AYI NEDJIMI Consultants

SentinelOne Singularity : XDR Autonome Powered by AI

10 mai 2026 • Mis à jour le 17 mai 2026 • 21 min de lecture • 4585 mots • 74 vue

SentinelOne Singularity est la plateforme XDR autonome propulsée par l'IA agentique, fondée en 2013 par Tomer Weingarten et cotée au NYSE depuis l'IPO de juin 2021 (ticker S). Cette page entity-first détaille l'architecture autonome (ActiveEDR, Storyline, rollback ransomware VSS), les modules Singularity Endpoint / Identity (Attivo) / Cloud Workload (PingSafe) / Data Lake (Scalyr) / Ranger / Purple AI, le pricing 2026, le MDR Vigilance et les comparatifs face à CrowdStrike Falcon, Microsoft Defender XDR et Trellix.

SentinelOne est l'éditeur américain de cybersécurité fondé en **janvier 2013** par **Tomer Weingarten** (CEO), **Almog Cohen** et **Ehud Shamir**, qui a popularisé le conc d'*EDR autonome* capable de détecter, contenir et remédier une attaque **sans connectivité cloud permanente**. Sa **plateforme Singularity** est aujourd'hui la principale alternative à CrowdStrike Falcon dans le c u Gartner pour Endpoint Protection Platforms et Magic Quadra autour d'u

agent unique sur Windows, macOS, Linux, mobile, Kubernetes et IoT, Singularity combine NGAV (next-gen antivirus), **ActiveEDR** avec moteur **Storyline** de corrélati contextuelle, **rollback automatique des ransomwares** sur Windows via VSS, protection des identités (Singularity Identity, ex-Attivo Networks), sécurité du clou (Singularity Cloud Workload Security, ex-Stratoshark/PingSafe), data lake (Singularity Data Lake, ex-Scalyr), MDR Vigilance et l'assistant génératif **Purple AI** Cotée au NYSE depuis le 30 juin 2021 sous le ticker **S**, l'entreprise a réalisé l'une d plus grandes IPO de cybersécurité de l'histoire (1,2 Md$ levés, valorisation ~10 Md au premier jour). Cette page entity-first détaille l'architecture autonome, les modu de la plateforme, le pricing 2026, les comparatifs face à CrowdStrike, Microsoft Defender et Trellix, ainsi que les leçons à tirer pour évaluer Singularity en 2026.

À RETENIR

L'essentiel à retenir

Plateforme XDR autonome : détection et réponse fonctionnent *localement sur l'agent*, sans dépendance cloud temps réel — différenciateur historique vs CrowdStrike.

ActiveEDR + Storyline : chaque processus reçoit un identifiant de Storyline qui corrèle automatiquement toute la chaîne d'attaque, sans requête analyste.

Rollback ransomware : restauration automatique des fichiers chiffrés via Volume Shadow Copy (Windows), unique sur le marché.

Modules majeurs : Singularity Endpoint, Identity, Cloud Workload, Data Lake, Ranger (asset discovery), Purple AI, Vig

Réponse sous 24h

Devis gratuit →