COMPARISON · 01 · CORE CAPABILITIES

Dedicated ASM × EASM embedded in VM platforms

An objective, capability-by-capability comparison between CSURFACE — a dedicated Continuous Exposure Management platform — and the External Attack Surface Management modules offered by large-scale vulnerability management platforms.

Datasheet 2026
CSURFACE

The difference in one sentence. Defender EASM (the successor to RiskIQ), Tenable, Qualys and Rapid7 are mature, widely adopted platforms with real EASM modules; Microsoft Defender EASM, in particular, operates a broad discovery graph. CSURFACE concentrates its differentiation in **automatic ownership attribution**, **ML-based contextualization**, **dynamic prioritization by what is actually exploitable** and a **continuous detection cadence**. This comparison is honest and made capability by capability: the tables below show where each approach stands out.

CAPABILITY	CSURFACE	DEFENDER EASM	TENABLE EASM	QUALYS CSAM	RAPID7 SURFACE CMD.
Agentless continuous discovery External attack surface inventory, continuously updated, with no installation in the customer environment.	✓ Native	✓ Native	✓ Native	✓ Native	✓ Native
Automatic ownership attribution Links a discovered asset to the organization and the responsible business area, with no manual classification.	✓ Native · ML	◐ By global inventory	◐ By manual tag	◐ By manual tag	◐ By rule
Contextualization by Machine Learning Classifies assets across three dimensions: industry sector, owning business area, category — automatically.	✓ Machine Learning	○ Not native	○ Not native	○ Not native	○ Not native
Agentic decision layer An agent that synthesizes the model outputs and decides final ownership attribution, with human feedback in the loop.	✓ Native	○ Not documented	○ Not documented	○ Not documented	○ Not documented
Digital chain up to 3 levels Maps direct dependencies, sub-suppliers and the sub-supplier's sub-supplier (the Polyfill.io case category).	✓ 3 levels · headless	◐ L1 partial	◐ L1 partial	◐ L1 partial	◐ L1-L2 partial

✓ Native — Dedicated capability in the platform
◐ Partial — Via add-on module or indirect coverage
○ Not native — Not publicly documented / requires another product

Comparison built from public vendor documentation in May 2026. Each platform's capabilities evolve; consult the vendor to confirm the most recent version of the roadmap.

COMPARISON · 02 · PRIORITIZATION, RISK AND MODEL

Where the adjacent stops · and where the dedicated continues

The capabilities in which the divergence between dedicated ASM and EASM embedded in VM platforms becomes structural, a matter of architecture.

Datasheet 2026
CSURFACE

CAPABILITY	CSURFACE	DEFENDER EASM	TENABLE EASM	QUALYS CSAM	RAPID7 SURFACE CMD.
Dynamic threat intel Exploitation probability indices, active exploitation catalogs, active exploit, campaign indicators — a proprietary feed in each vendor.	✓ Own sensor	✓ Defender TI	✓ Tenable VPR	✓ Qualys TruRisk	✓ Insight TI
Detection speed for new vulnerabilities Interval between the publication of a CVE and its detection on monitored assets — continuous × scheduled.	✓ < 24h · continuous	◐ Periodic	◐ Periodic	◐ Periodic	◐ Periodic
Leaked credential monitoring Breach DBs, dark web, public repositories — with active non-destructive validation before the alert.	✓ Native · active validation	○ Not native	○ Not native	○ Not native	◐ Via IntSights
Exploitability validation Distinguishes "vulnerable" from "exploitable in the observed context" — removes noise from CVEs that are present but inaccessible.	✓ Native Active exploitability validation where test coverage exists, with passive monitoring across the rest of the surface.	○ Not native	◐ Via Tenable WAS	◐ Via Qualys WAS	◐ Via InsightVM
Cyber Risk Quantification (FAIR · ALE/VaR) Formal FAIR model with Monte Carlo simulation, ALE and P90/P99 VaR — a standard report for the board.	✓ CRQ module · FAIR	○ Not native	◐ Lumin · non-FAIR	◐ TruRisk · non-FAIR	◐ Own score
Standalone SaaS model Independent operation — does not require acquisition of the vendor's VM/XDR platform.	✓ Standalone	◐ Recommends XDR	◐ Tied to .io	◐ Part of VMDR	◐ Part of Insight

Where the adjacent stops, where the dedicated continues

The EASM modules in these platforms deliver established external discovery — Defender EASM, the successor to RiskIQ, with a particularly broad discovery graph — and work well within suites the organization already operates. CSURFACE's differentiation lies in automatic ownership attribution and ML-based contextualization, which reduce manual triage effort and steer prioritization toward what is actually exploitable.

The divergence appears mainly on four fronts: ML-based attribution and filtering, automatic contextualization (ownership, sector, category), a continuous detection cadence — CSURFACE operates within a sub-24h window, while the refresh of embedded modules varies by vendor — and active exploitability validation where test coverage exists, with passive monitoring across the rest of the surface.

Coexistence or replacement — it depends on the stage. In organizations that operate embedded EASM as a starting point, CSURFACE adds what is missing: intelligent filtering and automatic ownership attribution, ML-based contextualization, a continuous detection cadence and active validation. In more mature programs, CSURFACE can replace embedded EASM — the effective coverage with a low false-positive rate tends to justify the consolidation.

See the gap in your surface — Preliminary analysis