cybersecurity associates

SentinelOne®

OUTSTANDING TO WORK FOR 2023

ISO 27001 ISOQAR REGISTERED · UKAS MANAGEMENT SYSTEMS 0026

ISO 9001 ISOQAR REGISTERED · UKAS MANAGEMENT SYSTEMS 0026

CYBER ESSENTIALS CERTIFIED

CYBER ESSENTIALS CERTIFIED PLUS

CERTIFIED PLATINUM MSSP APPGUARD 2022

AUTHORISED DISTRIBUTOR APPGUARD 2022

CiSP Cyber-security Information Sharing Partnership

Microsoft Partner

gfirst LEP growing gloucestershire

ccoe Cyber Centre of Excellence Supporting Partner

FINALIST C2S Business Awards 2023

THE SOUTH WEST CYBER RESILIENCE CENTRE

SentinelOne Endpoint Security

Executive Summary

The SentinelOne Singularity security platform empowers SOC & IT Operations Teams with a more efficient way to protect information assets against today's sophisticated threats.

Singularity delivers differentiated endpoint protection, endpoint detection and response, IoT security, cloud security, and IT operations capabilities - consolidating multiple existing technologies into one solution. We offer resource efficient, autonomous "Sentinel" agents for Windows, Mac, Linux, and Kubernetes and support a variety of form factors including physical, virtual, VDI, customer data centres, hybrid data centres, and cloud service providers.

Sentinels are managed via our globally available multi-tenant SaaS designed for ease-of-use and flexible management that meets your requirements. Our CSA Managed Detection & Response (MDR) services subscription is available to back your security organization 24x7.

Singularity Platform Features & Offerings

- Global SaaS implementation. Highly available. Choice of locality (US, EU, APAC).
- Flexible administrative authentication and authorization: SSO, MFA, RBAC
- Administration customizable to match your organizational structure
- 365 days threat incident history
- Integrated SentinelOne Threat Intelligence and MITRE ATT&CK Threat Indicators
- Data-driven Dashboard Security Analytics
- Configurable notifications by email and syslog
- Singularity API-driven XDR integrations (SIEM, sandbox, Slack, 3rd party Threat Intel, etc)
- Single API with 340+ functions

WHY CHOOSE SENTINELONE?

- We do endpoint security and we do it well. SentinelOne truly converges EPP+EDR so that you can eliminate redundant endpoint agents and lower OPEX.
- 97% customer support satisfaction
- 96% of customers recommend SentinelOne
- Customizable console with time saving workflows
- Ransomware solved through superior behavioural AI
- Autonomous protective responses trigger instantly
- Time saving, fatigue-reducing Storyline™ with ActiveEDR™ designed for incident responders and threat hunters
- Affordable EDR data retention
- Easy XDR integrations to other vendors

Singularity Control

Control is made for organisations seeking the best-of-breed security found in SentinelOne Core with the addition of “security suite” features for endpoint management. SentinelOne Control features include:

- **Built-in Static AI and Behavioural AI analysis** prevent and detect a wide range of attacks in real time before they cause damage. Core protects against known and unknown malware, Trojans, hacking tools, ransomware, memory exploits, script misuse, bad macros, and more.
- **Sentinels are autonomous** which means they apply prevention and detection technology with or without cloud connectivity and will trigger protective responses in real time.
- **Recovery is fast** and gets users back and working in minutes without re-imaging and without writing scripts. Any unauthorized changes that occur during an attack can be reversed with 1-Click Remediation and 1-Click Rollback for Windows.
- **Secure SaaS management access**. Choose from US, EU, APAC localities. Data-driven dashboards, policy management by site and group, incident analysis with MITRE ATT&CK integration, and more.
- **Firewall Control** for control of network connectivity to and from devices including location awareness
- **Device Control** for control of USB devices and Bluetooth/BLE peripherals
- **Rogue visibility** to uncover devices on the network that need Sentinel agent protection
- **Vulnerability Management**, in addition to Application Inventory, for insight into 3rd party apps that have known vulnerabilities mapped to the MITRE CVE database

Singularity Complete

Complete is made for enterprises that need modern endpoint protection and control plus advanced EDR features that we call ActiveEDR™. Complete also has patented Storyline™ tech that automatically contextualizes all OS process relationships [even across reboots] every second of every day and stores them for your future investigations. Storyline™ saves analysts from tedious event correlation tasks and gets them to the root cause fast. SentinelOne Complete is designed to lighten the load on security administrators, SOC analysts, threat hunters, and incident responders by automatically correlating telemetry and mapping it into the MITRE ATT&CK® framework. The most discerning global enterprises run SentinelOne Complete for their unyielding cybersecurity demands. Features include:

- All SentinelOne Core + SentinelOne Control features.

- Patented Storyline™ tech for fast RCA and easy pivots.
- Integrated ActiveEDR™ visibility to both benign and malicious data.
- 14 - 365+ historical EDR data retention + usable query speeds at scale.
- Hunt by MITRE ATT&CK ® Technique.
- Mark benign Storylines as threats for enforcement by the EPP functions.
- Automated Storyline™ Active Response (STAR) watchlist functions.
- Timelines, remote shell, file fetch, sandbox integrations, and more.

To find out more about our Managed Detection & Response service or to organise a live demonstration please contact us.