POSITIVE TECHNOLOGIES

PT Network Attack Discovery

Makes hidden threats visible

BENEFITS

Detects malicious activity in east-west traffic

Keeps attacks private
Information on attacks and aftermath is not transmitted to the outside

Detects even modified malware

Provides faster protection from zero-day vulnerabilities in Microsoft's products

HOW IS YOUR COMPANY BEING ATTACKED?

Check your network and perimeter. Request a free PT NAD trial on our website:

PT Network Attack Discovery is a deep network traffic analysis system that detects attacks on the perimeter and inside the network. The system makes hidden threats visible, detects suspicious activity even in encrypted traffic, and helps investigate incidents.

Get the full view

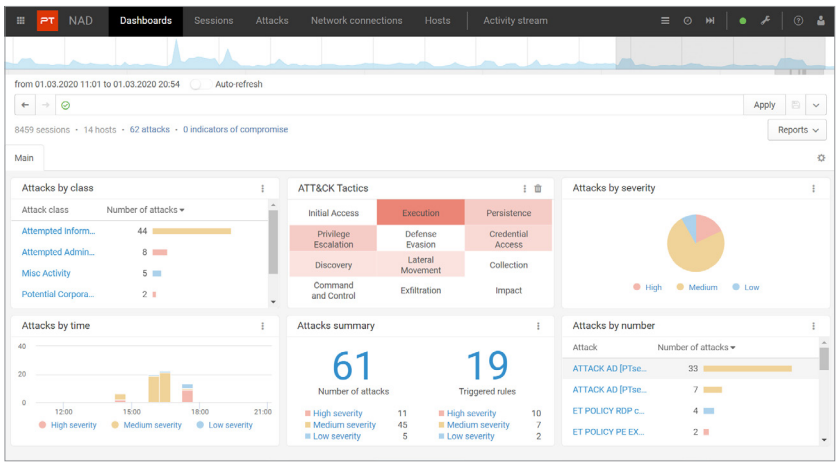
PT NAD identifies over 85 protocols and parses the 30 most common ones up to and including the L7 level. This provides a complete picture of what is going on in the infrastructure and helps identify security flaws that can enable attacks.

Detect hidden threats

The system automatically detects attacker attempts to penetrate the network and identifies hacker presence on infrastructure based on multiple indicators, including use of hacker tools and transmission of data to attackers' servers.

Make SOCs more effective

PT NAD provides security operations centers with full network visibility. They can easily verify whether an attack was successful, reconstruct the kill chain, and gather evidence. To do this, PT NAD stores metadata and raw traffic, helps quickly find sessions and identify suspicious ones, and supports exporting and importing traffic.



The dashboard helps security specialists to investigate and quickly react to suspicious activity

PT NAD DETECTS:

- Threats in encrypted traffic
- Use of hacker tools
- Lateral movement
- Network anomalies
- Exploitation of network vulnerabilities
- Malware activity
- Signs of previously unnoticed attacks
- Attempts to hide activity from security tools
- Connections to automatically generated domains
- Non-compliance with security policies

Usage scenarios

Monitoring of policy compliance

PT NAD detects misconfigurations and instances of security policy non-compliance that can pave the way for attackers. Examples include credentials stored in cleartext, weak passwords, remote access utilities, and tools that hide network activity.

Detection of attacks on the perimeter and in the network

Thanks to embedded advanced analytics, unique threat detection rules, indicators of compromise, and retrospective analysis, PT NAD detects attacks both at the earliest stages and after attackers have already penetrated infrastructure.

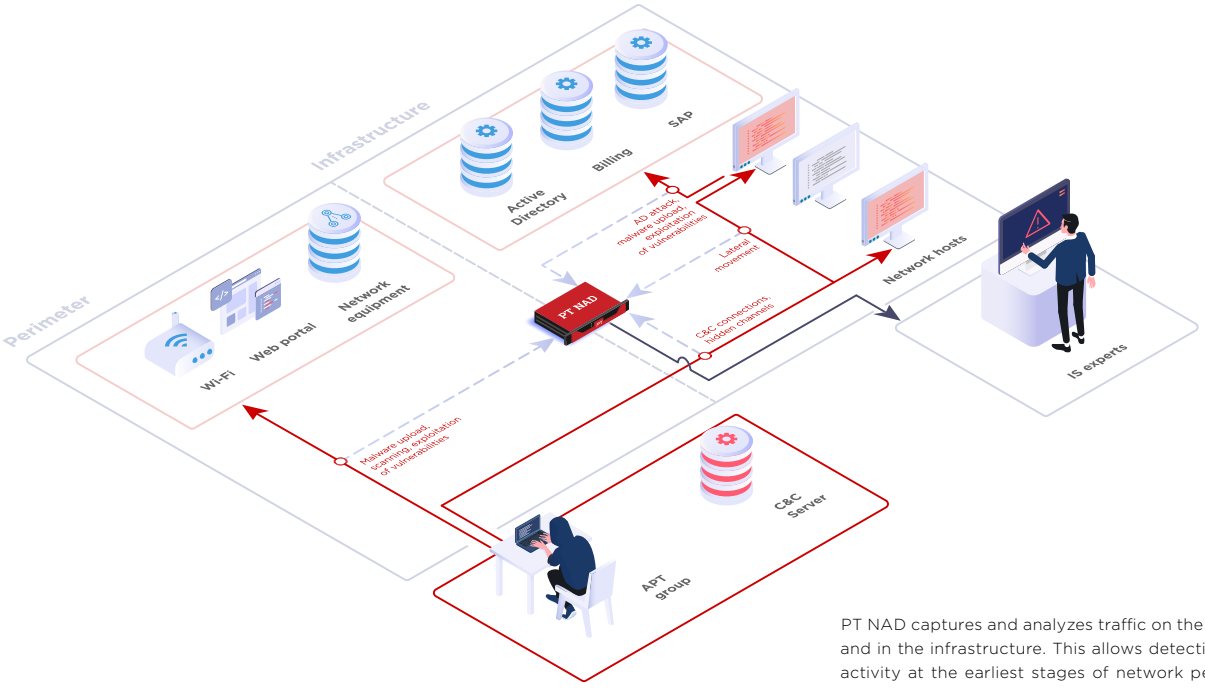
Investigation of attacks

With PT NAD, investigation experts can localize an attack, trace kill chain, detect vulnerabilities in infrastructure, and implement countermeasures to prevent future incidents.

Threat hunting

PT NAD is great for threat hunting. Companies can test hypotheses about their state of security and detect the hidden threats that slip by ordinary cybersecurity solutions.

How it works



PT NAD captures and analyzes traffic on the perimeter and in the infrastructure. This allows detecting hacker activity at the earliest stages of network penetration, as well as when intruders attempt to get a foothold in the network and pursue their attack.