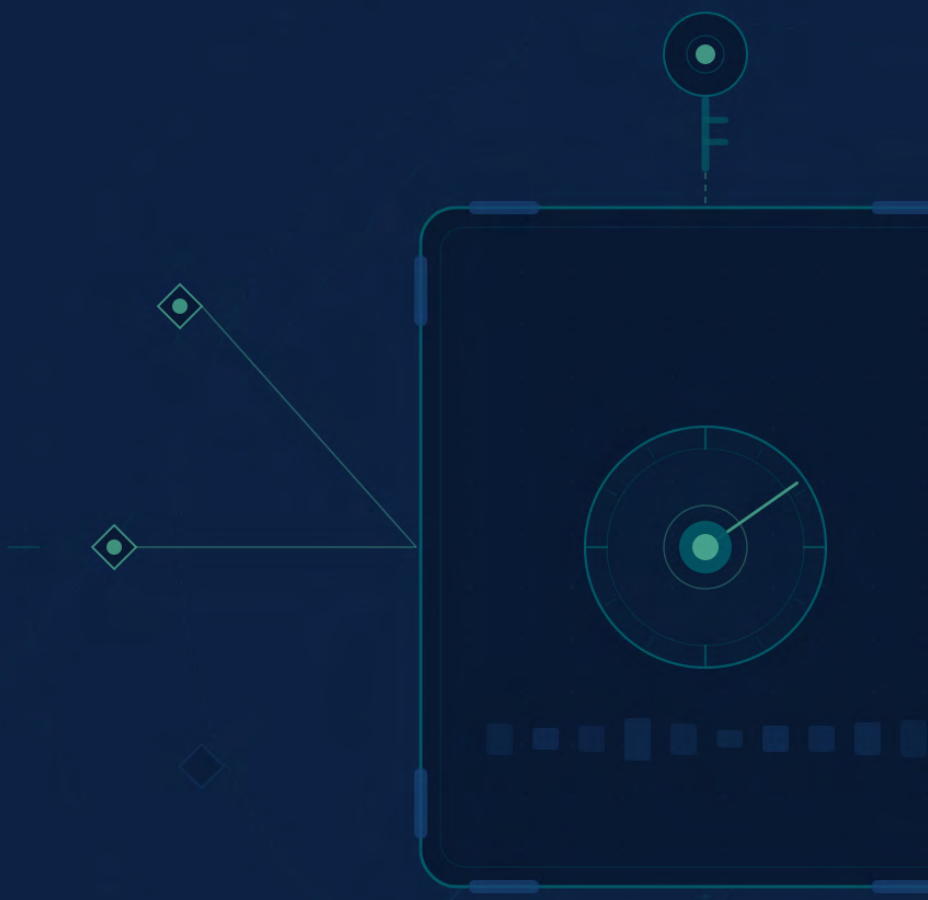
NETCLEAN **PROACTIVE** CLOUD

SERVICE OVERVIEW

Alert Vault



www.netclean.com

NetClean.

Table of contents

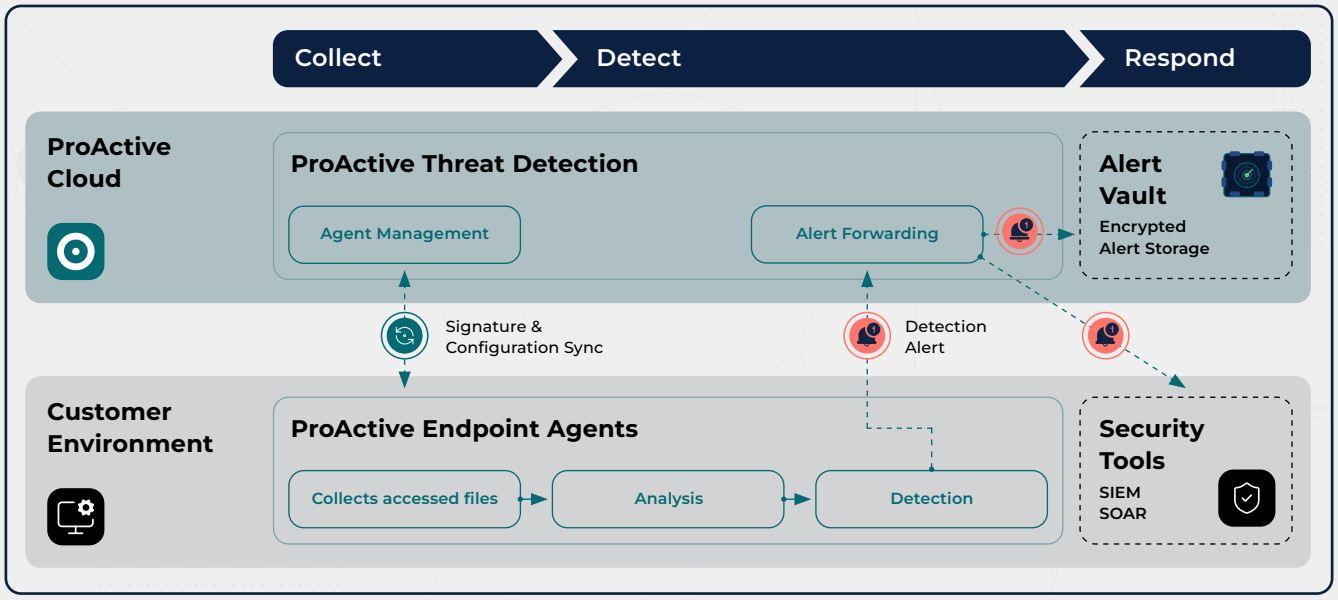
Introduction

ProActive Alert Vault is a secure, encrypted storage module available on the ProActive Cloud Threat Intelligence Platform for Human Insider Risk. It is designed as a platform-level capability — built to receive and store detection alerts from ProActive services, with the ambition to grow as the platform expands. Today, Alert Vault is used with the File Threat Detection for Endpoints service.

Alert Vault addresses a fundamental challenge: detection alerts for high-risk insider threats are sensitive by nature — often legally consequential and subject to strict access controls. General-purpose security tools such as SIEMs, SOARs, and MDR platforms are not designed to hold this kind of data. Alert Vault provides a dedicated, organization-controlled storage layer where alert data is kept encrypted, accessible only to authorized personnel, and entirely outside NetClean's reach.

The module complements — rather than replaces — existing alert forwarding. Organizations can run Alert Vault alongside webhook-based forwarding, or use it as a standalone storage surface where no forwarding target exists.

How it works



Respond: Acting on threats

Alert Vault supports the respond phase of the threat detection lifecycle. Once a detection alert has been generated and delivered, Alert Vault gives authorized personnel a controlled environment to assess the alert and decide how to proceed.

Initial assessment Authorized users log in to Alert Vault using a personal vault password. Alerts are presented in a three-level structure — endpoint, indicator, and detection event — giving responders a clear overview of what was detected, where, and when. This structure supports triage: understanding the scope of activity before deciding on next steps.

Two paths forward From Alert Vault, responders can proceed in two ways depending on their organization's setup and the nature of the incident.

Organizations with webhook-based alert forwarding already in place can use that channel to trigger workflows, playbooks, or case management processes in their existing security tools. The webhook carries the data needed for automation — while the full, sensitive alert record remains in the vault under the organization's own encryption.

For organizations handling investigations more discretely, or where the incident requires careful evidence handling outside standard security tooling, Alert Vault supports CSV export of key alert data. This allows responders to extract what is needed for a deeper investigation — sharing only what is relevant, with the people who need it, through channels the organization controls.

What Alert Vault does not replace Alert Vault is a storage and assessment surface, not an investigation or case management system. It does not replace existing IR workflows, legal processes, or HR procedures. Organizations are expected to bring their own processes — Alert Vault provides the controlled data layer that supports them.

How to set up the service

Setup is completed by a System Owner in ProActive Cloud and typically takes less than an hour. It involves activating the module, creating the vault password and encryption key, configuring alert notifications, and inviting users.

Full setup instructions, encryption management guidance, and user administration are documented in the ProActive Help Centre.

Ongoing management

Alert Vault requires minimal ongoing management. Authorized users receive email notifications when new alerts arrive and log in to review them as needed.

There are no automatic retention rules — organizations define and apply their own data retention policy in line with applicable legal requirements and internal data governance practices. Guidance on data retention considerations is available in the ProActive Help Centre.

If vault passwords are lost or users need to be added or removed, System Owners manage this directly in vault settings. At least two System Owners with active vault access is recommended at all times.

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

- **Insider risk and incident response teams**
  Alert Vault is designed for the teams that handle sensitive, human-centric incidents. It gives authorized investigators access to full alert detail in a controlled environment — separate from general security infrastructure — supporting careful evidence handling and coordination with HR or legal functions.
- **Organizations with strict data governance requirements**
  The HYOK encryption model ensures that alert data is encrypted with a key the organization owns and controls. NetClean cannot access, read, or decrypt stored alert data at any point. This makes Alert Vault suitable for organizations subject to strict internal policies or legal frameworks governing where sensitive data may be stored and who may access it.
- **Organizations using webhook-based alert forwarding**
  For organizations already forwarding alerts to a SIEM or security operations platform, Alert Vault adds a complementary layer. Webhook carries what is needed for automation and workflow triggers. Alert Vault holds the complete record — creating a split-purpose architecture where sensitive data never enters general security tooling.
- **Organizations without an existing forwarding target**
  For organizations that have deployed File Threat Detection for Endpoints but do not have a security tool configured to receive webhook alerts, Alert Vault provides a standalone storage and review surface — ensuring no alert data is lost and authorized personnel can always access it.