

Managed Security

IntegraONE's Managed Security enables a complete, end-to-end cyber security offering, encompassing a 24/7/365 Security Operations Center, Security Information and Event Management. It leverages SIEM technology to collect, analyze, and correlate information from network devices, endpoint logs, and threat intelligence feeds, and uses this information to identify security incidents, policy violations, fraudulent activity, and more.

- **Endpoint Log Monitoring**

- Monitoring key log files to identify and correlate events that could be malicious by directly integrating into clients' servers, routers, switches and firewalls.

- **Common Network Device Monitoring**

- Leverage out-of-the-box integrations with network devices commonly seen in client environments.

- **Behavioral Analysis**

- Detect and address changes in systems and user behavior with real-time processing and advanced correlation rules for intrusion and insider threats.

- **Threat Intelligence Integration**

- Enable a quick and accurate detection of threats on a network by interacting with valuable threat data feeds from our technology partners.

- **Security & Compliance Reporting**

- Increase your network's security strength and maintain compliance by receiving daily reports based on 23 common regulations.

- **Detection & Remediation of Security Threats**

- Fast detection and remediation of threats by IntegraONE's SOC, that evade anti-virus and firewall products, allow your organization to increase operational efficiency. Have more time to focus on your business without having to worry about threats that can harm your day to day operations.