

Endpoint Detection and Response



Robust Threat Prevention for Desktops, Laptops and Servers

EDR Features

- Real time automated protection against evolving threats at each endpoint
- AI engines to provide static and behavioral analysis on new threats
- Machine learning to evolving threat responses
- Blocks devices with custom policies to defend against zero-day and fileless attacks
- Includes a Windows OS roll back feature to potentially reverse ransomware in minutes
- Instantly stops threats with network disconnect
- Reports threat issues 24/7 to Nims' monitoring and alert system
- False positive filtering

Take your protection from cyber attacks to the next level with SentinelOne® endpoint threat detection and response (EDR).

New threat patterns like ransomware, fileless, and zero-day threats require a new approach. Cyber threats constantly evolve and change at a rapid pace. Cyber-criminals are using artificial intelligence (AI) against businesses and all their devices. Anti-virus with scheduled scans alone cannot always keep up with the frequency of attacks as they become more and more sophisticated.

EDR looks for patterns of behavior along all endpoints. Although a known threat may not be detected, EDR will alert you if it finds what it deems suspicious behavior so that you can take proactive and corrective action to make sure your business is protected.

Contact Nims & Associates for security strategy to protect your systems from all of today's threats.



E: info@nimsassociates.com
Call: 877-454-3200
Web: www.nimsassociates.com