packet watch

PacketWatch MDR

Managed Detection & Response

Uncover Malicious Activity

Expose Misconfigured Devices

Identify Vulnerable Assets

Reveal Policy Violations

Increase Network Visibility

Detecting What Others May Miss

Are you worried that your current cybersecurity investments aren't 100% effective at protecting your network? Your hunch is probably right.

Traditional cybersecurity technologies, managed internally or by a MSSP, are valuable components of a cybersecurity strategy, but the protection they offer is limited in scope and visibility. The challenge with these conventional tools is that they may not protect you from "unknown" (zero-day) threats or monitor every asset, activity, and employee on your network. In order to detect unknown threats, you will need to begin proactive threat hunting with specially-designed tools, processes and training.

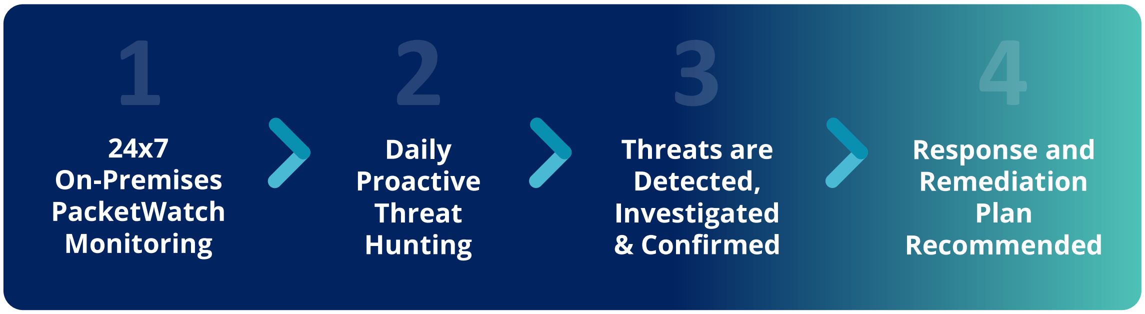
Threat Hunting with PacketWatch MDR

PacketWatch Managed Detection and Response is an expert threat hunting service delivered with our proprietary, on-premises PacketWatch^{SM} network monitoring, analysis and investigation platform. The platform incorporates full-packet-capture network monitoring, multiple intrusion detection systems (IDS), several threat intelligence feeds, big data analytics, high-speed search and robust machine learning to detect known and unknown threats and provide total network visibility.

The PacketWatch platform provides our security operations team with the tools they need to proactively and continuously monitor your network and execute daily threat hunting activities. When threats are detected, investigated and found to be credible, your assigned security consultant will contact you to discuss the details of the threat and recommend a course of action for remediation.

The affordable, monthly subscription service provides 24x7 concierge support, dashboards, monthly reporting and peace of mind. PacketWatch Advisory Services are available for clients that need additional help with professional incident response, vulnerability management, or digital investigation and forensic services.

How PacketWatch MDR Works



1 24x7 On-Premises PacketWatch Monitoring

2 Daily Proactive Threat Hunting

3 Threats are Detected, Investigated & Confirmed

4 Response and Remediation Plan Recommended

PacketWatch Managed Detection & Response

Responsive Expertise

PacketWatch Managed Detection and Response is designed to quickly and efficiently identify and verify anomalous and malicious activities on your network. Different from other security services, PacketWatch MDR is human-based. Your threats will be detected, investigated, and confirmed by the PacketWatch team; and communicated to you via a live, personal phone call. With PacketWatch MDR, you will immediately strengthen your team with cybersecurity experts, proven threat hunting processes, and powerful tools focused on reducing your security risk and responding quickly to known and unknown threats lurking within your network.

We are a boutique information security consultancy that prides itself on delivering responsive 24x7 concierge-level support and the peace of mind that someone cares as much about your network and security as you do. PacketWatch MDR is easy to implement. We do not require endpoint agents, deploy network probes, or send your data to the cloud. Our appliance is passive; and installed on-premises, so your network data and intellectual property stay within your organization.

We are confident that we will continuously find noisy, rogue or malicious activity on your network, but if you are not satisfied with our PacketWatch MDR service, you can cancel without penalty after the initial 30-day assessment.

Expert Threat Hunting

Global Threat Intelligence

Full Packet Capture

Network Traffic Replay

Dashboards & Reporting

24x7 Concierge Support

Detection Tools and Processes

PacketWatch was purpose-built by and for expert threat hunters. The on-premises platform imports your network data into a powerful analytics engine that uses proprietary algorithms and machine learning to quickly identify, correlate and triage potential threats. The sophisticated dashboard provides total visibility of your network activities, anomalies and trends. Threat indicators are investigated using a wide array of integrated, industry-leading open-source tools and threat intelligence feeds. Our consultants can even go back in time using packet-level network recordings to research intermittent beacons or historical behaviors of known and unknown advanced persistent threats that often go undetected by point-in-time security tools.

Expert Investigators

Our cybersecurity consultants are expert threat investigators with extensive backgrounds in federal law enforcement, national security agencies, global enterprises, and regulated industries. As experienced investigators, they know what they are looking for—patterns, anomalies, and things that an untrained eye may miss. They are trained to forensically research your threats to eliminate false positives and document their findings with actionable remediation recommendations. Your assigned consultant will continue to support and track your case until you have completed your remediation steps. If you would like us to professionally design and manage your incident response process, ask about our PacketWatch Advisory Services.

PacketWatch Advisory Services

Virtual CISO

Security Program Development

Incident Response Plan Development

Risk Assessment

Digital Investigation & Forensics

Vulnerability Management

Penetration Testing

Education Programs

Call 480-444-7070 or visit www.packetwatch.com for more information.