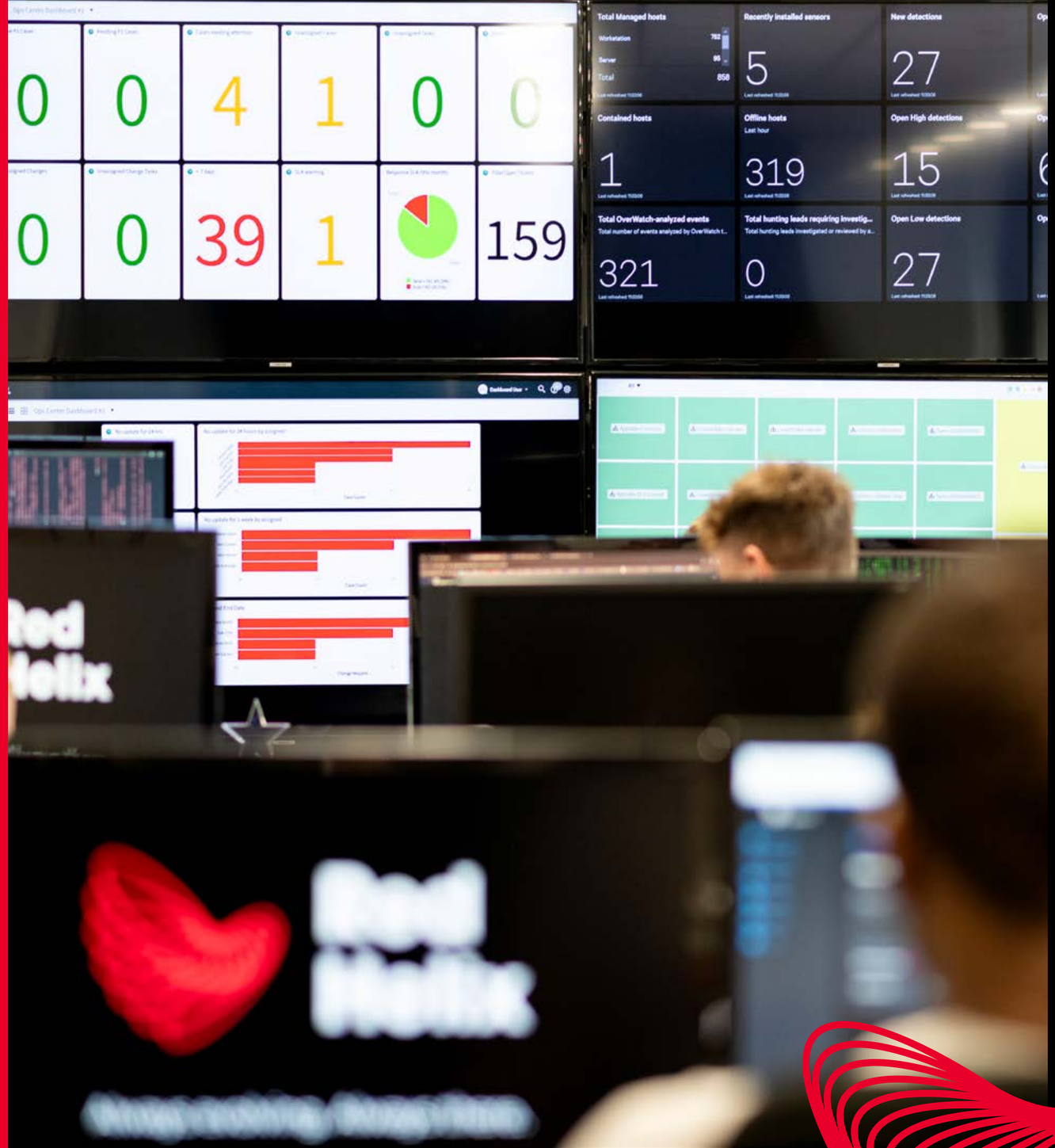

EDR Demystified: The Essential Playbook for Modern Cyber Defence

Red Helix

CONTENTS

What is EDR?

Endpoint Detection and Response (EDR) is a cyber security solution designed to continuously monitor an organisation's endpoint activity across devices such as computers, mobile devices, and servers. It detects, investigates, and responds to potential threats, providing threat intelligence that helps security teams understand how attacks occur and how to prevent future incidents.

By giving visibility into activities happening at the endpoint, EDR enables security teams to detect suspicious activity that may have otherwise gone unnoticed. It also contains threats before they spread across the network, and guides security teams on how to respond effectively.

Why you need an EDR?

The modern threat landscape is evolving at an unprecedented pace, rendering legacy security solutions insufficient. Cyber criminals now employ sophisticated attack methods, including fileless malware, zero-day exploits, and the use of stolen credentials to bypass traditional security defences. These advanced tactics make it increasingly difficult for organisations to detect and mitigate threats before they cause significant damage.

Compounding these risks is the looming shift towards a post-quantum era. Malicious actors are actively exfiltrating encrypted and unencrypted data, operating under the assumption that future quantum advancements will enable them to decrypt and exploit stolen information. This proactive approach by cyber criminals underscores the need for organisations to implement robust security measures that can detect and prevent unauthorised access in real-time.

Additionally, the shift to remote and hybrid workforces in the post-COVID era has introduced new vulnerabilities. Employees frequently connect to corporate networks from unsecured locations, increasing the risk of cyber attacks. Traditional security solutions often lack the visibility and response capabilities necessary to protect endpoints beyond the corporate perimeter, leaving organisations exposed to potential breaches.

Regulatory compliance is another pressing concern. With stringent legislation such as NIS2 and the Digital Operational Resilience Act (DORA) coming into effect this year, alongside the pending Cyber Security and Resilience Bill. Businesses must prioritise security measures that support compliance and reporting requirements. An EDR solution provides continuous monitoring, automated threat detection, and forensic analysis capabilities—critical features that help organisations meet these evolving regulatory obligations.

By adopting an EDR solution, companies gain real-time visibility into endpoint activity, enhanced threat detection powered by AI-driven analytics, and the ability to respond swiftly to incidents before they escalate. In an era where cyber threats are more sophisticated and regulatory pressures are mounting, investing in EDR is not just a strategic advantage, it is a necessity for securing business operations, protecting sensitive data, and ensuring long-term resilience.

EDR Core Functions

According to IBM, various studies estimate that as many as 90% of successful cyber attacks and 70% of successful data breaches originate on an endpoint. This is why protecting your endpoints is so vital. Detecting, and removing malware and stopping attacks before they cause harm is key.

Below are some of the core functions that the Red Helix EDR service provides:

Automatically detects attackers

Our EDR service offers unparalleled visibility across all endpoints, leveraging Indicators of Attack (IOAs) and advanced behavioural analytics to automatically detect traces of suspicious behaviour.

The tooling analyses security events as part of a broader sequence, applying CrowdStrike Intelligence to determine whether the sequence of events matches known IOAs.

If the pattern does match an existing IOA the activity is identified as malicious, and a detection alert is sent automatically. Clients can also write their own custom searches, with Falcon Insight's cloud architecture returning query results from the last 90 days.

Seamless threat intelligence integration

By integrating with CrowdStrike Adversary Intelligence, our EDR service provides rapid identification of malicious activities and attack tactics, techniques, and procedures (TTPs). This integration offers valuable context, including threat attribution where available, giving our security teams deeper insights into attackers and their methods.

Provides real-time and historical endpoint visibility

EDR technology will record relevant activity to catch incidents that evaded prevention. Customers are given comprehensive visibility into everything that is happening on their endpoints from a security perspective as the technology tracks hundreds of different security-related events, such as process creation, drivers loading, registry modifications, disk access, memory access or network connections.

This gives security teams the useful information they need, including:

- Local and external addresses to which the host is connected
- All the user accounts that have logged in, both directly and remotely
- A summary of changes to ASP keys, executables and administrative tool usage
- Process executions
- Both summary and detailed process-level network activity, including DNS requests, connections, and open ports
- Archive file creation, including RAR and ZIPS
- Removable media usage

This level of visibility allows security teams to monitor an adversary's activities in real time, observing which commands they are running and what techniques they are using, even as they try to breach or move around an environment.

Accelerates investigations

By storing, the endpoint activity using a situational model CrowdStrike endpoint detection and response can accelerate the speed of investigation and ultimately, remediation.

The situational model keeps track of all the relationships and contacts between each endpoint event, providing details and context rapidly and at scale, for both historical and real-time data. This enables security teams to quickly investigate incidents.

Enables fast and decisive remediation

The EDR service also enables 'network containment', allowing organisations to take swift and instantaneous action isolating potentially compromised hosts from all network activity, whilst still sending and receiving information from the CrowdStrike cloud.

How Does EDR Work?

Our EDR service provides threat detection, real-time visibility, and device remediation. To offer this level of visibility we use a combination of methods:

Continuous endpoint monitoring

EDR continuously collects and analyses endpoint data, including file activity, process execution, network connections, and user behaviour. This covers everything from file and network access, through to processes and system changes. Real-time monitoring helps detect unusual patterns that may indicate a security threat.

Threat detection using AI & behavioural analytics

EDR uses AI-powered behavioural detection and machine learning algorithms to proactively identify and prevent known and unknown threats, so we can detect malicious activities in real-time, stopping attacks before they can do any harm.

Incident investigation & threat hunting

Our SOC team investigate alerts by analysing forensic data, tracking attack timelines, and identifying how a threat entered the system. This investigates the entire lifecycle of the threat, providing insights into what happened, how it got in, where it has been, what it is doing now, and what to do about it. By containing the threat at the endpoint, EDR helps eliminate the threat before it can spread across your environment.

Automated response & containment

Compromised devices are isolated from the network to prevent further spread of malware or cyber attacks. It will automatically terminate malicious processes, delete harmful files, and block unauthorised access.

Integration with security tools

EDR technology integrates with Security Information & Event Management (SIEM) and Network Detection & Response (NDR) solutions to provide a broader security approach. This correlates data across multiple security layers (endpoints, cloud, email, and network). This combination of tools and monitoring is available via our MDR service.

Reporting capabilities

The EDR tools provides our SOC and your team with detailed logs, attack timelines, and forensic data for analysis and compliance audits. Allowing security teams to analyse and investigate security incidents and prioritise effectively.

What are the Latest Features

As a proud UK Managed CrowdStrike Provider, we have seen many changes to the platform over the past year. As of February 2025, we have witnessed several notable updates:

1. Falcon for Legacy Systems

The newest CrowdStrike update has been Falcon for Legacy Systems. This feature aims to protect legacy Windows systems with a comprehensive, cloud-native anti-malware solution. Its capabilities are fully integrated into the existing Falcon platform, enabling you to secure legacy endpoints via a single console, powered by cloud-based machine learning.

Advantages from this update include real-time and up-to-date detection and protection against threats. Additionally, the unified platform amplifies operational efficiency and reduces complexity. This safeguards existing infrastructures whilst causing minimal disruption and increases the potential number of CrowdStrike customers as their technology can now be installed on previously unsupported legacy systems.

2. Falcon Exposure Management

Last summer, CrowdStrike advanced its vulnerability management program, offering Falcon Exposure Management, a solution which builds upon their existing Falcon platform. This product provides visibility into assets, identifies vulnerabilities, and misconfigurations, and prioritises remediation efforts to minimise the risk of breaches. As a result, it can proactively manage and reduce an organisation's attack surface.

Currently, **76% of organisations have experienced an attack that originated from an unknown asset.** However, via Exposure Management tools, organisations can successfully address internal and external asset exposures, reducing external attack surfaces, mitigating risks, and fostering effective collaboration within the security team.

It has been reported that **62% of organisations have blind spots that weaken their security posture.** However, Exposure Management provides complete visibility of an attack surface to support security action or decisions. Therefore, remediation of known vulnerabilities can be identified and prioritised. The tool can also be integrated with other third-party monitoring platforms such as Security Orchestration Automation and Response (SOAR) and ServiceNow, ensuring a comprehensive remediation process.

Benefits of the Falcon Exposure Management platform include AI-driven vulnerability prioritisation, comprehensive visibility, maintenance-free assessments for a wide variety of exposures, and more. The feature also accurately uses data to calculate risk based on exposure to threats.

3. Falcon Next-Gen SIEM

CrowdStrike's Falcon Next-Gen SIEM platform is designed to unify data, threat intelligence, AI, and workflow automation into a single, streamlined solution. This leads to up to **150x faster search performance and reduces the total cost of ownership by 80% compared to traditional SIEMs.** Falcon transforms Security Operations Centre (SOC) operations with enhanced visibility and protection.

Key features include real-time alerts, live dashboards, and integrated world-class intelligence, all enabling faster detection and response. By consolidating tools and leveraging an AI-native platform, Falcon eliminates operational silos, reduces manual tasks through automation, and significantly cuts response times.

Additionally, the platform accelerates time-to-value with a growing library of data connectors and pre-integrated key data. By unifying data and leveraging advanced AI, Falcon empowers analysts to detect threats in real-time and investigate incidents in seconds. CrowdStrike's modern approach to SOC transformation streamlines operations and therefore achieves unparalleled security outcomes.

4. Falcon Cloud Security

CrowdStrike Falcon Cloud Security has spanned across cloud environments improving usability, visibility, and efficiency, empowering users to manage cloud security with greater precision and ease.

The UI enhancements are evident in features such as ‘Asset Relationship View’ with mini graph, which allows users to view asset relationships directly from the cloud assets table without navigating away. A new mini asset graph is available in the info panel of supported asset types. This feature includes zoom functionality and a button to access the full asset graph.

The containers inventory page introduces new columns and filters for image registry, image repository, and image tag. These updates simplify identifying container images and detecting unknown containers. Additionally, it has introduced an improved filter selection on the Cloud Assets Page. Users can now select all filters within a category using a single checkbox, with the option to refine results by deselecting specific filters. A new search box at the top of the filter list enables users to quickly locate specific filters, and relevant categories automatically expand as characters are entered.

Complete your free Cloud Security Health Check here.

4.5. Falcon Shield

As part of these cloud security enhancements, the rebranded Falcon Shield has been reintroduced as a bolt-on to their existing cloud security offerings. Falcon Shield’s SaaS Security Posture Management Suite (SSPM) removes this burden for your team by providing deep visibility and remediation for potential risks caused by misconfigurations. The platform features proactive, continuous and automated monitoring capabilities and a built-in knowledge base of compliance standards and benchmarks. The solution can be live within minutes, to allow clear visibility into your whole ecosystem, and send detailed alerts at the first sign of a security misconfiguration.

Key features include misconfiguration management, identity security posture, application discovery and control, and more. It aims to deliver actionable insights and real-time protection, enabling organisations to secure their cloud environments and strengthen their overall security posture.

5. Data Security Posture Management (DSPM)

CrowdStrike’s new Data Security Posture Management (DSPM) capabilities are designed to help organisations identify and secure sensitive data in their cloud environments. This provides visibility into sensitive information, such as customer data and payment details, and where it is stored, ensuring it is only located in appropriate areas with proper security controls.

DSPM empowers organisations with the ability to proactively manage sensitive data security, therefore enhancing compliance and reducing risks in their cloud operations.

DSPM scans sensitive data to correctly classify information into categories (e.g. Personally Identifiable Information (PII), Payment Card Industry data (PCI), and more). Additionally, post-scan, detailed insights are provided, as users can view data classifications on the Cloud assets inventory page. Asset detail panels can also provide granular classification.

What Does EDR Replace

AV software has been a trusted cyber security solution for over 30 years. It was designed to protect against malware, hackers, and cyber criminals. It identifies, blocks, and protects against any external threats which may infiltrate networks. Antivirus software scans foreign devices at a given point in time to look for and block viruses via signature detection and heuristic analysis. If your device gets infected, antivirus software will help you remove it.

EDR over AV legacy systems.

Antivirus software is installed directly on a system to protect it from malicious actors. It provides limited scope into system networks whereas EDR actively detects and prevents these threats whilst providing visibility. EDRs vastly expand the traditional capabilities of AV solutions.

They provide continuous visibility into endpoint activity which allows IT security teams the ability to respond to threats that a traditional AV software can't. Anti-virus programs are signature-based, which means they cannot detect malware containing an unknown signature. Additionally, they cannot prevent complex attacks like memory-resistant malware, designed to cover their tracks and block attempted removal. In contract, EDR solutions go much further and can detect unknown threats.

EDRs integrate AI intelligence into your security infrastructure in conjunction with machine learning to detect and respond to unknown threats. This means that the response automatically updates to deal with new, complex malware threats.

An EDR solution provides a response function which automatically contains endpoints on the network. It ensures swift resolution and prevents repeat attacks, which provides a much more effective remediation service.

According to the **CrowdStrike 2024 Global Threat Report, 75% of attacks are malware-free which means they evade legacy antivirus software searching for known file and signature-based malware.** Antivirus is designed to identify and stop viruses and malware; however, it's incapable of detecting and stopping sophisticated techniques employed by today's attackers. For example, traditional antivirus solutions can't detect attacks that are malware-free or that involve the use of valid identity credentials that have been stolen, which now make up most attacks. Cyber security tools are a major component of an effective defence, but you also need modern processes and people to run them.

By implementing an EDR solution into your security, you will dramatically reduce your cyber risk. This risk reduction increases even further when you combine it with other cyber security solutions.

Request a 15-day free trial here. Discover the power of real-time threat detection, simplified management, and proactive threat hunting.

EDR	AV
Detects malware via behavioural analytics, anomaly detection, and heuristics	Detects malware via signatures
Automatic incident response	Limited incident response
Proactive threat hunting	Reactive threat hunting
Integrates with network infrastructure	Standalone solution
Detects known and unknown malware	Detects known malware
Continuous monitoring	Periodic monitoring
Advanced behavioural analysis	Limited behavioural analysis

How do Red Helix Provide EDR Services?

While cyber attacks on large businesses dominate the headlines, small and medium sized businesses face an equally alarming threat from cyber criminals. Although they may not make the headlines, these businesses still hold valuable data and are increasingly profitable targets for malicious actors. Unlike large organisations with dedicated cyber security teams and advanced technology stacks, SMBs often lack the internal resource and dedicated team members to combat these attacks.

According to Veeam, 85% of ransomware attacks targeted SMBs in 2023, as cyber criminals recognise both the vulnerability and value of SMBs, viewing them as easy prey ripe for compromise, ransomware and data theft.

Many SMBs have legacy technology in place, like antivirus software, which cyber criminals have now evolved far beyond and can easily combat.

Managed EDR

At Red Helix, we partner with CrowdStrike to provide a managed Endpoint Detection & Response (EDR) service. While CrowdStrike's platform is cutting-edge, many SMBs face challenges managing its advanced tooling, keeping up with updates, or allocating the dedicated personnel required for 24/7 monitoring.

To internally manage CrowdStrike 24/7, a business would need at least three full-time staff members to consistently monitor alerts and keep up to date with the new features on the platform, which is a substantial investment. Outsourcing endpoint security to a Managed Security Service Provider (MSSP) allows organisations to concentrate on growth rather than managing security challenges.

By leveraging shared licensing models, we provide SMBs with access to advanced CrowdStrike solutions at a fraction of the cost. Our predictable monthly pricing model ensures organisations can scale their security as needed without overinvesting upfront.

The democratisation of advanced cyber security tools means that SMBs can finally level the playing field, staying protected with the same tools and expertise used by the world's largest organisations.

Managed Detection & Response (MDR)

If you want to go one step further our Managed Detection & Response service includes, Endpoint Detection & Response (EDR), Network Detection & Response (NDR), Security Information & Event Management system (SIEM) and 24/7 SOC monitoring.