SERVICES COMPARISON

Managed Detection and Response (MDR)

Everything You Need to Defend Against Security Threats

proarch

SECURITY TEAMS: OVERWHELMED & STRUGGLING TO GET AHEAD

The continuous growth of data, devices, and applications coupled with attackers' complex techniques have left IT and security teams buried in security alerts and unprepared in the event of a breach.

Cybercriminals leave little time to detect threats before damage occurs. Couple that with an unmanageable volume of alerts and possible missed signals from misconfigured and siloed tools, comprehensive security monitoring and response across the attack surface is not optional—it's a requirement.

ONE SOLUTION THAT STOPS THREATS AROUND THE CLOCK

ProArch's Managed Detection and Response (MDR) services are a turnkey solution for threat detection, investigation, containment, and response.

Attackers attempting to penetrate IT/OT environments are identified and stopped by tailored threat detection rules, AI-powered response, and ProArch's Security Operations Center.

Alerting you of malicious activity on your network is no help unless you have the bandwidth and skills to respond. Focus on reducing risk long-term and let ProArch handle 24x7 threat detection and response.

The SOC monitors alerts 24x7x365, remediates threats, and acts as an extension of your team providing guidance and recommendations.

Get coverage across the attack surface with a single solution, avoiding the pain of managing multiple point security solutions and their integrations.

Integrate your point solutions into the SOC to quickly enhance your defenses and make the most of existing investments.

Tailored threat detection rules reduce alerts noise up to 99%. Save time and effort with fewer false positives and focus on remediating critical threats.

Choose from flexible pricing and service options, scale at your own pace, and only pay for what you need.

MDR Services Comparison
Core vs. Premier

MDR Core

MDR Core is a starting point to secure essential layers that every organization should protect; endpoints, identities, and email.

These entry points are critical to business operations and are the most targeted by sophisticated cybercriminals.

MDR Core is the first step to consolidating point solutions, so response is faster and more efficient.

MDR Core is a fit for you if:

- **You need essential threat coverage and response**
- **Your internal security team requires additional support**

MDR Premier

Organizations looking for more granular and specific security measures should go with MDR Premier.

It expands coverage and visibility to cloud apps, cloud workloads, custom sources, and other advanced layers that require advanced skills.

Premier goes beyond Core and includes strategic advisory services and threat hunting for proactive security measures.

MDR Premier is a fit for you if:

- **You rely on external expertise to maintain and mature security**
- **You have complex security and regulatory requirements**

Why ProArch Skips Confusing EDR, IDR, XDR Labels

EDR, IDR, and XDR mean different things depending on the person or vendor you're talking to.

ProArch structures our MDR plans as Core and Premier to make it easier to understand what security coverage is included by focusing on the layers of protection, rather than the specific technologies or products involved.

After using EDR/IDR/XDR conventions for 5+ years we found that the confusion had reached a tipping point.

Core and Premier avoids mis-understanding about what is covered and makes it easy to add on layers when the time is right for your organization.

MDR Services Comparison
Core vs. Premier

	MDR Core	MDR Premier
24/7/365 SECURITY MONITORING & RESPONSE	Included	Included
MONTHLY THREAT HUNTING	-	Included
ENDPOINTS	Included	Included
IDENTITIES	Included	Included
COLLABORATION	Included	Included
SIEM HOSTS & NETWORKS	-	Included
CLOUD APPS	-	Included
CLOUD PLATFORMS	-	Included
OPERATIONAL TECHNOLOGY	-	Included
PROACTIVE INCIDENT RESPONSE	Included	Included
STRATEGIC SECURITY ADVISORY SERVICES	-	Included

MDR Core & Premier Both Include:

- Tailored Threat Intelligence Briefings
- Detection & Automation Rule Management
- Automation & Orchestration Playbooks
- Alert & Incident Management Portal
- Monthly Maintenance & Security Health Check Report

MORE PLAN DETAILS

MDR Services Comparison
What's Covered

Core & Premier

ENDPOINTS

- Servers: Linux, Windows
- Workstations: Linux, Windows, MacOS
- Mobile Devices: iOS, Android

TOOLSET

- Microsoft Defender for Endpoint
- Microsoft Defender for Servers
- CrowdStrike Falcon EDR

Core & Premier

COLLABORATION

- Exchange Online
- Microsoft Teams
- Microsoft SharePoint
- Microsoft OneDrive

TOOLSET

- Microsoft Defender for Office
- Mimecast

Premier

CLOUD APPS

- Microsoft 365 Apps
- Third-party Cloud Apps

TOOLSET

- Microsoft Defender for Cloud Apps

Premier

CUSTOMER SOURCES

- Databases
- Applications
- AI + Machine Learning
- Custom Integrations

TOOLSET

- Microsoft Sentinel

Core & Premier

IDENTITIES

- On-premises Active Directory
- Entra ID (Azure Active Directory)

TOOLSET

- Microsoft Defender for Identity
- CrowdStrike Falcon Identity

Premier

CLOUD INFRASTRUCTURES

- Microsoft Azure
- Amazon Web Services
- Google Cloud Platform

TOOLSET

- Microsoft Defender for Cloud

Premier

SIEM

- Workstations: Linux, Windows
- Network Devices: Firewall, Switches, Routers
- Logs: Web, Cloud, Identity, Security

TOOLSET

- Microsoft Sentinel

Premier

IoT/OT/ICS

- Manufacturing
- Health Care
- Transportation
- Utilities
- Energy
- Retail

TOOLSET

- Microsoft Defender for IOT

MDR Services Comparison
How MDR Works

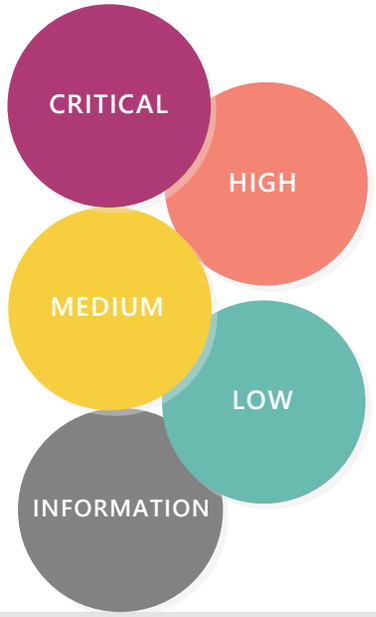
ALERT MONITORING

DATA COLLECTED FROM ACROSS THE ENVIRONMENT

- ENDPOINT
- IDENTITY
- COLLABORATION
- CLOUD
- NETWORK

ADVANCED DETECTION TOOLS

FIND INDICATORS OF COMPROMISE & PRIORITIZE ALERTS



INVESTIGATION & RESPONSE

THREATS ARE STOPPED QUICKLY & EFFICIENTLY

24/7 Security Operations Center

- Alert & Threat Investigation
- Threat Containment & Remediation
- Threat Hunting
- Client Communication & Coordination
- Escalation to Incident Response Team

MDR is monitoring for all the opportunities attackers can leverage to find their way in.

Advanced threat detection tools, including AI-powered automation, collects telemetry from all these points and identifies signals of attacker behavior.

Threat intelligence turns raw data into contextual information that feeds the SIEM platform to surface early detections and prioritize alerts.

Security Orchestration, Automation, and Remediation (SOAR) platform triages alerts through playbooks that resolve threats or escalate to the SOC.

If anything is found, that's when we act to contain the threats quickly and efficiently. Either through automation or the ProArch SOC. Our Security Analysts work with you to coordinate response actions and remediate weaknesses long-term.

proarch

Leverage our skilled SOC team and advanced threat technology to stop attackers in their tracks.

CONTACT PROARCH

WHAT OUR CLIENTS SAY

"We've made a lot of big strides on the security side in the last year, and ProArch has been a big part of that."

- CIO, Healthcare

"ProArch is helping us implement security best practices to stay compliant and ensure our cybersecurity is very locked down."

- Plant Manager, Power & Energy