
pennAware
Threat
Sharing

# Threat Sharing

ONE SAFE, ALL SAFE

GLOBAL DATA NETWORK

NETWORKED VIGILANCE

Pennaware's Threat Sharing technology enables community members to expand their threat intelligence reach by leveraging the collective network knowledge, reducing costs and accelerating implementation.

Built to extend the capability and effectiveness of our Incident Response platform, our Threat Sharing technology acts as an early warning network for all participants. There are three sources of threat sharing data.

## PENNAWARE INCIDENT RESPONSE PLATFORM

Our Pennaware IRP is deployed at each node of the network providing inbox level incident reporting, investigation and response giving users maximum agility and reducing response time.

After finding any instances of an attack PennAware IRP will now automatically share this intelligence to the rest of the community triggering investigations throughout the network.

Thanks to Threat Sharing, PennAware customers don't need to directly experience a malicious attack to initiate inbox investigations and close down attacks anymore, delivering even faster response times and proactive protection.

## PEER-TO-PEER THREAT SHARING

In addition to data from the PennAware IRP each organisation within the community can create a trust and reputation-based relationship with any other organisation on a decentralised, peer-to-peer basis using the Pennaware Threat Sharing APIs.

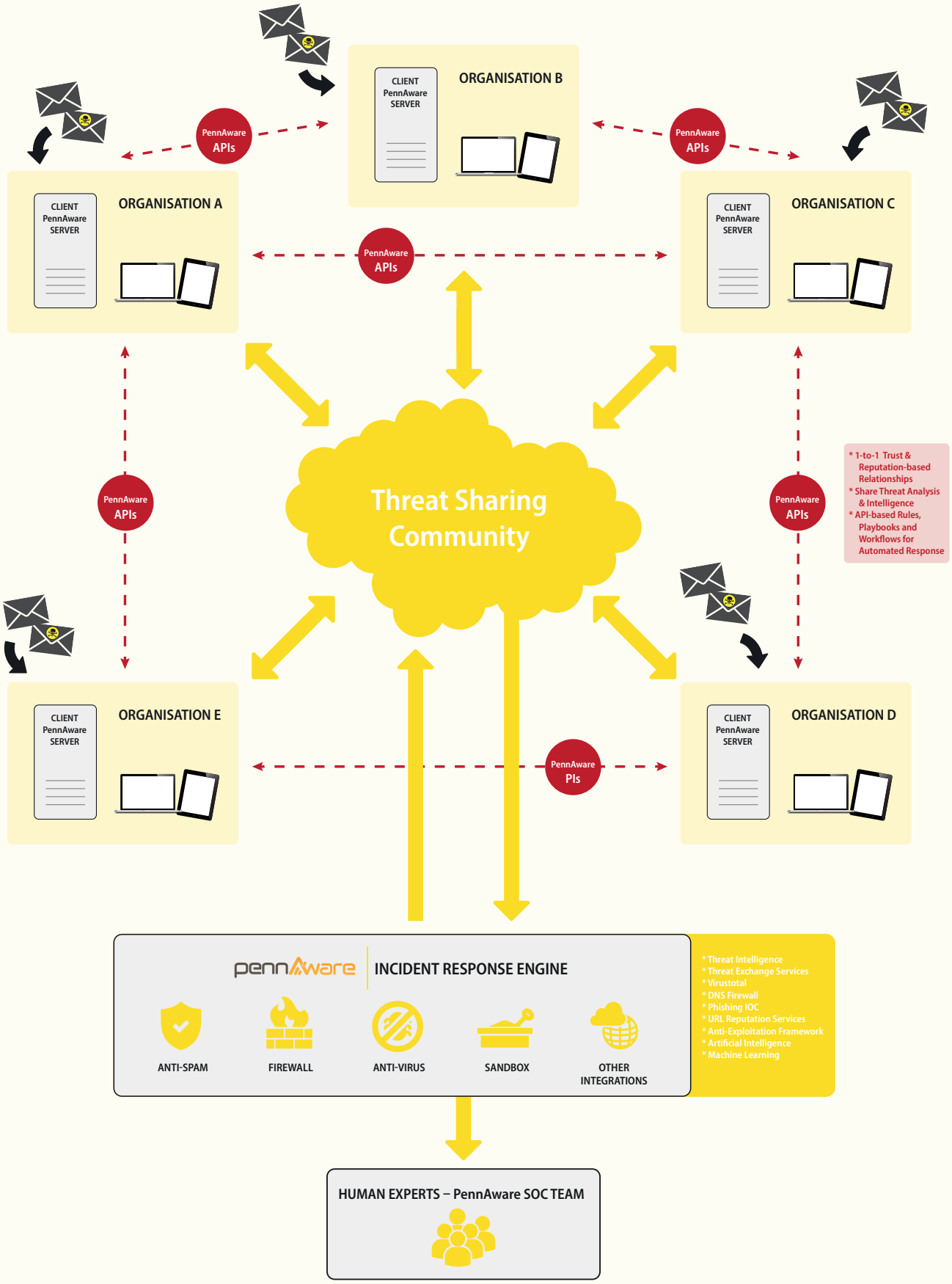
Rules, Workflows and Playbooks are defined on a case by case basis to control how the intelligence from the partner organisation are actioned. High trust relationships can be automated, connections with lower trust scores can require independent verification of the threat analysis before taking action.

## 3RD PARTY INTELLIGENCE SOURCES

Another feature of our Threat Sharing APIs is the ability for any member of the network to share threat intelligence obtained via their other cybersecurity products and services.

For example, using the same peer-to-peer architecture described previously, one organisation using a certain sandbox product can share threat analysis data with another organisation who may be using a different sandbox technology.

This cross referencing provides a greater detection probability of malicious attacks.


CLIENT PennAware SERVER
ORGANISATION B
PennAware APIs
CLIENT PennAware SERVER
ORGANISATION A
PennAware APIs
CLIENT PennAware SERVER
ORGANISATION C
Threat Sharing Community
PennAware APIs
PennAware APIs
* 1-to-1 Trust & Reputation-based Relationships
* Share Threat Analysis & Intelligence
* API-based Rules, Playbooks and Workflows for Automated Response
CLIENT PennAware SERVER
ORGANISATION E
PennAware PIs
CLIENT PennAware SERVER
ORGANISATION D
pennAware INCIDENT RESPONSE ENGINE
ANTI-SPAM
FIREWALL
ANTI-VIRUS
SANDBOX
OTHER INTEGRATIONS
* Threat Intelligence
* Threat Exchange Services
* Virustotal
* DNS Firewall
* Phishing IOC
* URL Reputation Services
* Anti-Exploitation Framework
* Artificial Intelligence
* Machine Learning
HUMAN EXPERTS – PennAware SOC TEAM

Powered by keepnet LABS

pennAware

www.pennaware.com