TUSKIRA BUYER'S SHEET · NOVEMBER 2026

Zero-Day Response Platforms Compared

11 platforms by how they find exposure, prove reachability, check your controls and act before a patch.

Tuskira

Platform	Finds presence by	Reachability and exploitability	Checks your controls	Acts before the patch	Best fit
Tuskira	Your existing scanners and tools, 200+ integrations	Reachable breach paths on a live model of your environment	Yes, against deployed controls, then re-tests	Recommends and applies a compensating control through tools you own, within limits you set	Teams that want one loop from disclosure to verified closure
CrowdStrike Falcon Exposure Management	Falcon sensor plus network scanning for unmanaged devices	ExPRT rating and attack path analysis	Falcon prevention context	Containment through Falcon response tools	Falcon-committed estates
Cymulate	Threat research mapped to your environment	Simulates new threats against your controls	Yes, breach and attack simulation	Pushes detection rules and IoCs to controls, then retests	Teams focused on control efficacy
Horizon3.ai NodeZero	Autonomous testing of your environment	Production-safe exploit tests for emerging CVEs	Classifies assets as exploitable, at risk or mitigated	No, retests after you fix	Teams that want exploit-level proof
Microsoft Defender Vulnerability Management	Defender for Endpoint	Exposure scoring	No	Blocks vulnerable application versions on Windows	Microsoft-centric Windows estates
Picus Security	Threat library and agents	Checks exploitability against your controls on disclosure day	Yes, step by step	Recommends a compensating control per step, then re-validates	Teams that want fast control-level validation
Qualys TruRisk Eliminate	Qualys agents, scanners and integrations	TruRisk scoring	Credits controls you already have	Patchless mitigation, isolation or custom fixes it deploys	Qualys-agent estates
Tenable One	Broad scanning across IT, cloud and OT	Exposure scoring and attack paths	Control validation added in 2026	Ticket and campaign-driven remediation	Teams that want the broadest detection
Vicarius vRx	Vicarius agent	Vulnerability prioritization	No	vShield blocks exploitation in memory without a patch	Mid-market teams with apps they can't patch
XM Cyber	Exposure data in its attack graph	Attack-graph context, with expert-reviewed CVE research	Models controls in its digital twin	Remediation plans to Jira and ServiceNow	Hybrid AD and cloud attack path visibility
Zafran	SBOM and connected tools	Runtime presence, internet reachability and threat intel	Checks how existing defenses are configured	Recommends mitigations through EDR, firewall and WAF	Vulnerability teams cutting backlog

Disclosure-day checklist

1. **Confirm the advisory.** Read the vendor advisory and CVE record for affected versions, configurations and prerequisites.
2. **Find presence.** Match affected versions against scanner results, SBOMs and asset inventory, including containers and internet-facing assets.
3. **Check exploit conditions.** Is the vulnerable component used, reachable from where an attacker would start, and does it need authentication?
4. **Check exploit activity.** Public proof of concept, CISA KEV listing, EPSS score, and active campaigns in threat intelligence.
5. **Map your controls.** Would a WAF virtual patch, IPS signature, EDR rule, segmentation or disabling the feature stop the attack?
6. **Apply and re-test.** Put the compensating control in place and re-test the path to prove it's closed.
7. **Track to the patch.** Patch when the fix ships, then retire the temporary control.
8. **Time it.** Measure disclosure to a verified closing control, not disclosure to ticket.

Descriptions reflect public vendor information as of October 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-zero-day-response-platforms**