
SentinelOne

SENTINEL ONE COMPLETE

Technical Overview – Enterprise Endpoint Protection Platform

1. Classificazione del Prodotto

Tipologia:
EDR / XDR Platform – Next Generation Endpoint Protection
Architettura:
AI-driven Autonomous Security Platform
Deployment:
Agent-based (Windows, macOS, Linux)
Console centralizzata cloud-based

2. Motore di Protezione

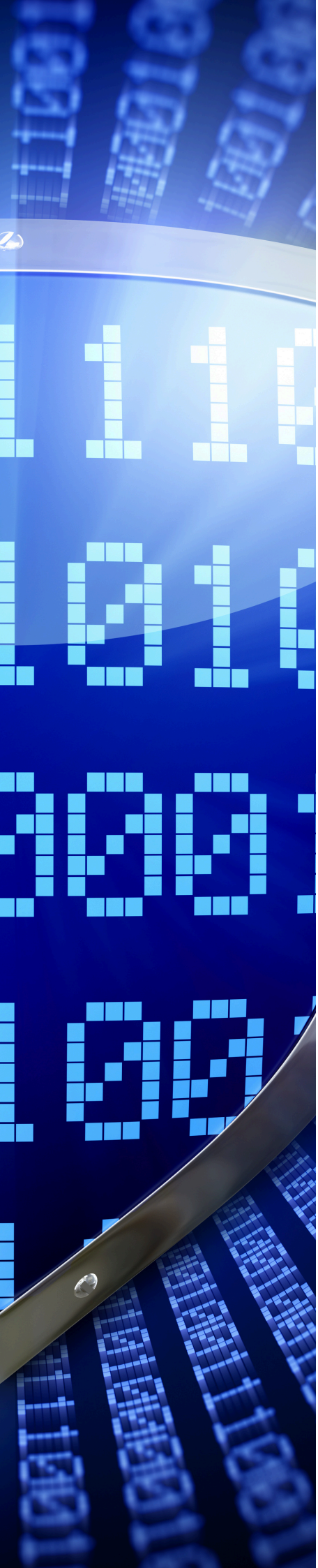
Multi-Layer AI Architecture
✓ Static AI (Pre-Execution)
- Machine Learning su file sconosciuti
- Analisi preventiva prima dell'esecuzione
- Classificazione senza dipendenza da firme

✓ Behavioral AI (On-Execution)
- Monitoraggio processi a livello kernel
- Analisi comportamentale in tempo reale
- Rilevazione pattern anomali

✓ Post-Execution Remediation
- Mitigazione automatica
- Eliminazione artefatti malevoli
- Rollback modifiche sistema

3. Capacità di Rilevamento

✓ Zero-Day Threat Detection
✓ Ransomware Detection & Rollback
✓ Fileless Attack Detection
✓ Exploit Prevention
✓ Privilege Escalation Detection
✓ Lateral Movement Detection
✓ Command & Control Communication Blocking



4. Visibilità e Telemetria

✓ Full Process Storyline™
Ricostruzione completa della catena di attacco.
✓ Deep Visibility™
Query avanzate su endpoint.
✓ MITRE ATT&CK Mapping
Classificazione tecnica delle tecniche utilizzate.
✓ Threat Hunting Support
Ricerca IOC e analisi forense.

5. Capacità di Risposta (Response)

✓ Autonomous Response Engine
Blocco automatico della minaccia.
✓ Device Network Isolation
Isolamento endpoint compromesso.
✓ Automated Remediation
Rimozione file, registry, servizi e persistenze.
✓ One-Click Rollback
Ripristino automatico dati compromessi da ransomware.

6. Differenze Architetturali rispetto Antivirus Tradizionale

Antivirus Legacy	SentinelOne Complete
Basato su firme	Basato su AI multilivello
Protezione file-based	Protezione file + memoria + processo + rete
Reazione manuale	Autonomous Response
Visibilità limitata	Deep Visibility & Storyline
Nessuna analisi forense	Forensic & Threat Hunting Ready

7. Integrazione e Scalabilità

✔ API Integration
✔ Supporto integrazione SIEM / SOC
✔ Multi-tenant Ready (MSP Environment)
✔ Gestione centralizzata cloud

8. Benefici Tecnici per MSP / Partner IT

- Riduzione Incident Response manuale
- Standardizzazione sicurezza su base cliente
- Maggiore controllo operativo
- Riduzione rischio reputazionale
- Livello Enterprise in ambienti SMB

9. Sintesi Tecnica

SentinelOne Complete combina:
Prevention
Detection
Autonomous Response
Remediation
Forensic Visibility
in un'unica piattaforma EDR/XDR.
Architettura progettata per ridurre l'intervento umano e aumentare la resilienza dell'endpoint.