Network Threat Hunting

Expose hidden threats before they trigger alerts

packet watch

Challenges Addressed

Most tools in a cybersecurity stack are reactive. They wait until they detect a malicious activity—then they trigger an alert.

Very few security tools focus on the network. But it's here that threat actors hide out, infiltrate systems, and collect information on how they should proceed. It may be months before they're detected.

If your endpoint security successfully detects an attack, the event may not be significant enough to break through the noise and warn the security operations team that there is a larger-scale threat learning, looming, and gathering momentum.

Our Approach

Our Network Threat Hunting platform sees everything—every packet that travels on your network is captured and stored for threat hunters to "rewind" and investigate when something doesn't look quite right.

Assisted by machine learning (ML) and artificial intelligence (AI) insights, human threat hunters can create sophisticated hypothesis-based hunts. Armed with a hunt lead, they'll craft filters and queries to zero in on only malicious and anomalous network activities.

Once your team starts thinking proactively, the use cases for this approach seem endless. Threat actors don't sit still for long. When they move or call back home, they won't be hidden anymore.

Visit www.packetwatch.com for an extensive list of use cases and platform features to help your team expose hidden threats before they trigger alerts in your conventional detection systems.

Benefits

- Change your vantage point and enable your team to think proactively
- See everything happening on your network with Full Packet Capture
- Get threat hunting help from our experts, or let us be your dedicated threat hunter
- See your network like never before—including hard-to-manage IoT and OT devices
- Integrates with CrowdStrike Falcon® for device telemetry and containment
- Built by threat hunters for threat hunters

> **"Adding PacketWatch to our existing environment is an absolute upgrade. We now have incredible visibility."**

Get Started

Contact sales@packetwatch.com for a demonstration, pricing, and help choosing a package.

Fully Managed

Complete Managed Service

- SaaS Platform Access Available
- Fully Managed Threat Hunting
- Dedicated Security Analyst
- 24/7 Monitoring and Response
- Bi-Weekly Meetings
- Quarterly Executive Reviews

Co-Managed

Shared Responsibility

- SaaS Platform Access, Coaching
- Collaborative Threat Hunting
- Dedicated Security Analyst
- Onboarding
- Advanced Training
- Priority Support

Self-Managed

Full Platform Control

- Complete SaaS Platform Access
- Self-service Deployment
- Standard Documentation
- Basic Training
- Standard Support
- Premium Services Available