NETCLEAN **PROACTIVE** CLOUD

SERVICE OVERVIEW

Web Threat List

www.netclean.com

NetClean.

Table of contents

Introduction

Proactive Web Threat List is part of the NetClean ProActive Cloud Threat Intelligence Platform, delivering a continuously updated set of high-risk web indicators.

It provides curated, high-confidence exposure indicators across multiple threat domains, enabling risk-based enforcement, policy automation, and signal correlation within SASE, SSE, and enterprise security platforms.

Indicator are designed for seamless integration into existing web security enforcement and monitoring architectures—where web traffic is already inspected and logged—allowing organizations to identify high-risk human-centric web activity not typically covered by traditional malware, phishing, or network-centric threat intelligence.

The service supports detection and investigation of serious human-driven web threats without requiring additional data collection, user tracking, or architectural changes.

How it works

Collect: Gathering signals

Web access activity is already inspected as part of standard security enforcement and logging. Requests to domains and URLs are evaluated at policy enforcement points where outbound web traffic is controlled, and the events are recorded with associated metadata.

Detect: Identifying threats from signals

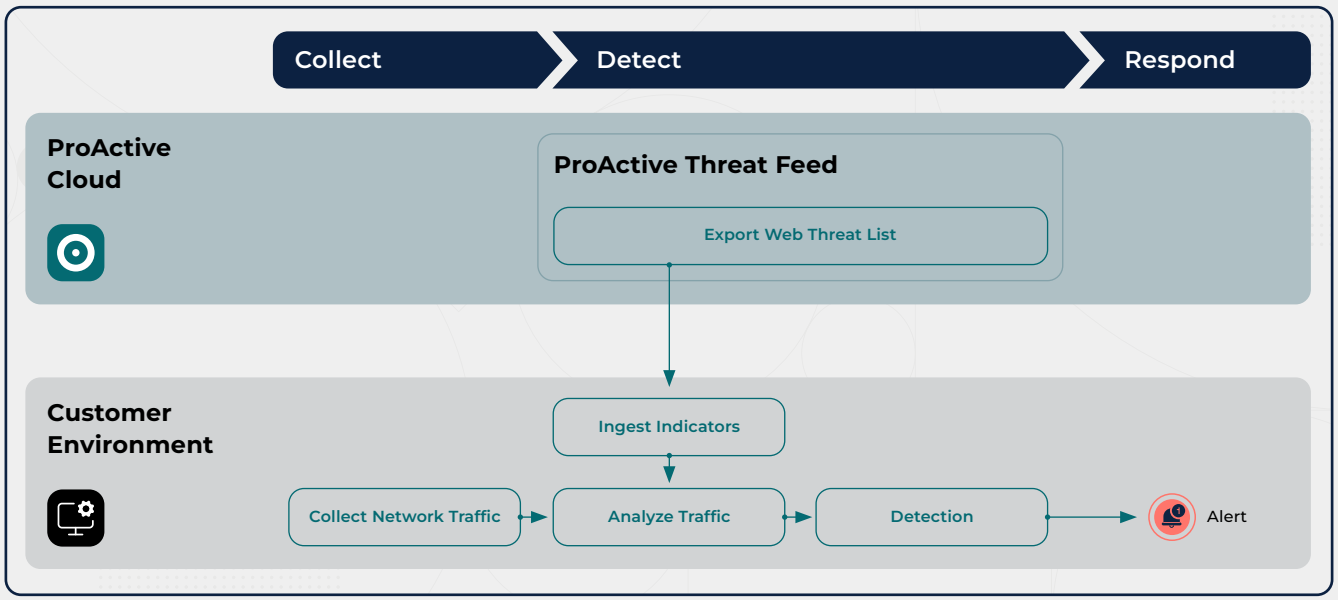
ProActive Web Threat List provides a curated set of high-risk web indicators consisting of domains and URLs associated with elevated human insider risk. Detection is based on matching observed web destinations (URLs and domains) against indicators in NetClean's Web Threat List.

Designed in structured format for easy integration, the indicator set strengthens your existing threat intelligence and enables detection of access to listed high-risk web destinations through standard monitoring and logging processes.

Respond: Acting on threats

When a match is identified, escalation and action are determined by the organization's existing security policies and work flows. Depending on configuration, responses may include logging, alerting, access restriction, or escalation to downstream investigation and response workflows accross the security stack..

Detected events enrich existing intelligence and can be correlated with other signals for further handling in line with organizational procedures for insider risk management.



How to access the service

ProActive Web Threat List is available through the NetClean ProActive Cloud portal. This service provides a downloadable CSV file containing the current set of high-risk web indicators.

The CSV file is updated on a continuous basis to reflect changes in the indicator set. Customers are responsible for retrieving the file and integrating it into their existing security enforcement, monitoring, or analysis workflows in accordance with their operational requirements.

Integration with security ecosystem

ProActive Web Threat List is designed for seamless integration with modern security architectures, including SASE-based environments and hybrid deployments. This includes both cloud-based SASE platforms and traditional security controls that perform equivalent enforcement, inspection, or logging functions.

The indicator set can be applied at multiple functional layers where web access activity is inspected, logged, or controlled:

- **Policy enforcement and web access control**
  Access attempts to domains or URLs included in the indicator set can be identified during web inspection and evaluated against existing security policies. Escalation and actions are determined by policy and configuration and may include logging, alerting, or access restriction.
- **Name resolution and DNS inspection**
  DNS queries can be evaluated against the indicator set to identify resolution attempts to listed domains as part of standard DNS inspection and logging processes.
- **Monitoring and analytics**
  Events associated with matches can be forwarded to monitoring and analytics platforms for correlation with identity, device, session context, and other security signals.
- **Endpoint and network telemetry**
  Web access events observed at the endpoint or network level can be compared against the indicator set to support broader detection, investigation, and attribution workflows.
- **Orchestration and response**
  Matches can be used as inputs to orchestration and response workflows, enabling consistent handling in accordance with organizational policies and procedures.

Value scenarios

- **Early detection**
  Identifies access to high-risk domains and URLs at DNS or web layer before threats execute.
- **Intelligence enrichment**
  Adds high-confidence web indicators to strengthen existing security telemetry.
- **Correlation**
  Enables linking web activity with other signals for higher-confidence detections.
- **Policy-driven response**
  Integrates with existing controls to support automated blocking, alerting, or escalation.
- **Easy integration**
  Fits seamlessly into existing security tools with minimal effort and overhead