AYI NEDJIMI Consultants

CrowdStrike Falcon : EDR/XDR cloud-native, modules et prix

10 mai 2026 • Mis à jour le 17 mai 2026 • 18 min de lecture • 3915 mots • 61 vues

CrowdStrike Falcon est la plateforme EDR/XDR cloud-native fondée en 2011 par Dmitri Alperovitch et George Kurtz. Cette page entity-first détaille l'architecture single-agent, le Threat Graph, les modules (Prevent, Insight, OverWatch, Identity, Cloud Workload, LogScale, Charlotte AI), le pricing 2026, les comparatifs SentinelOne / Defender / Sophos et les leçons retenues de l'incident Channel File 291 du 19 juillet 2024.

CrowdStrike Falcon est la plateforme de cybersécurité cloud-native lancée en 201 par CrowdStrike Holdings, fondée en 2011 par Dmitri Alperovitch et George Kurtz. Conçue autour d'un agent unique léger (Sensor) déployé sur les endpoints (Windows, macOS, Linux, mobile, conteneurs, charges Cloud), elle agrège la télémétrie en temps réel dans le Threat Graph, base de données distribuée traitan plusieurs trillions d'événements par semaine. Falcon de nouvell génération (NGAV), détection et réponse sur les end sion XDR

multi-domaines, gestion des vulnérabilités (Spotlight), protection des identités (Falcon Identity), sécurité du cloud (Cloud Workload Protection) et chasse aux menaces managée (OverWatch, 24/7). Sa promesse : un breakout time moyen de minutes pour les attaques d'État-nation neutralisées avant propagation latérale, grâce au machine learning, aux Indicators of Attack (IOA) comportementaux et à la threat intelligence collectée par CrowdStrike Intelligence sur plus de 230 acteurs malveillants nommés (FANCY BEAR, COZY BEAR, WIZARD SPIDER, etc.). Cotée au NASDAQ depuis juin 2019 (CRWD), CrowdStrike a marqué l'industrie le 19 juillet 20 avec un incident mondial sans précédent (Channel File 291) provoquant le BSoD d 8,5 millions de machines Windows. Cette page entity-first détaille l'architecture, le modules, le pricing, les comparatifs concurrentiels et les leçons retenues de l'incident pour vous aider à évaluer Falcon en 2026.

À RETENIR

L'essentiel à retenir

Plateforme cloud-native : agent unique <50 Mo, télémétrie temps réel agrégée dans le Threat Graph (trillions d'événements/semaine).

Modules clés : Falcon Prevent (NGAV), Insight (EDR), Discover (asset mgmt), Spotlight (vuln), Identity Protection, Cloud Workload, LogScale (SIEM), OverWatch (chasse 24/7), Charlotte AI (assistant génératif).

Détection : ML supervisé + IOA comportementaux (vs IOC statiques), efficacité validée par MITRE ATT&CK Evaluations 2024 (100% détection technique).

Pricing : Falcon Go (PME) ~60 €/endpoint/an, prise ~185 €, Elite ~225 €, Complete (MDR) sur de

Réponse sous 24h

Devis gratuit →