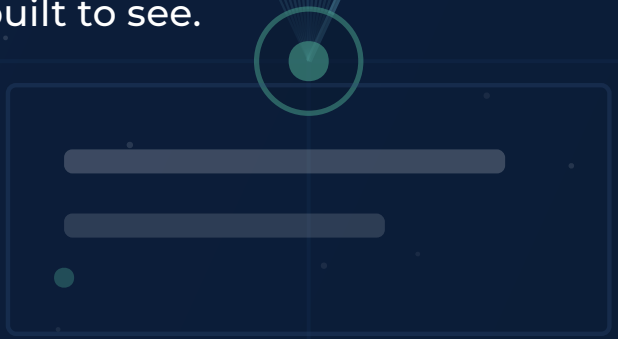
NETCLEAN **PROACTIVE**

SOLUTION OVERVIEW

Human Insider Risk Intelligence.

Identify and respond to verified human insider risk that traditional security tools are not built to see.



www.netclean.com

NetClean.

NAVIGATION

Table of contents

NetClean ProActive

Introducing NetClean ProActive 1
Intelligence built on verified indicators 2
Three ways to use ProActive 3

Detection Services

How Detection Services work 4
Detection capabilities and alert handling 5

Analysis Services

How Analysis Services work 6
Analysis capabilities and integration options 7

Intelligence Services

How Intelligence Services work 8

ProActive in your environment

From match to response 9
Built for your security ecosystem 10

Why ProActive

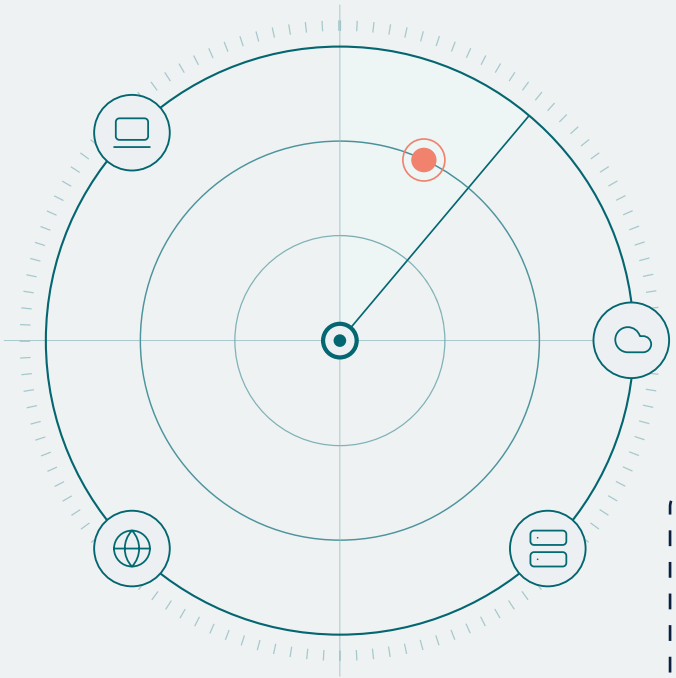
Specialized intelligence built for real-world security operations 11
Take the next step 12

NETCLEAN PROACTIVE

Introducing NetClean ProActive

ProActive Human Insider Risk Intelligence Platform: identify and respond to verified human insider risk.

ProActive adds specialized intelligence to help organizations find verified matches for risks that existing security controls are not designed to detect. It complements existing security operations, adding a focused human insider risk intelligence layer without requiring organizations to replace the tools and workflows already in place.



Specialized human insider risk intelligence

Purpose-built intelligence for human insider risk that traditional cybersecurity controls are not designed to identify.

Privacy-first

Focused matching against verified Risk Indicators rather than broad content or behavioral analysis.

Verified intelligence

Verified Risk Indicators from trusted sources provide a precise basis for matching and decision support.

Integration-first

Designed to work with existing security data, controls and operational workflows.

THE RISK IN CONTEXT

Nearly 270,000 enterprise devices analyzed for the Verizon DBIR 2026 showed that roughly one in 500 employees had handled compromising or high-risk material on a corporate device. That material increases susceptibility to coercion, and when trusted employees are coerced, legitimate access can become a risk that may go undetected.

NETCLEAN PROACTIVE

Intelligence built on verified indicators

ProActive intelligence is organized into Risk Domains and delivered as verified Risk Indicators. A Risk Indicator is intelligence NetClean provides, for example a file hash, URL or domain, against which data in the customer environment can be matched.

RISK DOMAINS:

Child Sexual Abuse Material (CSAM)

NetClean pioneered the detection of CSAM in organizational environments. Current file-based intelligence uses verified cryptographic indicators to identify known CSAM without inspecting the underlying content.

Terrorist and Violent Extremist Content (TVEC)

ProActive also includes intelligence for TVEC, including official terrorist propaganda, glorification and supporter-generated material, instructional material, and perpetrator-authored content.

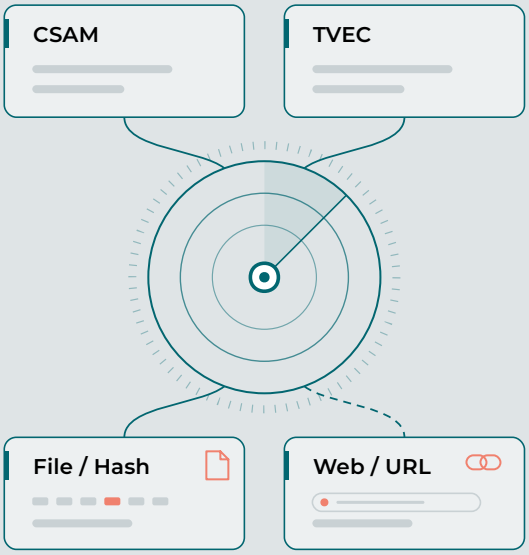
Two risk indicator types. One intelligence foundation.

Indicator types

- **File Risk Indicators:** verified file hashes used for file-based intelligence
- **Web Risk Indicators:** verified URLs and domains used for web intelligence

Core principles

- Trusted and verified intelligence sources
- Privacy-first matching
- High-confidence results designed to minimize noise



Three ways to use ProActive

Organizations can apply the same verified ProActive intelligence in three different ways, depending on how data is collected and where matching and response to takes place.

NetClean ProActive Platform

Detection Services

WE IDENTIFY

Screen endpoints for verified Risk Indicators and surface matches as alerts.

- File Detection for Endpoints
- Alert Vault
- Workstation Event Screening and Alert Forwarding are capabilities within File Detection for Endpoints.

Analysis Services

YOU QUERY

Check file hashes already available in your environment against verified File Risk Indicators.

- File Analysis API
- File Analysis OnDemand
- Confiugraions and connections to existng security platforms
- Works on hashes from existing security data.

Intelligence Services

WE DELIVER

Feed machine-readable Risk Indicators into controls you already operate.

- Web Indicator List
- Machine-readable Risk Indicators
- DNS, SASE and SSE integrations.

ONE INTELLIGENCE FOUNDATION. THREE SERVICE MODELS.

The service model changes how Risk Indicators are delivered and matched, not the underlying principle of verified, privacy-first intelligence.

DETECTION SERVICES

How Detection Services work

ProActive Detection Services continuously screen endpoints for verified Risk Indicators and make alerts available for investigation and response.

The core service, File Detection for Endpoints, screens supported file activity directly on the endpoint and creates a detection event when a match is found.

001 - COLLECT

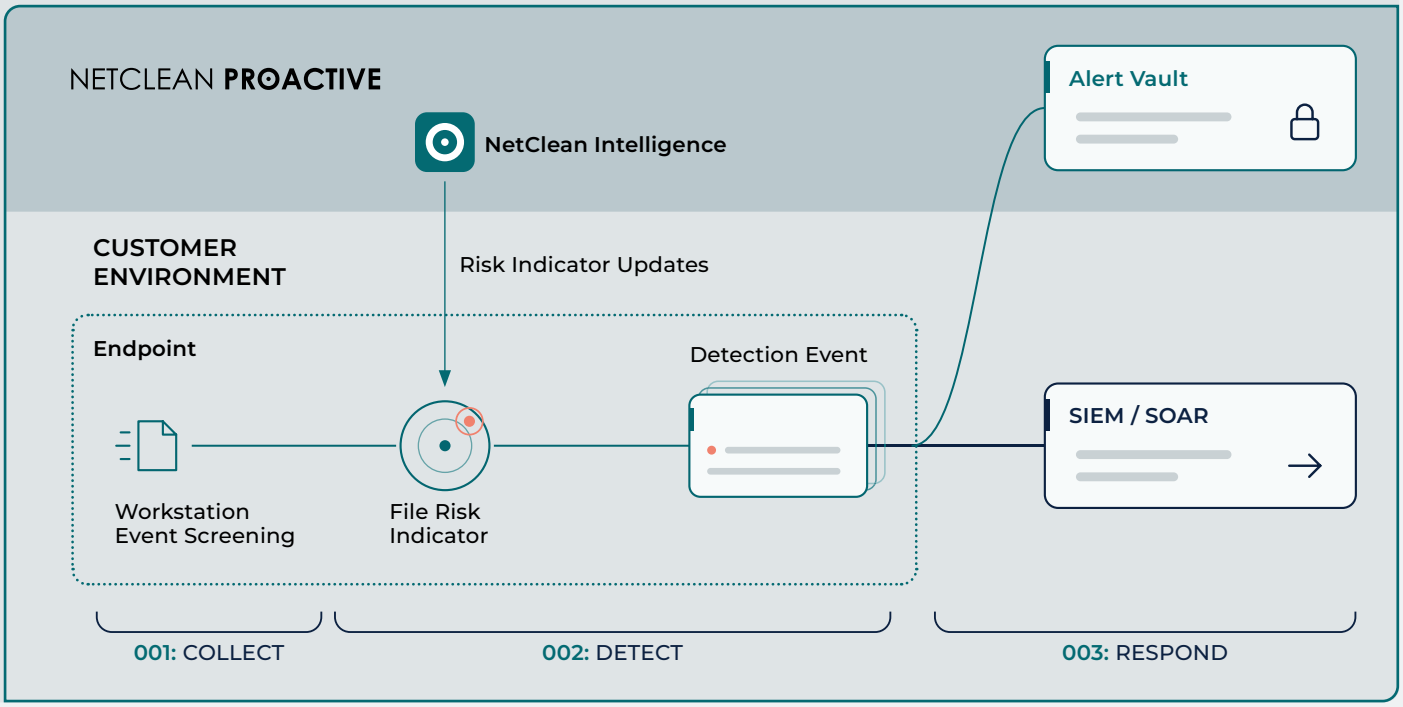
Workstation Event Screening runs in the background and is triggered by real-time file events on supported endpoints.

002 - DETECT

Files are matched locally against verified File Risk Indicators. A match is recorded as a detection event, including when the device is temporarily offline.

003 - RESPOND

Alerts are made available in Alert Vault and/or forwarded into existing SIEM, SOAR and security workflows, for example via webhook.



KEY CAPABILITIES

- Continuous endpoint screening triggered by real-time file events
- Online and offline detection
- Local matching against verified File Risk Indicators
- Minimal setup and fast time-to-value
- Automatic Risk Indicator and configuration updates
- Support for Windows and macOS endpoints

DETECTION SERVICES

Detection capabilities and alert handling

Detection Services currently combine two services: File Detection for Endpoints for endpoint screening and alert delivery, and Alert Vault for controlled storage and review of sensitive alerts.

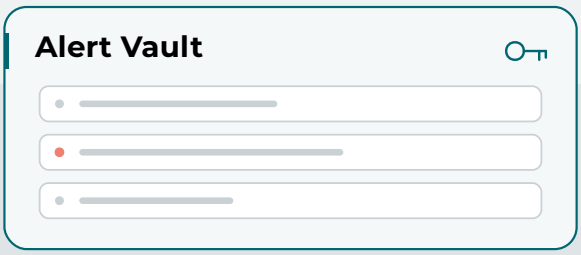
FILE DETECTION FOR ENDPOINTS

Workstation Event Screening

Runs in the background and is triggered by real-time file events, screening file activity against verified Risk Indicators.

Alert Forwarding

Forwards alerts into existing SIEM, SOAR and security workflows, for example via webhook. This supports automation while allowing teams to continue working in established systems.



Protect sensitive alerts with ProActive Alert Vault

Alert Vault securely stores and presents sensitive alerts under a Hold Your Own Key (HYOK) model. The customer holds the encryption keys and controls who can access alert information.

- Forensic-grade alert information organized by endpoint, Risk Indicator and detection event
- Controlled access for authorized users
- Customer-defined retention and governance
- CSV export for controlled downstream handling when required
- Can be used alongside Alert Forwarding or as the primary review surface
- A storage and assessment surface - not a replacement for investigation, case management, HR, legal or incident-response processes

TWO COMPLEMENTARY PATHS

Use Alert Forwarding for automation and downstream workflows.
Use Alert Vault for controlled review of the full sensitive alert record.

ANALYSIS SERVICES

How Analysis Services work

Analysis Services let organizations apply NetClean intelligence to file hashes they already collect. No new agent is required.

Existing security tools collect the relevant hashes, ProActive checks them against verified File Risk Indicators, and the result returns to the customer workflow.

001 - COLLECT

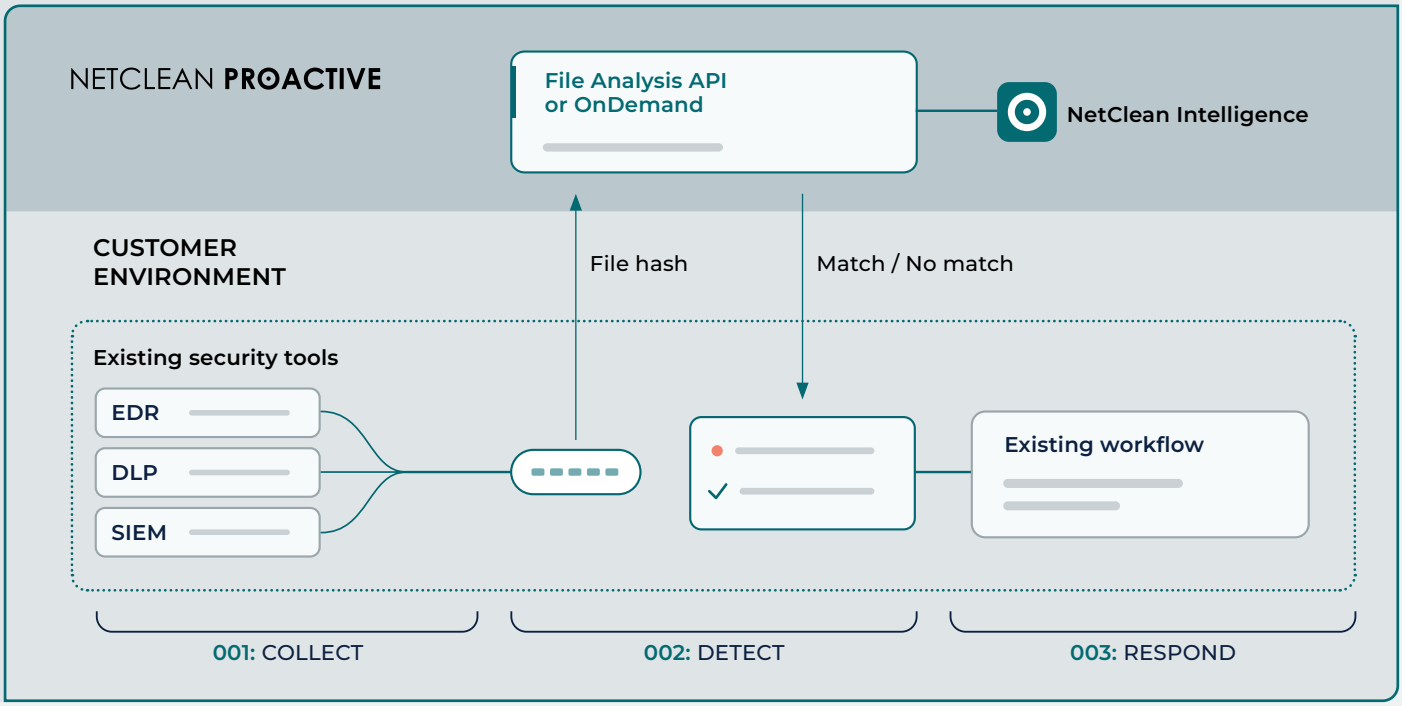
Collect file hashes from existing EDR, DLP, SIEM, forensic or other security tooling.

002 - DETECT

File Analysis API or File Analysis OnDemand checks the submitted hashes against verified File Risk Indicators.

003 - RESPOND

The match or no-match result returns into the existing workflow for alerting, enrichment, investigation or other handling.



KEY CAPABILITIES

- A match is verified. No match provides a high-confidence clearance.
- No new agent required.
- Automated or investigator-driven analysis.
- Reuses data and collection capabilities already available in the environment.
- Uses verified File Risk Indicators from NetClean's intelligence sources.
- Integrates with existing security workflows.

ANALYSIS SERVICES

Analysis capabilities and integration options

Analysis Services provide two ways to query verified file intelligence, plus a Splunk connector that brings the File Analysis API into existing Splunk environments.

File Analysis API

For continuous, automated analysis. Returns a real-time match or no-match response for up to 2,000 hashes per request.

File Analysis OnDemand

For investigator-driven checks of selected file hashes, available directly in the ProActive portal with no integration effort.

Splunk connector

Brings the File Analysis API into existing Splunk environments and workflows, so hashes can be checked and results used in searches, dashboards, alerts and playbooks.

MICROSOFT INTEGRATION OPTIONS



PRIVACY BY DESIGN

Only the file hash leaves your environment.
No file content, filenames or identity data are submitted or stored.

How Intelligence Services work

Intelligence Services deliver curated, machine-readable Risk Indicators for use inside the security controls an organization already operates.

The current service, Web Indicator List, provides continuously updated domain and URL indicators for supported Risk Domains.

001 - COLLECT

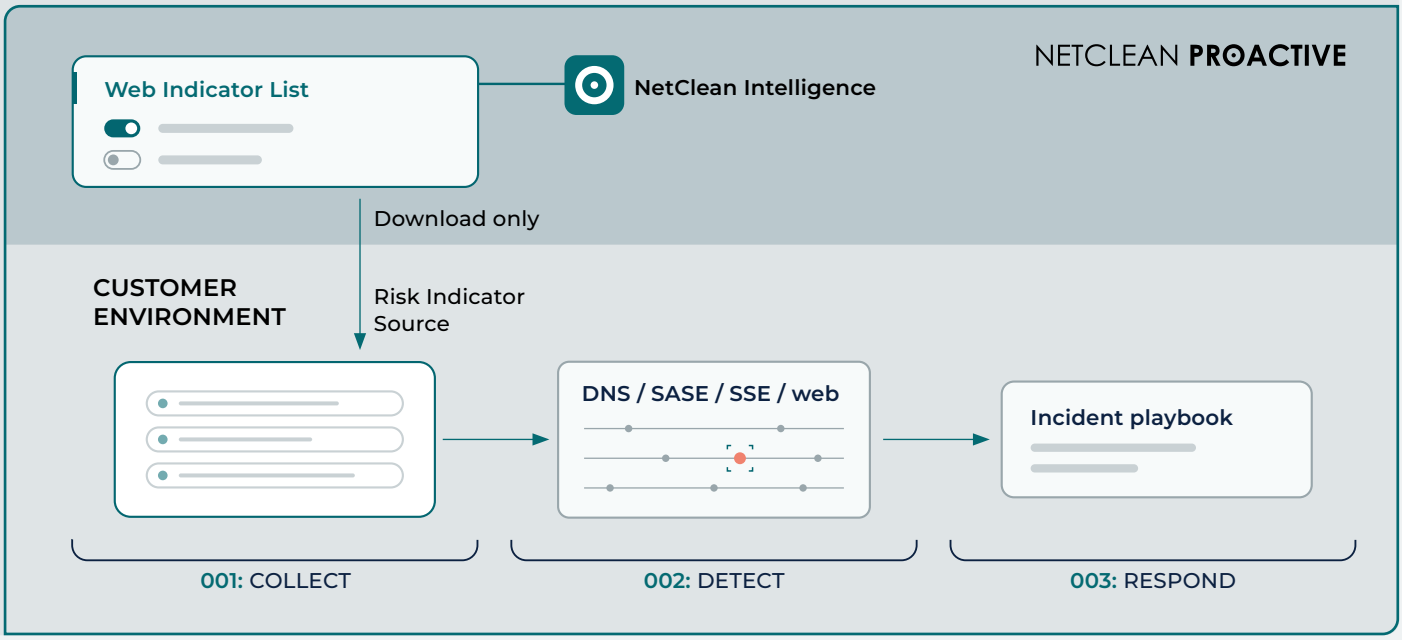
Risk Indicators are ingested into the customer infrastructure as a source in existing security pipelines.

002 - DETECT

Existing DNS, SASE, SSE or web security controls match observed traffic against the Risk Indicators.

003 - RESPOND

The customer's existing incident playbook takes over, for example logging, alerting, access restriction or escalation.



WEB INDICATOR LIST

- Curated, verified domain and URL indicators, continuously updated
- Customers choose which Risk Domains to include
- Read-only and download-based: no customer data is submitted, processed or stored
- Added as a source in existing pipelines, not introduced as a new system
- Designed for existing DNS, SASE, SSE and web security infrastructure
- Current TVEC coverage is delivered as Web Risk Indicators through Web Indicator List

PROACTIVE IN YOUR ENVIRONMENT

From match to response

Every ProActive service follows the same operating model: Collect, Detect, Respond. What changes is where the data comes from and where the match takes place. What stays the same is who decides what happens next.

One model, three paths

Detection Services

Workstation Event Screening collects file events and matches them locally on the endpoint.

Analysis Services

Existing security tools collect file hashes, and File Analysis API or OnDemand checks them against verified File Risk Indicators.

Intelligence Services

Web Risk Indicators are ingested into existing controls, and the customer's DNS, SASE, SSE or web security infrastructure performs the match.

Respond: your process, your decision

01 Assess

Understand what was identified, where and when, and combine the ProActive result with the available technical and organizational context.

02 Investigate

Apply existing security and investigative processes to understand the wider context and determine what additional information is needed.

03 Act

Determine the appropriate organizational response in line with internal policies, responsibilities and applicable procedures.

RESPONSIBILITY

NetClean provides the intelligence and context.
The organization determines the appropriate investigation and response.

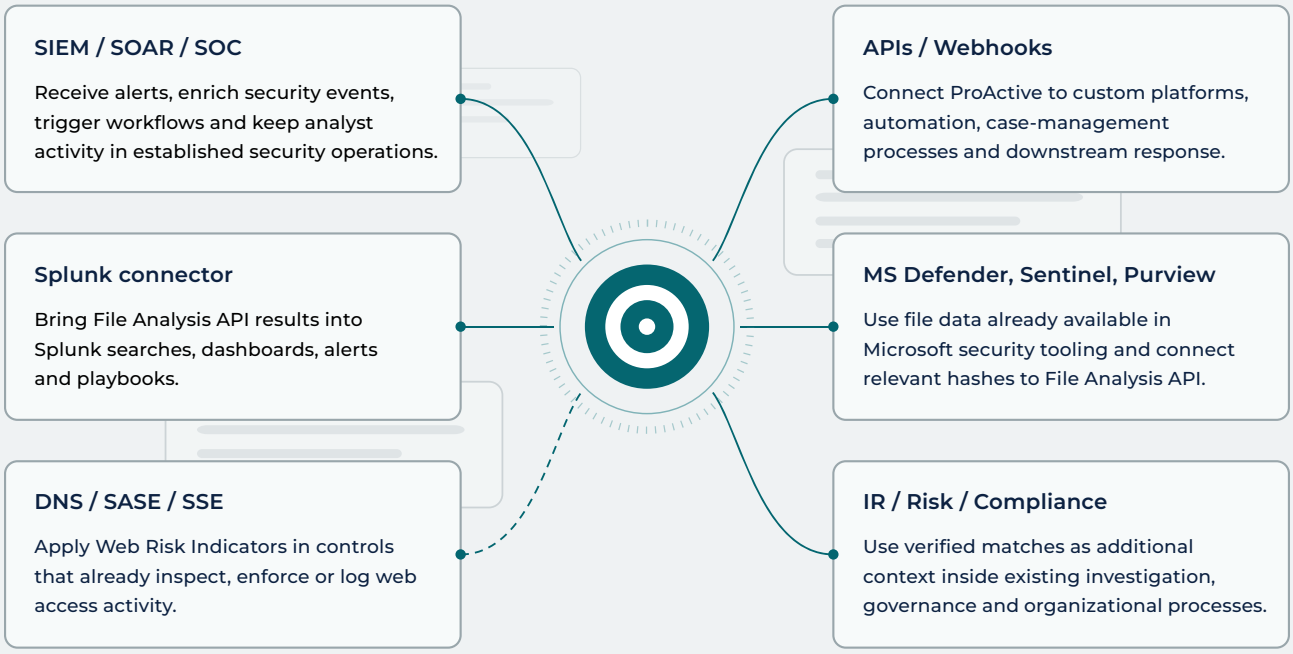


PROACTIVE IN YOUR ENVIRONMENT

Built for your security ecosystem

ProActive is designed to add a specialized human insider risk intelligence layer to the security technologies, data sources and operational workflows organizations already use. Detection, Analysis and Intelligence Services provide different entry points into the same verified intelligence foundation.

Strengthen your security stack. Don't replace it.



A SPECIALIZED INTELLIGENCE LAYER

ProActive is designed to fit around the security architecture already in place, not force replacement of core tools or workflows.

WHY PROACTIVE

Specialized intelligence built for real-world security operations

Verified intelligence

Specialized intelligence from trusted and authoritative sources, focused on verified Risk Indicators.

High confidence

A match is verified.
No match is a high-confidence clearance.

Privacy-first

Screens only for verified Risk Indicators. Nothing else is analyzed.

Integration-first

Designed to work with the security infrastructure and operational workflows organizations already use.

Flexible delivery

Start where you are. Add endpoint detection, enrich the data you already collect, or feed your existing controls. Same verified intelligence in every case.

Proven expertise

Built on NetClean's long-standing specialization in identifying high-risk content in enterprise environments.

NETCLEAN AT A GLANCE

1.5M
active licenses

110+
countries

20+
years of expertise

DBIR 2026
Contributor to the Verizon Data Breach Investigations Report 2026

SEE WHAT YOUR SECURITY STACK ISN'T SEEING.

Explore how ProActive can bring verified human insider risk intelligence into your existing security environment.

Talk to an expert

NetClean.

NetClean.

netclean.com
info@netclean.com