helping confirm whether suspicious files are linked to human misconduct or policy violations. This clarity reduces guesswork when deciding whether to escalate to HR/legal or keep the case technical, enabling faster containment and minimizing the risk of missteps under pressure.
- **Security Due Diligence (e.g., Mergers & Aquisation)**
  ProActive enhances due diligence processes by identifying file-based indicators of insider risk or compliance breaches. This capability ensures that strategic transactions are evaluated not only on financial metrics but also on cultural and legal risk factors. Detecting behaviors such as mishandling sensitive data or storing prohibited content helps prevent reputational damage and post-transaction liabilities.
- **SOC & Threat Hunting**
  ProActive improves detection workflows by elevating high-confidence indicators linked to insider risk behaviors. This enables analysts to prioritize alerts associated with illicit or high-risk content, reducing false positives and operational noise. By focusing on threats that carry significant legal or reputational impact, security teams can allocate resources more effectively and accelerate response actions.
- **Compliance & Governance**
  ProActive supports regulatory reporting and policy enforcement by providing auditable insights during investigations of insider misconduct or policy violations. This ensures compliance teams can demonstrate due diligence and meet regulatory standards without introducing additional operational overhead. The result is a defensible, streamlined process for managing insider risk in alignment with governance requirements.