Cyber **security**

MANAGED CROWDSTRIKE EDR & EPP

THREAT READY



LRQA SOC
SECURITY OPERATIONS CENTRE

LRQA
Your Risk Management Advantage

CONTENTS

3 Managed Endpoint Detection, Response & Protection

4 What is Managed EDR/EPP?

6 About CrowdStrike

7 Why do you need EDR & EPP?

8 Benefits of Managed EDR & EPP

9 Managed EDR & EPP – Service Features

10 LRQA Value Proposition

MANAGED ENDPOINT DETECTION, RESPONSE & PROTECTION

LRQA is an award-winning cybersecurity organisation with unparalleled capability in delivering managed security services.

Through our managed UK-based Security Operations Centres (SOCs) we can deliver round-the-clock services that secure our clients and detect and respond to sophisticated cyber threats, providing assurance that your organisation is protected.

Technology alone cannot completely mitigate the risk from cyber threats. Instead, businesses must respond through a well-managed security service considering all aspects of risk and using processes that extend through technology and into the workforce.

A Managed EDR or EPP service can provide a level of visibility and security that can be difficult to maintain in-house, both in terms of availability and expertise. The LRQA Managed EDR/EPP service can be utilised for organisations that have limited resources and expertise to assist with the provision, management and monitoring of EDR and EPP technologies to provide a world-class capability in detection and response.

LRQA SOC SECURITY OPERATIONS CENTRE

CROWDSTRIKE

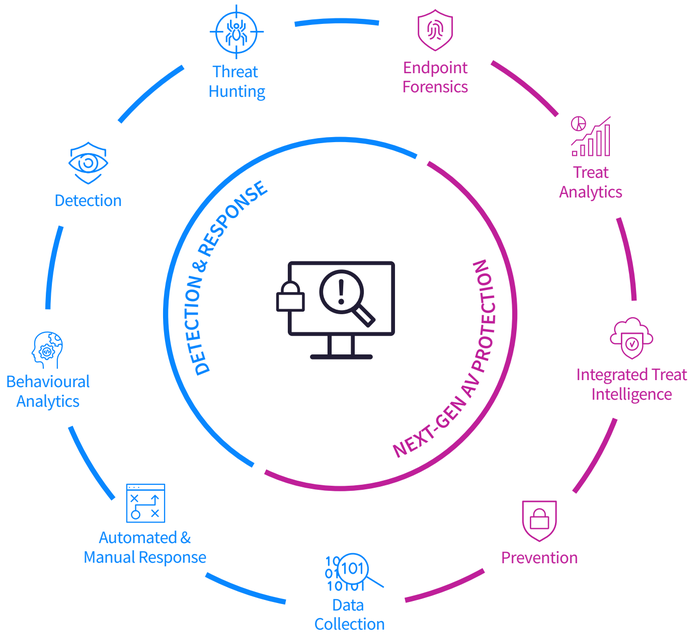


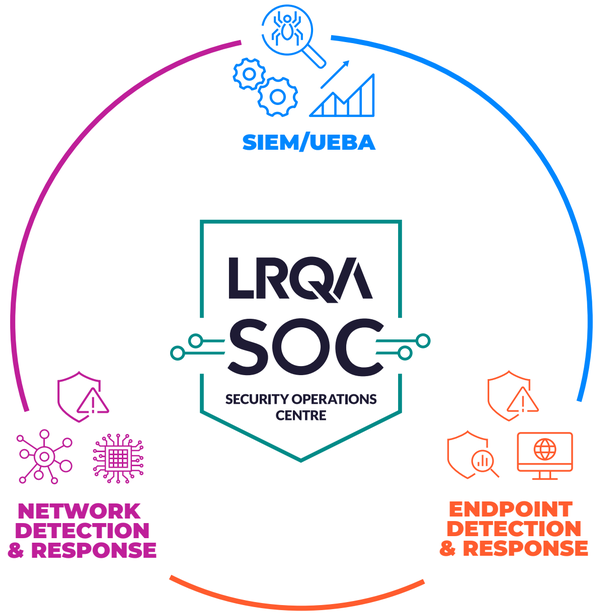
WHAT IS MANAGED EDR/EPP?

Endpoint Detection and Response (EDR) tools provide an integrated endpoint security solution that provides real-time continuous monitoring and detection, combined with response and analysis capabilities.

Endpoint Protection Platform (EPP) is an evolution of the next-generation anti-virus capabilities, providing prevention, detection, and monitoring for both file-based and file-less malware using static Indicators of Compromise (IOCs), signatures, and behavioural analytics.

Advanced endpoint protection solutions provide integrated EDR and EPP capabilities in a single deployable agent. Endpoints are a critical area for both monitoring and protection as the majority of attacks will land there and are where an attacker will look to get the execution of their tooling, achieve privilege escalation, and lateral movement. The importance of endpoint security monitoring was recognised by Gartner and forms the cornerstone of their security monitoring triad.





ABOUT CROWDSTRIKE

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, USB device control, vulnerability management, and IT hygiene capabilities.

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, able to operate across Windows, MacOSX, Linux, mobile devices, as well as servers and containers in modern hybrid multi-cloud data centres.



BENEFITS OF MANAGED EDR & EPP

The LRQA Managed EDR and EPP services significantly reduce the likelihood of an adversary completing their attack, leading to a data breach or other malicious action.

It also reduces the time to detect and respond to an incident. These metrics (known as Mean Time to Detect or MTTD and Mean Time to Respond or MTTR) are key indicators of an effective detect and respond capability.

The specific objectives of the service will be customised to each client collated through the BI workshop and service reviews on an ongoing basis. This is because every client will face different threats and operate a unique set of critical assets.
LRQA understands this and therefore can customise the detection through a unique set of use cases.



DEFENCE SOPHISTICATION

Next-Gen Endpoint Security is far superior to traditional Anti-Virus technologies.

Designed to prevent and detect sophisticated threats including Ransomware.

Leverage Machine learning, Threat analytics & Intelligence.



REDUCED COMPLEXITY

Security Architectures can be incredibly complex, Simple cloud-based SaaS solution.

Single lightweight agents deployed within minutes.

Easily integrated into other security products and tools to achieve automation & orchestration.



ADVANCED EXPERTISE

Security tools need expertise and training to ensure they are deployed, configured and managed properly.

Using LRQA managed service provides world-class expertise that's always on and always available.



EFFICIENCY

Built-in automated actions covering containment and response managed through a single management console.

Log-based and traditional AV generate large amounts of false positive alerting.

Advanced Next-Gen protection means more threats are blocked at the point they land, meaning less remediation.



RAPID RESPONSE

Traditional monitoring only solutions don't 'Block' which means complex attacks like Ransomware are not prevented.

Sophisticated detection, response & forensic capability allows defensive teams time to contain and limit harm.

Automated blocking & live response features ensure a rapid response in real-time.

MANAGED EDR & EPP – SERVICE FEATURES

LRQA's Managed Endpoint Detection and Response service provide the most highly accredited expertise combined with Gartner Magic Quadrant leading security technology to deliver industry-leading protection for your organisation.

Our approach is proactive, and threat led; informed by our offensive and threat intelligence teams to shape our defensive stance and protect against the latest industry threats providing in-depth unrivalled detection and alerting capability where it is needed most.

24/7/365 ALWAYS ON

24/7 x 365 Expert Security Analysis: always there, monitoring & alerting and advising for your peace of mind.

GLOBAL DELIVERY

LRQA has been at the forefront of cyber security SOC Operations since 2003. Our Managed EDR & EPP services can be deployed and managed globally through our UK-based SOC

GLOBAL EXPERTISE

Certified expert knowledge within Offensive and Defensive Cyber operations, our SOC team are on hand as an extension of your teams to provide expert advice, guidance and remediation where required.

SECURITY SIMPLICITY

Security architecture and security tools deployment can be complex. LRQA Managed EDR & EPP service is provided using a cloud-based SaaS solution through a single lightweight agent that can be rapidly deployed.

LEADING TECHNOLOGY

Managed EDR & EPP solutions are Gartner leaders in protection, detection, prevention and response providing your organisation with best-in-class defensive capability.

DASHBOARD & REPORTING

Custom real-time dashboards created in line with your business requirements combined with our Security & Service reporting to provide you complete visibility and insight to your security stance.

PERFORMANCE & AVAILABILITY

LRQA maintains best-in-class performance across our Managed Security Services covering MTTD, MTTR and MTTE. Ensuring a rapid response to sophisticated cyber threats.

CUSTOMISATION & ENGINEERING

LRQA has certified experts that can assist in customisation, configuration and engineering to ensure complete coverage of bespoke systems and applications.

ABOUT LRQA

LRQA is a leading global risk management partner.

Through our connected risk management solutions, we help you navigate an evolving global landscape to keep you one step ahead.

From certification and cybersecurity, to safety, sustainability and supply chain resilience, we work with you to identify risks across your business. We then create smart, scalable solutions, tailored to help you prepare, prevent and protect against risk.

Through relentless client focus, backed by decades of sector-specific expertise, data-driven insight and on-the-ground specialists across assurance, certification, inspection, advisory and training, we support over 61,000 organisations in more than 150 countries.

LRQA – Your risk management advantage.

GET IN TOUCH

Visit **LRQA.com** for more information or email **enquiries.uk@lrqa.com**

LRQA
1 Trinity Park
Bickenhill Lane
Birmingham
B37 7ES
United Kingdom

Care is taken to ensure that all information provided is accurate and up to date; however, LRQA accepts no responsibility for inaccuracies in or changes to information.

LRQA
Your Risk Management Advantage