seemplicity

The Exposure Management Platform Buyer's Checklist

Core features to look for in a vendor solution

When evaluating Exposure Management platforms, organizations should prioritize solutions that go beyond traditional vulnerability management. The ideal platform should provide continuous exposure visibility, automated remediation workflows, and seamless cross-team collaboration to ensure vulnerabilities and exposures are resolved efficiently. Below is a checklist of must-have capabilities to help guide vendor selection.

☐	**CENTRALIZED RISK VISIBILITY**	Consolidates security findings across testing solutions for a single source of truth.
☐	**SMART REMEDIATION GROUPING**	Consolidates multiple security findings that require the same fix into a single remediation task, reducing duplicate efforts and improving efficiency.
☐	**CUSTOMIZABLE SCORING MODELS**	Allows organizations to adjust risk scores according to their organization's unique risk tolerance, frameworks and business objectives.
☐	**INTELLIGENT TEAM ASSIGNMENTS**	Supports nested business units, security groups, and team-based remediation assignments, ensuring the right teams handle the right issues.
☐	**AUTOMATED REMEDIATION WORKFLOWS**	Auto-generates tickets, assigns remediation tasks, and tracks resolution.
☐	**SEAMLESS IT & DEVOPS INTEGRATION**	Works natively with tools like ServiceNow, Jira, and CI/CD pipelines.
☐	**EXCEPTION & RISK ACCEPTANCE MANAGEMENT**	Provides workflows to document, track, and periodically re-evaluate accepted risks, false positives, and justified exceptions.
☐	**AUTOMATED SLA TRACKING & RISK-BASED ESCALATIONS**	Monitors remediation timelines, triggers alerts for overdue tasks, and escalates vulnerabilities if SLA deadlines are approaching.
☐	**FIX CLOSURE VERIFICATION**	Uses incoming scanner results to verify that vulnerabilities marked as "fixed" are no longer detected, preventing false closures.
☐	**NO PROFESSIONAL SERVICES REQUIRED**	Straightforward setup with intuitive automation workflows.