DATASHEET

CRITICAL**START**® Cyber Risk Dashboard

Holistically assess, monitor, and mitigate cybersecurity risk.

KEY BENEFITS

- ✓ **Gain real-time visibility** into cyber risk to promptly respond to emerging threats
- ✓ **Proactively manage** cyber risk with prioritized recommendations and evidence-based insights
- ✓ **Assess potential business impact** to focus on areas of greatest risk impact
- ✓ **Gain executive decision support** with a clear understanding of security program performance compared to industry peers
- ✓ **Drive continuous improvement** and facilitate informed decision-making that optimizes security resources

Mitigate the Risk of Not Knowing What You Don't Know

Do you know how much cyber risk your organization has? Do you understand what items to fix or which new controls and programs to implement for the greatest risk reduction?

Blind spots and limited security programs introduce more risk, hinder the ability to prioritize investments, and deter an organization from being able to allocate resources most effectively.

Security leaders face ongoing pressure to showcase their ability to effectively manage cyber risk relative to business and budget pressures. However, accessing and analyzing various data sets required to communicate cyber risk in a manner that informs business decisions regarding security investments and projects can be challenging.

A pivotal part of the **Critical Start Cyber Operations Risk & Response™ platform**, the Cyber Risk Dashboard provides a holistic perspective for continuously assessing, monitoring, and mitigating your cyber risk exposure.

Three user-friendly views in the Cyber Risk Dashboard are tailored to provide in-depth insights into different dimensions of organizational cybersecurity.

- **Risk Overview -** a holistic overview of your organization's real-time status, urgent items, and next steps
- **Risk-Ranked Recommendations -** tailored action suggestions backed by evidence and peer benchmarking to facilitate informed decision-making based on Financial Loss, Probability, Impact, and Level of Effort (rough order costs to implement)
- **MITRE ATT&CK® Mitigations Recommendations -** enable proactive risk management configurations and controls to prevent a successful attack from occurring

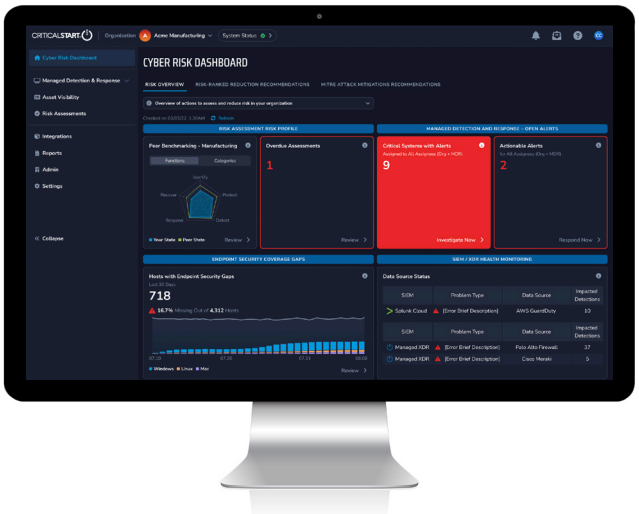
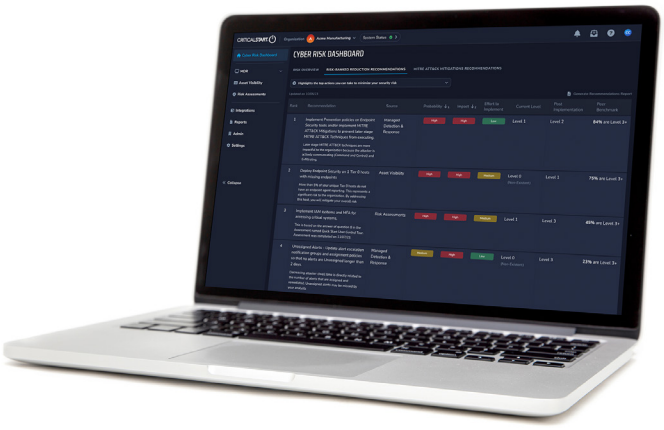


Fig. 1 - The Cyber Risk Dashboard provides a holistic perspective for continuously assessing, monitoring, and mitigating your cyber risk exposure.

Key Features



- **Risk Overview -** See a unified view of security statuses, urgent action items, and next steps based on operational elements of the **Critical Start Cyber Operations Risk & Response™ platform**. This single view enables you to take actions focused on the largest risk reduction effort per dollar you can deliver for your organization.
- **Risk-Ranked Recommendations -** Real-time data received is used to personalize risk reduction recommendations to your organization so you can prioritize resources on improvements that deliver the greatest risk reduction impact. Appropriate permission levels allow your team to refine recommendations even further through manually adjustments. Each recommendation lists an action, source of finding, and technology impacted, prioritized from highest to lowest probability of exploitation. You can also view the risk impact, effort level to implement, risk reduction value, and detailed audit trail for each recommendation. Benchmarking displays how you compare to industry peers for that risk item. Recommendation reports can be generated to share progress over time across your organization.
- **MITRE ATT&CK Mitigations Recommendations -** Benefit from recommended preventative controls aligned to the MITRE ATT&CK® Framework. By analyzing confirmed threats detected by our MDR service that have been in your environment for over 90 days, the Platform recommends specific configuration and control mitigations that will prevent those threats from successfully executing in the first place. For each mitigation, you will see details like Mitigation ID and Name, number of related alerts, associated Technique ID and Name, and a description of how to implement the mitigation. Reliable, contextual insights allow you to shift focus to protecting your organization from cyber-attacks instead of responding to attacks.

Key Use Cases

- **Real-Time Visibility and Prompt Response -** Leverage the Risk Overview feature to gain real-time visibility into the organization's cyber risk status. By monitoring urgent action items and next steps, you can promptly respond to emerging risks.
- **Proactive Cyber Risk Management -** The Risk-Ranked Recommendations features provide personalized, evidence-based insights for prioritized risk reduction. Proactively manage cyber risk by focusing on tailored action suggestions with benchmarking against industry peers.
- **Assessing Business Impact and Risk Focus -** Assess potential business impact using the Risk Overview and Risk-Ranked Recommendations features. These views help in understanding financial loss, probability, impact, and level of effort associated with different cyber risks. With a clear picture, you can focus on areas of greatest risk impact, aligning security efforts with business priorities.
- **Executive Decision Support and Peer Benchmarking -** The Risk Overview and Risk-Ranked Recommendations features offer executive decision support by providing a clear understanding of a security program's performance relative to industry peers. Leverage benchmarking data to communicate effectively with other executives, demonstrating the organization's cyber risk management capabilities and making informed decisions regarding security investments.
- **Proactive Risk Management -** Leveraging the MITRE ATT&CK® Mitigations feature enables proactive risk management by implementing recommended preventative controls aligned with the MITRE ATT&CK® Framework. By analyzing confirmed threats and receiving specific configuration and control mitigations, leaders can focus on preventing cyber attacks before they occur, shifting their attention from responding to attacks to actively protecting the organization.