DATASHEET

CRITICALSTART® Vulnerability Management Service

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

KEY BENEFITS

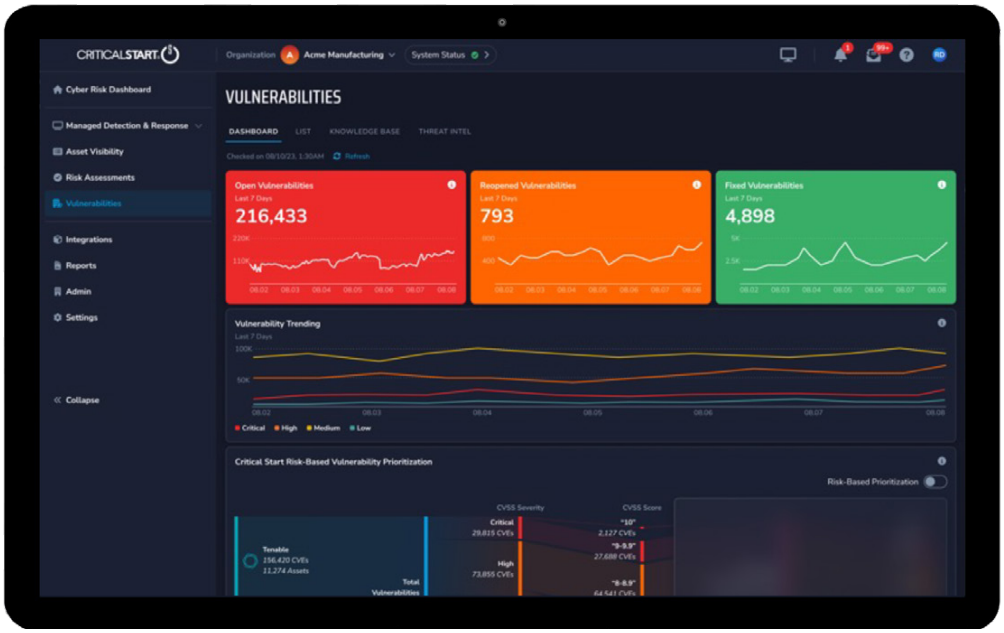
- ✓ Best in class vulnerability management service with two service offerings so you can choose the option that fits your requirements and budget.
- ✓ Rich, asset-aware, threat-informed vulnerability detection reports with expert analysis based on multi-vector intelligence.
- ✓ Turnkey program operationalization that provides asset visibility, scan configurations, predictable vulnerability scanning, and measurable results.
- ✓ Risk-Ranked Recommendations and Patch Catalogs that eliminate guesswork so you can rapidly reduce risk.
- ✓ Regular 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 measure, articulate, and manage cyber risk, 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. With two service tiers to choose from, VMS delivers turnkey managed vulnerability scanning and 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 VMS gives you comprehensive vulnerability management coverage across diverse operating environments with lightweight agents and remote scanning options. Using best-in-class tools or acting as a service wrapper for your existing scanning solution, VMS is a turnkey program. It contextualizes findings based on your organization's assets and scan profiles, integrates directly with ticketing tools like ServiceNow, and automates communication so that your IT operations teams and application owners know what to fix, when, and why it's important. With two tiers to choose from, VMS offers an array of internal and external scans, and managed or self-service scanning options to fit your needs today while allowing you to grow your vulnerability management program. Critical Start's analysts help you conduct asset analysis and configure scanning profiles. Then, they conduct scans based on the tier selected, continually monitor your operations, and provide customizable contextualized reports and a concise Patch Catalog so you can stay ahead of vulnerabilities and reduce cyber risks.



Key Features

Features of the Critical Start Vulnerability Management Service include the following:

- **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.
- **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.
- **Customized Scan Configurations** – 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 quickly remediate vulnerabilities to maximize risk reduction.
- **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, including Patch Tuesdays, Zero-day Events, and more, all built and delivered by Critical Start's vulnerability management expert.
- **Risk Based 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 prioritize the vulnerabilities based on the risk they pose.
- **Clear Communications** – Organizations can easily integrate with ticketing systems to organize vulnerability findings, create tickets, communicate patch recommendations to IT operations and application owners, and track patch management efforts.
- **Ongoing Risk Assessments** – Organizations can clearly articulate cybersecurity maturity with included access to Quick Start Risk Assessments. By answering just 15 questions, organizations gain risk-ranked recommendations based on target maturity levels and peer benchmark data.