REDSCAN

DETECT & RESPOND

ThreatDetect™ Endpoint MDR

Extending your threat monitoring capabilities to the endpoint

Compromising endpoints is a common tactic used by cybercriminals to establish a foothold on a network. Rapid detection and response to attacks targeting hosts such as desktops, laptops and servers should therefore be integral to your IT security.

ThreatDetect™ Endpoint Detection and Response (EDR) is a fully managed service supplying the expert professionals, technology and industry intelligence needed to hunt for, lockdown and remediate attacks.

By monitoring endpoints and conducting comprehensive incident response and forensics, our expert Cyber Security Operations Centre (CSOC) professionals obtain a real-time awareness of attackers' movements in order to enhance threat discovery.

Reducing the dwell time of attacks

With the number of breaches increasing at an unprecedented rate, every organisation needs to reduce the amount of time it takes to detect and respond. For an affordable monthly subscription, ThreatDetect EDR provides the essential capabilities needed to eliminate wide-ranging actors.

Included as part of the service:

- ✓ Proactive threat hunting and investigation
- ✓ Endpoint detection technology from Carbon Black*
- ✓ Detailed incident reporting and analytics
- ✓ Fully integrated incident response
- ✓ Regular stakeholder and compliance reporting

*A Visionary in the Gartner Magic Quadrant for Endpoint Protection

Why choose Redscan's Endpoint ThreatDetect service?

Greater threat visibility

Relying exclusively on network-based monitoring can leave your cyber security open to blind spots. By providing immediate visibility of what is happening on endpoints at any given moment in time, ThreatDetect EDR enhances awareness of threats across your whole IT infrastructure. It also greatly improves the efficiency of response efforts by helping to prioritise remediation and reduce needless investigation of false positives.

Enhanced detection capabilities

As the tactics and procedures used by attackers evolve, being able to view deep into your endpoints enables our CSOC professionals to identify actors that could otherwise be overlooked. With both encrypted and non-malware attacks on the rise, the ability to proactively and continuously monitor processes and binaries across network hosts can help to detect threats that traditional preventative security solutions such as AV can miss.

Swifter incident response

ThreatDetect EDR facilitates enhanced incident response by performing in-depth forensic analysis of endpoint devices' memory and disk space in order to quickly identify the root cause of attacks. As soon as malicious activity is detected, infected hosts can be quickly isolated and the responsible threat actor promptly shut down and eliminated before it spreads across your environment.

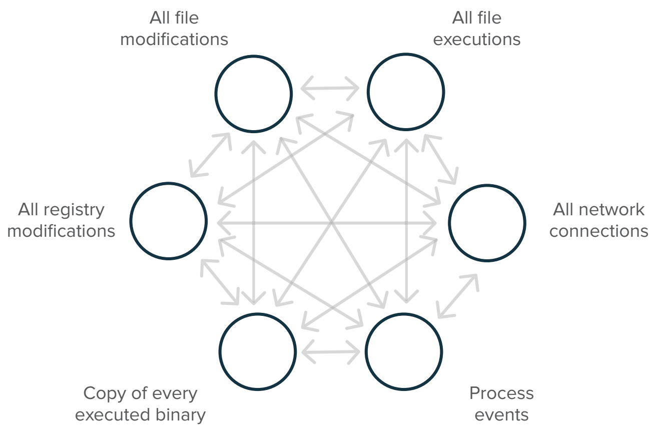
Improved threat hunting

Using the latest endpoint technology from Carbon Black and a wide range of industry intelligence, our dedicated threat hunters proactively search for known and unknown attack vectors. Applying our collective knowledge of the latest hacking techniques, experience of threat detection across industries and in-house Redscan Labs security research, we create custom watchlists that monitor for suspicious patterns of behaviour across your endpoints.

REDSCAN

DETECT & RESPOND

Minimising the cost, complexity and duration of traditional incident response



Advanced threat detection across your endpoints

By recording each and every file execution and modification, registry change, network connection and binary execution across all your organisation's hosts, endpoint technology empowers Redscan's security professionals to inspect deeper into your IT environment in order to hunt for, detect and terminate known and unknown threats.

> *"With a managed endpoint detection and response service, identifying and resolving threats on your endpoints takes minutes rather than months"*

Service features

+ Continuous data collection

Collecting threat data post-detection makes it almost impossible to understand lateral movement or the root cause of advanced attacks. By monitoring processes, binaries and IP addresses in real-time, endpoint security makes it possible to track malicious actors in progress and understand the full context of incidents.

+ Unlimited data retention

Endpoint technology maintains a centralised store of data records captured across every endpoint in your environment, enabling Redscan's threat hunters to identify past and present attacks and provide an historical timeline of evidence, as mandated by the breach reporting requirements of legislation such as the General Data Protection Regulation.

+ Attack kill chain visualisation

Being able to quickly uncover and visualise attacks unfolding within your business' environment enables our CSOC team to quickly uncover the root cause and scope of each intrusion.

+ SIEM integration

To enhance threat detection efforts further, endpoint protection can be integrated with the Security Information and Event Management (SIEM) technologies offered as part of our ThreatDetect Network MDR service to support the correlation of both network events and endpoint data.

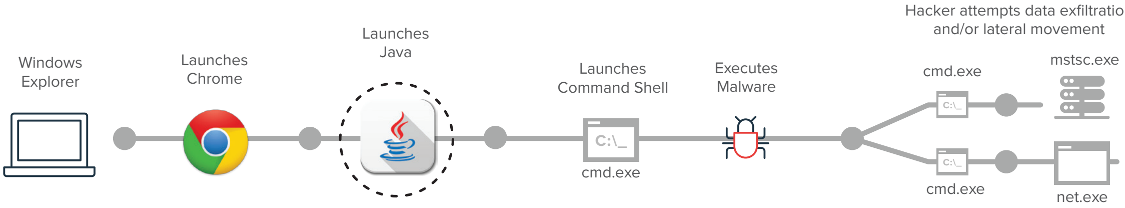
+ 20+ threat feeds

By layering threat intelligence feeds from sources including VirusTotal, ThreatExchange and SANS, with Redscan's own in-house threat intelligence, our managed service keeps your endpoint technology optimised to detect the latest threats and reduce reporting of false positives.

+ Unlimited scalability

Designed to scale to fit even the largest enterprises, ThreatDetect EDR's underlying endpoint technology supports on-premise and cloud deployments. Individual lightweight sensors are installed on each endpoint and operate silently to avoid impacting your end users.

Visualising the attack kill chain helps Redscan's CSOC analysts to discover the root cause and scope of each attack



EMAIL US

✉ info@redscan.com

CALL US

☎ 0800 107 6098

ONLINE

redscan.com

REDSCAN

Carbon Black