THREATDETECT™

Award-winning managed detection and response for networks and endpoints

info@redscan.com

0800 107 6098

redscan.com
“Providing the security expertise, tools and intelligence needed to respond to threats and breaches"
Advanced protection against threats

Defending against the latest cyber threats is a constant battle. With over a million new threats reported daily and a growing range of sophisticated hacking techniques capable of evading traditional security, it’s no longer a case of if your business will be breached but when.

The challenges of in-house detection

To make significant improvements to your organisation’s cyber security posture and achieve compliance standards, having the capability to identify and eliminate attacks before they cause damage is now essential.

For many businesses however, acquiring the resources needed to hunt for threats is simply not viable. From the cost of hiring qualified personnel to provide around-the-clock support, through to sourcing the most up-to-date technology, running an in-house security operation can represent a huge upfront and ongoing expense.

Introducing a cost-effective MDR service

ThreatDetect™ from Redscan arms your business to respond swiftly and effectively to breaches without the need for large upfront investment.

Offering complete detection and response capabilities for an affordable subscription, this award-winning MDR service delivers enterprise-grade cyber security protection for a price that, in many instances, is less than hiring just one in-house security engineer.

“Understanding how hackers operate to better protect your business”
Why proactive security protection is a must

The proliferation of cloud services, Bring Your Own Device (BYOD) and remote working means that the latest threats now have an even wider surface to compromise your business. Against new attack vectors capable of bypassing traditional perimeter security, being able to detect and respond to malicious activity inside your network is vital.

Malware

Malware is malicious code designed to compromise your computer systems in order to access personal information. It is introduced through a wide range of sources, including bogus email attachments and downloads.

- Viruses
- Trojans
- Worms
- Ransomware
- Spyware
- Adware

Password Attacks

Brute force is a common technique used by cybercriminals to obtain access to user accounts. By using specialist software to enter thousands of common word and number combinations in sequence, hackers are able to crack weak password credentials in minutes.
Denial-of-Service Attacks

By flooding a network with high volumes of useless requests and data, DoS attacks overload vital services until they no long function. A distributed DoS attack is conducted by many, often thousands of, sources so if not detected early can be very difficult to stop.

Social Engineering

Posing as communications from trusted contacts or businesses, social engineering scams trick users into clicking infected links or divulging personal information such as passwords. Highly personalised spear phishing attacks are designed to target high privilege network users and can be highly damaging.

- Phishing
- Spear Phishing
- Vishing
- Physical attacks

Man-in-the-Middle

Impersonating endpoints in online information exchange enables criminals to intercept sensitive information such as bank account details. These difficult to detect attacks target key communication channels such as Wi-Fi, meaning rigorous monitoring is required.
Effective defence against attacks

Integrating leading security professionals, advanced network detection and endpoint technologies, and latest industry intelligence, ThreatDetect provides the complete capabilities your business needs to hunt for, detect and respond swiftly to threats before they become problematic.

Included as part of this affordable subscription service:

1. Leading security professionals
2. Advanced network detection and endpoint technologies
3. Latest industry intelligence
4. 24/7 event monitoring and investigation
5. Cyber incident investigation & response
6. In-depth security reporting and analysis
1. Full system deployment and management

ThreatDetect includes the latest detection, deception and incident response technologies, all fully installed, optimised and maintained.

- Offers SIEM, intrusion detection, behavioural monitoring, endpoint analytics, and more
- Extensive health monitoring of all included hardware and software
- Hassle-free updates, upgrades and backups to minimise business disruption

2. Event monitoring and investigation

Experienced cyber security experts undertake around-the-clock network and endpoint monitoring to provide early incident notification.

- Genuine threat alerting alleviates background noise and false positives
- Detailed security insight enhances understanding of threats
- Helpful remediation advice provides actionable intelligence and aids threat prioritisation

3. Cyber incident investigation & response

Qualified incident responders are on hand to minimise business disruption by ensuring a rapid response to threats and breaches.

- Detailed forensic investigations help to identify the source of attacks and any compromised assets
- Optional remote/and or onsite assistance, as required
- Clear advice about how to resolve immediate and long-term security risks

4. In-depth reporting and analysis

Custom security reporting provides the clear advice needed to enhance situational awareness and track service performance.

- Advanced security analytics provides key security and performance metrics
- Daily, weekly and monthly reports offer a clear picture of security health
- Regular service reviews help to ensure that business needs continue to be supported
Benefits of ThreatDetect

Quickly determine whether your business is under attack
With proactive threat hunting and investigation, significantly improve detection and response to reduce the dwell time of attacks and minimise disruption.

Treat security as an operating, rather than a capital, expense
By including everything needed to detect and respond to threats, a monthly ThreatDetect subscription removes the need to invest upfront in resources that can quickly become obsolete.

No need to recruit and train specialist staff
By supplying cyber security experts, ThreatDetect removes the need to recruit and train in-house personnel to perform essential yet time consuming tasks such as 24/7 event monitoring.

Receive actionable outputs
Leveraging the latest security technology and research, ThreatDetect supplies the actionable intelligence and noise-free incident notifications needed to respond swiftly and effectively to attacks.
Achieve superior threat awareness

Regardless of where your business’ IT infrastructure is located and how it’s architected, ThreatDetect provides far-reaching threat visibility.

From supplying and deploying the most suitable technology, through to ongoing system configuration and management, this flexible service ensures that your threat detection and response capabilities are always optimised.

Monitoring your on-premise and cloud-based infrastructure

ThreatDetect offers comprehensive monitoring of on-premise, cloud, virtual and hybrid environments. Supported platforms include:
The Redscan Cyber SOC

Redscan’s 24/7 Cyber Security Operations Centre is the heartbeat of our ThreatDetect MDR Service. Utilising cutting-edge technologies and intelligence, our dedicated team of security professionals work tirelessly to monitor clients’ networks and provide the remediation support necessary for rapid incident response.

**Experienced experts**
Our team of security analysts, engineers and researchers are trained to the highest professional standards to ensure that they can identify and are always ready to respond to known and unknown threat actors.

**Integrated intelligence**
Through the aggregation of internal cyber research from Redscan Labs and live threat intelligence from leading exchanges such as CiSP, we ensure our customers benefit from up-to-the-minute security information to help shape defensive actions and policies.

**Cutting-edge technology**
By investing in the latest detection and deception technology, we ensure businesses benefit from an advanced security analytics platform incorporating SIEM, Intrusion Detection, Behavioural Monitoring Asset Management, Endpoint Analytics and more.

**True threat visibility**
CyberOps, the real-time threat notification and analytics platform included as part of ThreatDetect, enables our CSOC personnel to provide swift incident notification and remediation guidance to organisations’ in-house IT and security teams.
Cyber incident response

Our experienced team of professionals are skilled at mitigating the damaging effects of cyber-attacks, investigating how they propagate and providing swift, clear remediation support.

Advanced analytics

By collecting, processing and correlating network event data, our advanced systems use a combination of behavioural analytics, proprietary algorithms and custom rule sets to generate security alarms, which are then analysed by our team of experts to separate genuine alarms from large volumes of false positives.

Tried and tested processes

Certified to ISO9001, ISO27001 and PCI DSS standards, Redscan follows proven best practice to ensure our service is secure, reliable and meet the needs of businesses across all industries.

Detailed reporting

By distilling complex threat intelligence into clear, actionable outputs our team ensures that all key personnel, from IT staff to board members, widely understand the latest security risks.
Latest detection technology

By including the latest security technology as part of an affordable subscription, ThreatDetect removes the need for up-front investment in expensive systems that can quickly become obsolete.

▶ ThreatDetect Network MDR

+ SIEM
This powerful technology collects, manages and correlates log information from a variety of sources in order to flag anomalous activity and generate alerts for investigation.

+ Intrusion Detection
Network (NIDS) and host-based intrusion detection (HIDS) systems identify unauthorised or anomalous behaviour.

+ Vulnerability Assessment
Automated network assessments identify and monitor insecure configurations as well as unpatched and unsupported software.

+ Asset Discovery
Identifies information about all IP-enabled devices on a network, including installed software and configuration details, enabling assets to be monitored and assessed.

+ Behavioural Monitoring
Network behaviour and full protocol analysis help to build a picture of regular system behaviour so that suspicious activity is easier to identify.

+ Honeypot Sensors
By emulating existing systems such as servers and switches, honeypot sensors act as traps to lure attackers and malware.

▶ ThreatDetect Endpoint EDR

+ Endpoint Analytics
Next generation AV technology monitors the security of your PCs and servers in order to enhance threat hunting and incident response.
In-depth threat investigation

With ThreatDetect, alleviate the resource pressures of in-house threat investigation by trusting your security needs to a team of dedicated CSOC analysts that are fully trained to perform the time-consuming and complex task of threat hunting, monitoring and investigation.

By understanding the way that attackers operate and fully utilising the latest security tools and intelligence, our professionals possess the skills needed to greatly enhance detection of known and unknown threats, remove large volumes of erroneous alerts and provide clear actionable guidance.

Some of the detailed analysis conducted by our CSOC experts:

- ✔ Researching vulnerabilities
- ✔ Reviewing packet data and logs
- ✔ Forensic analysis
- ✔ Creating new correlation rules and watchlists
- ✔ Isolating genuine alerts from false positives
- ✔ Identifying suspect IP addresses and URLs

“Defending your business through an 'offensive' approach to security”

Redscan’s approach to defence reflects the belief that the only way to successfully safeguard against the latest attacks to ruthlessly adopt the mindset and techniques of the adversary.

Redscan Labs is a specialist hub within our CSOC dedicated to in-house threat research and analysis. Our expert team of Labs researchers closely monitor the security landscape to understand the latest tools, tactics and procedures used by criminal attackers and apply this knowledge to ensure ThreatDetect delivers the greatest benefit possible.
Stay informed with CyberOps™

Included as part of ThreatDetect, the CyberOps platform combines the extensive insight of Redscan’s CSOC experts and threat information from the latest security technologies and intelligence feeds to provide:

**Noise-free alerts**
Receive genuine incident notifications, thoroughly triaged by our specialists to save your in-house team the time and effort of investigating scores of false alarms.

**Actionable outputs**
Obtain the detailed incident information and remediation guidance needed to respond swiftly to threats before they spread.

**Advanced security analytics**
Stay abreast of changes to your organisation’s cyber security with powerful data visualisations that help measure key performance metrics.
“Delivering the intelligence to respond to attacks via one customisable monitoring, incident alerting and analytics platform”

Features of this intuitive threat management platform

- **Technology agnostic**
  Benefit from one versatile platform capable of integrating with latest security technologies.

- **Customisable dashboards**
  Choose from a wide range of widgets to visualise crucial performance indicators.

- **Instant email notifications**
  Receive customisable security alerts fully compatible with IT management systems.

- **Highly efficient workflow**
  Manage incidents and requests through to resolution.

- **Full access controls**
  Manage users and teams plus view activity logs for auditing and compliance.

- **Regular stakeholder reporting**
  Download summary reports to enhance situational awareness.
Integrated incident response

Working as an extension of your in-house team, Redscan’s experienced security experts are always on-hand to ensure a rapid response to threats and breaches.

By keeping up-to-date with the latest attack vectors and conducting in-depth threat investigation and analysis, we help you to fully understand risks posed to your business. This includes the root cause and scope of intrusions, as well as the actions needed to achieve effective remediation.

Optional onsite assistance

Should your organisation ever need additional resources to aid its response to attacks, Redscan’s CREST-accredited cyber incident response team can provide, as an optional service, remote and/or onsite support as required.
Reasons to choose us

+ **An offensive approach to security**
  We understand the latest hacking techniques and apply this knowledge to improve the range of techniques we use to detect known and unknown threats.

+ **Focused on business needs**
  By fully understanding and evolving with business needs, we ensure that our service supports growing levels of cyber security maturity.

+ **Trusted experts**
  As one of the most qualified security teams around, we can be relied upon to provide the level of insight needed to achieve a swift and effective response to advanced attacks.

+ **Best-in-class tools and intelligence**
  By continually reviewing the latest security technology, we ensure that our service always utilises the most effective threat detection tools available today.

+ **Clear advice**
  Through the aggregation of the threat feeds and internal Redscan Labs research, we stay informed about the latest malicious actors and provide actionable, prioritised outputs.

+ **Highly affordable**
  For a cost-effective monthly subscription, we supply the expertise and resources needed to achieve comprehensive threat detection and incident response capabilities.
What our customers say

Redscan delivers managed detection and response to organisations across industries. Learn what some of our clients think about us:

**iCG**

“Our partnership with Redscan has been one of the most successful that we have ever undertaken. ICG recognises that it is significantly cheaper and more convenient to leverage Redscan’s subscription-based ThreatDetect service than try to build a similar facility in-house”

Lee Lambard, IT Director
Intermediate Capital Group PLC

**TT INTERNATIONAL**

“ThreatDetect is a cost effective service that gives us peace of mind that we are doing all we can to protect our clients, our business, our staff, our counterparties and other partners”

Ben Lloyd, Head of IT Infrastructure
TT International

**KING EDWARD VII’S HOSPITAL**

“Redscan staff are always on hand to provide swift, clear advice. They help us keep a constant eye on our network and respond quickly to incidents to ensure systems remain operational”

Richard Andrews, Head of IT
KEVII’s Hospital
“Possessing a deep understanding of offensive security, Redscan’s ThreatDetect security experts provide the insight needed to hunt for threats across your environment”
SAFEGUARD YOUR BUSINESS TODAY

Choose ThreatDetect for award-winning managed threat detection and response