COMPARATIVA · 01 · CAPACIDADES CENTRALES

ASM dedicado × EASM integrado en plataformas de VM

Comparativa objetiva, capacidad a capacidad, entre CSURFACE — plataforma de Continuous Exposure Management dedicada — y los módulos de External Attack Surface Management que ofrecen las plataformas de gestión de vulnerabilidades de gran escala.

Ficha técnica 2026
CSURFACE

La diferencia en una frase. Defender EASM (heredero de RiskIQ), Tenable, Qualys y Rapid7 son plataformas maduras y ampliamente adoptadas, con módulos de EASM reales; Microsoft Defender EASM, en particular, opera un grafo de descubrimiento amplio. CSURFACE concentra su diferencial en la **atribución automática de propiedad**, la **contextualización por ML**, la **priorización dinámica por lo que es de hecho explotable** y una **cadencia de detección continua**. Esta comparativa es honesta y hecha por capacidad: las tablas siguientes muestran dónde se destaca cada enfoque.

CAPACIDAD	CSURFACE	DEFENDER EASM	TENABLE EASM	QUALYS CSAM	RAPID7 SURFACE CMD.
Descubrimiento continuo sin agente Inventario externo de la superficie de ataque, actualizado de forma continua, sin instalación en el entorno del cliente.	✓ Nativo	✓ Nativo	✓ Nativo	✓ Nativo	✓ Nativo
Atribución automática de propiedad Vincula el activo descubierto a la organización y al área de negocio responsable, sin clasificación manual.	✓ Nativo · ML	◐ Por inventario global	◐ Por etiqueta manual	◐ Por etiqueta manual	◐ Por regla
Contextualización por Machine Learning Clasifica los activos en tres dimensiones: sector de la industria, área de negocio propietaria, categoría — automáticamente.	✓ Machine Learning	○ No nativo	○ No nativo	○ No nativo	○ No nativo
Capa agéntica de decisión Agente que sintetiza las salidas de los modelos y decide la atribución final de propiedad, con retroalimentación humana en el loop.	✓ Nativo	○ No documentado	○ No documentado	○ No documentado	○ No documentado
Cadena digital hasta 3 niveles Mapea dependencias directas, subproveedores y el subproveedor del subproveedor (la categoría del caso Polyfill.io).	✓ 3 niveles · headless	◐ N1 parcial	◐ N1 parcial	◐ N1 parcial	◐ N1-N2 parcial

✓ Nativo — Capacidad dedicada en la plataforma
◐ Parcial — Vía módulo adicional o cobertura indirecta
○ No nativo — No documentado públicamente / requiere otro producto

Comparativa elaborada a partir de la documentación pública de los proveedores en mayo de 2026. Las capacidades de cada plataforma evolucionan; consulte al proveedor para confirmar la versión más reciente del roadmap.

COMPARATIVA · 02 · PRIORIZACIÓN, RIESGO Y MODELO

Dónde se detiene lo adyacente · y dónde continúa lo dedicado

Las capacidades en las que la divergencia entre el ASM dedicado y el EASM integrado en plataformas de VM adquiere carácter estructural, de arquitectura.

Ficha técnica 2026
CSURFACE

CAPACIDAD	CSURFACE	DEFENDER EASM	TENABLE EASM	QUALYS CSAM	RAPID7 SURFACE CMD.
Threat intel dinámico Índices de probabilidad de explotación, catálogos de explotación activa, exploit activo, indicadores de campaña — feed propietario en cada proveedor.	✓ Sensor propio	✓ Defender TI	✓ Tenable VPR	✓ Qualys TruRisk	✓ Insight TI
Velocidad de detección de vulnerabilidades nuevas Intervalo entre la publicación de una CVE y su detección en activos monitoreados — continuo × programado.	✓ < 24h · continuo	◐ Periódico	◐ Periódico	◐ Periódico	◐ Periódico
Monitoreo de credenciales filtradas Breach DBs, dark web, repositorios públicos — con validación activa no destructiva antes de la alerta.	✓ Nativo · validación activa	○ No nativo	○ No nativo	○ No nativo	◐ Vía IntSights
Validación de explotabilidad Diferencia "vulnerable" de "explotable en el contexto observado" — elimina el ruido de CVEs presentes pero inaccesibles.	✓ Nativo Validación activa de explotabilidad donde hay cobertura de pruebas, con monitoreo pasivo en el resto de la superficie.	○ No nativo	◐ Vía Tenable WAS	◐ Vía Qualys WAS	◐ Vía InsightVM
Cyber Risk Quantification (FAIR · ALE/VaR) Modelo FAIR formal con simulación de Monte Carlo, ALE y VaR P90/P99 — informe estándar para el consejo.	✓ Módulo CRQ · FAIR	○ No nativo	◐ Lumin · no-FAIR	◐ TruRisk · no-FAIR	◐ Score propio
Modelo SaaS standalone Operación independiente — no requiere la adquisición de la plataforma de VM/XDR del proveedor.	✓ Standalone	◐ Recomienda XDR	◐ Vinculado al .io	◐ Parte del VMDR	◐ Parte del Insight

Dónde se detiene lo adyacente, dónde continúa lo dedicado

Los módulos de EASM de estas plataformas entregan un descubrimiento externo consolidado — Defender EASM, heredero de RiskIQ, con un grafo de descubrimiento particularmente amplio — y funcionan bien dentro de suites que la organización ya opera. El diferencial de CSURFACE está en la atribución automática de propiedad y en la contextualización por ML, que reducen el esfuerzo de triaje manual y orientan la priorización hacia lo que es de hecho explotable.

La divergencia aparece sobre todo en cuatro frentes: atribución y filtrado vía ML, contextualización automática (propiedad, sector, categoría), cadencia de detección continua — CSURFACE opera en una ventana inferior a 24h, mientras que la actualización de los módulos integrados varía según el proveedor — y validación activa de explotabilidad donde hay cobertura de pruebas, con monitoreo pasivo en el resto de la superficie.

Coexistencia o sustitución — depende de la etapa. En organizaciones que operan EASM integrado como punto de partida, CSURFACE suma lo que falta: filtrado inteligente y atribución automática de propiedad, contextualización por ML, cadencia de detección continua y validación activa. En programas más maduros, CSURFACE puede sustituir al EASM integrado — la cobertura efectiva con baja tasa de falsos positivos suele justificar la consolidación.

Vea el gap en su superficie — Análisis preliminar