TUSKIRA BUYER'S SHEET · NOVEMBER 2026

CTEM Platforms Compared

13 platforms by the CTEM stages they cover best, how they validate, how they close exposures, best fit and main caveat.

Tuskira

Vendor	Strongest stages	Validation model	Mobilization model	Best fit	Main caveat
Tuskira	Validation, mobilization (cross-stack)	Simulates exposures against deployed controls on a live context graph	Compensating controls deployed through your existing multi-vendor tools, then revalidated	Teams with mature discovery whose programs stall between list and closure	Consumes your existing discovery tools rather than replacing them
CrowdStrike Falcon EM	Discovery, prioritization, mobilization (in-platform)	Exposure context enriched by Falcon telemetry and threat intel	Automated response and remediation through Falcon Fusion SOAR	Falcon-committed shops wanting exposure management without another agent	Strongest where Falcon's sensors and ecosystem reach
Cymulate	Validation, mobilization (control-side)	Continuous control testing against known techniques (BAS)	Auto Mitigation and direct control updates via Mitigation Hub	Continuous evidence of control efficacy	Closure model is control-engineering and BAS-led, not full exposure-to-investigation-and-response
Horizon3.ai NodeZero	Validation, prioritization	Autonomous pentesting that chains real attack paths in production	Fix guidance plus Quick Verify retesting; integrations route findings to SOAR and SIEM	Teams that want frequent, attacker-proven pentest results without scheduling consultants	Center of gravity is offensive testing; discovery and closure lean on your other tools
Microsoft Security Exposure Management	Discovery, prioritization	Exposure graph with attack path simulation and choke points	Patch, mitigate, and fix items through Defender Vulnerability Management	Microsoft E5 and Defender shops wanting exposure context in the Defender portal	Third-party connectors move to consumption pricing at GA; public cloud only, no sovereign clouds
Palo Alto Networks Cortex EM	Prioritization, mobilization (in-platform)	AI-driven Precision Filtering across native and third-party scanner data	Ticketed patching or immediate mitigation through security controls	Cortex XSIAM customers consolidating vulnerability data into the SOC platform	Runs on Cortex XSIAM and its data lake, so fit is strongest where Cortex already anchors operations
Pentera	Validation	Continuous and on-demand execution of real attack techniques	Remediation workflows, ticket routing, and retesting, extended by DevOcean remediation operations	Teams that require exploit-level proof	Center of gravity is adversarial validation rather than cross-stack exposure-to-response
Picus Security	Validation, mobilization (control-side)	BAS, autonomous pentesting, and exploit-chain validation against your controls	Vendor-specific mitigations and compensating control recommendations, then revalidation	Teams that want control testing and exploitability proof from one vendor	Sold as individually licensed products, so full-loop coverage depends on which ones you buy
Qualys ETM	Discovery, prioritization, validation	TruRisk quantification plus TruConfirm validation orchestrated by Agent Val	Patch workflows plus TruRisk Eliminate patchless mitigations	Teams already standardized on Qualys agents	Strongest inside the Qualys ETM, agent, and remediation ecosystem
Rapid7 Exposure Command	Discovery, prioritization	Exploit likelihood and reachability scoring, plus runtime validation for cloud workloads	Remediation projects, SLAs, ticketing, and no-code automation	Rapid7 customers extending VM into cloud and attack surface exposure	Attack-based validation beyond cloud runtime comes mainly through Vector Command, a managed red team service
Tenable One	Discovery, prioritization	Exposure scoring, attack path context, and exploitability checks	Remediation workflows and Hexa AI ticket routing; one-click fixes for cloud/IAM surfaces	Broad exposure foundation across VM, cloud, identity	Closure is strongest within its own surfaces and ticketing
XM Cyber	Prioritization, validation (attack side)	Graph-based attack path and choke-point analysis	Prioritized fixes at choke points	Attack path visibility to crown jewels in hybrid AD/cloud	Defensive-control context and cross-stack closure are narrower
Zafran	Prioritization, validation (defense-aware)	Maps exposures against deployed controls to find what's effectively mitigated	Mitigation-first plans plus consolidated remediation tickets	Backlog reduction through control-aware prioritization	SOC investigation and response is not the main reason buyers choose it

Questions to ask every vendor

1. Run the evaluation **on your own data**.
2. Show a **low-severity finding you escalated**, with the evidence.
3. Show a **critical finding you deprioritized**, with the evidence.
4. Which **CTEM stages** does the product cover itself, and which does it hand off?
5. How does it **validate** an exposure: scoring, attack paths, simulation, or real exploit tests?
6. How does it **close** an exposure: tickets, patches, or changes to controls you already own?
7. Does it **re-test** after a fix to prove the exposure is closed?
8. What does it cost **for the stage you're fixing**?

Descriptions reflect public vendor information as of November 2026. Performance figures are vendor-reported; verify current capabilities with each vendor. Tuskira is one of the platforms listed. Platforms are listed alphabetically after Tuskira, not ranked. Full guide, with each platform's details and FAQ, at **tuskira.ai/blog/best-ctem-tools**