NETCLEAN **PROACTIVE** CLOUD

SERVICE OVERVIEW

File Threat Detection for Endpoints

www.netclean.com

NetClean.

Table of contents

Introduction

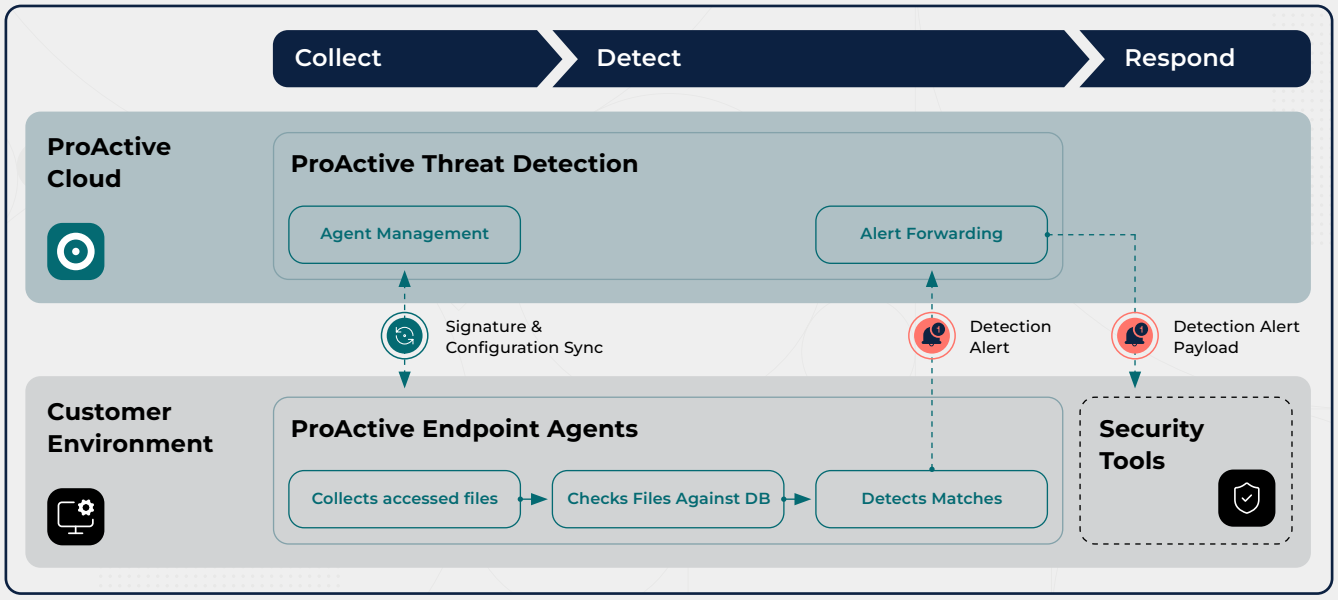
ProActive File Threat Detection for Endpoints is a core service available on the ProActive Cloud Threat Intelligence Platform for Human Insider Risk. It detects verified compromising or high-risk content on corporate laptops and workstations—material that violates organizational policies or legal frameworks and poses serious compliance, security, and insider-risk concerns. At present, this detection capability is focused on files classified within the Child Sexual Abuse Material (CSAM) threat domain.

This service empowers security teams to detect, investigate, and respond to high-risk insider threats without adding any extra noise, and the alerts are integrated into existing security tools and workflows. Designed for continuous file activity observation, it supports both security and compliance objectives – helping organizations respond with confidence.

The service combines:

- NetClean's verified file signature database, where each signature includes a collection of metadata and several types of file threat indicators, e.g. hashes, for a file classified as containing illicit or high-risk content. New signatures are continuously added by law enforcement and other trusted organizations dedicated to child sexual abuse prevention.
- Lightweight endpoint agents installed on Windows, macOS, and Linux endpoints, that perform real-time file checks and detection on file access.
- A cloud backend component that handles configuration, integration, and signature updates.
- The ProActive Cloud portal - the interface for managing the service.
- Automatic alert forwarding to the customer's existing security tool.

How it works



Collect: Gathering signals

The ProActive endpoint agent runs discreetly in the background, observing each file event indicating file interaction either by user or system on local and removable drives in real-time.

Detect: Identifying threats from signals

The agent compares accessed files with a local copy of NetClean's verified database of cryptographic indicators – hashes - used to identify known high-risk content. A file match against this database confirms the presence of a human risk threat and should be treated as a critical security and compliance alert.

When a file match is detected:

1. The endpoint agent triggers a detection alert to the cloud backend.
    - Even if a device is offline, detections are preserved and alerts are sent as soon as connectivity is restored - ensuring that no high-risk activity goes unnoticed.
    - To strengthen the incident assessment, the service also collects information about nearby files in the same folder. This helps incident responders distinguish isolated events, possibly mistakes, from patterns of very high-risk behavior.
2. The cloud backend sends a webhook callback with a JSON payload containing the essential detection information such as detection timestamp, computer name and IP, file and storage details and the user logged on at the time of detection.
    - NetClean does not store alert data in its cloud service once the webhook callback has been successfully delivered.
3. The endpoint agent triggers a detection alert to the cloud backend.

Respond: Acting on threats

An alert should be treated as a verified human insider threat and handled with urgency and care. As a best-practice approach, incident response typically follows parallel tracks.

- Compliance actions involving HR and Legal help manage the situation from both an organizational and employee perspective.
- In parallel, Cybersecurity teams conduct security investigations to assess the surrounding security landscape - including the user and their device - and to ensure any compromised assets are properly secured.

How to set up the service

Preparations:

- Choose a security tool that will receive detection alerts.
- Establish or update an incident response plan for handling Human Insider Threat incidents generated from ProActive.

Onboarding is straightforward and typically completed in days. Necessary functionality and software for setting up the service is available in ProActive Cloud.

Onboarding includes:

- Configuring alert forwarding by setting up the webhook for integration and configure workflows for handling alerts.
- Deploying the endpoint agents by accessing software (msi/pkg/deb packages) and installation scripts and rolling out widely via a UEM (Intune, SCCM, etc.).
- Performing an end-to-end service validation with demo images.

Ongoing management

Most organizations spend very little time per month managing the detection service.

The management includes:

- Keeping the endpoint agents updated and running.
- Following internal incident case-handling procedures should detections occur.
- Performing periodic end-to-end service validation (e.g., generating demo alerts).

Updates of the signature database are automatically and discreetly distributed to the connected agents, without the need for any manual action.

How ProActive File Threat Detection for Endpoints fits into your security and compliance ecosystem

ProActive File Threat Detection for Endpoints identifies serious human insider threats that other security tools miss, enhancing your threat intelligence with new threat domains.

- **Incident response & insider risk teams:** High-confidence alerts are best suited for specialized incident response or insider risk functions, where sensitive, human-centric threats require careful investigation, evidence handling, and coordination with HR or legal teams.
- **MDR & security operations:** Alerts can serve as authoritative triggers for managed detection and response (MDR) or security operations teams, initiating structured investigations and escalation processes for high-risk insider activity.
- **Compliance & policy enforcement:** Provides verifiable, actionable evidence to support compliance, reporting, and audit requirements. Organizations can meet legal obligations and enforce internal policies with confidence.
- **Flexible integration:** Alerts are delivered via secure webhooks, designed to integrate into existing case management, incident response, or insider risk workflows - ensuring sensitive incidents are handled by the right teams.