DATASHEET

CRITICAL**START**® Asset Visibility

Gain visibility into your assets for improved security posture and risk reduction

KEY BENEFITS

- ✓ **Identify coverage gaps** by finding hosts in your network that do not have an endpoint agent or SIEM coverage so you can reduce the risk of compromise.
- ✓ **Utilize industry best practices for Asset Criticality** to make informed, risk-reduction prioritizations and threat response with enhanced asset context.
- ✓ **Improve your NIST CSF maturity levels** with a continuous asset inventory view of hosts, criticality, and endpoint coverage gaps.
- ✓ **Enrich asset visibility and vulnerability insights** with data from additional sources, including Qualys, Tenable, Microsoft Entra ID (Azure Active Directory), and others.
- ✓ **Support audits** and maintain regulatory compliance.
- ✓ **Recover costs** by surfacing outdated/unused software no longer protecting assets.

You can't protect what you don't know you have.

Your Managed Detection and Response service is only as good as the security signals it receives. Without a comprehensive, automated asset inventory to find visibility gaps in Endpoint Security Agents (**EDR/EPP**), firewalls, and other controls, you run the risk of allowing undetected threat actors to slip through the cracks.

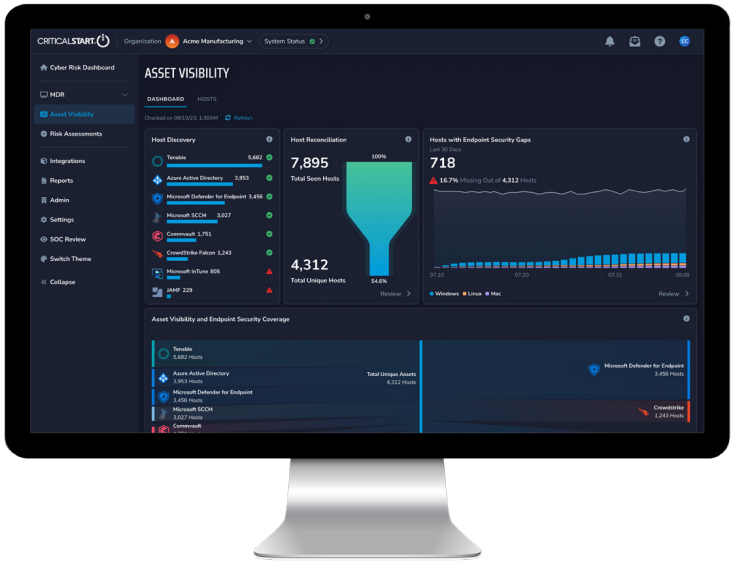
Visibility is critical for effective risk identification and mitigation.

CRITICAL**START**® Asset Visibility is a fundamental component of our Managed Detection and Response (**MDR**), Vulnerability Management Service (**VMS**), and Vulnerability Prioritization offerings. This pivotal platform capability delivers extensive, filtered data to support detailed cybersecurity operations. This enables you to:

- Verify security tools are deployed where needed.
- Prioritize fixing endpoint and Security Information and Event Management (**SIEM**) coverage gaps based on asset criticality for the greatest risk reduction.
- Monitor asset inventory changes over time.
- Find stale or orphaned security agents not checking in for updates.

We help you find gaps before attackers do.

Asset Visibility unifies data from your existing security tools, including Endpoint Security Agents and asset sources such as Microsoft Entra Identity Protection, Vulnerability Management tools, and more, to continuously monitor and find unmanaged and unsecured host assets before attackers can exploit them.

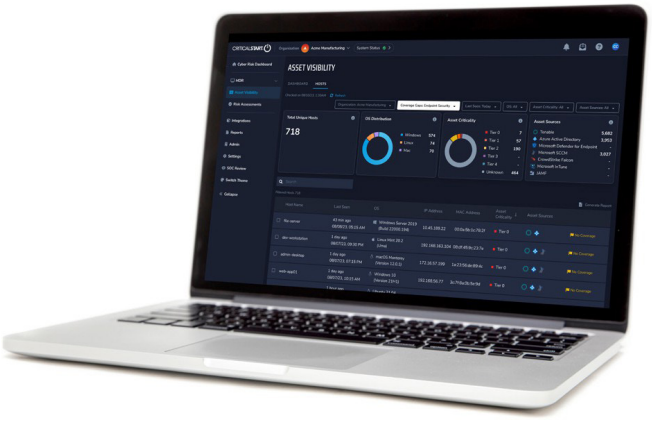


(Fig 1) Asset Visibility helps you find gaps before attackers do

Asset Criticality allows you to focus on risks with the greatest business impact.

Use Asset Criticality designations designed to represent the risk impact to your organization for a cyber event to enrich security alerts, accelerate remediation efforts, and prioritize closing endpoint coverage gaps.

- Tier 0 – Systems with root of trust, allowing access to the entire IT environment (including identity and directory services, patch management and endpoint security, Root CA, and cryptographic services)
- Tier 1 – Mission Critical (breaks in service are intolerable and significantly damaging)
- Tier 2 – Business Critical (requires continuous availability, but short outages are not catastrophic; required for effective business operations)
- Tier 3 – Business Operational (contributes to efficient business operations but are out of the direct line of service to the customer)
- Tier 4 – Administrative (office productivity tools for organizations to operate; failures do not affect customers)
- Unknown – Not rated or not needing to be rated



Asset Criticality represents risks with the greatest business impact

Features and Capabilities

Asset Visibility helps Critical Start Managed Detection and Response (**MDR**), Vulnerability Management Service (**VMS**), and Vulnerability Prioritization customers maintain a comprehensive inventory of all IT assets to detect vulnerabilities and ensure all endpoints are protected and monitored for suspicious activities. Asset Visibility includes:

Essential, Focused Insights

Asset Inventory

- Integrates with an organization's security and asset data sources to build a normalized host inventory

Asset Criticality

- Provides accurate criticality ratings so that you can prioritize remediation based on potential impact

Endpoint Coverage Gaps and SIEM Health Monitoring

- Focuses on hosts with "No Coverage" (hosts missing an endpoint agent or Security Information and Event Management (**SIEM**) coverage), pinpointing unknown cyber risks and reporting for actionable

Advanced Reporting and Visualizations

- Asset Criticality ratings (Tiers 0—4, Unknown)
- Automated asset criticality ratings with supported external integrations (including Qualys VMDR)
- Unified host asset inventory with de-duplication
- Asset management capabilities including exclusion and removing from inventory
- Configuration Management Database (**CMDB**) augmentation
- Comprehensive insights for in-depth analysis and mitigation
- Data exports and reporting
- Search and filter
- End-of-life systems identification

Get Started Today

Schedule a customized demo to see how Critical Start's MDR, VMS, and Vulnerability Prioritization with foundational Asset Visibility helps you proactively identify security risks across your environment. www.criticalstart.com/contact/request-a-demo/

CRITICALSTART®