Enhancing MDR Outcomes through Asset Visibility:
A Strategic Guide

CRITICALSTART®

The Gist

Your Managed Detection and Response (**MDR**) service is only as good as the signals it receives — and the most important signal for any MDR is endpoint, which is why traditional MDR solutions are no longer sufficient without ensuring comprehensive endpoint coverage. Critical Start is the only MDR provider to offer endpoint coverage gap analysis by integrating asset visibility into our MDR services. *Enhancing MDR Outcomes through Asset Visibility: A Strategic Guide* explores how an up-to-date asset inventory transforms MDR effectiveness and examines Critical Start's innovative approach to identifying security gaps through asset visibility capabilities.

Key Takeaways:

- **Visibility Gaps**: Up to 70% of critical assets remain unidentified in many organizations. Asset Visibility helps identify endpoint protection gaps and monitor vulnerability scanner coverage to prevent blind spots.
- **Asset Visibility's Role**: Integrated into our MDR services, Asset Visibility helps ensure complete security signal coverage by maintaining a continuous inventory of hosts. This enables organizations to identify and mitigate hidden assets and unmonitored infrastructure to ensure protection is in place where it's needed most.
- **Asset Criticality**: Asset criticality designations empower organizations to focus on risks with the greatest business impact. This information can be used to enrich security alerts, accelerate remediation efforts, and prioritize closing coverage gaps.
- **SOC Signal Assurance**: Security Operation Centers (**SOC**) can verify they're receiving the expected security signals, helping improve threat detection accuracy and response efforts.

Benefits:

- **Enhanced Visibility**: Maintain an accurate inventory of your assets and identify where protection might be missing.
- **Improved Security**: Get faster, more precise incident handling with confidence that you're receiving the security signals you need for effective detection and response.
- **Risk-Based Prioritization**: Focus on what matters most with asset criticality ratings that help you understand business impact and identify end-of-life operating systems to control cyber risk.
- **Streamlined Compliance**: Support audit and compliance efforts with up-to-date, normalized asset inventories.
- **Optimization**: Identify outdated or unused security tools to help control costs.

This eBook emphasizes that integrating asset visibility into MDR solutions not only enhances security operations but also proactively reduces risk and strengthens an organization's security posture.

Table Of Contents

04 Introduction: The Foundation of Effective MDR

05 The Endpoint Coverage Challenge

07 Optimizing MDR ROI with Asset Visibility

09 The Complete Picture: Ensuring Comprehensive Protection

10 The Key Benefits of Critical Start's Enhanced MDR for Organizations

11 The Future of Cybersecurity: Evolving MDR with Advanced Asset Visibility

12 Key Takeaways and Next Steps

13 Recommended Resources

Introduction: The Foundation of Effective MDR

The effectiveness of any MDR service depends entirely on its access to security signals — with endpoint being the most critical. Asset Visibility — foundational to Critical Start and any solid MDR — focuses specifically on endpoint hosts (workstations and servers), ensuring we have an accurate inventory and can identify where security signals might be missing.

According to the Critical Start 2024 Cyber Risk Landscape Report**, 83%** of organizations have been breached in the past two years despite having traditional security measures in place. That's why, ***even before our service starts***, we ensure comprehensive signal coverage by collecting the most important signals for any MDR to monitor — those from your endpoints. A primary reason? Incomplete endpoint coverage leaves critical assets unprotected. Therefore, we identify missing and misconfigured endpoint security agents using telemetry from different asset sources before establishing an API connection. The result is complete signal coverage and a SOC that is confident all expected threat signals are being received.

The Endpoint Coverage Challenge

Security teams are under immense pressure to keep up with the growing complexity of cyber threats and increasingly sophisticated attack vectors.

Without the proper processes and tooling in place, there will always be several endpoints that are part of your enterprise without endpoint security software deployed. This leaves security leaders unsure if critical endpoints have proper endpoint security controls installed and functioning, opening the door to breaches. This lack of confidence is especially true today when teams like DevOps and IT have more autonomy to self-provision endpoints aligned to their needs. This freedom can create blind spots as they may misconfigure endpoints in ways that compromise security.

Organizations face three primary challenges in maintaining robust cybersecurity defenses:

Incomplete Endpoint Coverage: Many organizations lack visibility into whether all their assets have endpoint protection installed and properly configured.

Technology Transitions: Organizations struggle to maintain complete coverage when transitioning between endpoint security tools.

Unmanaged Assets: Hidden or unmonitored endpoints provide attackers with entry points that bypass security controls.

Real-World Impact: The Advanced Persistent Threat "Sandworm" (APT44) demonstrates why endpoint visibility is crucial. Active since 2014, this threat actor is known for leveraging unmonitored infrastructure to gain initial network access before moving laterally across systems. Complete endpoint visibility through asset visibility helps detect such sophisticated threats early, before they can establish a foothold.

The Endpoint Coverage Challenge (continued)

Why Traditional MDR Falls Short

Traditional MDR solutions often focus solely on threat detection and response without addressing the fundamental need for comprehensive visibility. Even well-resourced organizations struggle to maintain accurate visibility of their assets. According to industry insights, up to 70% of critical assets remain unidentified due to reliance on manual inventory processes. These blind spots leave organizations vulnerable to:

Complete Signal Coverage: Building a Stronger Security Foundation

At Critical Start, we take a different approach. Through the technology of our Cyber Operations Risk & Response™ (**CORR**) platform, we go beyond traditional MDR with enhanced proactive and reactive security capabilities to help organizations maintain visibility of their security posture and identify areas needing attention.

We identify hidden assets and monitor unprotected infrastructure to prevent critical blind spots, empowering your Security Operations Center (**SOC**) with confidence in its signals and the effectiveness of its security operations. With Critical Start, you gain visibility where it matters most, ensuring that your security is robust, seamless, and always assured.

Optimizing MDR ROI with Asset Visibility

Critical Start has a comprehensive approach to MDR that includes asset visibility as a foundational component to enhance detection and response capabilities. By continuously identifying and monitoring unmanaged and unsecured host assets within an organization's environment, asset visibility enhances MDR's ability to detect threats more accurately, prioritize risks based on business impact, and streamline response efforts. This integration ensures that MDR services can address emerging threats in real time while providing a comprehensive view of the organization's security posture.

Critical Start MDR maintains a comprehensive view of endpoint hosts through:

- ✓ Unified, normalized asset inventory
- ✓ Integration with existing security tools, including:
  - Microsoft Entra Identity Protection
  - Vulnerability Management tools
  - Other supported asset sources
- ✓ Continuous monitoring for security control gaps
- ✓ Visibility of vulnerability scanner coverage
- ✓ Asset criticality ratings based on business impact

Technology Transition Support

Critical Start's Asset Visibility capabilities are particularly valuable during security tool migrations. When organizations transition between endpoint security tools (for example, from CrowdStrike to Microsoft), our solution ensures that as you remove one agent, all assets are covered by the new technology without any lapse in monitoring coverage.

Optimizing MDR ROI with Asset Visibility (continued)

Asset Criticality

Tiered criticality ratings (0-4)

Systems With Root of Trust
Allows access to the entire IT environment (including identity and directory services, patch management and endpoint security, Root Cause Analysis (**CA**), and cryptographic services)

Mission Critical
Breaks in service are intolerable and significantly damaging

Business Critical
Requires continuous availability, but short outages are not catastrophic; required for effective business operations

Business Operational
Contributes to efficient business operations but are out of the direct line of service to the customer

Administrative
Office productivity tools for organizations to operate; failures do not affect customers

Not rated or not needing to be rated

Asset Visibility: Myth vs. Reality

Myth: Asset visibility within MDR is a standalone solution that doesn't integrate with existing security tools.

Reality: Asset visibility is embedded in Critical Start's MDR service, working seamlessly with other tools to provide a unified, comprehensive view of an organization's security posture.

The Complete Picture: Ensuring Comprehensive Protection

For organizations to fully benefit from MDR, they must choose a service where asset visibility is built into the MDR ecosystem rather than being treated as a separate solution. At Critical Start, this integration begins before service deployment, with verification of endpoint signal coverage to identify any protection gaps.

This proactive approach continues throughout the service lifecycle, as **Critical Start MDR** uses the **CORR platform** to unify data from security tools and maintain visibility of endpoint hosts. The resulting comprehensive visibility helps improve security outcomes by reducing operational overhead and giving the SOC confidence that expected threat signals are being received. This SOC Signal Assurance is a key outcome of complete signal coverage, supplying the SOC with the critical data it needs to prevent breaches and avoid business disruption.

Finally, with the information provided through asset visibility, organizations can use MITRE ATT&CK® Mitigations Recommendations to enact controls that reduce the likelihood of a repeat event and further improve their security posture.

The Key Benefits of Critical Start's Enhanced MDR for Organizations

Critical Start MDR services, enhanced with proactive capabilities like asset visibility, deliver:

Improved detection for faster, more precise response efforts.

Reduced risk by identifying and ensuring that the most critical threats are addressed first.

Streamlined compliance and reporting with up-to-date asset inventory.

Improved Detection and Response	Asset Criticality-Based Protection	Complete Endpoint Coverage
• Continuous endpoint monitoring • SOC confidence in endpoint signal coverage • Rapid response with MOBILE**SOC**®	• Asset criticality ratings for risk-based decisions • Identify and prioritize coverage gaps based on asset criticality	• Gap identification • Migration validation

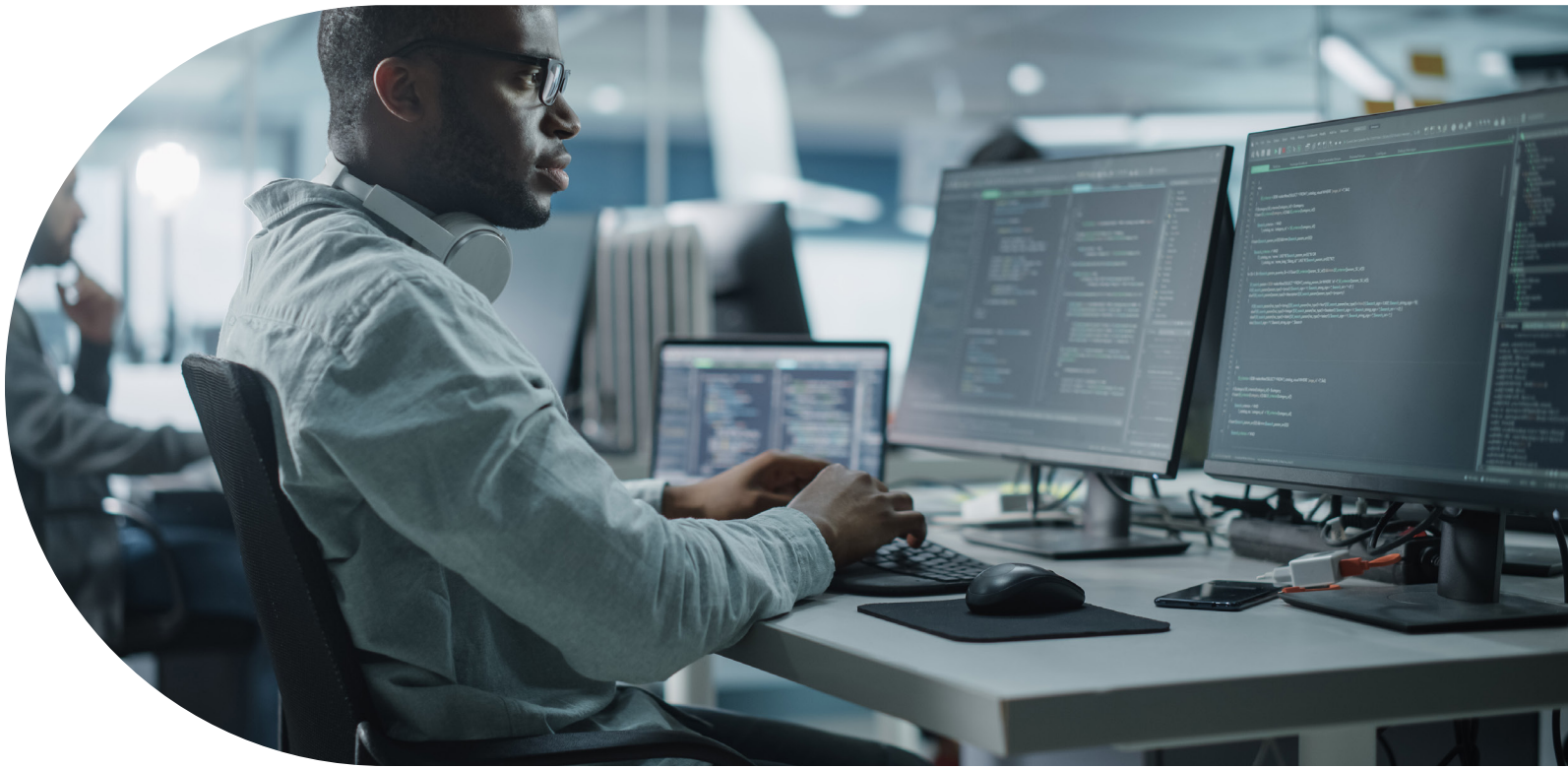
The Future of Cybersecurity: Evolving MDR

As the cyber threat landscape evolves, comprehensive endpoint visibility becomes a necessity. Critical Start's MDR service provides:

- MOBILE**SOC**® for flexible threat response
- Remote containment capabilities
- Real-time threat isolation
- Reduced risk by identifying and ensuring that the most critical threats are addressed first

Key Takeaways

Asset visibility is essential to enhancing MDR outcomes. Integrating asset visibility into your MDR strategy can improve detection, streamline response, and significantly reduce risk. Asset visibility identifies hidden assets and unmonitored infrastructure. It monitors vulnerability scanner coverage, resulting in SOC signal assurance, while our MOBILESOC® enables real-time incident response, reducing dwell time and enhancing mobility. Asset criticality ratings and proactive threat management help you prioritize risks and optimize your security operations.



Recommended Resources

If you're ready to see what enhanced MDR can do, get in touch. We'll schedule a personalized demo to show you how Critical Start MDR with Asset Visibility uncovers blind spots so you can protect unmanaged and unsecured host assets before attackers can exploit them. Schedule Now.

Want to learn more about how Critical Start can help you stop fearing risk and start managing it? Use the links below for details.

- CRITICAL**START**® Managed Detection and Response (MDR) Services
- Asset Visibility | Close Security Gaps
- The Critical Start Security Operations Center (SOC)
- Critical Start MOBILE**SOC**®
- CRITICAL**START**® MDR for Operational Technology (OT)
- CRITICAL**START**® MDR for Microsoft Security
- CRITICAL**START**® Security Services for SIEM
- Critical Start 2024 Cyber Risk Landscape Peer Report
- IDC MarketScape: Worldwide Emerging Managed Detection and Response (MDR) Services 2024 Vendor Assessment
- 2024 Gartner® Market Guide for Managed Detection and Response Services

For more information, contact us at:
https://www.criticalstart.com/contact/