RoundClock Endpoint Detect & Respond
Powered by SentinelOne

mother technologies

Global ransomware attacks are at an all time high. SentinelOne – the technology behind RoundClock EDR – is the global leader in endpoint protection outstripping every major competitor with a 100% prevention score

100% Protection	100% Detection	100% Real-time delays
9 of 9 MITRE ATT&CK Tests	19 of 19 Attack Steps	0 Delays

Traditional antivirus no longer provides endpoints with adequate protection against modern cyber threats. It falls short because it relies on virus signature updates which struggle to keep up with new daily threats. Consequently, threat detection happens too late.

RoundClock EDR (Detect and Respond) is powered by the Gold Standard in Endpoint Protection, proactively safeguarding your endpoints using advanced artificial intelligence. It ensures security by identifying, mitigating, and remediating incidents with zero delay.

Zero Day Attacks
Network vulnerabilities that attackers exploit before vendors or developers have even learned of the hole in their product.

Weaponised Documents
Seemingly harmless PDF email attachments that execute attacks once they have entered your network.

Fileless Threats
Many malware threats are difficult to detect because they live only in the memory of an infected machine.

Ransomware Attacks
Cyber-attackers disable your network and demand huge ransoms in order for services and data to be restored.

Why choose RoundClock EDR?

RoundClock EDR provides best-in-class technology with 100% prevention and one-click endpoint remediation and rollback.

Ransomware Defence & Recovery
Escape the clutches of ransomware with the ability to revert devices to their pre-infection condition. This capability ensures that even in the face of ransomware attacks, your systems can be restored to a secure state.

AI Powered Threat Prevention
Leverage the power of AI to proactively identify and thwart both existing and emerging threats. The platform's constant updates guarantee that you remain protected against the latest risks.

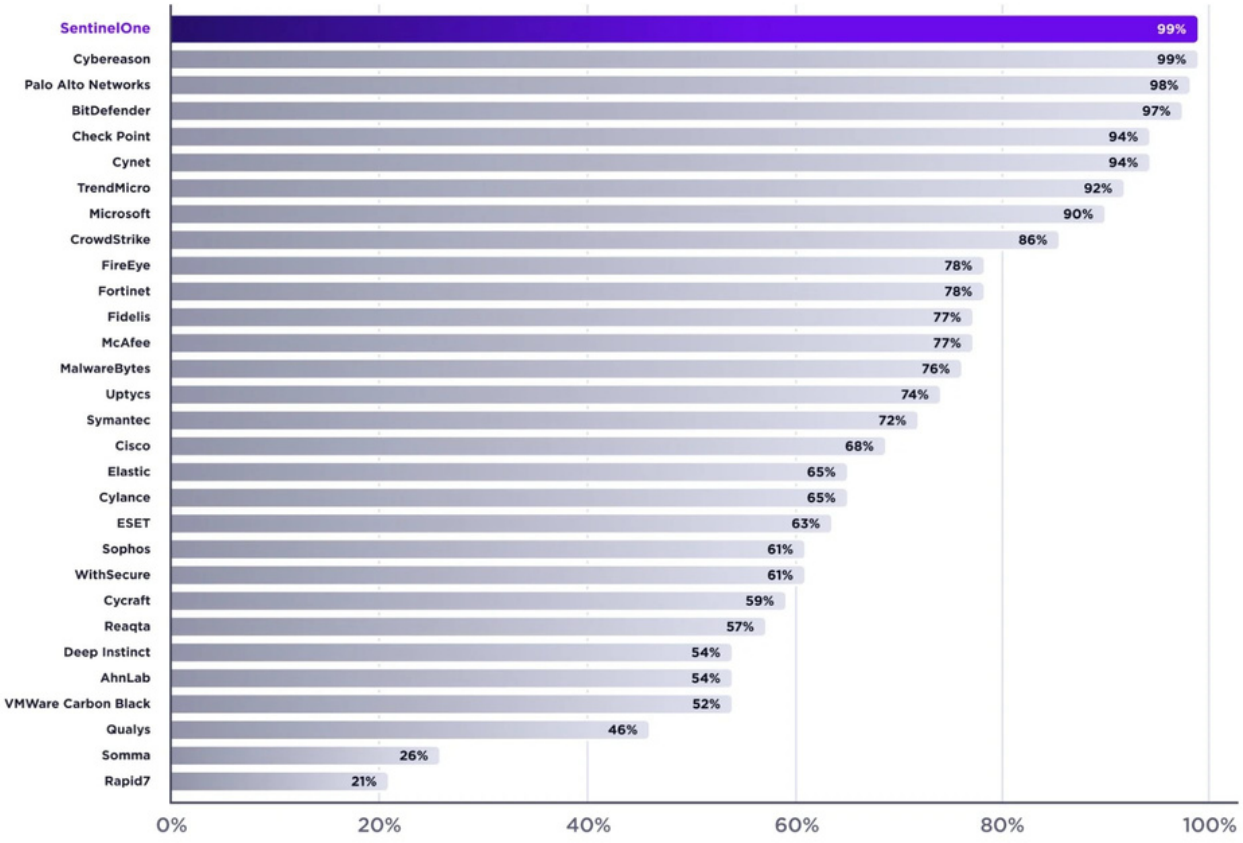
Automated System Remediation
Streamline your threat incident response with automated system remediation. Swift actions can be taken to counter threats, ensuring that potential breaches are swiftly neutralised.

Comprehensive Threat Monitoring
Monitor processes comprehensively, spanning before, during, and after execution. This holistic approach prevents threats from infiltrating your systems, safeguarding your environment.

Real Time System Monitoring
Ensure the safety of your systems in real-time. By actively monitoring your environment, you can promptly detect and address any suspicious activities or anomalies that may arise.

Uninterrupted Device Performance
Maintain optimal device performance by engaging in continuous threat monitoring. This proactive approach guarantees that security measures are in place without compromising the efficiency of your devices.

Analytical Coverage
SentinelOne recorded the highest number of analytic detections for the last 3 years in MITRE Engenuity's published results. Higher than any other participant in the evaluation.



Benefits of EDR

Never worry about ransomware again with RoundClock EDR. Just click and restore your devices to their pre-infection state.

Increase Employee Productivity

Eliminate threats that outwit traditional AV solutions and maintain faster device performance, creating fewer distractions that eat into employee productivity.

Minimise Costly Downtime

Prevent downtime with rapid threat response via AI-based detection, containment, and automated remediation in Managed EDR, efficiently safeguarding productivity and your bottom line.

Leave it to Experts

Don't spend time trying to support and manage your own systems and security. Focus on running and growing your business, with ongoing support from the Mother team.

Traditional Antivirus ✗	RoundClock EDR ✓
Can't roll back to a pre-infection state, increasing your ransomware risks.	Help prevent ransomware by rolling back devices to their pre-infection state.
Use signatures to identify threats, meaning capabilities lag behind cyberattackers' latest strategies.	Use artificial intelligence (AI) to detect and prevent both current and emerging threats.
Fly blind during execution, creating an entry point for new threats from savvy attackers.	Monitor processes before, during, and after execution, to prevent new threats from executing.
Rely on daily or weekly scans, increasing your risks due to a time lag.	Monitor your systems in real-time.
Can slow down your device performance with long scans.	Keep device performance fast with continual monitoring.