DATASHEET

CRITICAL**START**®
Vulnerability Management Service

Take the burden out of vulnerability management while continuously reducing the risk of a breach.

KEY BENEFITS

- ✓ **Best in class vulnerability management** service built on top of Qualys VMDR. Don't have Qualys? No problem. We'll supply the license and help you get started.
- ✓ **Rich, asset-aware, threat-informed vulnerability detection** reports with expert analysis based on multi-vector intelligence.
- ✓ **Turnkey program operationalization** that provides asset visibility, scan configurations, predictable vulnerability scanning, and measurable results.
- ✓ **Prescriptive Patch Catalogs** that eliminate guesswork of which patches to apply to remediate vulnerabilities.
- ✓ **Regular Cyber Risk Reviews** with Critical Start's expert analysts keep you on track for continuous improvement.
- ✓ **Simplified compliance** with vulnerability scan results that can be used for certification and against regulations such as PCI-DSS, SOC2, HIPPA, NIST CSF, and more.

Today's organizations are under pressure to **reduce the risk of a breach,** including those risks introduced by security vulnerabilities. However, the volume and velocity of new vulnerabilities places a significant burden on teams that are already resource- and time-constrained. They need a clear path toward knowing what's at risk so that they can successfully remediate and report movement toward improved security posture, regulatory compliance, and risk reduction.

The CRITICAL**START**® Vulnerability Management Service (**VMS**) relieves the burden of vulnerability management by setting security and operational teams up for success. VMS delivers turnkey managed vulnerability scanning, expert Vulnerability Prioritization, and rich, multi-level reporting. Stakeholders can leverage expert guidance to make sound, data-driven remediation decisions that reduce risk to the organization, all without overextending internal teams or budgets.

How it Works

Critical Start's Vulnerability Management Service is a fully managed service that enables security leaders to effectively run a vulnerability management program by offloading burdensome operational tasks. The managed service leverages Critical Start's partnership with Qualys utilizing their industry leading end-to-end vulnerability management, detection, and response solution, Qualys VMDR.

Critical Start's managed services engineers provide operational execution of vulnerability scanning, ongoing operational monitoring, and detailed reporting, all of which contribute to a comprehensive view of an organization's exposure landscape. All findings provided through rich, contextualized VMS dashboards and reports are based on expert analysis of vulnerabilities and potential exposures in the customer environment. Customers receive concise directions and prescriptive patching guidance for effective and efficient vulnerability management that help them reduce cyber risk and minimize their attack surface.

CRITICALSTART®

Key Features

Critical Start Vulnerability Management Service increases the value of your Qualys subscription with:

- **Asset Discovery and Assessment Reports** – Critical Start conducts discovery scans to determine the scope of hosts and assets that require vulnerability scanning. This discovery reports includes all known assets while also alerting you to unknown hosts within your network.
- **Integrated Asset Inventory** – Provides a unified, automated list of assets with accurate Asset Criticality ratings and Endpoint/ SIEM Coverage Gaps so that you can ensure complete scanning coverage and expedite fixes for critical systems.
- **External and Internal Scanning Options** – External vulnerability scanning specifically examines an organization's security profile from an external viewpoint (i.e., how the assets appear from the internet). Internal vulnerability scanning operates inside the organization's firewalls to identify real and potential vulnerabilities inside the network.
- **Lightweight Agent Scanning Options** – Critical Start provides frictionless coverage for diverse operating environments that won't diminish the performance of your endpoints. Agent-based scanning supports remote/traveling users, remote offices that can't deploy a virtual scanner, cloud-based compute resources, and systems that do not allow remote authenticated scanning.
- **Managed or Self-Service Scanning** – VMS offers flexibility in scan management. Customers can choose from self-managed scans they conduct in-house, or fully managed scans that are executed by expert analysts in the Critical Start Risk and Security Operation Center.
- **Patch Tuesdays, Zero-day Events, and more, all built and delivered by Critical Start's vulnerability management expert.**
- **Vulnerability Prioritization** – Prioritization is critical when you have high volumes of vulnerabilities and limited time for remediation. VMS prioritizes vulnerabilities based on crucial factors, including weaponization, exploitability, and asset criticality. Critical Start correlates the findings from VM solution with a competitive up-to-date thread feed and helps customers **stop guessing and patch with confidence.**
- **Customized Scan Con igurations** – Scan policies and customizable configurations provide effective analysis by tailoring scans for each organization's unique requirements related to networks, services, hosts, vulnerabilities, scan performances, and more.
- **Prescriptive Patch Catalog** – Critical Start provides this definitive list of patch recommendations derived from internal and external analysis, allowing the organization to know exactly which patches to use to remediate vulnerabilities.
- **Reporting and Dashboard Flexibility** – Critical Start's VMS includes customizable vulnerability and remediation reports and dashboards, with dozens of available metrics to help organizations measure and articulate the performance of their vulnerability management program. Additionally, the VMS Dashboard Toolkit offers timely views of critical vulnerability intelligence.
- **Improve MDR Outcomes** – Critical Start's turnkey Vulnerability Management Services are designed to enhance our 24x7x365 monitoring, investigation, and response (MDR) for IT & OT environments. By leveraging our Cyber Operations Risk & Response™ platform, we seamlessly integrate industry-leading tools and **human-driven security operations** into the Security Operations Center (SOC). This unified approach combines comprehensive asset inventory, identification of **endpoint and vulnerability** coverage gaps, asset criticality ratings, **and MITRE** ATT&CK® mitigations. Together, these elements **enable** a proactive defense strategy, ensuring more accurate threat detection, prioritized responses, and faster incident resolution, thereby significantly improving overall MDR effectiveness.