



SentinelOne To One **Hundred**

Level your SentinelOne offering up
to 100% with additional services

Cloud Workshop Protection

Kubernetes Sentinel Agent

Cloud-native containerised workloads need runtime security protection and EDR just like any other compute. SentinelOne delivers these capabilities to SecOps and DevSecOps teams.

Kubernetes Sentinel agents supplement pre-production CI/CD container scanning with real time protection for live, in-production containers. Runtime protection is vital to identify and stop previously unknown threats that pre-production scans miss.

Kubernetes Sentinel enforcement points are managed within the same multi-tenant console alongside other Sentinels for Windows, macOS, and Linux. Administration is flexible, distributed, and managed via role-based access controls that match your organization's structure.

Ranger IOT

Cloud-Delivered Network Visibility & Control

The proliferation of IoT use in business, open BYOD policies, and a global remote workforce exponentially increases the quantity of unmanaged IP-enabled devices directly neighbouring enterprise infrastructure.

SentinelOne addresses this risk with Ranger, which turns endpoint Sentinel agents into distributed network sensors. Sentinel Rangers enable control of the enterprise network attack surface in real time by discovering, identifying, and containing any device-based threat.

Vigilance Respond

SOC Augmentation MDR / Digital Forensics / Incident Response

SentinelOne's Vigilance service subscriptions are designed to supplement endpoint security SaaS offerings.

The Vigilance MDR Team is the human side to SentinelOne's AI-based Singularity™ platform – a 100% in-house, non-outsourced team of Tier-1, Tier-2, and Tier-3 cybersecurity experts monitoring millions of endpoints. Vigilance Respond & Respond Pro empower customers to focus only on the incidents that matter making it the perfect endpoint add-on solution for overstretched IT/SOC teams.

Global Support Services

Customer Support that Exceeds Your Expectations

SentinelOne Global Support Services (GSS) is a team of customer-focused Tier-1, Tier-2, and Tier-3 product experts trained in all aspects of the SentinelOne Singularity platform and are ready 24x7x365 to provide assistance. Their job is to assist customers who experience product problems they themselves cannot solve.

Technical Account Manager

Technical Account Manager (TAM) is an extension to the Enterprise Support level option and a suite of services to proactively assist with execution of SentinelOne products in your environment.

Designated Technical Account Managers serve as customer advocates and single points of contact during regional business hours. Your TAM gets to know your Team and your environment at a deeper, more personal level. TAMs are pros at deployment planning, implementation assistance, advising on periodic upgrades, and measuring deployment environment health. TAMs also work hand-in-hand with SentinelOne's global, follow-the-sun Technical Support Team to drive support issues to resolution on your behalf and keep you up to speed on status.