Progent™

SentinelOne Partner

SentinelOne Complete with MDR Package from Progent

SentinelOne

SentinelOne *Complete with Vigilance MDR – 24x7 Monitoring and Threat Mitigation Co-Managed Environment*

We know that managing an organization's assets and the threats against them takes a toll on your team. SentinelOne Complete with Vigilance MDR is made for organizations that need modern endpoint security and control, threat hunting options for SOC, and also advanced forensics with all threats mitigated and responded to. SentinelOne *Complete with MDR* fulfills the needs of SOC analysts, security administrators, and Incident Responders while providing you a fully Managed Detection and Response Service.

All *Control* Features Included:

- **Endpoint Prevention (EPP)** to stop a wide range of malware, Trojans, hacking tools, and ransomware before they start
- **ActiveEDR Basic for Endpoint Detection & Response (EDR)** works in real-time with or without cloud connectivity. ActiveEDR detects highly sophisticated malware, memory exploits, script misuse and other fileless attacks as they attempt to do damage.
- **ActiveEDR Recovery** gets users up and running in minutes and includes 100% remediation as well as rollback for all supported non legacy Microsoft Windows.
- **Device Control** for Policy-based control of all USB device and Bluetooth peripherals (Win, Mac)
- **Firewall Control** for Policy-based control of network connectivity to and from assets, including location awareness (Win, Mac, Linux)
- **Vulnerability Management**, in addition to Application Inventory, for insight into 3rd party apps that have known vulnerabilities mapped to the MITRE CVE database
- **Full Secure Remote Shell** capability for direct endpoint access by incident responders and forensics personnel
- Autonomous Sentinel agent **Storyline Engine**
- Integrated **Static AI** and SentinelOne Cloud Intelligence file-based attack prevention
- **Behavioral AI** fileless attack detection
- Autonomous Threat, **Remediation**, and **Rollback** Response
- **Quarantine** device from network, Incident **Analysis**, Agent **Anti-tamper**, **App inventory**
- **Rogue** device discovery

All *Complete* Features Included:

- **Co-Managed** environment with Progent receiving alerts and notifications of all threats and activities in your environment. Client is responsible for resolving threats in their environment and optional support time and material is available
- **ActiveEDR Advanced** adds visibility of all benign data.
- **ActiveEDR Advanced** adds enterprise threat hunting. SentinelOne differentiates with ease-of-use personified by the active nature of the solution in autonomously responding to attacks.
- **Storyline** technology for **Automated Forensics** and fast root cause analysis (RCA). All OS stories are automatically contextualized with SentinelOne's patented TrueContext function, saving analysts tedious event correlation tasks and getting them to the root cause with reduced MTTR.
- **Storyline Active Response (STAR)** mitigates zero-day threats with custom detection and hunting rules.
- **Deep visibility Storyline Pivot and Hunt** by MITRE ATT&CK technique
- **EDR Hunting Data** retention options from 14 days standard to 365 days optional
- **Timelines, file fetch, file integrity monitoring, sandbox integrations**
- Additional response options are available and customized to your needs. Includes 1 hour of training in advanced features and day to day management of the SentinelOne portal. During this time, we will train in the creation of **Exclusions, Blocklists, Mitigation, Agent Updates, Notifications**, Client **Reports**, **Application** Features, **Activity** Logs and UI configuration **Alerts**.

Optional monthly client portal review and threat recommendations are available.

SentinelOne *Complete with MDR* adds **24x7 Monitoring with Near Real Time Threat Response, Remote Script Orchestration and Ranger:**

- **Fully Co-Managed Environment** with Progent receiving alerts and notifications of all threats and activities in your environment combined **SOC response**, providing 3 levels of **24x7x365 Detection and Response**. All threats are mitigated and responded to in near real-time. Additional remediation options after threat mitigation are available and customized to your individual needs.
- **Remote Script Orchestration** empowers enterprises to send scripts to one machine, a few hundred machines, or even millions of machines, to respond to present and future cyberattacks at machine speed. Security Teams can send custom scripts or select from a wide range of tasks – ranging from incident response to forensics artifact collection and even IT administration. In combination with SentinelOne **Storyline Active Response (STAR)**, analysts benefit from automated workflows that take incident response to the next level.
- **Ranger** provides unparalleled visibility into your environment. Ranger is network-efficient by intelligently electing a few SentinelOne agents per subnet to participate in network mapping missions. Elected "Rangers" passively listen for network broadcast data including ARP, DHCP, and other network observances. Admins can customize active scan policies and specify multiple IP Protocols for learning including ICMP, SNMP, UDP, TCP, SMB, and more. Rangers correlate all learned information within the backend to fingerprint known and unknown devices. Ranger device inventories reveal what is connected to your environment, where and the protocols the devices listen on. Ranger allows you to find and close SentinelOne Agent deployment gaps with Ranger Deploy, a peer-to-peer deployment (Windows, Mac, Linux). Ranger allows you to monitor how unknown devices communicate with managed hosts and isolate suspicious devices from managed devices with a click.

Includes 1 hour of training in advanced features and day-to-day management of the SentinelOne portal. During this time, we will train clients in the creation of **Exclusions, Blocklists, Mitigation, Agent Updates, Notifications,** Client **Reports, Application** Features**, Activity** Logs and UI configuration **Alerts**. Progent offers specialized additional training for your organization's needs on a time and materials basis.

Contact Progent About SentinelOne Protection Suite Packages

For more information, call **800-993-9400** or send email to **information@progent.com**