CrowdStrike vs. Microsoft Defender for Your Endpoint Security

At Red Helix we choose to incorporate CrowdStrike into our Managed Detection and Response Service (MDR). It underpins our threat detection and alerts us to signs of attack 24/7. This cloud-centric solution can be used in conjunction with other security solutions such as Network Detection and Response (NDR) and Security Information and Event Management (SIEM).

Where Microsoft Defender Falls Short

Microsoft Defender is built primarily on legacy signature-based antivirus models, supplemented by add-ons.

In practice, this results in:

1. Inconsistent Protection

Protection varies by OS version and licensing tier.

Security should not depend on which edition is deployed.

2. Operational Burden

- Frequent OS-level upgrades
- Reboots that disrupt business operations
- Multiple consoles for management

This increases pressure on internal teams and fragments SOC workflows.

3. Hidden Cost Model

Critical capabilities such as:

- Threat analytics
- Server protection
- Advanced hunting

Often sit outside base licensing.

4. Fragmented Visibility

Multiple management consoles create blind spots and slow investigation.

Modern attackers exploit exactly this kind of complexity.

Red Helix

The CrowdStrike Advantage

CrowdStrike Falcon is a cloud-native, AI-driven platform built for modern threat environments and designed for breach prevention.

Key Advantages

CrowdStrike	Microsoft
Rapid deployment, with instant protection	Upfront reboots and upgrades to ensure a successful deployment
Automatic Updates	Frequent reboots, and daily signature updates
Advanced threat detection	Signature based AV threat detection
Transparent licencing with no hidden costs	Extra costs for platform maintenance and add-ons
Red Helix will manage and implement the platform	Added internal staff needed to maintain the platform
Single pane of glass view to have visibility of the entire platform	Multiple consoles
Is compatible with the Red Helix's MDR service	Not compatible with Red Helix MDR service

Why This Matters Commercially

Most breaches begin at the endpoint.
The difference between containment and catastrophe is:

- Detection speed
- Response speed
- Clarity of visibility

CrowdStrike:

- Identifies threats behaviourally, not just by signature
- Uses AI and global telemetry to anticipate attack patterns
- Enables proactive investigation
- Reduces alert fatigue
- Removes manual workload

Red Helix

Introducing Next-Gen SIEM

Legacy SIEM systems:

- Store vast log volumes
- Detect threats retrospectively
- Require heavy storage infrastructure
- Demand large internal teams

CrowdStrike Next-Gen SIEM

CrowdStrike's Next-Gen SIEM is built differently.

- It processes telemetry in real time.
- It integrates natively with the Falcon platform.
- It prioritises endpoint-level intelligence.

Business Benefits

Capability	Business Outcome
Real-time threat detection	Faster containment, reduced impact
AI-driven correlation	Higher accuracy, fewer false positives
Cloud-native architecture	Lower infrastructure cost
Reduced log storage dependency	Lower operational overhead
Endpoint-focused intelligence	Deeper attack visibility
Scalability	Future-ready security

Delivered Through Red Helix 24/7 SOC

Technology alone is not protection. Monitoring, investigation, and response determine outcome. Red Helix provides:

- 24/7 threat monitoring
- Incident response
- Continuous optimisation
- Expert-led investigation
- Escalation and containment

You gain enterprise-grade security capability without building it in-house.

Red Helix