imagineX

Qualys.

Qualys CSAM
Service Offering

CSAM

Improve asset visibility and reduce mean time to remediation with Qualys

Gaining comprehensive visibility and control over your entire IT asset landscape is foundational to a strong security posture. This includes understanding all internal and external-facing assets – from servers and workstations to cloud instances, web applications, and network devices – which collectively form your potential attack surface. Incomplete asset inventories leave critical blind spots that attackers can exploit.

Qualys CyberSecurity Asset Management (CSAM) provides continuous discovery, classification, and remediation across your complete IT ecosystem. By delivering a unified, real-time inventory of both known and previously unknown assets, Qualys CSAM empowers you to proactively identify vulnerabilities, manage technical debt, and strengthen your overall security. This comprehensive visibility extends to your external attack surface, ensuring you're aware of and can secure all internet-facing assets before attackers can leverage them.

With Qualys CSAM, you gain a centralized platform for managing your entire asset lifecycle, improving IT hygiene, and reducing risk. This includes enhanced visibility into your external footprint, allowing you to proactively address potential exposures and build a more resilient security posture from the inside out.

- Complete asset and software visibility across distributed hybrid environments
- Improve threat prioritization with asset criticality ratings (Reduce MTTR)
- Reduce technical debt with real-time EOL/EOS software tracking compliant with CISA guidelines
- Synchronized with CMDB for comprehensive inventory of managed and unmanaged assets

Why ImagineX

ImagineX accelerates the realization of value from Qualys deployments, combining extensive product knowledge with practical, security-focused services honed over 50+ collective years.

ImagineX provides targeted expertise across the Qualys suite, including CSAM, VMDR, Policy Audit, Patch Management, TotalCloud, and ETM/mROC. We accelerate time-to-value through tailored implementation strategies, insightful assessments that identify critical gaps, and seamless custom integrations that enhance existing security ecosystems.

Trusted by leading organizations, including top 500 enterprises, ImagineX has a demonstrated history of enhancing Qualys implementations. With over 150 successful projects delivered since 2016, our expertise translates into tangible security gains for complex environments.

ImagineX's status as a Qualys mROC Alliance Partner signifies our enhanced capabilities in delivering full-spectrum Qualys services. We bridge the gap between technical findings and business impact, ensuring risk management decisions are strategically informed and aligned with your organization's risk appetite.

ImagineX and Qualys

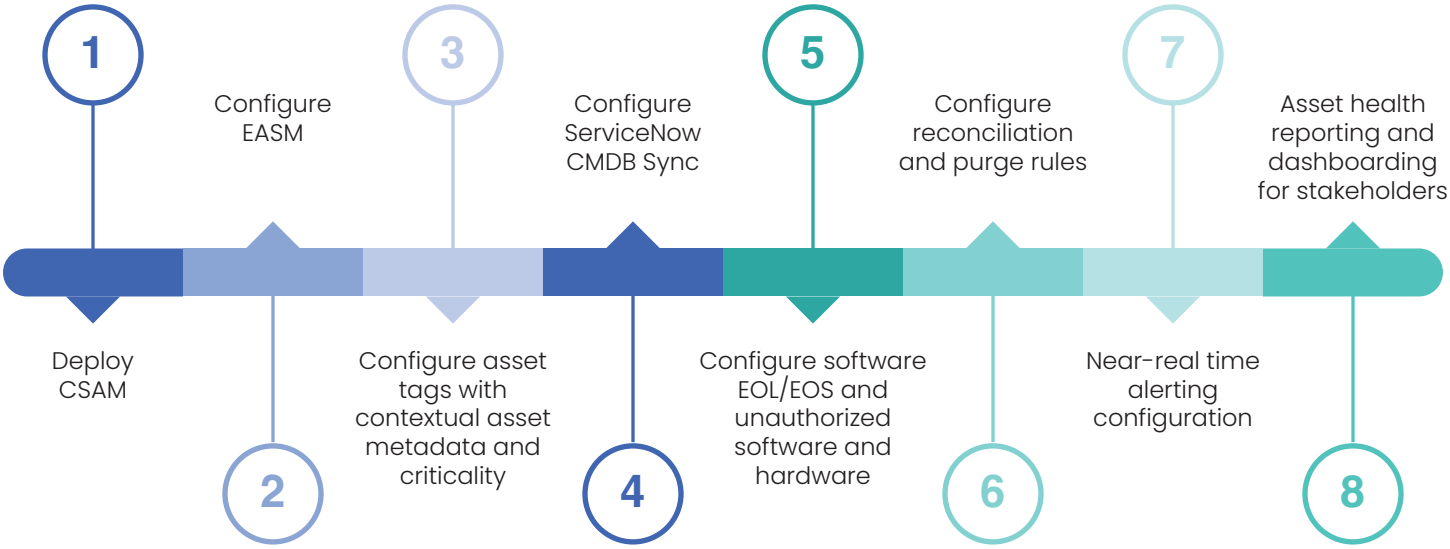
82	1 of 3	150+
World Class Net Promoter Score	U.S. Qualys mROC Alliance Partners	Qualys-related projects

Contact us at Qualys@imaginexdigital.com

Methodology

An effective implementation of Qualys CSAM will enable organizations to manage their cybersecurity posture continuously. Steps in this methodology include: defining the assessment scope, configuring the CSAM platform and sensors, and analyzing data to identify cybersecurity issues. Remediation of any issues coupled with ongoing monitoring ensures that your environment remains secure.

8-Step Implementation Plan



CSAM SERVICES

We work with our client stakeholders, tailoring our services to address the specific needs in three key areas: Discovery, Detection, and Reporting.

Discovery and Inventory

- Architecture and deployment plan for sensor implementation optimized for continuous discovery of IT, OT, and IoT assets
- Deploy cloud agents, scanners, cloud connectors, and container sensors
- Integration with Shodan.io for external attack surface management
- Normalize, categorize, and organize assets via tagging design and implementation
- Provide asset contextualization and criticality, threat intelligence, TruRisk and ServiceNow CMDB sync for risk prioritization

Detect and Monitor

- Setup tracking for authorized and unauthorized hardware, OS, and hardware product lifecycle information
- Configure the management of authorized and unauthorized software
- Establish detection for misconfigurations such as unsanctioned open ports, open servers, expired certs, and old applications

Report and Respond

- Configure IT health reports and dashboards
- Configure IT health alerts and responses to proactively manage EOL & EOS software