Progent™

SentinelOne Partner

SentinelOne Complete Package from Progent

SentinelOne

SentinelOne *Complete - Co-Managed Environment*

SentinelOne *Complete* is made for organizations that need modern endpoint security and control plus threat hunting options for SOC and advanced forensics. SentinelOne Complete fulfills the needs of security administrators, SOC analysts, and Incident Responders. SentinelOne *Complete* includes all the features of SentinelOne *Control*:

- **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 plus 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

SentinelOne *Complete* adds co-management with reporting, alert configuration, Forensic Threat Hunting and Storyline Deep Visibility to events in your environment. SentinelOne *Complete* also adds threat hunting tools for DFIR teams. Added features include:

- **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.

Contact Progent About SentinelOne Protection Suite Packages

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

 ■ Headquarters: 2570 N. First Street, 2nd Floor, San Jose, CA 95131
■ information@progent.com ■ Web: www.progent.com ■ Phone: 800-993-9400 ■ Fax: 800-325-5300

P/N 031024B