COMPARATIVO · 01 · CAPACIDADES CENTRAIS

ASM dedicado × EASM embutido em plataformas de VM

Comparativo objetivo, capacidade a capacidade, entre a CSURFACE — plataforma de Continuous Exposure Management dedicada — e os módulos de External Attack Surface Management oferecidos por plataformas de gestão de vulnerabilidades de larga escala.

Datasheet 2026
CSURFACE

A diferença em uma frase. O *EASM embutido* em plataformas de VM oferece descoberta básica — limitada à enumeração de subdomínios sobre nomes informados pelo cliente e à inspeção de SANs em certificados para inferir outros nomes possíveis. Sem filtragem de relevância nem inteligência de atribuição, o resultado tende a monitorar majoritariamente o que o cliente já conhece e a gerar volume elevado de falsos positivos. O *ASM dedicado* opera com foco em **descoberta com inteligência**, **velocidade de detecção contínua**, **priorização dinâmica** e **contextualização automática**. As tabelas abaixo mostram a divergência, capacidade a capacidade.

CAPACIDADE	CSURFACE	DEFENDER EASM	TENABLE EASM	QUALYS CSAM	RAPID7 SURFACE CMD.
Descoberta contínua sem agente Inventário externo da superfície de ataque, atualizado de forma contínua, sem instalação no ambiente do cliente.	✓ Nativo	✓ Nativo	✓ Nativo	✓ Nativo	✓ Nativo
Atribuição automática de propriedade Vincula ativo descoberto à organização e à área de negócio responsável, sem classificação manual.	✓ Nativo · ML	◐ Por inventário global	◐ Por tag manual	◐ Por tag manual	◐ Por regra
Contextualização por Machine Learning Classifica ativos em três dimensões: setor da indústria, área de negócio proprietária, categoria — automaticamente.	✓ Machine Learning	○ Não nativo	○ Não nativo	○ Não nativo	○ Não nativo
Camada agêntica de decisão Agente que sintetiza as saídas dos modelos e decide atribuição final de propriedade, com feedback humano em loop.	✓ Nativo	○ Não documentado	○ Não documentado	○ Não documentado	○ Não documentado
Cadeia digital até 3 níveis Mapeia dependências diretas, subfornecedores e subfornecedor do subfornecedor (categoria do caso Polyfill.io).	✓ 3 níveis · headless	◐ N1 parcial	◐ N1 parcial	◐ N1 parcial	◐ N1-N2 parcial

✓ Nativo — Capacidade dedicada na plataforma
◐ Parcial — Via módulo adicional ou cobertura indireta
○ Não nativo — Não documentado publicamente / requer outro produto

Comparativo construído a partir da documentação pública dos fornecedores em maio de 2026. Capacidades de cada plataforma evoluem; consulte o vendor para confirmação da versão mais recente do roadmap.

COMPARATIVO · 02 · PRIORIZAÇÃO, RISCO E MODELO

Onde o adjacente para · e onde o dedicado segue

As capacidades em que a divergência entre ASM dedicado e EASM embutido em plataformas de VM assume caráter estrutural, de arquitetura.

Datasheet 2026
CSURFACE

CAPACIDADE	CSURFACE	DEFENDER EASM	TENABLE EASM	QUALYS CSAM	RAPID7 SURFACE CMD.
Threat intel dinâmico índices de probabilidade de exploração, catálogos de exploração ativa, exploit ativo, indicadores de campanha — feed proprietário em cada fornecedor.	✓ Sensor próprio	✓ Defender TI	✓ Tenable VPR	✓ Qualys TruRisk	✓ Insight TI
Velocidade de detecção de vulnerabilidades novas Intervalo entre a publicação de uma CVE e a sua detecção em ativos monitorados — contínuo × agendado.	✓ < 24h · contínuo	◐ ~30 d · agendado	◐ ~30 d · agendado	◐ ~30 d · agendado	◐ ~30 d · agendado
Monitoramento de credenciais vazadas Breach DBs, dark web, repositórios públicos — com validação ativa não-destrutiva antes do alerta.	✓ Nativo · validação ativa	○ Não nativo	○ Não nativo	○ Não nativo	◐ Via IntSights
Validação de exploitabilidade Diferencia "vulnerável" de "explorável no contexto observado" — elimina ruído de CVEs presentes mas inacessíveis.	✓ Nativo	○ Não nativo	◐ Via Tenable WAS	◐ Via Qualys WAS	◐ Via InsightVM
Cyber Risk Quantification (FAIR · ALE/VaR) Modelo FAIR formal com simulação de Monte Carlo, ALE e VaR P90/P99 — relatório padrão para conselho.	✓ Módulo CRQ · FAIR	○ Não nativo	◐ Lumin · não-FAIR	◐ TruRisk · não-FAIR	◐ Score próprio
Modelo SaaS standalone Operação independente — não requer aquisição da plataforma de VM/XDR do fornecedor.	✓ Standalone	◐ Recomenda XDR	◐ Vinculado ao .io	◐ Parte do VMDR	◐ Parte do Insight

Onde o adjacente para, onde o dedicado segue

O EASM embutido em plataformas de VM entrega uma camada inicial de descoberta — útil como ponto de partida em organizações que já operam essas suítes. A cobertura, contudo, é restrita à enumeração sobre nomes informados pelo cliente e à inferência por SAN em certificados, sem filtragem de relevância nem atribuição automática. A consequência operacional é dupla: o programa investe esforço monitorando o que já é conhecido, e a fila de alertas inclui volume material de falsos positivos.

A divergência aparece em quatro frentes: descoberta com filtragem inteligente via ML, contextualização automática (propriedade, setor, categoria), velocidade de detecção contínua (< 24h × ~30 dias agendados) e validação ativa em duas camadas (exploitabilidade e credenciais). Essas capacidades não são acessórios: definem se o programa opera com janela de exposição de dias ou de meses.

Coexistência ou substituição — depende do estágio. Em organizações que operam EASM embutido como ponto de partida, a CSURFACE soma o que falta: descoberta com filtragem inteligente (reduzindo o ruído do EASM básico), contextualização automática, velocidade de detecção contínua e validação ativa. Em programas mais maduros, a CSURFACE pode substituir o EASM embutido — a cobertura efetiva com baixa taxa de falso positivo costuma justificar a consolidação.

Veja o gap na sua superfície — Análise preliminar