SentinelOne

SCHEDA DATI

SentinelOne Endpoint Security

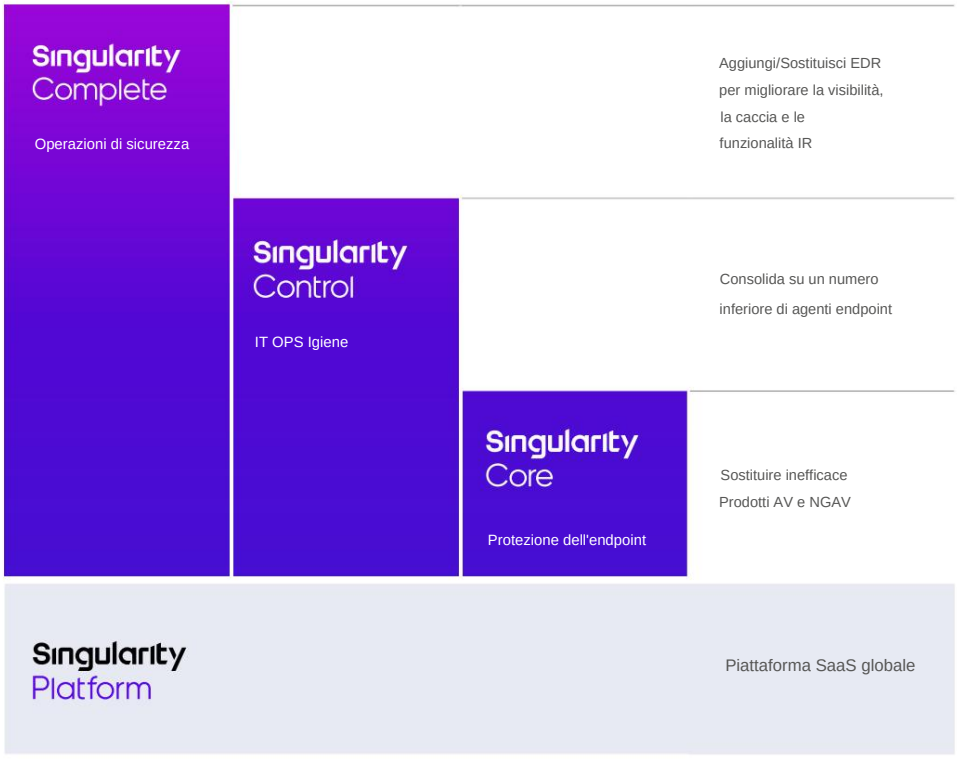
Pacchetti di prodotti della piattaforma Singularity

La piattaforma di sicurezza SentinelOne Singularity offre ai team operativi SOC e IT un modo più efficiente per proteggere le risorse informative dalle minacce sofisticate di oggi.

Singularity offre protezione differenziata degli endpoint, rilevamento e risposta degli endpoint, sicurezza IoT , sicurezza cloud e funzionalità delle operazioni IT, consolidando più tecnologie esistenti in un'unica soluzione. Offriamo agenti "Sentinel" autonomi ed efficienti in termini di risorse per Windows, Mac, Linux e Kubernetes e supportiamo una varietà di fattori di forma tra cui fisici, virtuali, VDI, data center dei clienti, data center ibridi e provider di servizi cloud.

Le sentinelle sono gestite tramite il nostro SaaS multi-tenant disponibile a livello globale, progettato per una gestione flessibile e di facile utilizzo che soddisfi le tue esigenze. Il nostro abbonamento ai servizi Vigilance Managed Detection & Response (MDR) è disponibile per supportare la tua organizzazione di sicurezza 24 ore su 24, 7 giorni su 7.

Questa scheda tecnica descrive le nostre offerte di prodotti a più livelli note come SentinelOne Core, Control e Complete. Ogni pacchetto di prodotti si basa su quello sottostante.



PERCHÉ SCEGLIERE SENTINELONE?

- Ci occupiamo di sicurezza degli endpoint e lo facciamo bene. SentinelOne fa convergere realmente EPP+EDR in modo da poter eliminare gli agenti endpoint ridondanti e ridurre l'OPEX.
- 97% di soddisfazione dell'assistenza clienti
- Il 96% dei clienti consiglia SentinelOne
- Consolle personalizzabile con flussi di lavoro che fanno risparmiare tempo
- Ransomware risolto attraverso un'intelligenza artificiale comportamentale superiore
- Protettivo autonomo le risposte si attivano istantaneamente
- Risparmio di tempo, riduzione della fatica Storyline™ con ActiveEDRTM progettato per i risponditori di incidenti e i cacciatori di minacce
- Conservazione dei dati EDR conveniente
- Facili integrazioni XDR con altri fornitori

PRONTO PER UNA DEMO?

Visita il sito web di SentinelOne per maggiori dettagli

Caratteristiche e offerte della piattaforma Singularity

Tutti i clienti SentinelOne hanno accesso alle seguenti funzionalità della console di gestione SaaS:

- Implementazione globale SaaS. Altamente disponibile. Scelta della località (USA, UE, APAC).
- Autenticazione amministrativa flessibile e autorizzazione: SSO, MFA, RBAC
- Amministrazione personalizzabile per abbinarsi la tua struttura organizzativa
- Cronologia degli incidenti di minaccia di 365 giorni
- SentinelOne Threat Intel ligence e MITRE ATT&CK Threat integrati Indicatori
- Sicurezza del dashboard basata sui dati Analitica
- Notifiche configurabili tramite e-mail e syslog
- Integrazioni XDR basate su Singularity API (SIEM, sandbox, Slack, terze parti Minaccia Intel, ecc.)
- API singola con oltre 340 funzioni

Singularity Core

Core è il fondamento di tutte le offerte di sicurezza degli endpoint di SentinelOne. È il nostro prodotto entry level per la sicurezza degli endpoint per le organizzazioni che desiderano sostituire AV o NGAV legacy con un EPP più efficace e facile da gestire. Core offre anche funzioni EDR di base che dimostrano la vera fusione delle capacità EPP+EDR. Threat Intelligence fa parte della nostra offerta standard ed è integrata attraverso le nostre funzioni AI e
Nube Sentinella. Le funzionalità principali di SentinelOne includono:

- **L'IA statica integrata e l'analisi dell'IA comportamentale** prevengono e rilevare una vasta gamma di attacchi in tempo reale prima che causino danni. Core protegge da malware noti e sconosciuti, trojan, strumenti di hacking, ransomware, exploit della memoria, uso improprio di script, macro dannose e altro ancora.
- **Le sentinelle sono autonome ,** il che significa che applicano la tecnologia di prevenzione e rilevamento con o senza connettività cloud e attiveranno risposte protettive in tempo reale.
- **Il ripristino è rapido** e consente agli utenti di tornare al lavoro in pochi minuti senza dover ricreare l'immagine e senza scrivere script. Eventuali modifiche non autorizzate che si verificano durante un attacco possono essere annullate con Correzione in 1 clic e rollback in 1 clic per Windows.
- **Accesso sicuro alla gestione SaaS.** Scegli tra località USA, UE, APAC. Dashboard basati sui dati, gestione delle policy per sito e gruppo, analisi degli incidenti con integrazione MITRE ATT&CK,
e altro ancora.

Singularity Control

Il controllo è rivolto alle organizzazioni che cercano la migliore sicurezza disponibile in SentinelOne Core con l'aggiunta di funzionalità di "suite di sicurezza" per la gestione degli endpoint. Le funzionalità di SentinelOne Control includono:

- **Tutte le funzionalità principali di SentinelOne**
- **Firewall Control** per il controllo della connettività di rete da e verso dispositivi tra cui la consapevolezza della posizione
- **Device Control** per il controllo di dispositivi USB e Bluetooth/BLE periferiche
- **Visibilità non autorizzata** per scoprire i dispositivi sulla rete che ne hanno bisogno Protezione dell'agente sentinella
- **Gestione delle vulnerabilità,** oltre ad Application Inventor ry, per informazioni sulle app di terze parti che presentano vulnerabilità note mappate al database MITRE CVE

SENTINELONE BLOCCA RANSOMWARE E ALTRO ATTACCHI SENZA FILE CON AI COMPORTAMENTALE E FORTI FUNZIONI DI RIMEDIO AUTOMATICO

Singularity Complete

Complete è pensato per le aziende che necessitano di protezione e controllo moderni degli endpoint oltre a funzionalità EDR avanzate che chiamiamo ActiveEDR™.
Complete dispone anche della tecnologia brevettata Storyline™ che contestualizza automaticamente tutte le relazioni tra i processi del sistema operativo [anche durante i riavvii] ogni secondo di ogni giorno e le memorizza per le tue indagini future. Storyline™ salva gli analisti dalle noiose attività di correlazione degli eventi e li porta rapidamente alla causa principale. SentinelOne Complete è progettato per alleggerire il carico di amministratori della sicurezza, analisti SOC, cacciatori di minacce e soccorritori di incidenti correlando automaticamente la telemetria e mappandola nel framework MITRE ATT&CK®. Le aziende globali più esigenti utilizzano SentinelOne Complete per la loro inflessibile sicurezza informatica

richieste. Le caratteristiche includono:

- **Tutte le funzioni SentinelOne Core + SentinelOne Control**
- **Tecnologia brevettata Storyline™** per RCA veloce e perni facili
- **Visibilità ActiveEDR™ integrata** per entrambi benigni e dati dannosi
- **Conservazione dei dati storici EDR da 14 a 365+** + velocità di query utilizzabili su larga scala
- **Hunt by MITRE ATT&CK ® Tecnico**
- **Contrassegna le trame benigne come minacce** per l'applicazione da parte di le funzioni del PPE
- **Risposta attiva StorylineTM automatizzata** (STAR) funzioni di lista di controllo
- Timeline, shell remota, recupero file, integrazioni sandbox, e altro ancora

Gartner peerinsights™

> “
> Funzionalità di gestione molto flessibili in aggiunta alle potenti funzionalità EPP/EDR.
>
> **Gov't/PS/ED 5.000 - 50.000 dipendenti**
>
> 13 marzo 2020

> “
> Buona liberazione ransomware... SentinelOne fuma la concorrenza!
>
> **Vendita al dettaglio 1 mld - 3 mld di dollari**
>
> 20 marzo 2020

> “
> La configurazione e l'implementazione sono state estremamente semplici. Il dashboard cloud è semplice da usare.
>
> **250 milioni - 500 milioni di dollari**
>
> 2 luglio 2020

Servizi MDR di vigilanza Sottoscrizione

SentinelOne Vigilance Managed Detection & Response (MDR) è un abbonamento al servizio progettato per aumentare la sicurezza delle organizzazioni dei clienti.
Vigilance MDR aggiunge valore assicurando che ogni minaccia venga esaminata, affrontata, documentata e intensificata secondo necessità. Nella maggior parte dei casi interpretiamo e risolviamo le minacce in circa 20 minuti e ti contattiamo solo per questioni urgenti. Vigilance MDR consente ai clienti di concentrarsi solo sugli incidenti che contano, rendendola la perfetta soluzione aggiuntiva per gli endpoint per i team IT/SOC sovraccaricati.

Maggiori informazioni: https://s1.ai/s1mdr

Servizi di preparazione SentinelOne Sottoscrizione

SentinelOne Readiness è un servizio di consulenza in abbonamento progettato per guidare il tuo team prima, durante e dopo l'installazione del prodotto con una metodologia strutturata che ti consente di essere operativo rapidamente e di mantenere l'installazione integra nel tempo. I clienti Readiness vengono guidati attraverso le migliori pratiche di implementazione, ricevono assistenza periodica per l'aggiornamento degli agenti e ricevono controlli trimestrali sullo stato di salute ONEscoreTM per assicurarsi che il proprio patrimonio SentinelOne sia ottimizzato.

Maggiori informazioni: https://s1.ai/ready

Funzionalità in bundle

	Singularity Complete	Singularity Control	Singularity Core
Piattaforma SaaS globale. Accesso sicuro, alta disponibilità, amministrazione delle policy EPP, risposta agli incidenti EDR e ricerca delle minacce, analisi, controllo IoT (con opzione Ranger)	✓	✓	✓
Funzionalità EDR per le operazioni di sicurezza			
Visibilità profonda ActiveEDRTM	✓		
Perno Deep Visibility StorylineTM	✓		
Caccia alla visibilità profonda con la tecnica MITRE ATT&CK ®	✓		
Watchlist Automated StorylineTM Active Response (STAR).	✓		
Recupero file manuale/automatico (Windows, Mac, Linux)	✓		
Visibilità profonda Contrassegna il risultato benigno come minaccia per la risposta dell'applicazione	✓		
Archiviazione dati storici EDR estesa (disponibile 14-365 giorni)	✓		
Secure Remote Shell (Windows Powershell. Mac e Linux bash)*	✓	✓	
OPS IT/Igiene della sicurezza e funzionalità della suite			
Controllo OS Firewall con riconoscimento della posizione (Win, Mac, Linux)	✓	✓	
Controllo dispositivo USB (Win, Mac)	✓	✓	
Controllo Bluetooth® / Bluetooth Low Energy® (Win, Mac)	✓	✓	
Rilevamento di dispositivi non autorizzati	✓	✓	
Vulnerabilità delle app (Win, Mac)	✓	✓	
Funzionalità di protezione degli endpoint di base			
Motore Autonomous Sentinel Agent StorylineTM	✓	✓	✓
IA statica e prevenzione degli attacchi basati su file di Sentinel Cloud	✓	✓	✓
Rilevamento di attacchi senza file di intelligenza artificiale comportamentale	✓	✓	✓
Autonomous Threat Response/Kill, Quarantine (Win, Mac, Linux)	✓	✓	✓
Risposta di riparazione autonoma/1 clic, senza script (Win, Mac)	✓	✓	✓
Risposta al rollback autonomo/1 clic, senza script (Win)	✓	✓	✓
Metti in quarantena il dispositivo dalla rete	✓	✓	✓
Analisi degli incidenti (MITRE ATT&CK®, timeline, explorer, annotazioni del team)	✓	✓	✓
Agente antimanomissione	✓	✓	✓
Inventario delle app	✓	✓	✓

* incluso con Singularity Control per un periodo di tempo limitato

Supporto globale e offerte di servizi

Supporto tecnico per telefono, web ed e-mail	**Incluso**
Centro risorse all'interno del prodotto/Accesso al portale di supporto	**Incluso**
Supporto standard 9x5	**Incluso**
Supporto aziendale 24x7x365, Follow-the-Sun per Sev 1 e 2	Disponibile
Technical Account Manager designato + supporto aziendale	Disponibile
Abbonamento Vigilance Managed Detection & Response (MDR).	Disponibile
SentinelOne Readiness Deployment e abbonamento Health in corso	Disponibile

SUPPORTO DEL SISTEMA OPERATIVO

SentinelOne supporta un'ampia gamma di distribuzioni Windows, Mac e Linux, nonché sistemi operativi di virtualizzazione.
Le eccezioni software comuni sono documentate nel nostro portale di supporto.

Agente Windows Sentinel
Tutte le workstation Windows a partire da 7 SP1 tramite Windows 10
Tutti i server Windows a partire da 2008 R2 SP1 fino a Server/Core 2019

Agente Mac Sentinel
macOS Catalina, Mojave, High Sierra

Agente Linux Sentinel
Ubuntu, Redhat (RHEL), CentOS, Oracle, Amazon AMI, SUSE Linux Enterprise Server, Fedora, Debian, Virtuozzo, Scientific Linux

Agente precedente di Windows
XP, Server 2003 e 2008, POS2009

Piattaforme container supportate
Kubernetes autogestito v1.13+ (autogestito, AWS Kubernetes (EKS), Azure AKS)

Virtualizzazione e VDI
Citrix XenApp, Citrix XenDesktop, Oracle VirtualBox, VMware vSphere, VMware Stazione di lavoro, VMware Fusion, VMware Orizzonte, Microsoft Hyper-V

AWS GovCloud · SE Labs AAA Enterprise Endpoint Protection · VB100 VIRUS virusbtn.com · MITRE ATT&CK · TEVORA Attestazione HIPAA · TEVORA Attestazione PCI DSS · ISO 27001 CERTIFIED by schellman · Gartner peerinsights customers' choice 2020

SentinelOne è un'azienda al primo posto per il cliente

La misurazione e il miglioramento continui ci spingono a superare le aspettative dei clienti.

96%

96% di Gartner Peer Insights™
"La voce del cliente" I revisori consigliano SentinelOne

97%

Soddisfazione del cliente
(CSAT) anche ~97%

Net Promoter Score nella gamma da "ottimo" a "eccellente".

Informazioni su SentinelOne

SentinelOne fondata nel 2013 e con sede a Mountain View, in California, è una società di software per la sicurezza informatica. SentinelOne Singularity è una piattaforma per prevenire, rilevare, rispondere e ricercare nel contesto di tutte le risorse aziendali.

sentinelone.com
sales@sentinelone.com
+1 855 868 3733