



TECH DRIVEN. PEOPLE POWERED.

Solution Brief: Wingman Endpoint Detection and Response (EDR)

Wingman Endpoint Detection and Response (EDR) offers organisations a powerful combination of industry-leading EDR software with the advanced threat investigation capabilities of the SEP2 24/7/365 eyes-on SOC. Providing a fully comprehensive service from protection, through to detection and root cause analysis for all confirmed threats, Wingman EDR allows you to get the most from your product investment without the need to increase your internal workload.

Endpoints are widely accepted as one of the top cyber security risk factors, with adversaries taking advantage of human fallibility to attempt to breach organisations. The risk exposure has only increased over recent years due to an increasing mobile workforce and the spread of data from central datacentres to SaaS cloud environments. EDR is required more than ever to ensure your sensitive corporate and personal data is secured.





The SEP2 SOC provides staffed, eyes-on 24/7/365 services from our dedicated SOC in Leeds, UK. The SOC investigates threats, responds to alerts and guarantees uninterrupted handling of our customers' security incidents around the clock. The SEP2 SOC is fully staffed by SEP2 employees: no outsourcing, no subcontracting & no offshoring.

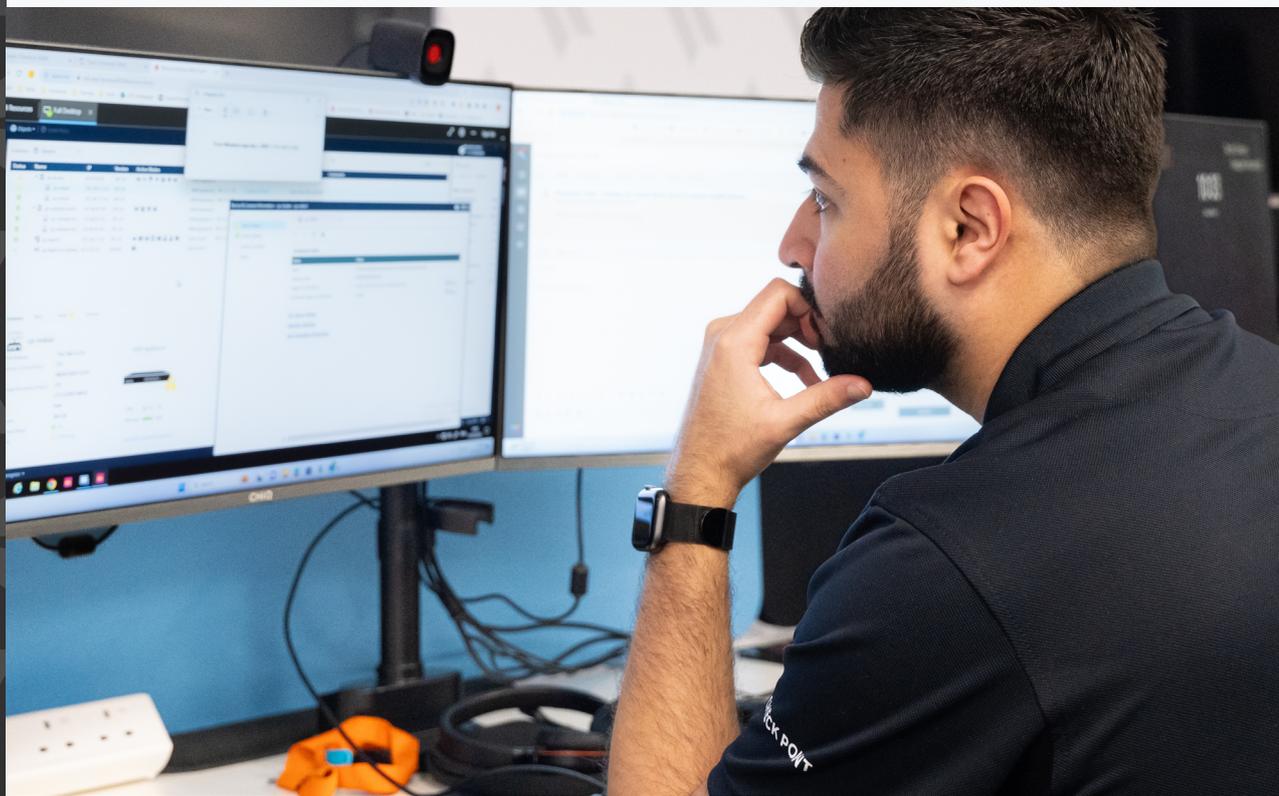
As an integral part of the Wingman XDR offering, EDR provides key monitoring and data collection from your endpoints, enhancing the information available to our SOC. This allows us to deliver a comprehensive monitoring, detection, alerting and remediation service across your entire environment.

Clever automation

Taking advantage of our advanced knowledge of SOAR and automation, Wingman EDR leverages our investment in

technology to provide expedited investigations and false positive detections.

By layering threat intelligence methodologies on top of the detections from the protection product, we can quickly identify the real threats from the fakes, ensuring you are only alerted when there is a true threat present. Going beyond this, our automated and manual threat hunting exercises ensure that even hidden threats don't stay that way for long, uncovering the unknown on your devices.





Service levels

At SEP2, we recognise that not every organisation has the same needs, nor are they at the same place in their cyber security journey. To help cater to all, Wingman EDR is available in different packages designed to best fit all types and sizes of organisations.

From basic deployment and support services for organisations with skilled technology teams of their own, to automated threat confirmation and investigation, and even fully managed threat hunting, Wingman EDR offers a spectrum of solutions to enhance and improve your cyber security.

*BESPOKE PACKAGE AVAILABLE. ADDITIONAL SERVICES ON REQUEST.

FEATURES*	BASIC	STANDARD	ENHANCED
INITIAL DEPLOYMENT			
POLICY MANAGEMENT			
ENDPOINT SOFTWARE UPGRADES			
UNLIMITED CHANGE REQUESTS			
ENDPOINT TROUBLESHOOTING			
VENDOR ISSUE ESCALATION			
24/7/365 AUTOMATED THREAT INVESTIGATION			
24/7/365 AUTOMATED THREAT RESPONSE			
HUMAN EYES-ON THREAT CONFIRMATION			
DETAILED THREAT INVESTIGATION			
THREAT HUNTING			
SERVICE THREAT REPORTING			

SEP2 also offer MDR. Interested in our True eXtended Detection and Response (MXDR) service? Get in touch at info@sep2.security