

SenseOn MXDR: Overcoming SMB Security Challenges

Over 50% of cyberattacks target SMBs. The advanced tactics used by attackers slip through the cracks of traditional security tools like anti-virus and EDR. SenseOn offers a comprehensive Managed XDR solution that empowers resource and budget conscious IT leaders to deliver enterprise-level security, without the enterprise price tag.



Common Challenges for SMBs:

Resource Constraints:

- Limited budget for cybersecurity
- Lack of in-house security expertise
- Time constraints for managing complex security systems

SenseOn Solution: Our cost-effective platform requires no in-house expertise. Advanced detection models and machine learning ensure only real threats are raised, optimising your team's time and resources.

Complexity and Overhead:

- Difficult and time-consuming deployment of traditional security solutions
- Resource-intensive maintenance and management

SenseOn Solution: Simple deployment of one piece of software, and minimal ongoing management saves time and money. Our AI learns about your organisation, eliminating the need for complicated and time-consuming tuning.

Increasing Cyber Risk:

- Lack of confidence in current approach to cyber security
- Limited visibility into the digital landscape increases risk
- Difficulty in identifying and prioritising threats

SenseOn Solution: Our Universal Sensor and Cloud/SaaS connections analyses data from various sources, providing contextual AI-driven alerting, clear insights, and easy monitoring of your business's threat landscape.

Wedlake Bell

"SenseOn alerts us as soon as something appears on the network..."

They remediate straight away with 24/7 coverage when hackers are most active outside of office hours, while our teams are not available."

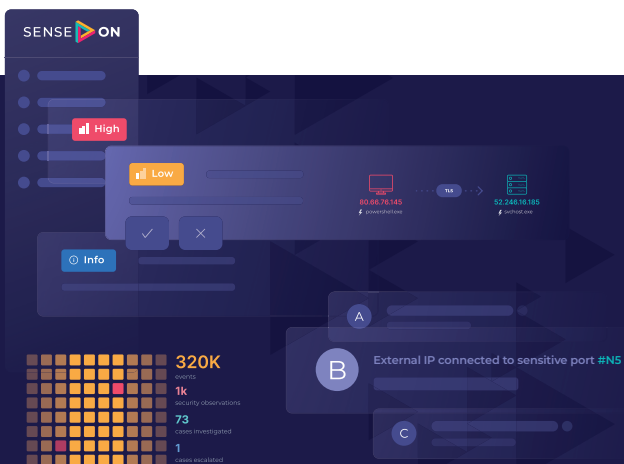
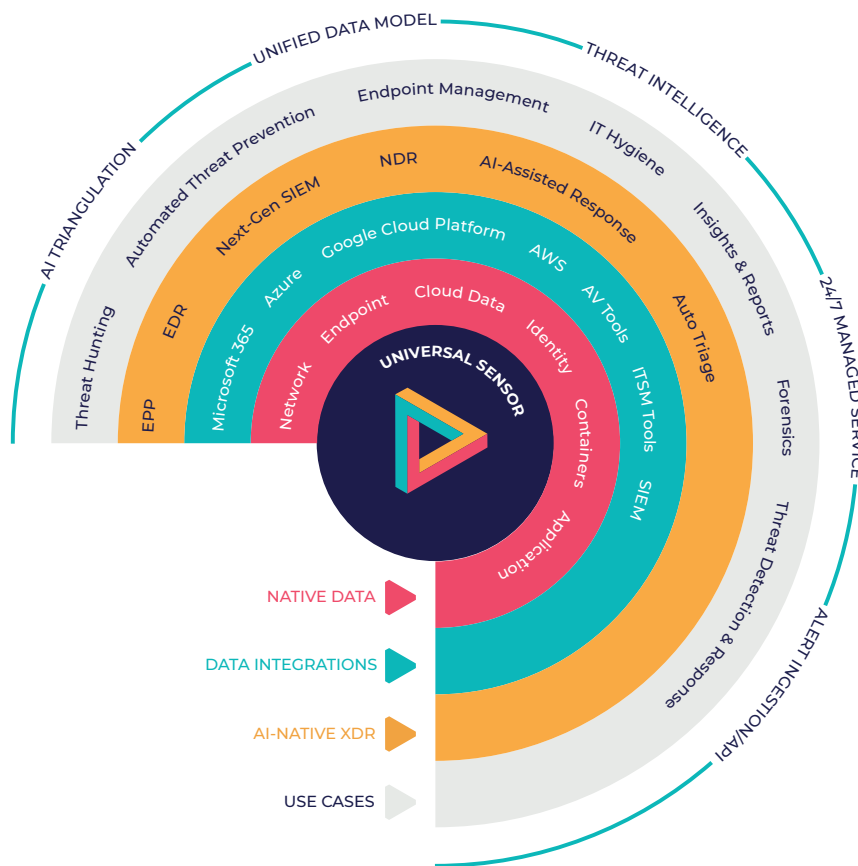
David Hymers, IT Director at Wedlake Bell

The SenseOn difference.

Unlike traditional security solutions, SenseOn's unified approach streamlines data collection and analysis, reducing costs and complexity. Our platform delivers enterprise-grade protection at a price point comparable to basic SMB offerings from competitors, while addressing the unique challenges faced by small and medium-sized businesses.

SenseOn's key capabilities

- **Endpoint Protection Platform (EPP):**
 - AAA-rated by SE Labs (99.63% malware detection, zero false positives)
 - ML-powered detection of known and zero-day threats
 - Automatic file quarantine and process termination
- **Endpoint Detection and Response (EDR):**
 - Continuous threat library updates, with 1000's of custom built detections available from day one
 - Coverage across the MITRE ATT&CK framework
 - Response capabilities combine quick containment actions with fully remote endpoint forensics
- **Network Detection and Response (NDR):**
 - Turns every endpoint into a network probe
 - Deep Packet Inspection at the endpoint
 - Combines endpoint and network data for enhanced threat detection
- **Extended Detection and Response (XDR):**
 - Correlates data from users, endpoints, networks, SaaS apps, and cloud environments
 - AI Triangulation reveals evolving attack paths
 - Augments alerts from Microsoft, Google Workspace, and AWS Security Hub, stopping attacks missed by cloud vendors
- **Managed XDR Service:**
 - 24/7 SOC with Mean Time to Resolution (MTTR) < 20 minutes
 - Expert threat containment and remediation, even at 4am



Discover SenseOn Today

Are you ready to automate your cybersecurity? Visit our website to learn more about SenseOn. Experience how our unique technology makes cybersecurity straightforward and powerful for businesses like yours.

Find out more at www.senseon.io or email info@senseon.io.