

Stop sikkerhedsbrud hurtigerere end noget menneske



SentinelOne

Data er blevet grundlaget for vores livsstil. Og for alle virksomheder og organisationer er beskyttelse af deres data en stadigt større og mere og mere kompleks opgave. Datakraft er svaret på, hvordan du kan besejre morgendagens nye cybertrusler.

Meget mere end en normal antivirusløsning

Fra endpoint til skyen - fra IoT-enhed til container. Med SentinelOne får du fuld beskyttelse mod både malware, exploits og insiderangreb - både kendte og ukendte. Løsningen er certificeret som en fulgyldig antivirus erstatning for Windows, OS X og Linux

Endpoint Protection Platform (EPP)

SentinelOne er en avanceret EPP løsning. I praksis betyder det, at løsningen ved hjælp af bla. Machine Learning og kunstig intelligens kan forhindre alle typer angreb. SentinelOne bygger på en teknologi, der hedder Active EDR (Endpoint Detection and Response).

De fleste indbyggede antivirus-løsninger bygger på heuristik og filbaserede malwaresignaturer. SentinelOne løsningen er mere intelligent, nemmere at implementere og belaster ikke det enkelte endpoint (fx. server, desktop eller mobiltelefon).

I modsætning til andre EPP løsninger behøver SentinelOne ikke at være forbundet i skyen for at kunne kende en trussel. Det hele foregår automatisk og i realtid. Hvordan SentinelOne skal handle på en given trussel kan defineres efter dit behov. Skal den isoleres? Fjernes? Skal der foretages rollback? Du bestemmer.

Med SentinelOne kan du:

- Genskabe din klient som før den blev ramt - med ganske få klik
- Få et nøjagtigt billede af en given trussel, og hvordan den påvirker eller har påvirket dit netværk
- Se omfanget af truslen, og hvordan du rydder op efter den
- Gemme data fra truslen til senere brug og analyse

SentinelOne anbefales af både **PCI**, **MITRE ATT&CK**, **Gartner** og **NSS Labs**.

norwegian

Norwegian får den bedste EDR løsning med få ressourcer

[Se Norwegian video](#)



Staten Montana benytter SentinelOne til deres 15.000 endpoints ud fra økonomisk og ressourcemæssig prioritering

[Se The State of Montana video](#)



National Oilwell Varco fokuserer på de ukendte trusler som de finder med SentinelOne.

[Se NOV video](#)

Se en sammenligning af din nuværende antivirusløsning i forhold til SentinelOne

[Sammenligning](#)

SentinelOne features

Global SaaS Platform. Secure Access, High Availability, Hierarchical Policy Administration, EDR Incident Response & Threat Hunting, Analytics, IoT Control (with Ranger option), CWS	✓
Security Operations EDR Features	
Deep Visibility ActiveEDR® with Storyline™ context	✓
MITRE ATT&CK® Integration	✓
Storyline Active Response (STAR) Custom Detection Rules	✓
Storyline Active Response (STAR) Pro Custom Detection Rules	+
Binary Vault Live Malware Upload Repository	+
File Integrity Monitoring	✓
14-day EDR Hunting Data Retention	✓
Extended EDR Hunting Data Retention up to 365 days	+
Cloud Data Lake Streaming	+
Secure Remote Shell	✓
IT OPS / Security Hygiene & Suite Features	
OS Firewall control with location awareness (Win, Mac, Linux)	✓
USB device control (Win, Mac)	✓
Bluetooth® / Bluetooth Low Energy® control (Win, Mac)	✓
Rogue Device Discovery	✓
App Vulnerability (Win, Mac)	✓
Base Endpoint Protection Features	
Autonomous Sentinel agent Storyline™ engine	✓
Static AI & SentinelOne Cloud file-based attack prevention	✓
Behavioral AI fileless attack detection	✓
Autonomous Threat Response / Kill, Quarantine (Win, Mac, Linux)	✓
Autonomous Remediation Response / 1-Click, no scripting (Win, Mac)	✓
Autonomous Rollback Response / 1-Click, no scripting (Win)	✓
Quarantine device from network	✓
Incident Analysis (MITRE ATT&CK®, timeline, explorer, team annotations)	✓
Agent anti-tamper	✓
App Inventory	✓