Moon AR

Dedicated defences that protect your biggest vulnerabilities

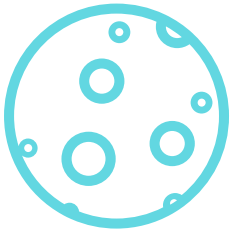
Technology advises, humans decide

Part of our Security Operations Centre (SOC) solutions, our specialist protections are a dedicated service that secures against specific risks to your business universe. Using a powerful combination of human and machine, our highly-skilled and experienced team harness information gathered by state-of-the-art tools, and enhance it with expert intelligence, analysis and action. This powerful blend enables us to deliver optimum results – identifying and solving security challenges with speed and efficiency.

With our Moon protections you can realise enterprise-grade defences that secure your business round the clock for a competitive price point that's a fraction of the cost of recruiting your own resource.

Moon AR

1 protection



Included in this SOC

- Anti-ransomware (AR)
- Threat Intelligence (GTIN)
- I3 – Incident Management Portal

Experts on watch

Our managed services provide peace of mind, with a dedicated SOC team on watch 24 hours a day, 365 days a year. A handpicked selection of security analysts, threat intelligence specialists and cyber security engineers combine their expertise to interpret technology insights and action defensive measures on your behalf.

Is Moon AR the right SOC for me?

Tailored to your specific needs, our Moon Anti-ransomware service reinforces your existing estate and extends the value of your security investments to deliver robust protection. Our leading defensive SOC service is configured to strengthen your defences in three important ways:

- **Proactive defence** – Prevention is better than cure. Our cyber threat intelligence system provides advanced warning of cyber threats targeting your organisation or sector. Coupled with vulnerability management, we stay one step ahead of attacks by hardening your organisational defences.
- **Reactive defence: automated** – The first wall of defence. Industry-leading security tools protect your users and systems in real-time by automatically blocking network and malware threats, and preventing data theft and exfiltration attempts.
- **Reactive defence: incident response playbooks** – Enhanced threat response. Going one step further than automated tools alone, our analysts interpret insight from threat hunting technology to seek out indicators of compromise in your networks and trigger best-practice incident response processes.

In depth: Moon AR benefits

- Rapid remote deployment of monitoring and protection software through cloud management.
- Key Risk Indicator and security maturity improvements delivered within 1 week of SOC deployment.
- Protect key data, intellectual property and client data from theft and accidental leakage.
- Detect targeted and sophisticated network attacks.
- Help protect against zero-day malware.
- Reduce employee overhead and improve speed of response through automated defence and remediation.
- Protect data stores and keep business operations moving with real-time anti-ransomware detection and prevention.
- Flexibility to evolve your service using our 'Roll Out Roll In' SOC protections.

In depth: Moon AR protections

Technology

Technology plays a vital role in protecting your IT. Your Moon protection is underpinned by state-of-the-art security tools:

- **AR virtual appliance**
  - Looks for encryption attacks, protecting your network and cloud file shares in real-time.
- **I3 Security Incident Management Portal**
  - Tracks security alerts and incidents through a centralised portal.
  - Contains security run books tailored to your needs.
  - Shows you the 'metrics that matter' through live security posture and risk indicator dashboards.
- **Global Threat Intelligence Network (GTIN)**
  - Uses a database of current threats, campaigns, botnets and malicious websites to seek out indicators of compromise.

People

Humans are critical to interpreting and acting on technology's advice, which is why they're a huge part of what we do for you. Your Moon SOC team includes:

- **Security Analyst:** Your eyes and ears. Monitors, analyses and investigates your IT estate 24x7.
- **Security Engineer:** Ensures your systems seamlessly integrate with ours so everything works as it should.
- **Security Assurance Consultant:** Answers the difficult questions and provides valuable guidance that supports your decisions.
- **Service Delivery Manager:** Oversees every element of your service from internal response process to coordination of different teams.
- **Threat Intelligence Specialist:** Looks beyond your perimeter to seek and stop cyber threats before they cause harm.

Process

We dot the I's and cross the T's by ensuring best-practice processes are meticulously followed during the deployment of our managed security services:

- **On-going tuning of alert and defensive rule sets:**
  Ensures your security stays matched to your organisation as it evolves.
- **Early warning threat intelligence:**
  Shows you how to best-protect your business before an attack strikes.
- **Active threat hunting:**
  Detects sophisticated attackers and advanced persistent threats.
- **Monthly Key Risk Indicator reporting:**
  Summarises the risks we've uncovered and prevented, benchmarked against key performance indicators.
- **Incident orchestration:**
  Resolves and remediates incidents through collaboration with your in-house teams.

Protection overview: Anti-ransomware

What is it?

Our Anti-ransomware virtual appliance monitors and protects your networks, file servers and cloud file shares against ransomware attacks.

Why do I need it?

Ransomware is on the rise – it is easier and quicker for hackers to deploy than ever before. All sectors have become targets, from charities and government bodies to financial institutions. In fact, our customers rate ransomware within their top 5 biggest security concerns.

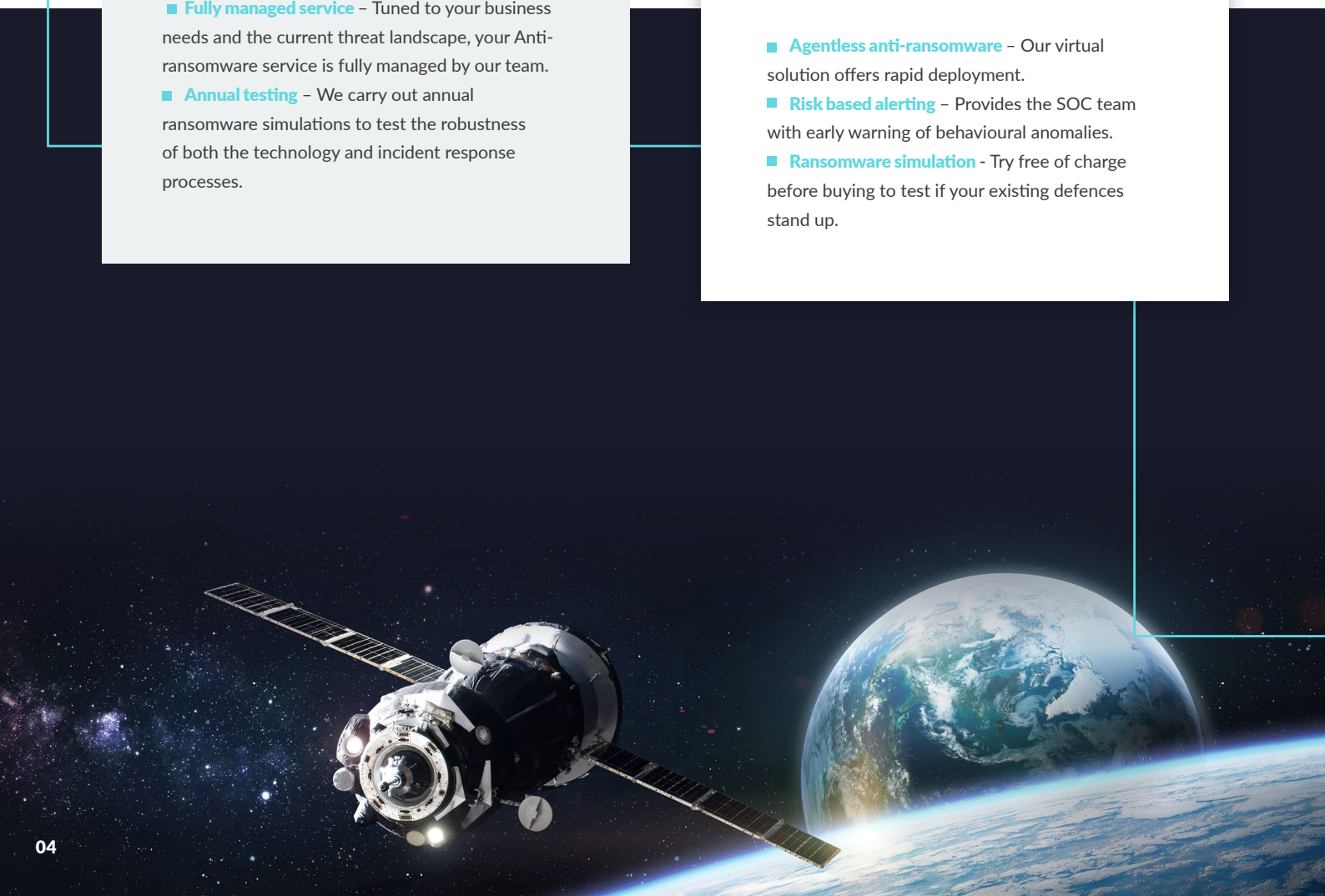
Our Anti-ransomware service detects and blocks file encryption in real-time, quarantining any compromised hosts which have become infected with ransomware. The system notifies the SOC team who immediately trigger a pre-defined incident response process. At the same time, our experts carry out root-cause analysis to identify patient zero and the entry method for the ransomware – preventing repeat attacks.

AR management

- **Fully managed service** – Tuned to your business needs and the current threat landscape, your Anti-ransomware service is fully managed by our team.
- **Annual testing** – We carry out annual ransomware simulations to test the robustness of both the technology and incident response processes.

Additional Anti-ransomware service features

- **Agentless anti-ransomware** – Our virtual solution offers rapid deployment.
- **Risk based alerting** – Provides the SOC team with early warning of behavioural anomalies.
- **Ransomware simulation** - Try free of charge before buying to test if your existing defences stand up.



SOC management

- **Alert use-cases** – Starting with a baseline security alerting ruleset, we evolve this over time to implement new alerts as required.
- **Fully managed service** – Our SOC analysts monitor your security alerts 24/7 and can supply ad-hoc reporting upon request.
- **Evolving service** – We continually adapt our monitoring and alerting methods to match the ever-changing threat landscape. Our SOC team are up-to-date with the latest threat trends and keep watch for new techniques, tactics and procedures being deployed by cyber attackers.
- **Scalable Capacity** – We can flex your SOC service capacity to match your security needs.

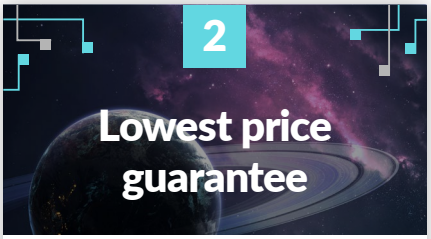
Reporting

- **Key Risk Indicator reports (KRI)** – Weekly or monthly KRI reports provide a full picture of your security monitoring service. These highlight the most important risks, whilst providing insight into recent threats and the steps taken to defend against them.
- **Key Performance Indicators (KPI)** – We benchmark our performance by tracking incident response and resolution times.
- **I3 access** – All customers have access to our I3 incident management portal, granting real-time visibility into how our analysts are investigating and responding to security incidents.
- **Flexible alert notifications** – When our analysts identify a threat, they'll notify you via your chosen method – through email, in the I3 portal, by telephone or through integrations with other incident management platforms.

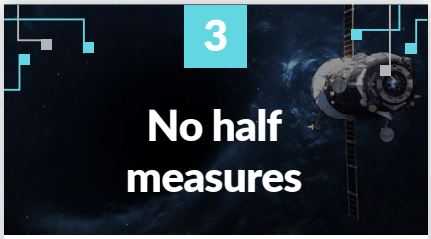
Our customer pledge

We want you to be completely satisfied with your SOC service – our promise to you:

Put us to the test and let us run your 24x7 Security Operations for free for the first month. You can benchmark our performance against pre-agreed success criteria – and if you're not convinced after the pilot, it won't cost you a penny.



Our mission is to make high-quality, tailored managed security services affordable to the mid-market – and we stand by our word. If you find another provider who can offer a like-for-like SOC service for lower cost, we will refund the difference.



When you take part in our pilot you can expect the full Zepko service, not a trimmed down version. We'll run a full 24x7 SOC operation, providing access to our specialist SOC team, process models and procedures, at the same level as our existing customers.

Take the next step

Found the right protection for you? Get in touch with us to start your 1-month pilot or for more information about our services.

+44 (0) 845 074 0790 | **info@zepko.com**

Get in touch

zepko