Qualys.

VMDR with ServiceNow

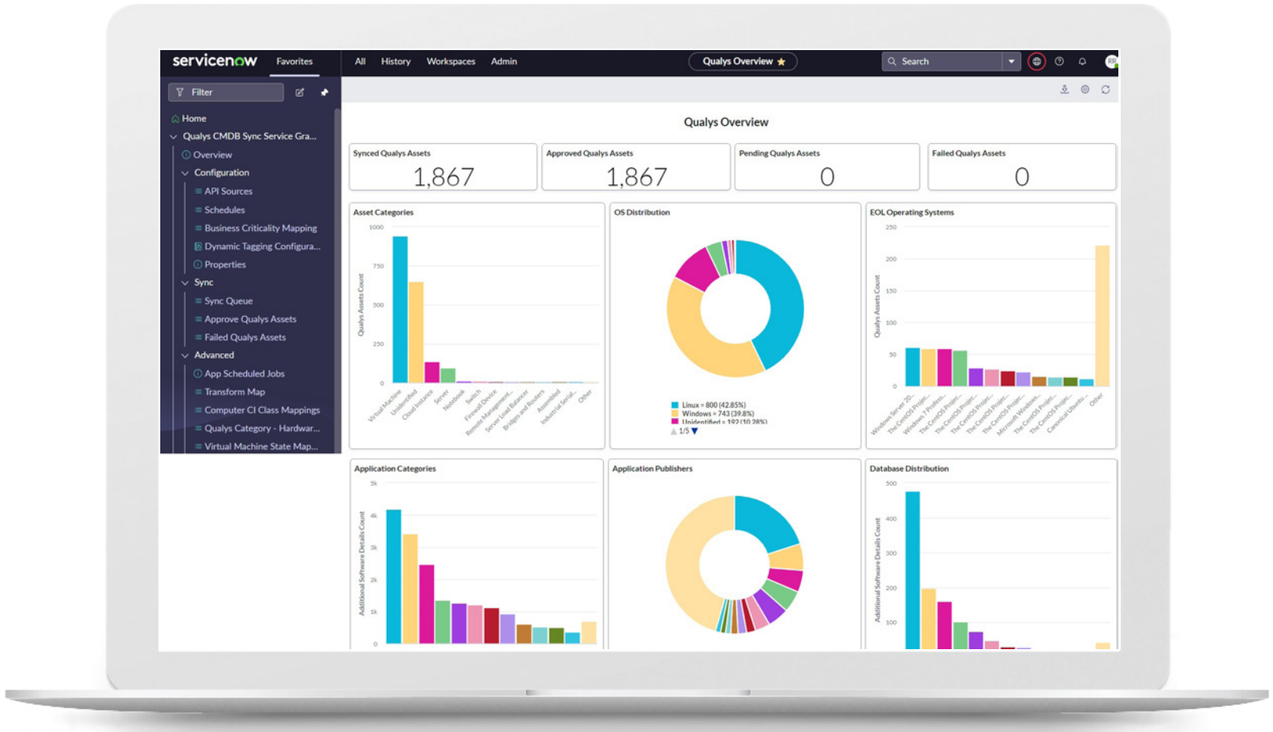
Bridging the Gap Between IT and Security

As organizations face the growing challenge of managing vulnerabilities, both IT practitioners and security analysts struggle to address the end-to-end lifecycle of vulnerability management. Traditional manual processes, such as sending spreadsheets or PDF reports, are insufficient for IT teams to effectively prioritize and track the status of remediation efforts. Meanwhile, security teams are burdened with identifying and classifying vulnerabilities but struggle to ensure their recommendations are acted upon on time.

To achieve more effective vulnerability management, it is crucial for both IT and security teams to work together and align their efforts. This requires a unified solution that can integrate with existing tools and provide a shared context for vulnerability remediation. This solution should enable real-time collaboration between teams, prioritize remediation efforts, and allow for the tracking of remediation tickets from investigation to resolution.

By bridging the gap between IT and security, organizations can better manage vulnerabilities and reduce their overall cyber risk.

> *"On average, Attack Surface Management tools will find 30% more surface area assets than IT was aware of."*
>
> Forrester Research



Qualys VMDR with TruRisk automates the vulnerability management process by integrating with ITSM tools like ServiceNow and Jira. This eliminates manual spreadsheet-based workflows and enables organizations to automatically create tickets, assign them to rightful owners, and close them out once the vulnerabilities are remediated. Significantly streamlining the workflow and improving efficiency.

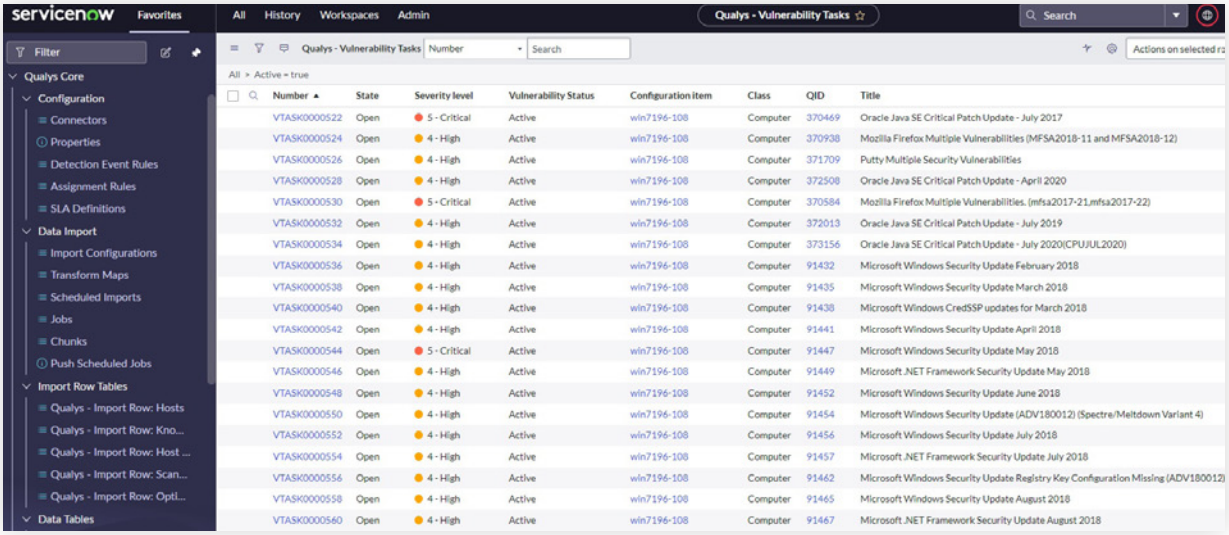
Maintaining an accurate asset inventory

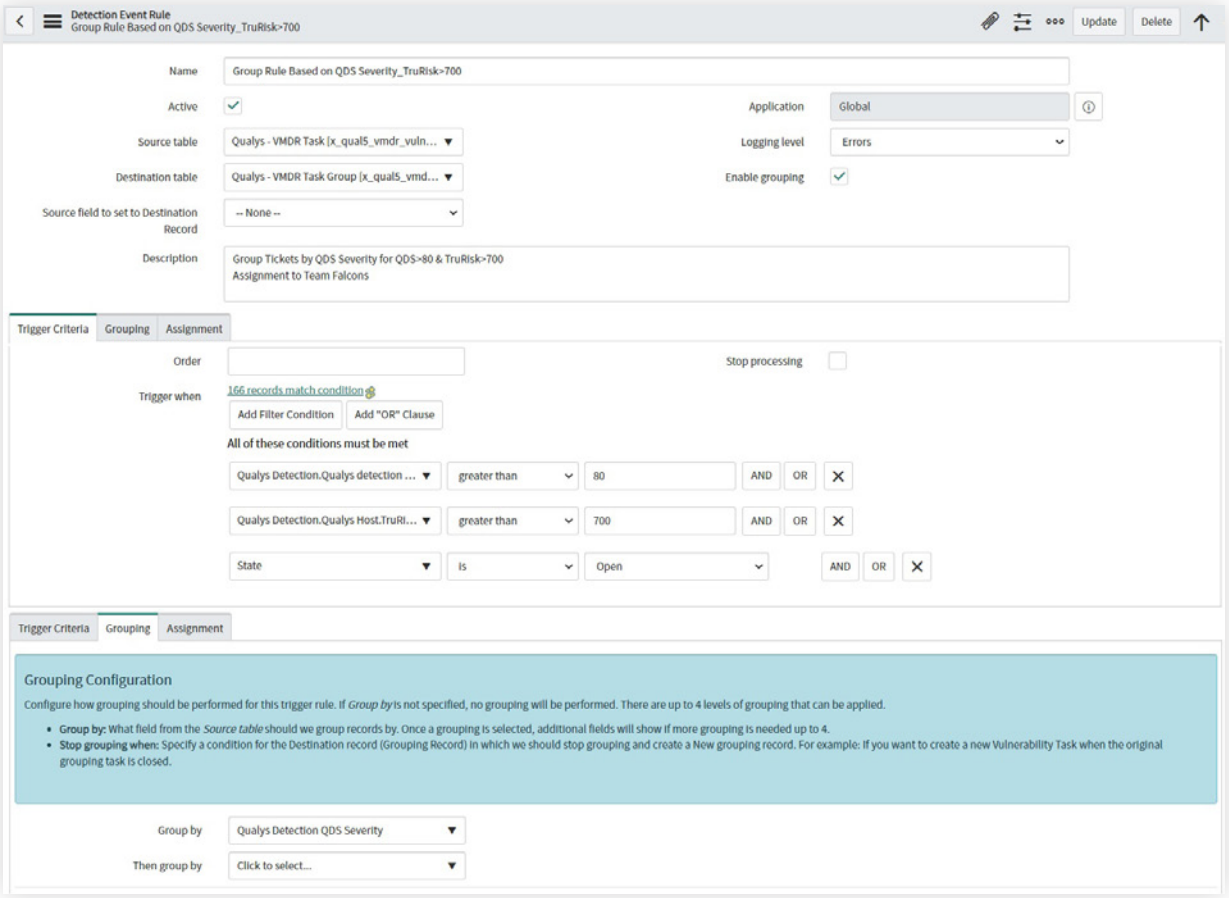
To reduce cyber risk and protect against hidden vulnerabilities, it is crucial to have a complete and accurate inventory of all assets and prioritize remediation efforts.

By adding Qualys Cyber Security Asset Management (CSAM) to the mix, organizations gain visibility into internal assets, but also get oversight over previously unknown, external internet-facing assets. With this extended External Attack Surface Management (EASM) capability, VMDR with TruRisk can automatically classify assets based on their criticality wherever they are located within the extended enterprise. With the CMDB plugin with solutions like ServiceNow, IT and security stakeholders can be assured both asset inventories and vulnerability management programs are operating with up-to-date asset criticality assessments for both internal and external assets.

Key Use Cases for VMDR with ServiceNow

USE CASE CHALLENGE	SOLUTION	OUTCOMES
Maintain Accurate CMDB With brokered IT and security infrastructure, combined with hybrid, multi-cloud environments, maintaining an accurate CMDB is both time-consuming and difficult.	VMDR and Qualys Cyber Security Asset Management (CSAM) are directly integrated with ServiceNow CMDB to maintain an accurate inventory of all assets across your organization.	Customers with Qualys VMDR, and CSAM can match up to 96% of the assets in Qualys Cloud Platform and ServiceNow CMDB, ensuring an accurate and always up to date CMDB for organizations.
Bridging the Gap between IT & Security Processes of vulnerability discovery, patch management, and remediation span several steps of action that require multiple tools and include various stakeholders from both IT and security teams. As a result, security and IT stakeholders are challenged with cyber risk becoming an overarching concern and shared KPI between both departments.	VMDR, Qualys Patch Management and CSAM with EASM integrate with ITSM tools, including ServiceNow and Jira to automatically create tickets, assign them to rightful owners, and close them out upon remediation. Providing end-to-end visibility for all security and IT stakeholders.	With VMDR, and Qualys Patch Management practitioners can remediate vulnerabilities up to 40% faster. More time spent in high-value tasks and less time spent on vulnerability analysis and reporting due to reduced ticketing complexity, automated reporting and improved coordination between security operations, IT operations and respective cyber risk leaders and C-level executives.
Achieving Oversight Over External Internet-facing Assets Unknown internet-facing assets are about 30% of any organization's application infrastructure, resulting in blind spots and elevated cyber risk. While VM is the cornerstone of a security stack, External Attack Surface Management (EASM) is increasingly necessary for organizations to improve security coverage and reduce their exposure to cyber risk.	VMDR and CSAM with EASM provides consolidated asset and vulnerability insights for a unified view over the entire attack surface. Deployed with the Qualys lightweight agent or via the comprehensive Qualys sensor ecosystem, you achieve improved threat detection, automated remediation workflows, and a risk-based approach to cybersecurity that works across the entire enterprise.	Reduced MTTR and better asset visibility lets you measure cyber risk improvements over time with a single, consolidated platform. With VMDR and CSAM with EASM, you can now extend the best in VM and ITSM functionality to external, previously unknown asset security. IT and security teams can work in concert and transparency to close out vulnerabilities everywhere.
Managing Organization from EOL/EOS Software The hybrid conventional security perimeter is from the datacenter to remote, external internet-facing assets. This creates new challenges for VM and security practitioners, including securing their environment from unapproved, exploited, or EOL/EOS applications. Organizations require accurate asset inventories that include software applications in addition to traditional assets.	VMDR and CSAM with EASM comes with EOL/EOS software tracking compliant with CISA guidelines to help expose baseline discrepancies, including VMs, containers, and functions-as-a-service. By identifying deviations from established baselines, VMDR and CSAM with EASM discover and support remediation of untracked, external-facing software instances and services.	Continuous enumeration of unknown assets and services automatically baselines asset inventories across the entire ecosystem, improving security hygiene, optimizing IT-security coordination, and reducing exposure to cyber risk. Shadow-IT risk is inherently and automatically mitigated as a result.
Risk Based Prioritization Assets and applications are exposed to a rising number of vulnerabilities and targeted malware that can infect various areas of the network due to increased connectivity between IoT and IT networks. 70% of vulnerabilities can be exploited without needing special privileges. Practitioners must identify and isolate vulnerabilities faster than ever before to minimize the risk of lateral movement of malware.	VMDR with TruRisk assigns criticality scores using tags that reflect the relative criticality specific to your individual business for assets in ServiceNow. Relying on the industry-leading risk-based prioritization with dynamic tagging, practitioners can prioritize the most critical assets and vulnerability actions accordingly.	Qualys VMDR with TruRisk combines business criticality information from ServiceNow, to measure and visualize cyber risk across your entire infrastructure. This provides a clear, concise picture of an organization's risk levels across business units and geographic locations. Allow organizations to make risk-based prioritization decisions, and take actions to reduce risk.





Learn more about VMDR with IT Service Management. Try it for 30 days.
qualys.com/try/vmdr/

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of disruptive cloud-based Security, Compliance, and IT solutions with more than 10,000 subscription customers worldwide, including a majority of the Forbes Global 100 and Fortune 100. Qualys helps organizations streamline and automate their security and compliance solutions onto a single platform for greater agility, better business outcomes, and substantial cost savings. Qualys, Qualys VMDR®, and the Qualys logo are proprietary trademarks of Qualys, Inc. All other products or names may be trademarks of their respective companies.

For more information, please visit **qualys.com**