NETCLEAN **PROACTIVE** CLOUD

CYBERSECURITY WHITEPAPER

NetClean ProActive Threat Detection for Endpoints

www.netclean.com

NetClean.

Table of contents

Introduction

ProActive Detection Services – Threat Detection for Endpoints is a specialized solution within the NetClean ProActive Cloud platform. This white paper focuses exclusively on the Threat Detection for Endpoints service, which is part of the broader Detection Services offering. It provides organizations with services/tools to proactively identify and respond to high-risk behaviours that may indicate misuse of IT resources, policy violations, or potential criminal activity, without compromising user privacy or operational integrity.

NetClean is committed to delivering a secure solution by adhering to robust internal information security policies and embedding security by design as part of the development process. In addition, there are rigorous verification and validation measures, such as external penetration testing, in place ensuring the product meets industry standards and internal security benchmarks.

This whitepaper provides a comprehensive overview of the solution's architecture, data processing practices, and security posture. It supports customers in completing Data Protection Impact Assessments (DPIAs), evaluating security controls, and making informed procurement decisions.

Intended audience

The intended audience are CISOs, IT Security Teams and Procurement Officers.

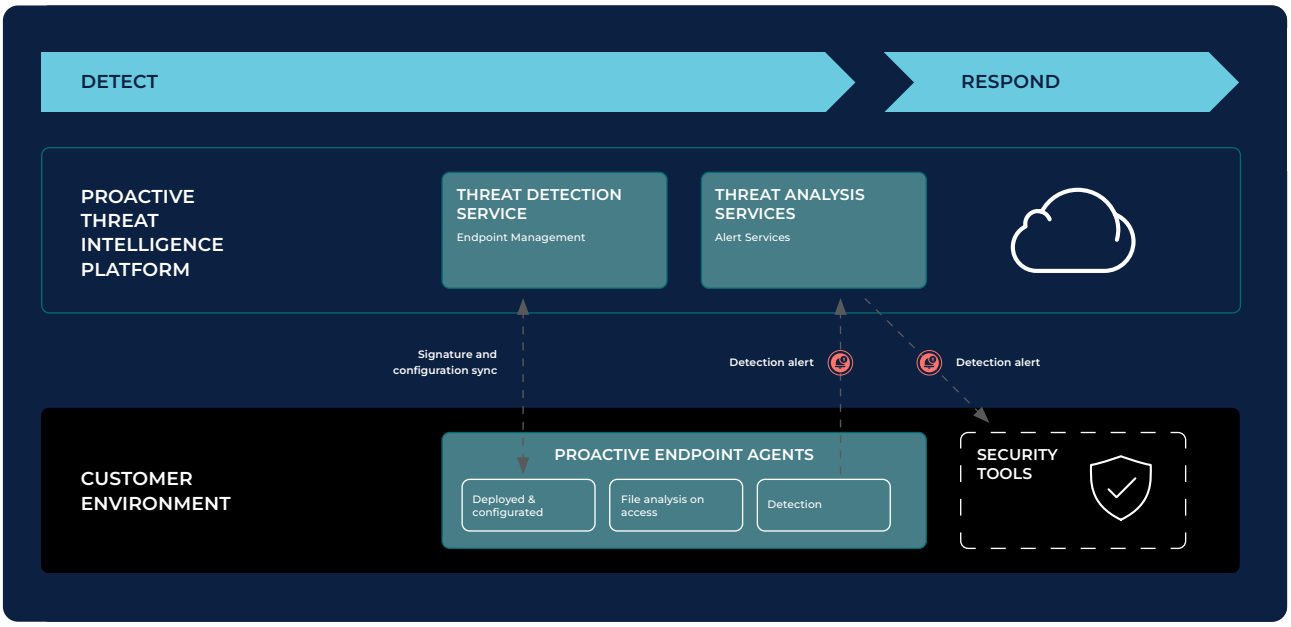
1. Threat Detection for Endpoints Overview

ProActive Threat Detection for Endpoints is a human insider risk detection service that identifies high-risk behaviours within organizations. It continuously monitors endpoints, detecting images and videos that law enforcement has classified as child sexual abuse material (CSAM). ProActive Threat Detection for Endpoints consists of three integrated components:

1. **ProActive Endpoint Agents**
   Lightweight agents for Windows, Mac, and Linux devices. They perform real-time, on-access file scanning using a local signature database and operate online and offline with queued alerting.

2. **Agent Management**
   A cloud-based control layer for agent configuration, signature updates, and lifecycle management.

3. **Alert Management**
   Forwarding service to customer configured system. Secure delivery of detection alerts to customer systems via webhook. No CSAM content is stored; only metadata and alert context are processed.



The SaaS platform is deployed in Azure with the agents deployed on site at the customers.

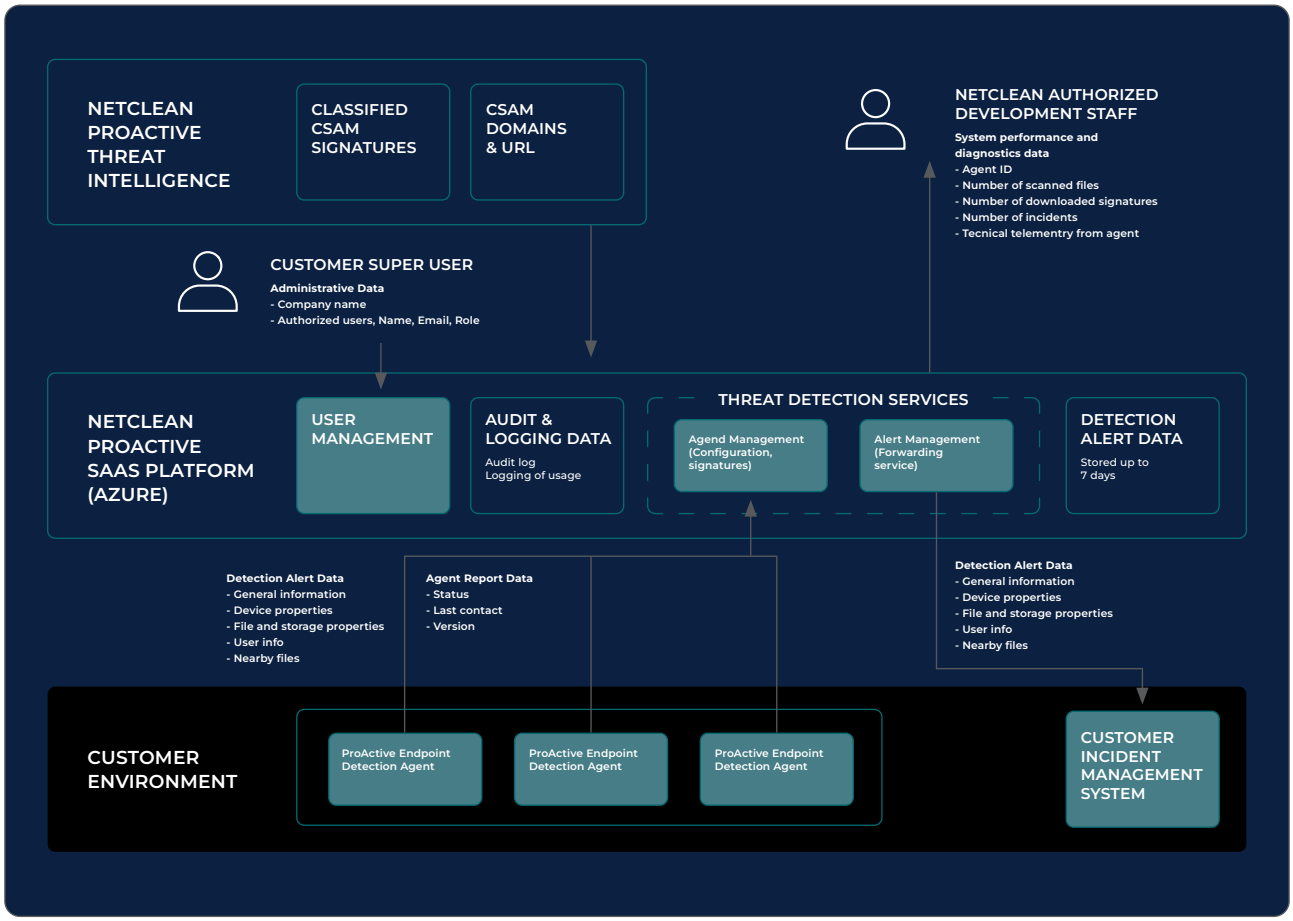
1.1 No CSAM content stored in the system

The system is designed to detect and manage Child Sexual Abuse Material (CSAM) based on the files signatures (uniquely identified hash values of the files) only. It never saves, stores or displays any CSAM images or videos, thus aligning with ethical and regulatory standards.

2. Data Flow

2.1. Description

This diagram shows the data being submitted to the system, exported from the system and handled between the different components of the system.



A system owner user with user administrative permissions can add/remove users to their own system and adjust their roles.

The Proactive Endpoint Agent regularly reports metadata, such as device properties and logged on users, to the server about itself and the environment where it is installed. This is used for maintenance and health checks.

In the event of a detection alert, detection data is also shared.

2.2. Exported data

- **Detection Alerts**
  If there is an detection alert, device properties, file and storage properties, logged on users and detection data is sent to the customer defined solution via a webhook.

- **Statistics**
  Telemetry data is collected for analysis and system maintenance. Note that no personal data is available in this data.

2.3. Personal data

Personal data handled by the system consists of information collected by the agent. This includes logged on user.

The system also stores username and email of the administrators of the system.

3. Data types

Administrative Data

The system stores company name and name and email address of users from the customer with access to the system.

Agent Report Data

General information

- Agent ID
- Identifier for the customer organization

Device properties

- Machine name, IP address, MAC address
- Windows localization, language and region settings

User info

- Logged-On Users and type of logon (locally and remotely)

Agent

- State
- Metrics
- Event History

Detection Alert Data

General information

- Identifier for the customer organization
- Agent ID

Device properties

- Machine name, IP address, MAC address
- Windows localization, language and region settings

User info

- Logged-On Users and type of logon (locally and remotely)

Detection data

- Timestamp
- Hash Type
- Detection Method
- Hash Source
- Accessing Processes

File and storage properties

- File name, path, owner, size and timestamps.
- The file's MD5 and SHA1 values
- Disk type and storage information

Nearby files

- File names and hash value for other files in the same folder as the file that triggered the alert

Audit and Logging Data

- Functionality accessed
- Logged on user
- Changes made

System Performance and diagnostics Data

- Agent ID
- Number of scanned files
- Number of downloaded signatures
- Number of Detection Alerts
- Technical Telemetry from Agent

4. Logging capabilities

The cloud service logs all activities such as user access and API requests in an audit log. For agent requests this includes tenant id and agent id.

Agent metadata is logged for statistical purposes, together with system performance data such as number of scanned files, number of alerts, amount of data.

5. Data Retention and Lifecycle Management

NetClean applies strict data retention policies to ensure that operational, administrative, and diagnostic data is handled securely and in accordance with legal and regulatory requirements.

Data type	Retention period	Notes
Agent Report Data	90 days	Used for troubleshooting and performance monitoring
Detection Alert Data	Up to 7 days	Removed upon confirmation of receipt by customer system or after 7 days if undelivered.
Audit and Logging Data	As long as required for purpose or legal obligations	Follows Swedish Data Protection Authority guidelines.
Administrative Data (Customer Company Data)	As long as required for purpose or legal obligations	Follows Swedish Data Protection Authority guidelines.
System Performance and Diagnostics	Until no longer deemed of value	Periodically reviewed and securely deleted when no longer needed.

These retention practices are designed to minimize data exposure, support compliance, and ensure that the ProActive Cloud platform operates efficiently and securely throughout its lifecycle.

6. Security Architecture

6.1. Overview

ProActive Threat Detection for Endpoints is built with a security-first mindset, ensuring that customer environments are protected through a layered and robust architecture. The platform's design reflects industry best practices and expectations, with a strong emphasis on data isolation, secure communications, access control, and transparency.

- **Multi-tenancy with strict logical separation:** Each customer operates within a logically isolated environment, ensuring that data and configurations are never shared or exposed across tenants. This separation is enforced at both the application and infrastructure layers.

- **Mutual TLS (mTLS) for agent authentication:** All communication between endpoint agents and the platform is secured using mutual TLS, providing strong cryptographic assurance of identity and preventing unauthorized access or data interception.

- **Role-based access control (RBAC) and audit logging:** Access to platform features and data is governed by fine-grained RBAC policies. Every action is logged, enabling full traceability and supporting forensic investigations, compliance audits, and internal governance.

- **Encryption at rest and in transit:** All sensitive data is encrypted using industry-standard algorithms, both when stored and during transmission. This protects against data breaches and ensures confidentiality even in the event of infrastructure compromise.

6.2. Key security principles

The solution has been designed and implemented in line with well-established security principles to ensure robust protection of data, systems, and users. The following principles have guided the architecture and development:

- **Zero Trust:** All access is continuously verified. No user, device, or system is inherently trusted, whether inside or outside the network. Authentication and authorization are enforced at every stage.

- **Least Privilege:** Users, applications, and services are granted only the minimum level of access required to perform their tasks, reducing the risk of misuse or exploitation.

- **Defense in Depth:** Multiple layers of security controls are implemented across the environment, ensuring that if one layer is compromised, others continue to protect critical assets.

- **Data Minimization:** Only the data strictly necessary for the solution's purpose is collected, stored, and processed. This reduces exposure in the event of a breach and aligns with data protection best practices.

- **Audit Trail:** Comprehensive logging of requests and API calls are in place to provide audit logging of activities performed on the system.

- **Centralized Identity:** A unified identity and access management system is used to streamline authentication, strengthen security policies, and simplify user lifecycle management across the solution.

6.3. External verification

Penetration Testing

To ensure the resilience of ProActive Threat Detection for endpoints against real-world threats, the platform undergoes regular and rigorous security testing. As part of this commitment, a full white-box penetration test was conducted, covering both the SaaS platform and agent endpoints.

The white-box approach provided testers with full access to source code, architecture documentation, and system configurations, enabling a deep and thorough assessment of potential vulnerabilities. This method ensures that even subtle or complex security flaws can be identified and addressed.

The penetration test was conducted by an independent, certified security firm, ensuring objectivity and adherence to industry standards.

Azure Cloud Security Review

To validate the security posture of its cloud infrastructure, NetClean commissioned an independent, certified security firm to perform a comprehensive review of its Azure resources. This external assessment ensures objectivity and alignment with industry best practices for secure cloud operations.

The review encompassed key areas of Azure security, including:

- **Identity and Access Management (IAM):** Evaluating role assignments, privilege boundaries, and authentication mechanisms.
- **Network Protection:** Assessing firewall rules, virtual network segmentation, and exposure of public endpoints.
- **Data Security:** Reviewing encryption configurations, access controls, and secure storage practices.
- **Monitoring and Threat Detection:** Verifying logging, alerting, and integration with security operations for proactive threat response.
- **Compliance and Governance:** Ensuring adherence to regulatory requirements through Azure Policy, resource tagging, and audit capabilities.
- **Disaster Recovery and Business Continuity:** Confirming backup strategies, failover readiness, and recovery procedures.

Outcome of the external Penetration Testing and Security Review

- **Critical vulnerabilities** were identified and immediately patched, demonstrating NetClean's rapid response capability and commitment to secure operations.
- **Remaining findings**, which were classified as non-critical or requiring architectural consideration, are currently under active implementation or review. These items are tracked through the internal security backlog and prioritized based on risk and impact.

7. System Lifecycle Management Security

NetClean ProActive Threat Detection for Endpoints is developed, deployed, and maintained with a comprehensive approach to system lifecycle security. This ensures that security is not a one-time effort, but an ongoing commitment embedded in every phase of the platform's existence.

1. Secure Development Practices

- Security by Design: Security requirements are integrated from the earliest stages of system design.
- Code Reviews and Static Analysis: All code undergoes peer review and automated security scanning to detect vulnerabilities early.

2. Secure Deployment

- Infrastructure as Code (IaC): Deployment is automated and version-controlled, reducing human error and ensuring consistency.
- Environment Hardening: Production environments are hardened according to best practices.
- Secrets Management: Sensitive credentials are stored securely using vault solutions and never hardcoded.

3. Operational Security

- Patch Management: Regular updates and security patches are applied to all components.
- Vulnerability Scanning: All 3rd party components are being monitored continuously for vulnerabilities with alerts integrated into the product development processes.
- Incident Response: A documented and tested incident response plan ensures rapid containment and recovery.

4. End-of-Life and Decommissioning

- Data Sanitization: When systems are retired, all customer data is securely wiped using certified methods.
- Component Retirement: Deprecated components are removed from the codebase and infrastructure to reduce attack surface.
- Customer Notification: Customers are informed of major lifecycle changes that may impact their environments.

8. Contact and Support

For technical details, security documentation, or DPIA support, please contact your NetClean account representative.