MANAGED SOC

24/7 Threat Monitoring

Stop advanced threats with Managed SOC managed detection and response solution powered by RocketCyber, the leading security operations center tailored for today's MSP.

COMPREHENSIVE MANAGED DETECTION & RESPONSE

Endpoint Security

Protect your endpoints with Windows, MacOS and Linux event log monitoring, advanced breach detection, malicious files and processes, threat hunting, intrusion detection, third-party next-gen AV integrations and more.

Network Security

Gain new levels of network protection with firewall and edge device log monitoring integrated with real-time threat reputation, DNS information and malicious connection alerts.

Cloud Security

Secure the cloud with Microsoft 365 security event log monitoring, Azure AD monitoring, Microsoft 365 malicious logins and overall Secure Score.

24/7 MANAGED SOC POWERED BY CYBERSECURITY EXPERTS

Managed SOC is a white-labeled managed detection and response service that leverages RocketCyber's Threat Monitoring Platform to detect malicious and suspicious activity across three critical attack vectors: Endpoint, Network and Cloud. Our team of cybersecurity veterans hunt, triage and work with your team when actionable threats are discovered. Services include:

- **Continuous Monitoring** – Round-the-clock protection with real-time advanced threat detection
- **Advanced Security Stack** – 100% purpose-built platform backed by more than 50 years security experience, optimized for managed service providers and their customers
- **Breach Detection** – We catch sophisticated and advanced threats that bypass traditional AV and perimeter security solutions
- **Threat Hunting** – An elite cybersecurity team proactively hunts for malicious activities so you can focus on other pressing matters
- **No Hardware Requirements** – Patent-pending, cloud-based technology eliminates the need for costly and complex on-premise hardware

MANAGED SOC

24/7 Threat Monitoring

MANAGED SOC – KEY FEATURES

We save you time and money by leveraging your existing tools and cybersecurity investments across endpoint, network and cloud. This allows you to focus on what matters most – your business.

SIEMless log monitoring

Monitor, search, alert and report on endpoint, network and cloud threat vectors, including key log data from Windows and MacOS, firewalls, networked devices, Microsoft 365 and Azure AD – all without requiring a SIEM or SIEM hardware.

Threat intelligence and hunting

Real-time threat intelligence monitoring, connecting to premium intel feed partners, gives our customers the largest global repository of threat indicators for our SOC analysts to hunt down attackers and find advanced threats.

Breach detection

Detect adversaries that evade traditional cyber defenses. We identify attacker tactics, techniques and procedures, aligning to the MITRE ATT&CK. This allows our SOC analysts to detect indicators of compromise before damage is done.

Intrusion monitoring

Real-time monitoring of malicious and suspicious activity, identifying indicators such as connections to terrorist nations, unauthorized TCP/UDP services, backdoor connections to command and control servers, lateral movements and privilege escalation.

Next-generation malware

Use your preferred malware prevention or leverage our command and control application for Microsoft Defender, backed up with a secondary line of defense using our malicious detection of files, tools, processes and more.

PSA ticketing

Our SOC analysts investigate each alert, triaging them to produce tickets for your PSA system along with the remediation details, so you can do more without having to hire additional staff.

SECURITY APP STORE

Get more by monitoring your existing tools. With our App Store, simply turn on the monitoring you want for more than 35 popular cybersecurity products, including:

- AV/AM monitoring with BitDefender, Cylance, Datto EDR, Deep Instinct, Defender for Business, SentinelOne, Sophos, Webroot, Windows Defender.
- Firewall analyzer & monitoring with Barracuda, Checkpoint, Cisco ASA, Cisco Firepower, Cisco Meraki, Fortinet, Juniper, Mikrotik, Palo Alto, PfSense, SonicWall, Sophos, Ubiquiti, Untangle, WatchGuard, Zyxel.
- Email and DNS monitoring with Barracuda, DNSFilter, Graphus IRONSCALES, Microsoft 365.
- ***And much more!***