DATASHEET

CRITICAL**START**® Asset Visibility

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

KEY BENEFITS

- ✓ Identify Endpoint Coverage Gaps (hosts in your network that do not have an endpoint security agent deployed on it) to help you reduce the risk of endpoint compromise
- ✓ Utilize industry best practices for **Asset Criticality** levels to make informed, risk-reduction prioritizations and threat response with enhanced asset context
- ✓ Improve your **NIST CSF** maturity levels with a continuous asset visibility view of hosts, criticality, and endpoint coverage gaps
- ✓ Enrich asset visibility and vulnerability insights with data from additional sources, including **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- ✓ Recover costs by surfacing outdated/unused software no longer protecting assets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.

Gaps in asset visibility allow attackers access to critical systems and data. Comprehensive, automated asset discovery provides the visibility to close security gaps by deploying Endpoint Security Agents (**EDR/EPP**), firewalls, and other controls needed.

Making MDR Different

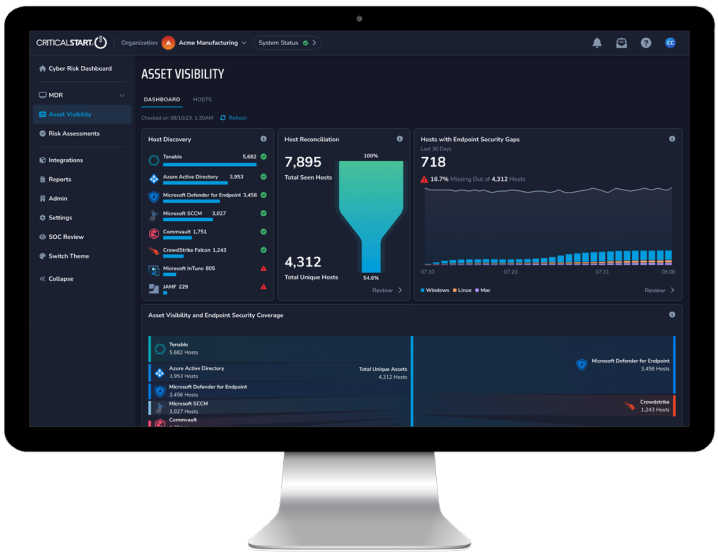
Your MDR service is only as good as the security signals it receives. For this reason, complete visibility and control over your technical assets are imperative to reducing risk exposure and maintaining compliance. Asset Visibility empowers you to optimize spending and make informed security investments by providing the inventory needed to:

- Verify security tools are deployed where needed
- Prioritize endpoint coverage gaps by critical assets 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.

Critical Start Asset Visibility *(Fig 1)* unifies data from your existing security tools, including **Endpoint Security Agents** and asset sources such as **Microsoft Entra Identity Protection, Vulnerability Management**, and more, to continuously monitor and find unmanaged and unsecured host assets before attackers can exploit them.

When integrated with **Critical Start Managed Detection and Response** (**MDR**), Asset Visibility strengthens threat monitoring, speeds response, and reduces risk.

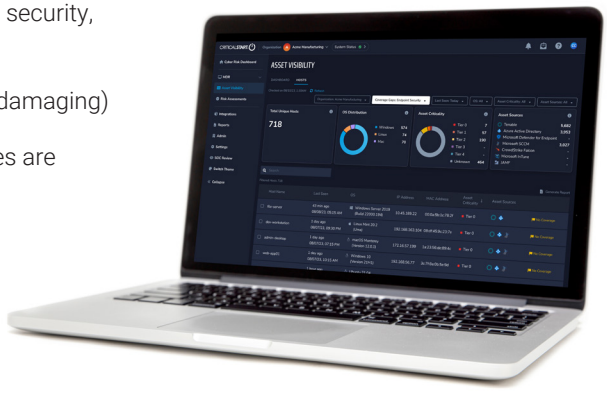


(Fig 1) Asset Visibility helps you find gaps before attackers do

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

Use **Asset Criticality** *(Fig 2)* 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



(Fig 2) Asset Criticality represents risks with the greatest business impact

Choose the right level of visibility for your needs.

Built as part of our **Cyber Operations Risk & Response™ platform**, Asset Visibility is available in two tiers to fit different cyber risk management needs:

- **Endpoint Coverage Gaps:** Included at no extra charge with Critical Start MDR services, it focuses on normalizing host assets and finding endpoint coverage gaps, providing essential insights into hosts without endpoint protection (prevention/detection).
- **Asset Visibility:** A paid upgrade for Critical Start MDR customers that provides enhanced visibility and management, including asset criticality designations, source- and time-based filtering, ad hoc searching, sorting, reporting, and exporting. Customers get access to future integrations at no charge as they're released.

Features and Capabilities

Included Standard with Critical Start MDR Provides essential, focused insights	**Unlocked with Full Asset Visibility** Features advanced reporting and visualizations
Asset Discovery • Integrates with security and asset data sources to build a normalized host inventory **Endpoint Coverage Gaps** • Focuses on hosts with "No Coverage" (hosts missing an Endpoint Security Agent), pinpointing unknown cyber risks and reporting for actionable remediation	**Asset Discovery and Endpoint Coverage Gaps, plus:** • Asset Criticality Ratings (Tiers 0—4, N/A) • Unified Host Asset Inventory • CMDB Augmentation • Comprehensive insights for in-depth analysis and mitigation • Data Exports and Reporting • De-duplication and Exclusion • Search and Filter

Get Started Today

Schedule a customized demo to see how Critical Start Asset Visibility proactively identifies security risks across your environment.
www.criticalstart.com/contact/request-a-demo/

CRITICALSTART®