Managed Detection and Response (MDR)

Services Comparison

Bringing together experienced security professionals, established processes, and advanced threat technology to stop cyber threats.

proarch

Managed Detection and Response (MDR)
Services Comparison

76% of ransomware attacks are executed outside of work hours.[1]

Organizations today are fighting an uphill battle to keep their resources protected against cyber threats. The exploding 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.

Enter ProArch's Managed Detection and Response (MDR) services. Even when your team has gone home for the day, our 24x7 Security Operations Center (SOC) Security Analysts are watching for malicious activity and containing it before compromise or interruption occurs.

With MDR, threat detection sources are collecting and analyzing telemetry while threat intelligence adds context to bring critical alerts to the surface for human intervention. Skilled security professionals then take over to perform threat investigation, containment, and response.

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.

- **100% cloud-native toolset enables rapid deployments in under 24 hours**
- **Expand security coverage to 24 hours a day, 7 days a week**
- **Proactive incident response from a team of threat hunters in your corner**
- **Save on hiring costs for cybersecurity pros and have a predictable security spend**
- **Coverage for Operational Technology (OT) systems**
- **Report and reduce time to detect and time to respond security metrics**
- **Reduce the impact and cost of security incidents**
- **Consultative guidance from SOC and Security teams**
- **Comply with regulatory compliance requirements and avoid fines/penalties**

1 FireEye 2020 Ransomware Deployment Trends

Managed Detection and Response (MDR)
Services Comparison

Endpoint Detection and Response (EDR) keeps threats off devices that are a clear path to corporate resources. EDR is considered next-gen antivirus that prevents attacks across endpoints, including servers, workstations, and mobile devices.

Unlike traditional antivirus software, EDR uses behavioral endpoint sensors that provide insight into malicious activity and automate remediation procedures. If a threat is detected, then ProArch's Security Operations Center (SOC) will intervene and respond. For organizations without 24x7 detection and response capabilities in place, EDR is the perfect place to start.

Identity Detection and Response (IDR) prevents corporate account compromises that lead to data breaches. IDR protects on-premises Active Directory accounts and cloud-native identities against credential-based threats.

Account compromise, specifically Office 365, through email phishing attacks and other intrusion methods have become increasing popular and endpoint security platforms alone can't protect against these attacks. With IDR, Security Analysts stop breaches 24x7 based on suspicious user behavior and risk-based conditional access policies. It is a natural progression for those who already have EDR in place.

Extended Detection and Response (XDR) delivers end-to-end attack prevention across networks, endpoints, and identities. XDR collects and correlates data across corporate resources and unifies them for ultimate insight into threat activity.

XDR enhances threat intelligence security information and event management (SIEM) and security orchestration automation and response (SOAR) functions for a more accurate response to threats. With added telemetry available for Security Analysts in the event of a breach, investigation and remediation workflows can be completed faster or fully automated. This is considered the gold standard of detection and response because it provides end-to-end attack prevention across the organization and a holistic view of security threats.

All MDR Services include:

- 24x7x365 Security Operations Center (SOC) performing threat hunting, investigation, containment, and eradication
- Seamless escalation to ProArch Incident Response Team in the event compromise occurs
- 100% cloud deployment process that takes hours, not weeks
- Quarterly reporting with trending data and recommendations prioritized by risk level
- Access to Security Consulting Team for guidance and questions

Managed Detection and Response (MDR)
Services Comparison

	Endpoint Detection and Response (EDR)	Identity Detection and Response (IDR)	Extended Detection and Response (XDR)
Protection For	Device Centric: Endpoints and Servers	Identity Centric: Cloud and On-Premises Identity	Logging Centric: Endpoints, Identities, Event Logs, and Custom Integrations
What's Covered	Workstations, servers, and mobile devices	On-premises Active Directory accounts and cloud-native identities	On-premises and cloud networks, endpoints, and identities
	Servers: Linux and Windows Workstations: Linux, Windows, MacOS Mobile Devices: iOS and Android	On-premises Active Directory accounts Cloud-native identities	Multi-cloud: Azure, Google, AWS Multi-platform: Windows, Mac, Linux, Android, iOS
Included	24x7 endpoint monitoring and detection performed by ProArch SOC	24x7 identity monitoring and detection performed by ProArch SOC	24x7 endpoint, identity and network monitoring and detection performed by ProArch SOC
	24x7 threat containment and eradication performed by ProArch SOC	24x7 threat containment, eradication, and remediation performed by ProArch SOC	24x7 threat containment, eradication, and remediation performed by ProArch SOC
	SIEM: ingestion and analysis of logs from security toolset	SIEM: ingestion and analysis of logs from security toolset	Advanced SIEM and SOAR and deployment of full log analytics
	Seamless escalation to Incident Response in the event of compromise	**Seamless escalation to Incident Response in the event of compromise**	**Seamless escalation to Incident Response in the event of compromise**
Security Toolset	• Microsoft Defender for Endpoint	• Azure Active Directory Premium P2 • Microsoft Defender for Identity	• Azure Log Analytics • Sentinel SIEM

**XDR requires EDR*

How MDR Works

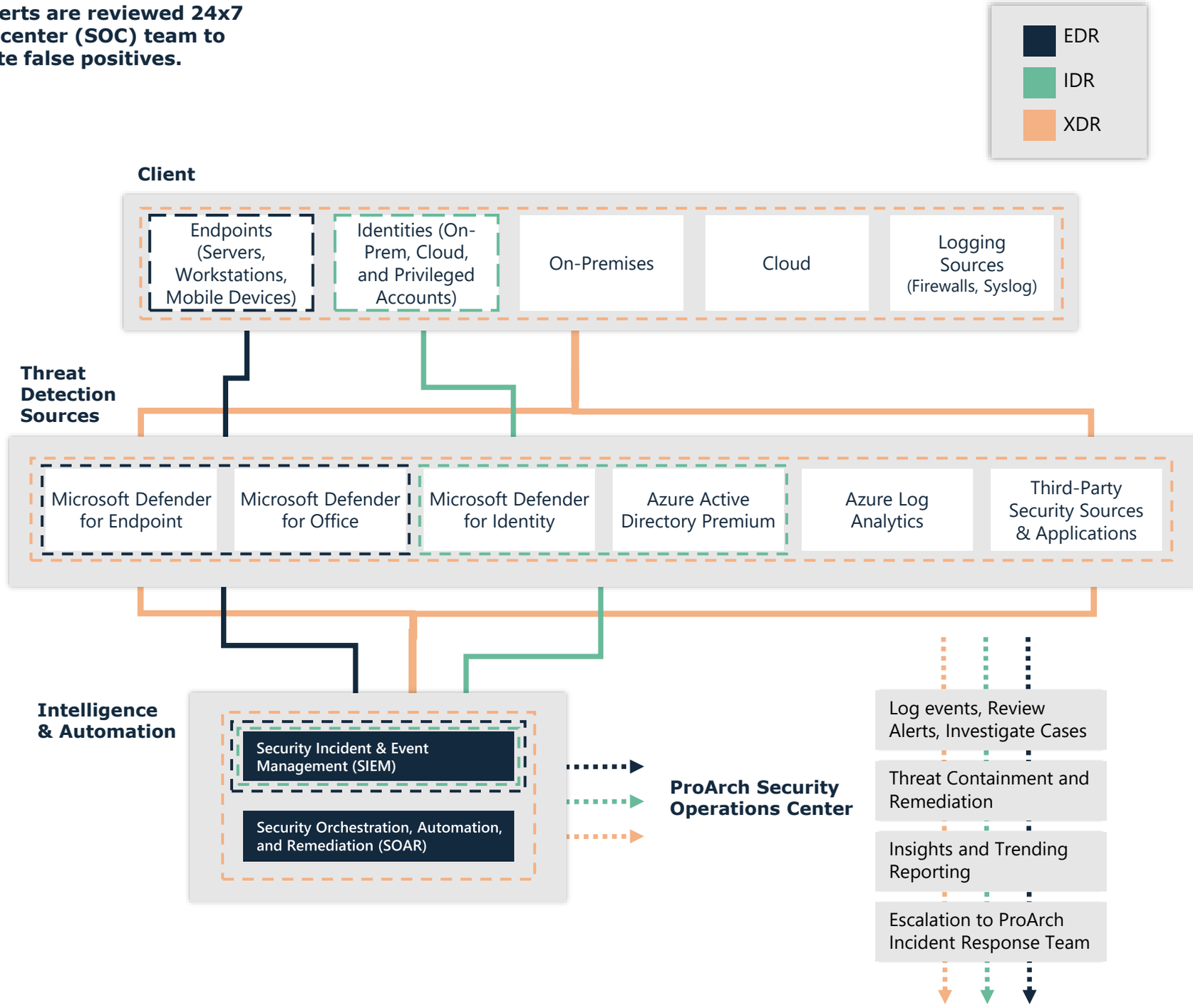
Potential malicious events and alerts are reviewed 24x7 by ProArch's security operations center (SOC) team to confirm compromise and eliminate false positives.

Threat detection sources and sensors are deployed across networks, cloud services, endpoints, and identities collecting and analyzing telemetry- making it possible to track down root cause quickly.

Threat intelligence backed by deep context, customer information, and the MITRE ATT&CK framework enhances alerts to categorize and prioritize.

The ProArch SOC team analyzes cases and performs a thorough threat investigation to confirm indicator of compromise or false positive- 24 hours a day.

Transition to ProArch Incident Response in the event of compromise.




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