Med Tech Solutions

Enterprise Cybersecurity – Product Comparison

MTS SentinelOne vs. Malwarebytes

FEATURES	MTS SentinelOne Singularity Complete*	ThreatDown Ultimate
Critical Incident Prioritization	✓	X
Device Control	✓	✓
Cross-Stack Visibility/Correlation	✓	X
Block Unwanted Applications	✓	✓
Vulnerability Assessment	✓	✓
Ransomware Rollback	✓	✓
Endpoint Detection & Response	✓	✓
Patch Management	✓	✓
Managed Threat Hunting	✓	✓
Managed Detection & Response	✓	✓
Website Content Filtering	✓	✓
24/7 SOC Service Team Support	✓	X
Reduced TCO with an Integrated Platform	✓	X

* coupled with other cybersecurity tools included in the MTS Secure platform

100% Protection and Detection
Across Operating Systems

100% Real-Time
Zero Delays

100% Realistic Information
Zero Configuration Changes - Customer Ready

Alert Consolidation
Prioritize critical incidents transforming noise into actionable intelligence

Why SentinelOne?

- Enterprise Security AI Platform
- #1 in Real-World Protection
- Aligned to MITRE ATT&CK framework

FEATURES	MTS SentinelOne Singularity Complete	Malwarebytes ThreatDown Ultimate
Device Isolation	Device and network isolation provided. Also allows control over USB and Bluetooth devices.	Offers three modes: Network, Process, and Desktop Isolation.
Remediation	Simplifies response and automates resolution – with one click, the analyst can execute remediation actions such as network quarantine, auto-deploy an agent on a rogue workstation, or automate policy enforcement across cloud environments.	Provides thorough remediation by meticulously finding and reversing all major and subtle changes made by malware.
Tracking	Features patented Storyline™ technology that automatically tracks all OS relationships, providing full context and understanding of an attack.	Features a proprietary Malwarebytes Linking Engine that tracks every artifact, change, and process alteration.
Threat Detection	Auto-enrich endpoint incidents with real-time threat intelligence. Empowers security teams to get additional contextual risk scores on Indicators of compromise (IOCs) such as IPs, hashes, vulnerabilities, and domains, enabling customers to accelerate threat investigation and triage capabilities.	Collects detailed endpoint threat info for analysis and investigation to search for indicators of compromise.
Real-Time Response	Best-in-class endpoint protection capabilities to easily manage complex configurations, conduct real-time monitoring, and stop attacks across the enterprise—all within a unified platform.	Finds and blocks threats before devices are infected.
Automated Remediation	Extensive AI-powered detections and autonomous controls easily integrated with Purple-AI to empower every analyst and accelerate investigation and response.	Linking Engine detects and removes dynamic and related artifacts, changes and process alterantions.
SOC Services	Includes both 24/7 SentinelOne Vigilance Respond MDR service and MTS SOC Service Teams to monitor and respond to threats. Digital forensics analysis and incident response (DFIR) capabilities are available as well, making it the perfect support service for overstretched IT/SOC teams.	Alert Monitoring and Response, as well as Incident Response, available 24/7.

FEATURES	MTS SentinelOne Singularity Complete	Malwarebytes Endpoint Protection
Threat Detection and Blocking	Grants peace of mind with industry-leading cross-surface visibility that takes real-time action for automated, enterprise-grade prevention, detection, response, and hunting across endpoint, cloud, and identity.	Finds and blocks threats before devices are infected by recognizing and preventing both hostile code and bad behavior.
Remediation	Simplifies response and automates thorough resolution with patented one-click remediation to reverse all unauthorized changes. Devices defend themselves autonomously by killing and quarantining threats in real-time. Seemless integration with any technology product or platform breaks data silos, eliminates critical blind spots, and enhances remediation accuracy.	Provides thorough remediation by meticulously finding and reversing all major and subtle changes made by malware
Tracking	Features patented Storyline™ technology that automatically tracks all OS relationships, providing full context and understanding of an attack. Logs stored for 365 days.	Features a proprietary Malwarebytes Linking Engine that tracks every artifact, change, and process alteration. Logs stored for up to 30 day.
Management	View dashboard in real time for event status and device health across your network. Console is customizable for time-saving workflows. Includes data-driven dashboard security analytics.	Provides a single dashboard with an easy-to-use interface, delivering real-time status of events and device health across your network.
Threat Hunting Capabilities	Includes Hunter's Toolkit, which includes MITRE ATT&CK framework, network isolation, secure remote shell, and integrates with sandboxes for dynamic analysis.	Available
Gartner Rating	For the third straight year, SentinelOne is named a Leader in the Gartner® Magic Quadrant™ for Endpoint Protection Platforms (2023). 96% of Gartner Peer Insights reviewers recommend SentinelOne.	[N/A]