Qualys

Qualys & ServiceNow

IT and Security Collaboration Made Easy

Organizations are exposed to a growing level of cyber risk that is increasingly unmanageable and distributed. Both IT and Security practitioners face the challenge of navigating their organization through an expanding attack surface with limited visibility of external assets, manual CMDB updates, and time-consuming patching and remediation workflows that reduce resiliency and increase exposure to cyber risk.

Qualys and ServiceNow are slashing cyber risk by bridging the IT-Security gap with an integration that provides:

Keep your CMDB updated and **increase visibility by up to 30%** with expanded views of all Internet-facing assets

Close tickets up to 50% faster with automated IT-SecOps bidirectional workflows

Measure tech debt with EOL/EOS software tracking

79%

of organizations acknowledge an **asset visibility gap**, leading to 3X more incidents.

Enterprise Strategy Group (ESG)

With the seamless integration of Qualys and ServiceGraph, customers can boost their CMDB with high-fidelity data, expand their visibility to all external and ephemeral internet-facing assets, and improve threat remediation with automated bi-directional workflows, operating out of the Qualys or ServiceNow interface. By bridging the gap between IT and security, organizations can better manage vulnerabilities and reduce their overall cyber risk.

Detecting and remediating vulnerabilities across the extended enterprise is hard enough. Why make things more complicated? Automate remediation activities and boost your CMDB with bidirectional workflows between ServiceNow and the Qualys Platform. Eliminate manual spreadsheet-based activities and enable IT and Security teams to automatically create tickets, assign them to rightful owners, and close them out once the vulnerabilities are remediated.

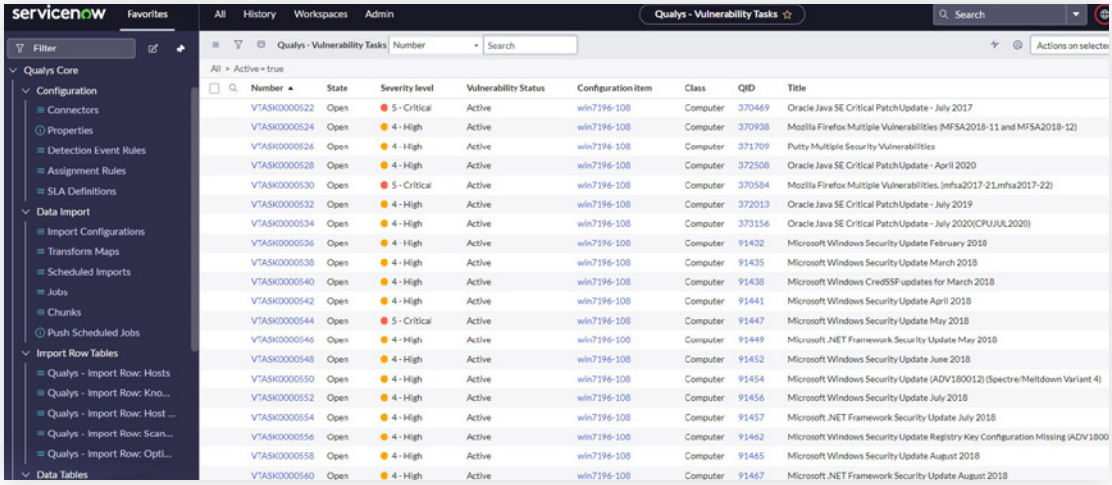
Key Use Cases for Qualys & ServiceNow

USE CASE CHALLENGES	SOLUTION	OUTCOMES
Boost CMDB with High-Fidelity Data With brokered IT and security infrastructure, combined with hybrid, multi-cloud environments, maintaining an accurate CMDB is time-consuming and difficult. Without an accurate CMDB, IT cannot accurately document what assets they have in the field or how they are impacting each other, leading to elevated cyber risk.	VMDR and Qualys Cyber Security Asset Management (CSAM) are directly integrated with ServiceNow CMDB, boosting CMDBs with high-fidelity data for all asset types.	With Qualys VMDR and CSAM, customers can match up to 96% of the assets in Qualys Cloud Platform and ServiceNow CMDB. This ensures an accurate and always up-to-date CMDB for organizations that both IT and Security teams can leverage.
Expand Visibility to 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 from Qualys provides consolidated asset and vulnerability insights for a unified view over the entire attack surface. With Qualys, IT and Security practitioners gain a complete 360-degree view across their entire network, including ephemeral external internet-facing assets that may have otherwise gone unnoticed and unreported.	Complete asset visibility lets you measure cyber risk improvements over time with a single, consolidated platform. With VMDR and CSAM with EASM, customers can now extend the best in VM and ITSM functionality to external, previously unknown assets within a hybrid environment.
Managing 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.
Automate IT-SecOps Workflows 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.	With the extensive Qualys platform, IT teams can leverage no-code workflows, drag-and-drop remediation monitoring, automated patching actions, and bidirectional workflows between Qualys apps and ServiceNow that make IT-SecOps collaboration fast, easy, and accurate.	Save up to 50% time on remediation with Qualys Patch Management and visualize cyber risk across your entire infrastructure thanks to unified dashboards for all geo-distributed network locations and assets within your network.

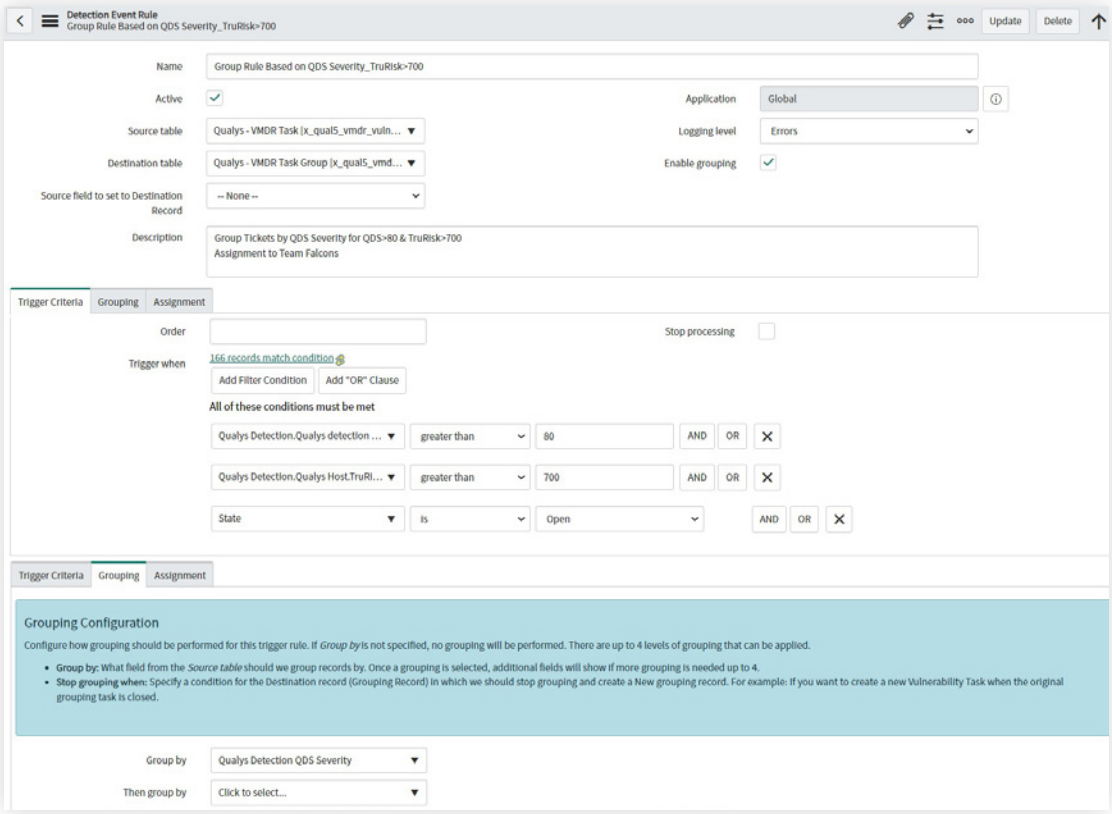
Bring IT and Security Teams Together

To reduce cyber risk and optimize IT-Security workflows, it is crucial to maintain an accurate CMDB and complete asset inventory. 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, the Qualys Platform can automatically classify assets based on their criticality wherever they are located within the extended enterprise. Together with ServiceNow, IT stakeholders can be assured both asset inventories and patching actions are up to date.



Monitor and prioritize vulnerability remediation using the ServiceNow interface thanks to bidirectional workflows from Qualys



Create rule-based trigger criteria for automated remediation actions across geo-distributed, multi-network environments.

Learn more about Qualys integrations with IT Service Management. Try it for 30 days.

qualys.com/free-trial

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**