wavenet

EBOOK

# CrowdStrike Falcon Endpoint Protection

Prevent, detect, investigate, and respond to advanced threats before they impact your business.

CROWDSTRIKE

# Endpoint Detection and Response (EDR)

Attackers are getting more and more sophisticated using new tools and creating malware. There is an increase in attacks using scripting tools such as PowerShell. The attackers are also finding clever ways to hide malware, by obscuring the payload so that traditional anti-virus programs don't detect this malicious activity.

Nearly all the known security breaches start with a compromised endpoint and protecting these endpoints against the 390,000 daily created new malware strains and sophisticated new attacks, is a never-ending battle.

Understanding the threats as they appear on the network is also critical, making sure that you can answer the following questions if needed.

- Who is being attacked?
- What data were the attackers after?
- When and where did the attack come from?
- How did it get there?
- Was the attack successful?
- What is the business impact?

EDR technologies take endpoint security to the next level by enhancing threat visibility and coverage beyond the scope of traditional antivirus and network monitoring tools. EDR sensors will capture important system events such as process executions, registry and file changes and use real-time behavioural monitoring to identify suspicious activity.

## How does it work?

The CrowdStrike Falcon® platform leverages real-time indicators of attack and threat intelligence to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritised observability of vulnerabilities.

The CrowdStrike Falcon platform is a Gartner leading technology, providing best of breed endpoint detection and response. It includes integrated threat intelligence and additional bolt-on modules including firewall management and USB device control.

CrowdStrike uses a lightweight agent that has no impact on user performance and prevents both commodity and sophisticated attacks for file-based and file-less attacks.

The solution provides real-time endpoint visibility and insight into applications and processes across the environment. It protects all workloads and is able to operate across Windows, MacOSX, Linux, mobile devices, as well as servers and containers in modern hybrid multi-cloud data centres.

# Attack Protection Capability

Wavenet's CyberGuard SOC offers fully managed detection and response services based on the following two versions of the CrowdStrike Falcon Endpoint solution.

| | MSSP Protect | MSSP Defend |
|---|---|---|
| Falcon Prevent | ✔ | ✔ |
| Falcon Control and Respond | ✔ | ✔ |
| Falcon Insight | | ✔ |

## CrowdStrike Falcon protects against all types of attack

### Key Capabilities

#### AI-Powered Next Generation Anti-Virus

- Fully protects endpoints online and offline.
- Protects against the entire spectrum of attacks, including ransomware, malware-free attacks and fileless attacks, adware and potentially unwanted programs (PUPs) without requiring daily updates.
- Combines the best prevention technologies including machine learning, artificial intelligence (AI), indicators of attack (IOAs) and exploit blocking to stop the execution and spread of threats via unpatched vulnerabilities.
- Quarantines blocked files and allows access for investigation.
- Script-based execution monitoring inspects and blocks malicious Microsoft Office macros.
- Sensor tampering protection stops user or process attempts to manipulate or disable the CrowdStrike Falcon® sensor.


CrowdStrike Falcon Prevent Dashboard Example

- Integrated threat intelligence that automatically determines the scope and impact of threats found in your environment. You can find out if you are targeted, who is targeting you and how to prepare and get ahead.
- Full attack visibility at a glance, providing context and history for every alert, unravelling an entire attack in one process tree.

- Prevents silent failure by capturing raw events for automatic detection of malicious activity, providing unparalleled visibility, proactive threat hunting and forensic investigation.
- Unravels an entire attack in the easy-to-use CrowdScore™ Incident Workbench, enriched with context and threat intelligence data.
- Provides powerful response action to contain, investigate and remediate compromised systems.

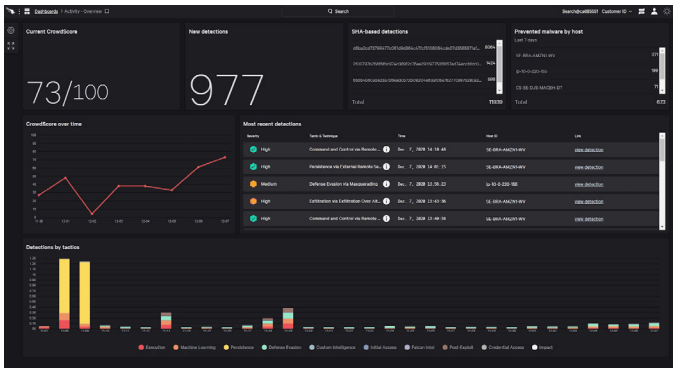
## Falcon Insight

The key difference between the two MSSP solutions is the addition of the Falcon Insight module within the MSSP Defend offering.

Falcon Insight provides complete EDR capabilities and visibility, allowing the platform to continuously monitor all endpoint activity and analyse the data in real time to automatically identify threat activity, enabling it to both detect and prevent advanced threats as they happen, enabling the security team to rapidly investigate incidents and respond to alerts.

### Key Capabilities

- Automatically detect attacker activities using indicators of attack (IOAs) to automatically identify attacker behaviour and send prioritised alerts to the Falcon user interface, eliminating time-consuming research and manual searches.
- Unravel entire attacks on just one screen with the Incident Workbench providing a comprehensive view of an attack from start to finish and deep context for faster and easier investigations.
- Respond decisively by acting against adversaries in real time to stop attacks before they become breaches allowing you to contain and investigate compromised systems.
- Real Time Response capabilities provide direct access to endpoints under investigation. This allows security responders to run actions on the system and eradicate threats with surgical precision.
- See the big picture in real time with CrowdScore delivering a simple metric that helps you to understand the threat level in real time. This makes it easy for security leaders to quickly understand if they are under attack and assess the severity of the threat so they can coordinate the appropriate response.
- Understand endpoint security posture with a Zero Trust Assessment (ZTA) that determines endpoint health across the organisation. With real-time security posture assessment, you can easily identify and update sensor policies and OS settings that are out-of-date or that increase risk.




**CrowdStrike Falcon Prevent Dashboard Example**

# Wavenet Managed Service

Operating from Wavenet's CyberGuard Security Operations Centre (SOC), our highly skilled team of security experts take responsibility for the implementation, configuration, and monitoring of our customers' environments, detecting, and investigating incidents and alerts in line with our priority-based SLA system.

## The following is included in the service:

- Triage and Investigation of alerts from the supported technologies and platforms.
- Carry out response actions based on alert investigation findings i.e., isolation of devices, removal of malicious files etc.
- Continual development and maintenance of the supported technologies to provide the highest level of protection against the latest and emerging threats whilst considering the requirements of the business.
- Ongoing development and implementation of detection analytics across the technologies used, to defend against threats appropriate to the organisations threat landscape.
- All alerts investigated and followed up within our defined priority-based SLAs.

| Priority | Time to first response | Time to resolution |
|---|---|---|
| Critical | 15 minutes | 1 hour |
| High | 15 minutes | 2 hours |
| Medium | 1 hour | 4 hours |
| Low | 4 hours | 24 hours |

WAVENET.CO.UK

# 0333 234 0011

Wavenet Limited
One Central Boulevard
Blythe Valley Park
Solihull, West Midlands
B90 8BG

**cyberguard@wavenet.co.uk**

wavenet

Networking & Connectivity

Unified Communications & Voice

Contact Centres

Mobile Solutions & IoT

IT, Cloud & Technology

Network Intelligence

Cyberguard