THE SYNERGY OF AV, EDR AND MANAGED SOC

Today's sophisticated cyberthreats require a higher level of security expertise and faster incident response than ever before. The combination of an endpoint detection and response (EDR) solution, next-generation antivirus (AV) technology and a managed security operations center (SOC) arms companies with the tools and expertise they need to conquer today's most dangerous cyberthreats.

What are the differences between AV, EDR and MDR?

EDR, AV and a managed SOC are a powerful trio. These solutions bolster cyber resilience by helping companies detect and handle cyberthreats while providing 360-degree visibility into an organization's threat picture and critical tools to speed up incident response.

EDR focuses on detecting and responding to threats at the endpoint level, such as laptops, servers and other computing devices. It employs advanced techniques, like behavioral analysis, machine learning and deep threat intelligence, to catch sophisticated threats that antivirus solutions may miss.

Managed SOC or MDR is a comprehensive security solution that encompasses people, processes and technology to detect, investigate and respond to security incidents across the entire organization. It's like having a dedicated security team monitoring the network and endpoints for any signs of malicious activity.

AV is designed to detect, prevent and remove malicious software, including viruses, worms, Trojans and other types of malware. It works by scanning files and programs for patterns characteristic of known malware and employing various methods to neutralize threats.

AV, EDR and managed SOC: A terrific trio

1. **Comprehensive Threat Detection:** AV provides the first level of protection, EDR detects threats at the endpoint and MDR covers the entire IT infrastructure, such as cloud, networks and various endpoints, ensuring a comprehensive defense against cyberthreats.
2. **Faster Incident Response:** AV conducts automatic quarantine and remediation for threats, while EDR can quickly detect and respond to sophisticated threats with its deep behavioral analysis. Adding managed SOC to the mix provides even faster incident response by correlating threat data from multiple sources and operating 24/7/365.
3. **Improved Threat Intelligence:** EDR and AV can provide valuable threat intelligence to managed SOC services which can help them improve their detection capabilities. For example, if EDR or AV detects a new type of malware, it can immediately send that information to managed SOC analysts, allowing them to update their detection capabilities.
4. **Reduced False Positives:** EDR can help reduce the number false positives generated by managed SOC services by providing more context around alerts. For example, if EDR detects a suspicious file on an endpoint, it can provide additional information about that file to the managed SOC analysts, allowing them to better determine whether it is a true threat or a false positive.
5. **Reduced Tool and Vendor Fatigue:** By leveraging a joint AV, EDR and managed SOC solution, IT professionals simplify their cybersecurity tool stack and reduce the number of disparate security vendors that they must use to stay secure. Not only does this save time and money but also makes the day-to-day workload more efficient for the IT professional.

THE SYNERGY OF AV, EDR AND MANAGED SOC

AV, EDR and managed SOC

EDR, AV and managed SOC are powerhouse technologies that complement each other perfectly and integrate seamlessly together. This winning combination can affordably provide organizations with a better defense-in-depth posture. MSPs can achieve faster incident response, improve threat intelligence and reduce false positives while minimizing tool and vendor fatigue, giving them and their clients the security edge needed in today's dangerous world.

Datto AV: Next-generation antivirus

Datto AV is your first line of protection by catching both known and unknown threats. Through its cloud-based threat intelligence, it consistently updates threat signatures to protect against adversaries.

- Its next-generation AV engine incorporates advanced techniques, like machine learning, heuristic analysis and built-in AI, to protect against threats.
- Automatic quarantine and remediation – Automatically stops and removes threats from your endpoints without user intervention.
- Efficacy meets performance – Top-notch antivirus security without compromising your system's performance.
- Strong self-defense – Anti-tamper technology stops unauthorized modifications to its processes, registry keys and files.

Datto EDR - Endpoint detection made easy

Datto EDR empowers IT teams to detect and respond to advanced threats quickly and efficiently. An easy-to- use cloud-based EDR solution that's purpose-built for managed service providers (MSPs), Datto EDR defends all endpoints — desktops, notebooks and servers — across Windows, macOS and Linux operating systems.

- Patented deep memory analysis ensures that you're informed of even the most elusive threat actors.
- Take action against advanced threats right from your alert dashboard to isolate hosts, terminate processes, delete files and more without wasting precious seconds.
- Alerts are mapped to the MITRE ATT&CK framework to provide context and helpful clarity to your team.
- Includes Ransomware Rollback, which instantly reverts encrypted files to their original state after a ransomware attack, ensuring normal business operations are up and running without loss of time, money or data.

RocketCyber Managed SOC

RocketCyber is a white-labeled managed service that leverages our threat monitoring platform to detect malicious and suspicious activity across three critical attack vectors: endpoint, network and cloud. Our elite team of security veterans hunt, triage and work with your team when actionable threats are discovered, including:

Continuous Monitoring — Round-the-clock protection with real-time threat detection.

World Class Security Stack — 100% purpose-built platform backed by over 50 years of security experience.

Breach Detection — The most advanced detection with to catch attacks that evade traditional defenses.

Threat Hunting — Elite security team proactively hunts for malicious activity.

No Hardware Required — Patent pending cloud-based technology eliminates the need for on-prem hardware.

SCHEDULE A DEMO TODAY!