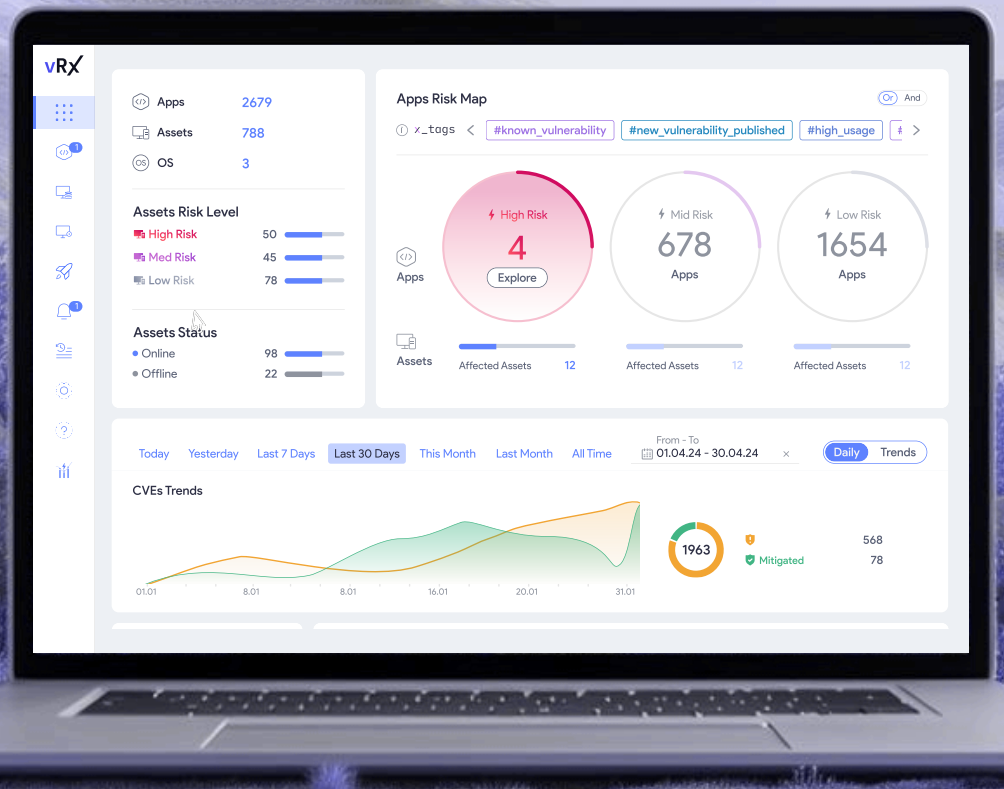
vicarius

How to choose the right Vulnerability Management Platform



Introduction

The attack surface is growing as remote work, BYOD, and cloud adoption expand. Traditional scans and patch cycles can't keep up. Now, hackers use AI to craft exploits in minutes, making speed essential. Organizations need tools that continuously find assets, prioritize risks, automate remediation, and deliver real-time visibility to act before attackers do.

This playbook focuses on **Vulnerability Management Platforms**, solutions that identify, assess, prioritize, and remediate vulnerabilities across an organization's environment. They provide continuous scanning, risk-based prioritization, and seamless integration with patching and security tools to reduce exposure and strengthen resilience.

Each section below lists must-have capabilities and practical tips for evaluating vendors, followed by a scorecard framework that buyers can customise to their needs.

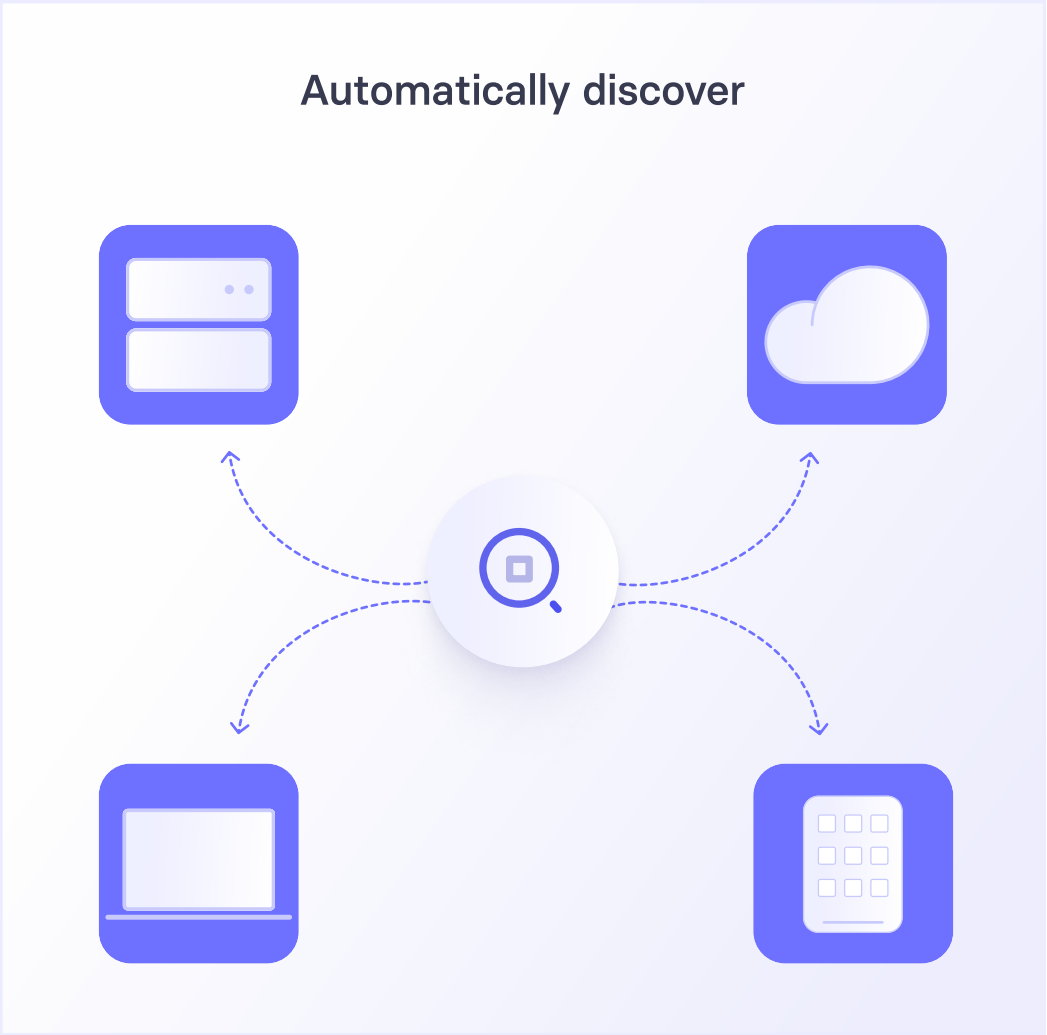
Vulnerability Management Platforms

Entity impacted

Vulnerability management is a **continuous, strategic process** focused on identifying, assessing, prioritising and remediating security weaknesses across an organisation's systems. Patch management is a tactical process within vulnerability management that applies software updates, but vulnerability management covers all exposures and involves asset discovery, scanning, risk assessment, remediation planning and continuous monitoring. The goal is to reduce overall risk exposure by mitigating as many vulnerabilities as possible.

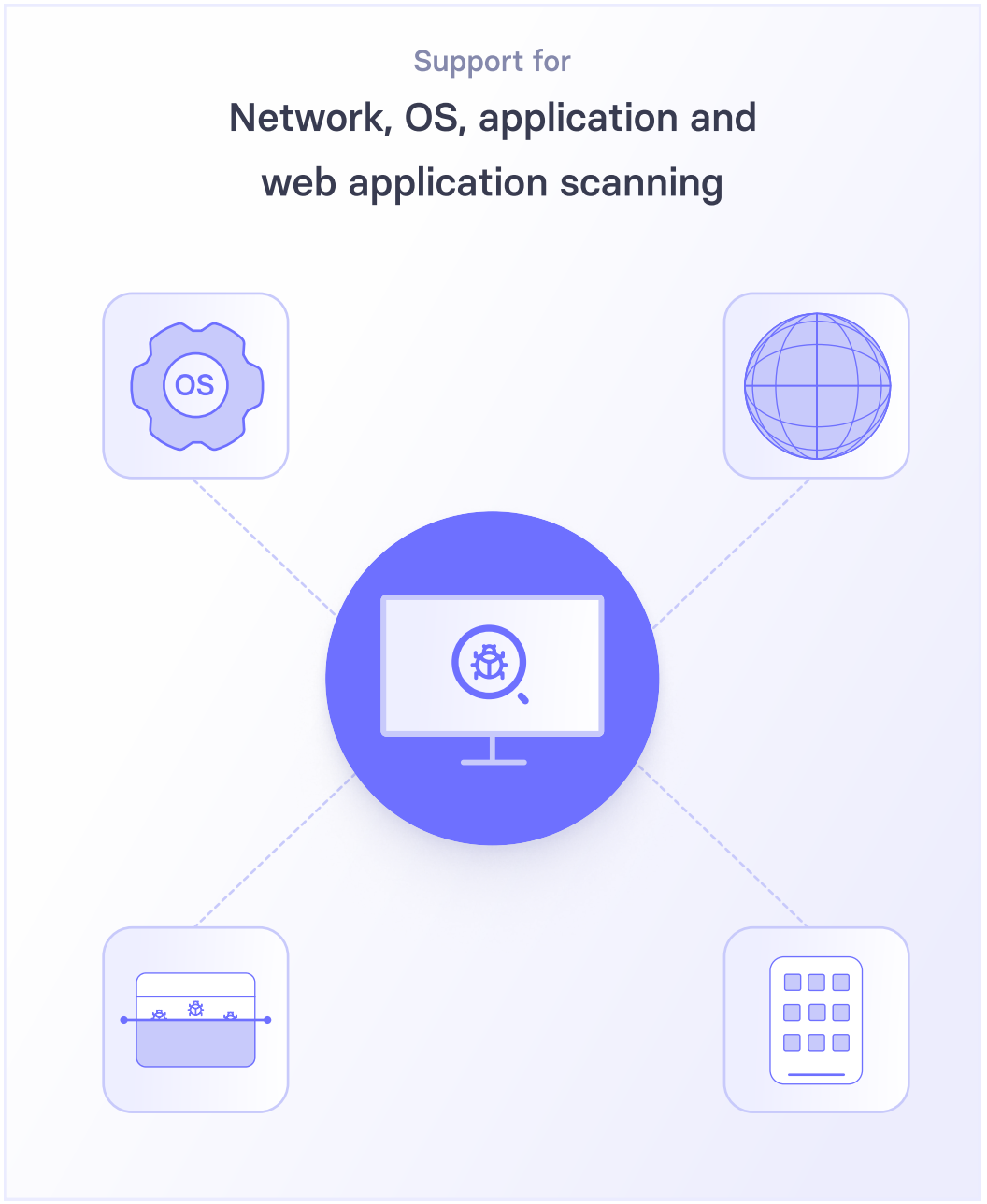
Continuous asset discovery & inventory

Vulnerability Management Platforms should automatically discover all devices, servers, applications, containers and cloud resources. Look for integration with asset inventory systems and support for on prem, cloud, OT and IoT, if available as part of a single platform all the better. Visibility is the foundation for scanning and patching.



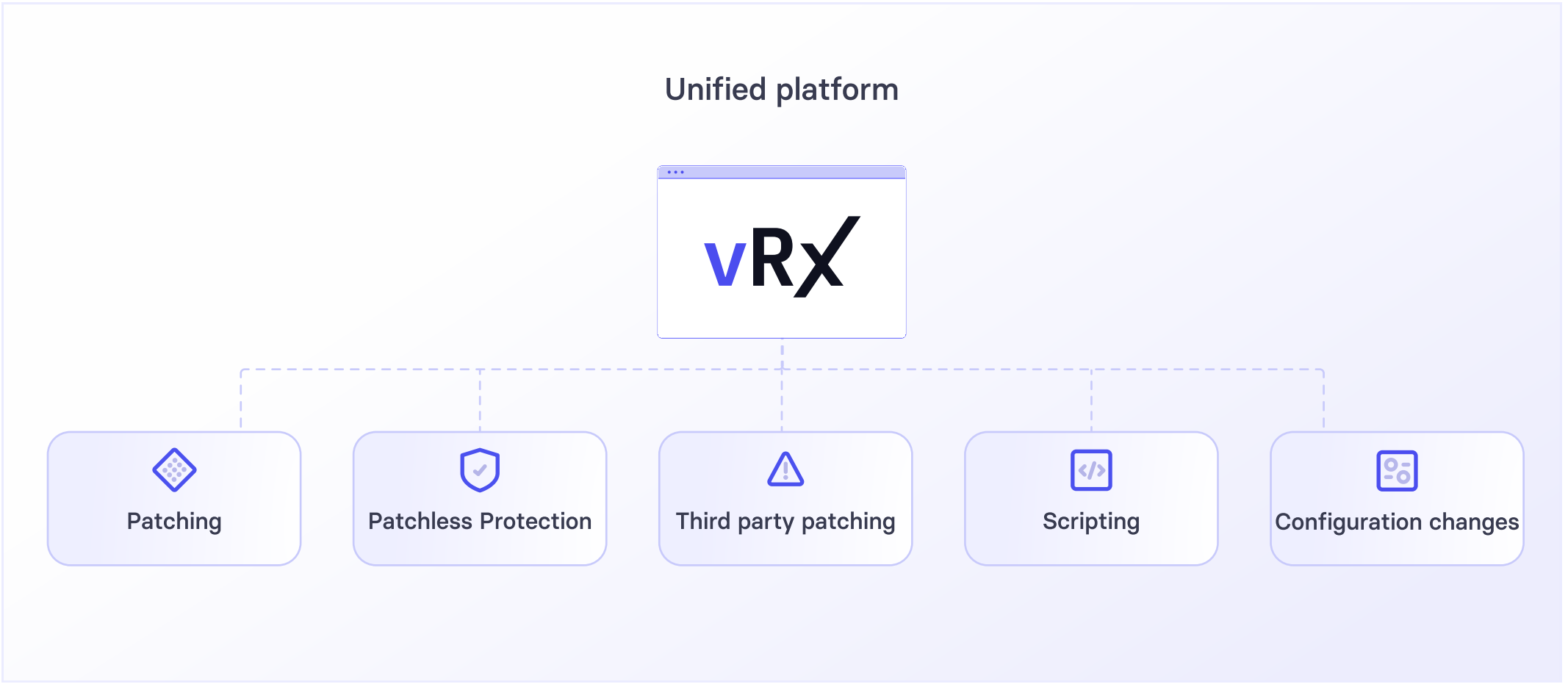
Comprehensive vulnerability scanning

Support for network, operating system, application and web-application scanning across heterogeneous environments. Prefer platforms that offer continuous scanning (scheduled and on-demand) and maintain up-to-date vulnerability feeds. Avoid tools that scan only once per month.



Patch management & automated remediation

Vulnerability Management Platforms should integrate with patch management systems or better yet and highly recommended provide built-in patching to deploy updates across OSs and third-party applications. Look for script-based remediation and virtual patching for cases where no official patch exists.

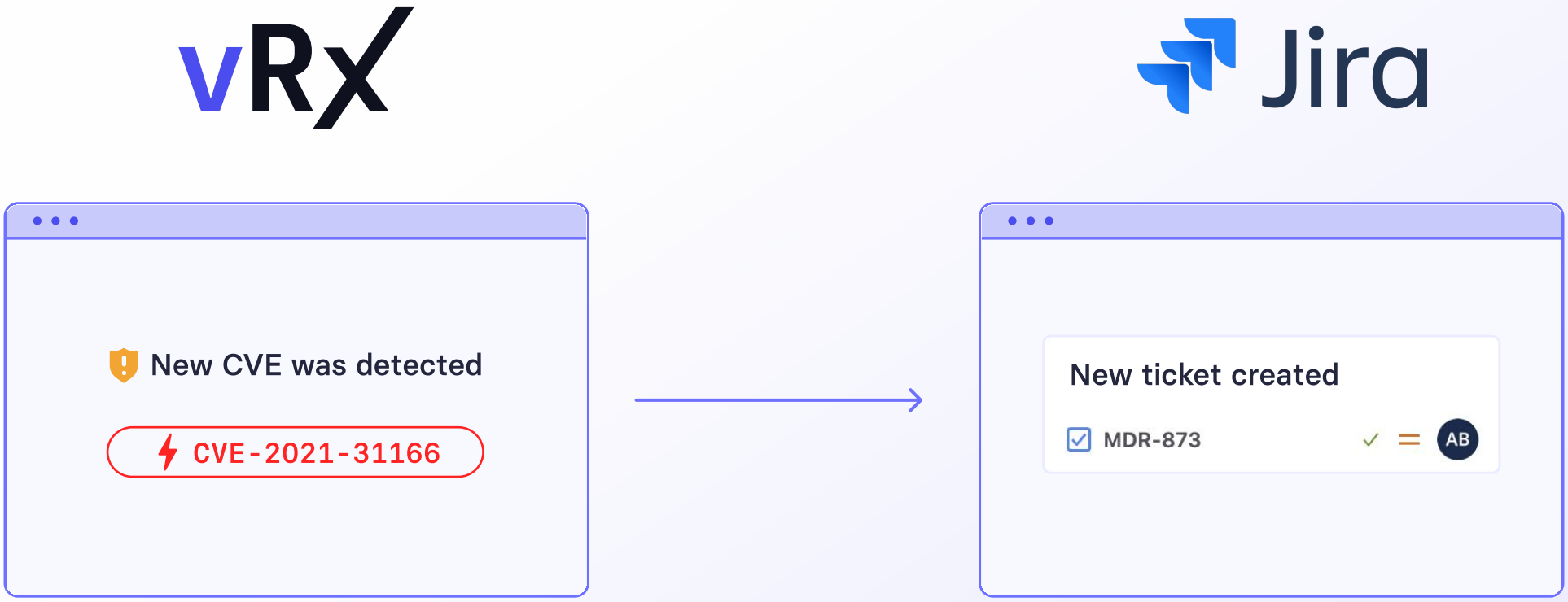


Risk-based prioritization

The platform should prioritise vulnerabilities using context beyond CVSS scores, considering exploit availability, asset criticality and business impact. This prevents teams from being overwhelmed by low impact issues. Choose vendors that provide custom risk scoring and integrate threat intelligence feeds.

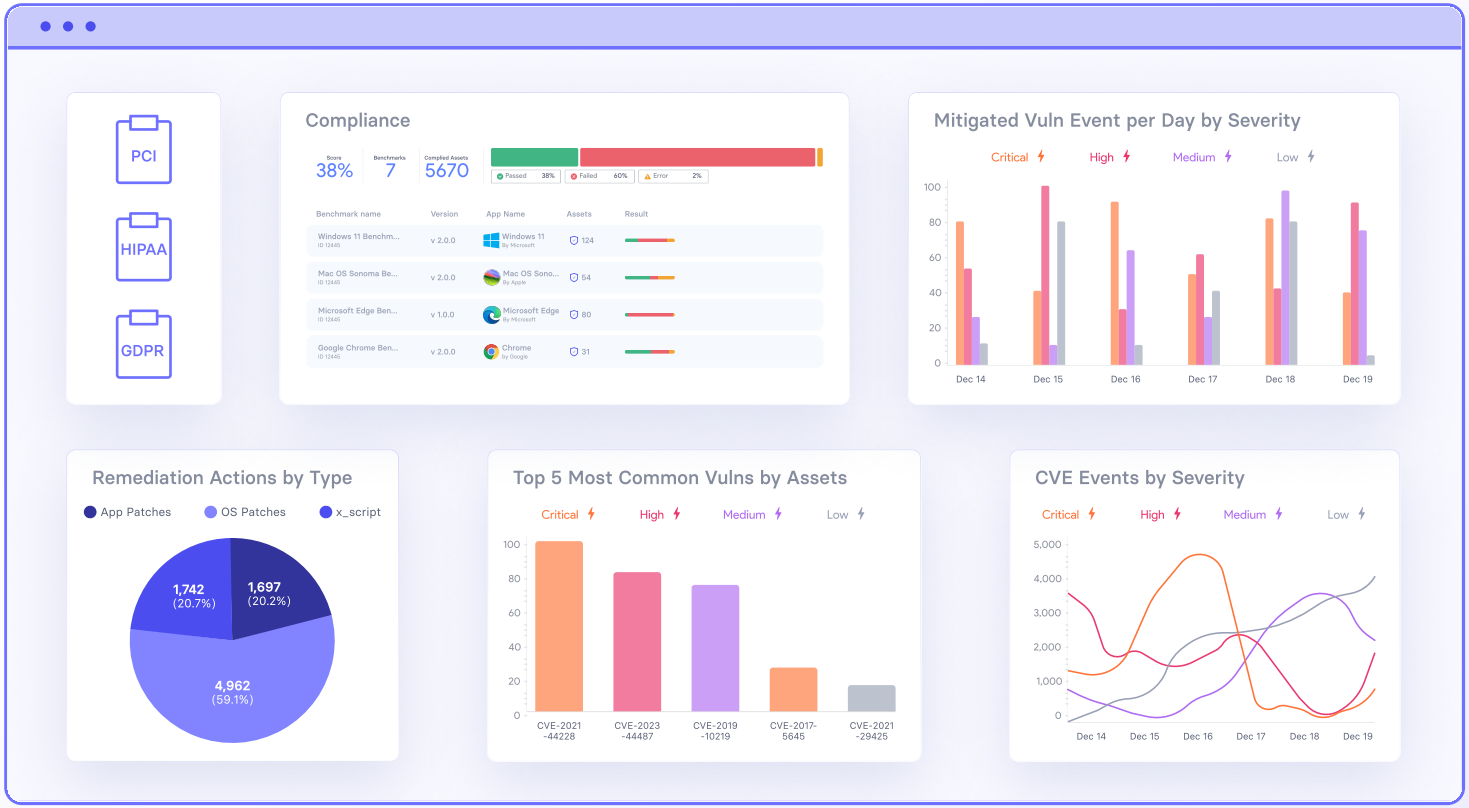
Workflow & ticketing integration

Ability to create remediation tickets in ITSM solutions (ServiceNow, Jira) and track progress through closure. Support for approval workflows, notifications and assignment to the right teams.



Reporting & compliance

Support for audit ready reports (PCI, HIPAA, GDPR) and dashboards showing vulnerability status, risk trends, mean time to remediate (MTTR) and SLA compliance.



Integration with SIEM, configuration management & threat intelligence

Look for built-in connectors to SIEM/SOAR platforms, configuration management databases (CMDB), and threat intelligence feeds. This enables correlation of vulnerability data with security events and misconfiguration checks.

Scalability & performance

Assess how the platform scales to thousands of endpoints and supports multi-tenant deployments. Evaluate performance impacts on network and endpoints during scans.

User experience & automation

A modern UI with dashboards, drill-down capabilities and visualisation helps teams understand risk. Policy-driven automation reduces manual workloads and headcount

Remediation guidance & knowledge base

The platform should provide clear fix recommendations, link to relevant CVE entries and support script creation or pre-built remediation scripts. Evaluate vendor documentation, community forums and support quality.

Score Card

Entity impacted

Rate each capability from 1 (Poor) to 5 (Excellent) for each vendor you evaluate.

Then, multiply each score by its Weight to calculate the Weighted Score.

Add up all weighted scores to get a total score out of 100.

Capability	Why It Matters	Weight	Your rate
Continuous Asset Discovery & Inventory	Foundation for visibility across all devices, cloud, OT, and IoT assets.	10	
Comprehensive Vulnerability Scanning	Identifies weaknesses across OS, network, apps, and web.	10	
Risk-Based Prioritisation	Focuses remediation on the most critical vulnerabilities using exploit data and asset value.	12	
Patch Management & Automated Remediation	Enables actual fixing, not just detection, key to faster MTTR.	12	
Workflow & Ticketing Integration	Ensures vulnerabilities are assigned, tracked, and closed.	8	
Reporting & Compliance Dashboards	Demonstrates audit readiness and ongoing progress to stakeholders.	8	
Integration with SIEM / CMDB / Threat Intel	Correlates vulnerabilities with events and misconfigurations for deeper insights.	8	
Scalability & Performance	Handles large, hybrid environments with minimal disruption.	7	
User Experience & Automation	Improves adoption, efficiency, and reduces analyst workload.	7	
Remediation Guidance & Knowledge Base	Provides clear, actionable fixes and scripts.	6	
Third-Party / Supply Chain Coverage	Detects vulnerabilities in dependencies and libraries.	4	
Cloud & Container Support	Secures modern workloads, registries, and serverless assets.	4	
Accuracy / False Positives Handling	Prevents alert fatigue and wasted remediation time.	2	
Data Privacy & Retention Controls	Meets your regulatory and compliance requirements.	2	