Redsquid. Cyber/Kill

A MANAGED SECURITY SERVICE BUILT ON XDR, SIEM AND SOC

Redsquid Cyber/Kill.

The way we work has gone through a radical change over the past couple of years with an increase in home-working and businesses taking their data off-site. With this we are seeing a dramatic rise in the number of cyber-attacks, but more importantly in the number of successful compromises.

Redsquid Cyber/Kill is a Managed Endpoint Detection and Recovery solution (MDR) backed by a SOC team of 30+ security professionals. Redsquid Cyber/Kill monitors all activity on your systems 24/7 and isolates suspicious devices and user accounts. Any damage done by a threat can easily be rolled back to a previous system state.

The solutions organisations have in place to protect themselves are no longer providing the amount of protection they once did. Businesses are now at risk from threats that cause disruption, fines, and damage to their reputation. On average, a single cyber-attack can cost a small business more than £175,000.

What Is Included?

Technologies

- BitDefender Enterprise Antivirus
- XDR (Extended detection & response)
- ATS (advanced threat security)
- SIEM (Security Information & Event Management)
- Application White Listing
- Application Ring Fencing
- Elevated Rights Control
- AI (Artificial Intelligence)

Services

- SOC (Security Operations Centre)
- Security Assessments
- Vulnerability Scanning
- Security Roadmap
- Executive Risk Report
- Dark Web Monitoring
- End User Security Policies
- User Awareness Training
- Attack Simulations

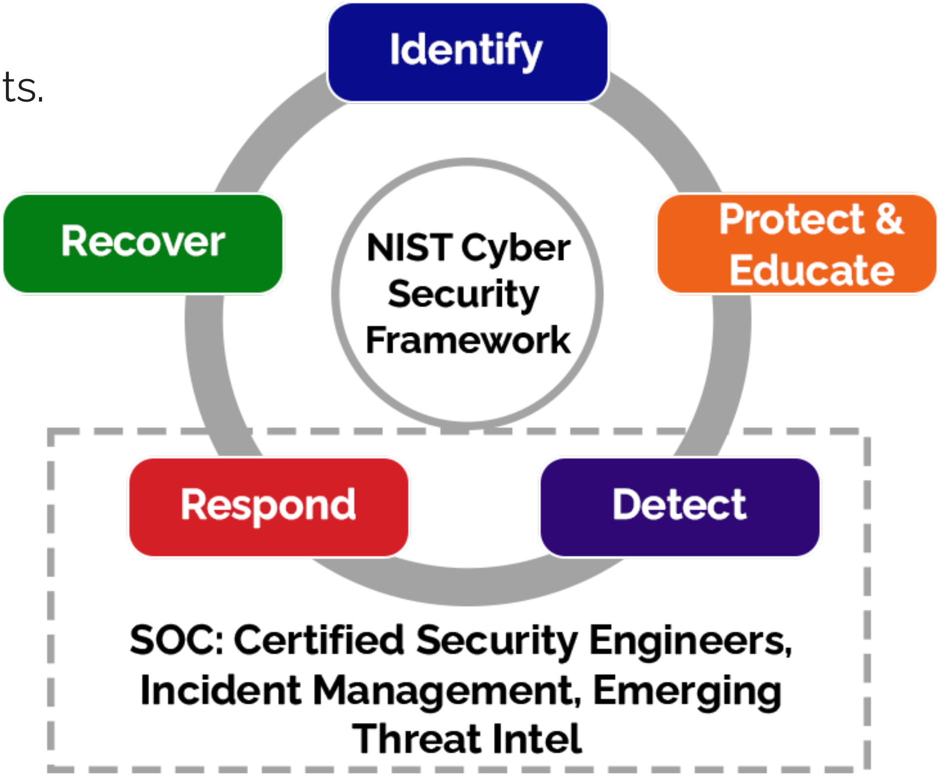
**Full glossary on page 15*

How Does It Work?

The core of Redsquid Cyber/Kill is the XDR and SIEM technology. XDR is built on BitDefenders number 1 rated enterprise antivirus solution. XDR is installed on all of your endpoints to provide real-time protection against incoming threats. At the same time data and log files from all of your endpoints and cloud solutions are collected and stored within our SIEM software.

These log files are analysed by our team of security specialists (SOC) to proactively look for and prevent threats. This human component of your security portfolio is now essential to properly protect your businesses.

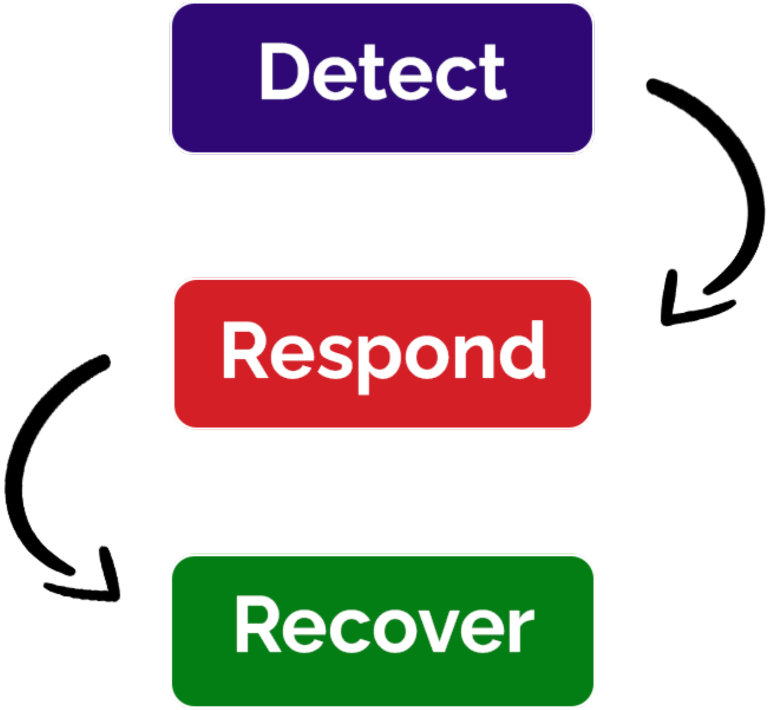
In addition to these technologies, our professional plan includes ThreatLocker. See XDR, SIEM and SOC as having an advanced alarm on your home. ThreatLocker is like sealing up all of the doors and windows. It blocks threats before they get anywhere near your system. We call this technology application whitelisting, application ring-fencing and elevated rights control.



SOC: Certified Security Engineers, Incident Management, Emerging Threat Intel

How Does It Work?

Technology combined with the human component is the best way to protect your systems. This is the reason we have decided to augment Redsquid Cyber/Kill with a set of services that truly enable you to protect your business from contemporary threats.

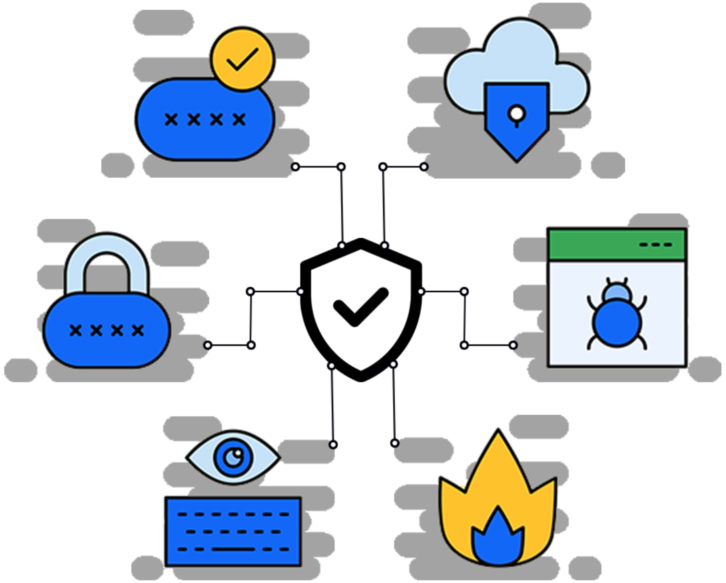


Alongside our SOC, our in-house team will manually review all elements of your IT estate **(security assessment and vulnerability scanning)** and make proactive recommendations to bolster your security **(security roadmap)**. This information can be presented to managers, directors and C-level employees **(executive risk report)** to give a clear insight into the strengths and weaknesses of your security portfolio.

When it comes to protecting your business, your team are your greatest strength, but can also be your biggest weakness. Educating your users is essential **(end-user awareness training)**. Bolstering their understanding with a clearly documented security policy **(end-user security policies)** ensures your whole team is playing its part to protect you and your business.

SOC & SIEM.

Our team of security specialists monitor your systems 24/7 to detect, respond and remediate critical cyber security incidents via all tools and methods available. The arsenal of the incident response team is constantly adapting to global threat patterns by developing new apps and integrations that blend machine and human learning & actions. The dual automated and manual approach provides a redundant layer of action to effectively detect, investigate, contain, report, and recover. We have partnered with RocketCyber for our SOC service. RocketCyber has a team of 30 highly trained security specialists dedicated to protecting your systems. These engineers have qualifications in all key areas - Bachelors in Cyber Security, Masters in Cyber Security, Certified Ethical Hacker (CEH) and Certified Information Systems Security Professional (CISSP)



We base our incident response model on the National Institute of Standards and Technology (NIST) Framework of Improving Critical Infrastructure Cyber security and the MITRE ATT&CK® Framework, among others. The frameworks enable organisations to apply the principles and best practices of risk management to improve the security and resilience of critical infrastructure. It provides organisation and structure to today's multiple approaches to cyber security by assembling standards, guidelines, and practices that are working effectively in the industry today. Our SOC keeps your security log files for twelve months using proprietary SIEM software.

SOC & SIEM.

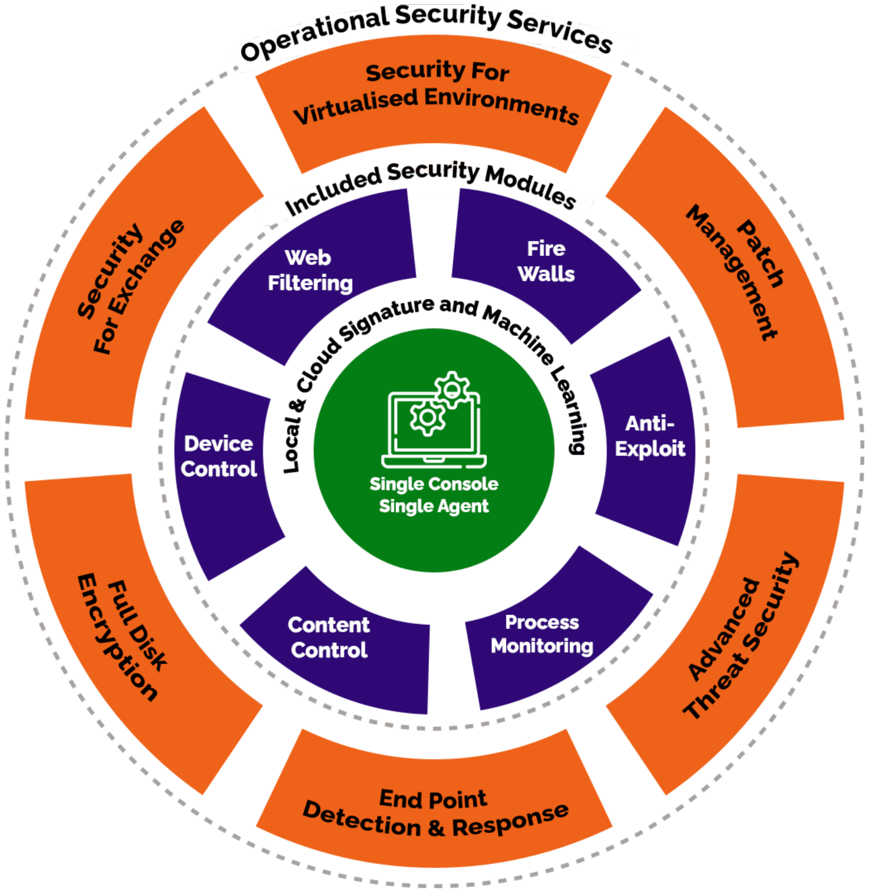
One of the approaches we follow is MITRE ATT&CK® Mapping to help us understand the adversary behavior as a first step in protecting networks and data. The MITRE ATT&CK® framework is based on real-world observations and provides details on 100+ threat actor groups, including the techniques and software they use. It helps identify defensive gaps, assess security tool capabilities, organise detections, hunt for threats or validate mitigation controls.

Should an attack be detected our SOC can isolate affected devices or user accounts to limit the spread of the breach. Detection typically happens in less than a minute and preventative measures are taken immediately. Some of the attack types our SOC will watch out for are:

- ✓ RDP hijacking
- ✓ Business Email Compromise
- ✓ Man-in-the-middle Attack
- ✓ Zero-day Exploits
- ✓ Denial of service
- ✓ Phishing
- ✓ Malware
- ✓ Ransomware
- ✓ Cryptojacking
- ✓ DNS Tunnelling
- ✓ Drive-by Attacks
- ✓ Eavesdropping Attack

BitDefender.

BitDefender provides advanced threat detection by using comprehensive search capabilities for specific indicators of compromise (IoCs), MITRE ATT&CK® techniques, and other artefacts to discover early-stage attacks, including fileless attacks, ransomware and other zero-day threats in real-time. BitDefenders' advanced risk analytics technology examines not only endpoints but also human behaviour, continuously analysing your organisational risk using hundreds of factors to identify, prioritise and provide guidance on mitigating user, network, and endpoint risks.



XDR provides innovative and easy-to-understand visualisations with rich context and threat intelligence that help IT staff understand attack paths and identify gaps in protection. These visualisations streamline the investigation and response, easing the burden on IT staff. The sandbox analyser enables staff to automatically execute suspicious payloads in a contained, virtual environment to isolate and neutralise suspicious files. BitDefender also includes web filtering to block malicious and inappropriate websites.

Security Assessment.

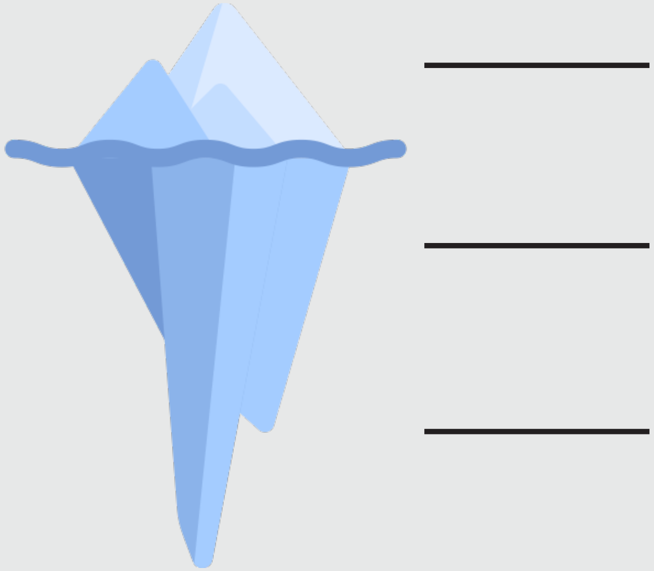
Security assessments give you a detailed insight into your current security posture and ensure you spend your security budget where it's most effective. Our comprehensive security review thoroughly checks your entire IT estate for misconfigurations, security flaws and best practices configurations. Once complete we produce a detailed report with high, medium and low priority recommendations in the form of a security roadmap. We will guide you through the process from start to finish and explain our findings in an easy-to-understand, non-technical manner. From here you can make an informed business decision on what items to prioritise and where to spend your security budget.

An executive security risk report is generated to give managers, directors and C-level employees a clear insight into the status of the organisation's security.

- ✓ M365 best practices and security configurations
- ✓ M365 Intune and Windows Defender configuration
- ✓ Email security
- ✓ Website security
- ✓ Administration and access configurations
- ✓ Vulnerability scan
- ✓ Network security
- ✓ Physical security
- ✓ Server best practices and security
- ✓ Authentication methods
- ✓ Backup and BCDR

Dark Web Monitoring.

The Dark Web is used by threat actors all over the world, to buy and sell information that can be used to attack your systems. Therefore a Dark Web Monitoring service is becoming an essential layer of security for organisations large and small. Our Dark Web scanning service uses a team of security experts, supported by AI to monitor and scan the dark web for information about your company's domain name, IP addresses and personal email addresses. When confidential or personal information about your company is found we will notify you and implement a solution to protect your business. We can also monitor personal email addresses, e.g. @hotmail.co.uk as some individuals within an organisation use their personal email for business purposes.



Surface - Everything that can be found with a search engine

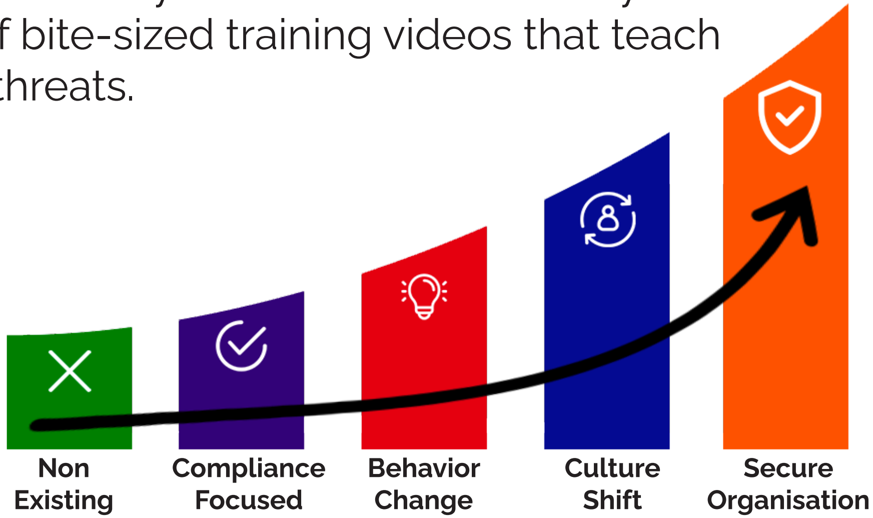
Deep Web - Everything that can not be found with a search engine

Dark Web - Hidden part of the Deep Web which can only be accesed by a special browser

Awareness Training.

End-user awareness training forms a key part of your cyber security defence. Each user at your organisation will be given access to a portal with a series of bite-sized training videos that teach them how to spot and defend themselves against current threats.

Users will then take a short test to assess their cyber security awareness. This training and testing can be taken as regularly as needed but it is recommended at user onboarding and every six months at a minimum. User progress can be centrally tracked by managers from the training portal.



Attack Simulations

To test your organisations cyber security readiness, attack simulations are conducted. These typically take form of a phishing test. An email is sent to the userbase to attempt to trick them into giving credentials or other sensitive information. User responses are tracked and this information can be used to provide extra training or security services where needed. Our XDR and SOC services can be tested at any time by running malicious activity on an isolated device. This is typically done by attempting to run malicious code.

ThreatLocker.

See XDR, SIEM and SOC as having an advanced alarm on your home. ThreatLocker is like sealing up all of the doors and windows. It blocks threats before they get anywhere near your system. Application whitelisting, also called allow listing puts you in control over what software, scripts, executables, and libraries can run on your endpoints and servers. Common apps are automatically updated so ThreatLocker won't interfere with your operations unnecessarily. If an app is blocked your user can easily request it be unblocked by clicking a link in the pop-up message, our team will be alerted and can resolve it for the user.

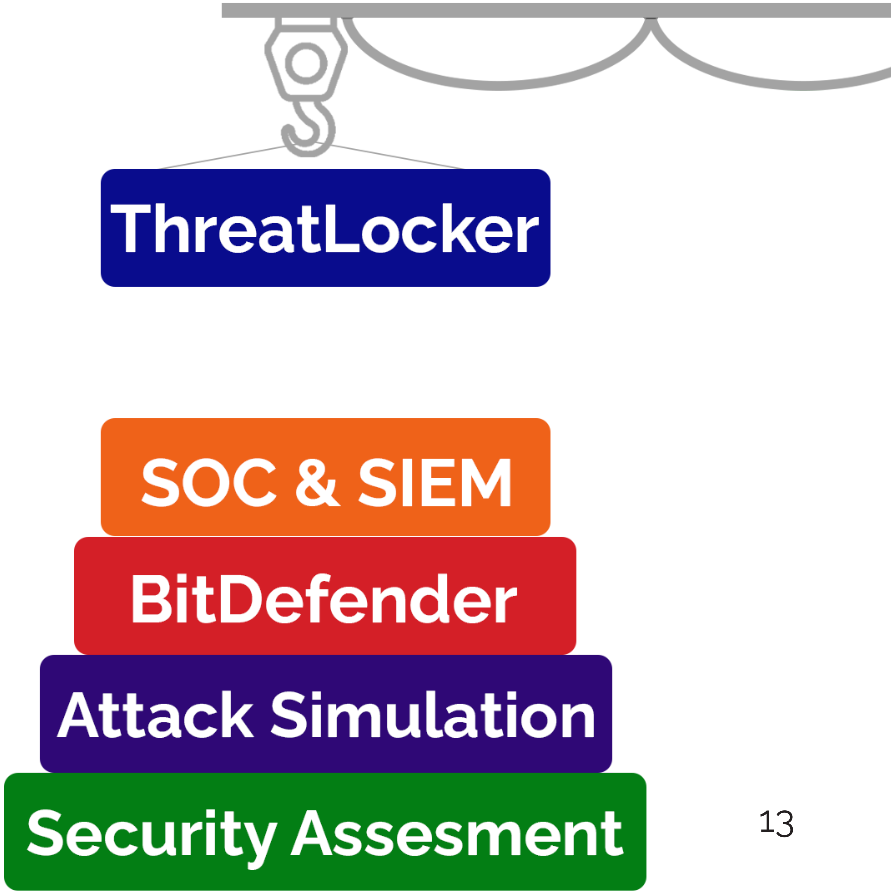
Controlling what software can run should be the first line of defence when it comes to better protecting yourself against malicious software. Ringfencing adds a second line of defense for applications that are permitted. First, by defining how applications can interact with each other, and secondly, by controlling what resources applications can access, such as networks, files, and registries. This makes ringfencing an invaluable tool in the fight against fileless malware and software exploits.

ThreatLocker.

When it comes to adding extra layers of security to your cyber security stack, it is important to always add a human layer. Users with admin access are often the weakest link across your network, so their movements must be monitored and tracked.

ThreatLockers Elevation Control provides an additional layer of security by giving IT administrators the power to remove local admin privileges from their users, whilst allowing them to run individual applications as an administrator.

- ✓ Gives you the ability to approve or deny an individual's administrator access to specific applications within an organisation even if the user is not a local administrator.
- ✓ Users can request permission to elevate applications and add notes to support their requests
- ✓ Enables you to set durations for how long users are allowed access to specific applications by granting either temporary or permanent access.



ThreatLocker

SOC & SIEM

BitDefender

Attack Simulation

Security Assesment

Our Plans.

Services	Plan 1	Plan 2	Plan 3
Antivirus	✓	✓	✓
XDR - Clients and Servers	✓	✓	✓
XDR - M365	✓	✓	✓
SOC	✓	✓	✓
Security Assessment and Vulnerability Scanning		Annual	Quarterly
Security Roadmap		Annual	Quarterly
Executive Risk Report		Annual	Quarterly
Dark Web Scan		Annual	Continuous
End User Security Policy		✓	✓
End User Security Training		✓	✓
Attack Simulations			Bi-Annually

**All plans can be augmented with ThreatLocker*

Glossary.

SOC – Security Operations Center

MDR - Managed Endpoint Detection and Recovery solution

EDR – Endpoint Detection and Response

XDR – Extended Detection and Response

SIEM – Security Information and Events Management

AI - Artificial Intelligence

CISSP - Certified Information Systems Security Professional

CEH - Certified Ethical Hacker

NIST - National Institute of Standards and Technology redsquid.

— MAKING A DIFFERENCE —

www.redsquid.co.uk
020 8166 4540
info@redsquid.co.uk