ramsac
the secure choice

secure+

from ramsac

Protecting your organisation from cybercrime

Introducing secure+

Cyber breaches are the most significant threat facing organisations today. During our 30 years of providing IT support and services to our clients, we have seen this threat develop and grow. To address this we have created secure+.

secure+ your peace of mind from cyber-attacks.

secure+ is a proactive cybersecurity monitoring service designed to hunt for signs of malicious activity or potential cyberbreach. We then act upon these threats and take the necessary actions to safeguard your systems and data.

ramsac
the secure choice

secure+
from ramsac

Proactively identifying potential breaches

In our experience, the most common breaches our clients see are through compromised accounts as a result of successful phishing or social engineering attempts.

Often for our clients, the first indication of a cyberbreach is when it's already too late; a customer might complain about phishing emails being sent from a compromised employee's mailbox, or a supplier complains that an invoice your finance team thought they had paid to the right account has never been received.

secure+ is a ramsac managed service, run by our dedicated Security Operations Centre (SOC) utilising industry-leading technology that allows us to detect a breach the moment it happens and take action to minimize damage to your organisation and your customers.

What is secure+

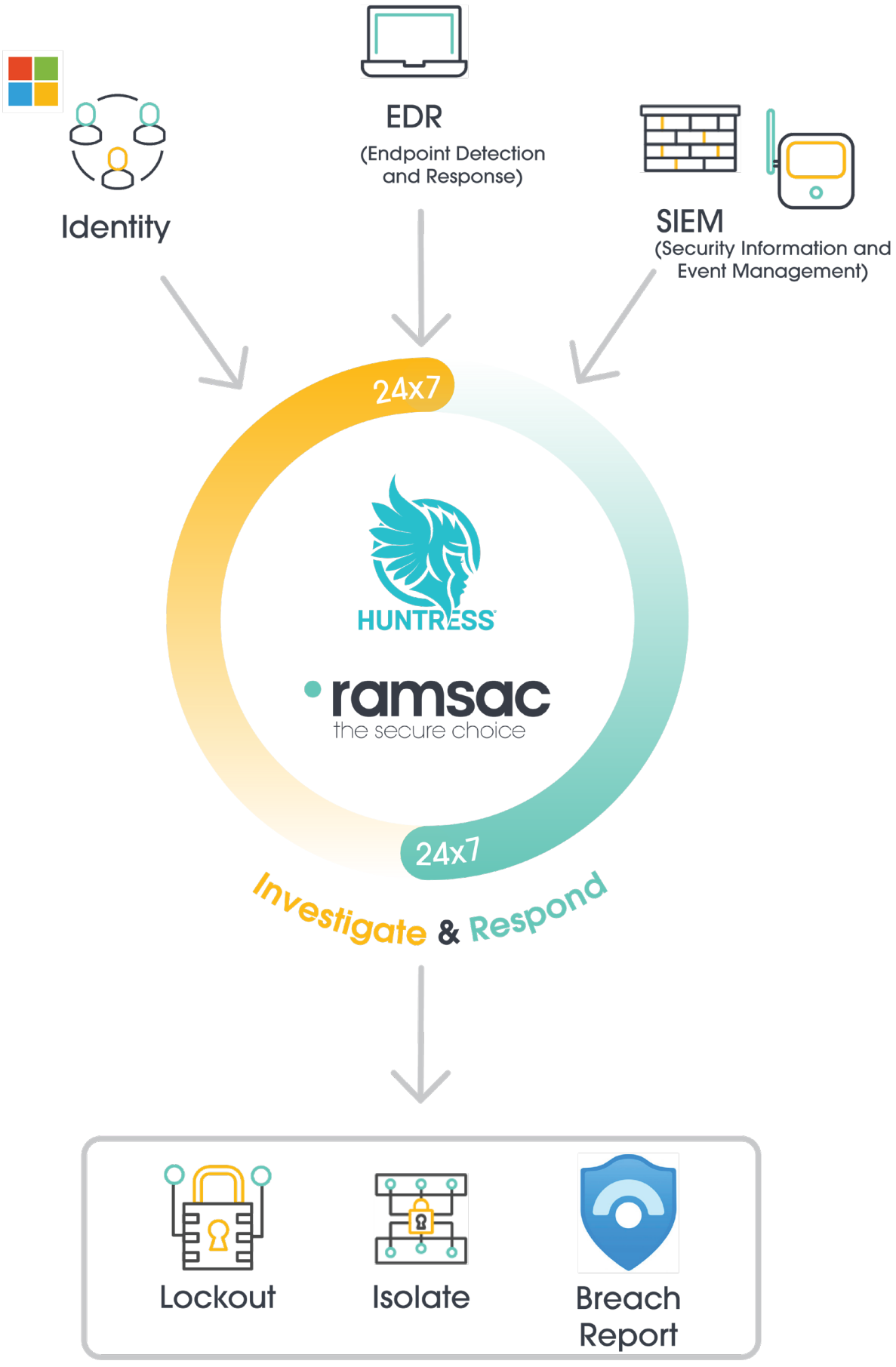
secure+ is the 24/7 watchful eye over your IT estate, helping you to protect your data and minimise the impact of cyber breaches. secure+ is delivered by our in-house Cybersecurity team of experts working in partnership with Huntress, a world-renowned cybersecurity technology provider.

We can detect potential breaches or security issues across your organisation's IT estate the moment they occur and then investigate and respond to these 24/7 within minutes, potentially initiating an account lockout or device isolation to stop an attack in its tracks!

We utilise a number of tools to help safeguard your environment, including Identity Threat Detection & Response (ITDR) looking at your Microsoft 365 environment, Endpoint Detection & Response (EDR) tools monitoring your workstations and servers, and a Security Information and Event Management (SIEM) system ingesting logs from your network devices such as your office Firewall.

How does secure+ work?

secure+
from ramsac



Security log retention = 1 year

How does secure+ work?

secure+ from ramsac

We ingest logs from all across your IT estate using our comprehensive set of tools, including:

- Microsoft 365 activity, for example sign-ins, mailbox rule creation and delegation, and file access.
- Telemetry from endpoints, such as potentially malicious processes running or ransomware being deployed.
- Security logs from servers and network devices such as Firewalls.

These logs are ingested into the Huntress platform which looks for indicators of a potential cyber breach across your organisation. If suspicious or risky behaviour is detected, we investigate immediately and take swift action to stop the breach in its tracks and safeguard your systems and data.

Once we have secured the threat, we do all of the necessary account clean up and provide you with a comprehensive breach report that explains what may have been accessed or changed during any attack.

We retain security logs from your systems for 1 year which is far greater than the standard 30 days for most organisations. This provides us with additional data for breach investigations and helps us build up a more accurate picture of what normal behaviour looks like across your organisation.

Each month we will provide you with a summary of your secure+ service which provides an overview of how many events and signals have been investigated and what incidents we have responded to. We'll also provide you with updates on emerging threats and things to be looking out for!

24/7 cybersecurity response

Cyber criminals don't work 9-5, so neither should your cybersecurity monitoring! Our SOC monitors your IT estate all day every day and will generate an alert for investigation whenever suspicious activity is detected.

Our response to this activity, including account lockouts and device isolation, is true 24/7, meaning that even over bank holidays and weekends (when cybercriminals love to strike!), your systems and data are being protected.

Often we can detect, investigate and stop a cyber breach within a few minutes, minimising the damage a cyber criminal can do to your organisation or data.

Following proactive action being taken at any time of day or night, we'll perform account clean up and investigation during business hours (8am – 5pm). But if you utilise our 24/7 Support contracts, your employees will be able to contact us at any time to get back into their accounts so they can keep working.

secure+ in action

An example of secure+ in action is the detection of a malicious login to an account through token theft via a phishing attack. Phishing attacks are very successful, being the number one vector of attack used by cyber criminals across the globe. The emergence of "Phishing as a Service" whereby common criminals can easily initiate their own phishing campaigns through a subscription on the dark web has made these even more prevalent.

Alex's account is compromised

Our security monitoring detects a successful login to Alex's account from a location in Europe, despite him already being signed in from the UK.

Immediate investigation

A signal is generated in our platforms and immediately investigated to determine whether this is malicious activity or not.

Alex's account is locked

There is a high chance this is a cyber breach, so we take action in minutes to lockout Alex's account and clear sessions, stopping the breach in its tracks.

Remedial action taken

We reset Alex's passwords, ensure MFA is enabled, and then get Alex back into his account. We also provide a comprehensive breach report to assess if any data was accessed by the cyber criminal.

Preventing reoccurrence

Our SOC investigate the breach to identify how it happened and what protections should be in place to prevent reoccurrence

About ramsac

ramsac has a clear mission
- to be the secure choice

ramsac provide so much more than just IT support. We help our clients to get the best out of technology – implementing, managing and supporting secure, resilient, flexible IT solutions. We work with small and mid-sized organisations, providing them with strategic IT input, proactive management, jargon-free IT support and solutions that help them to grow their own organisations efficiently and securely. Our exclusive Cyber Resilience Certification programme helps organisation achieve the highest level of cybersecurity protection and allows them to demonstrate their commitment to their own stakeholders via our Gold certification standard.

Whether it's designing a new infrastructure, migrating services to the cloud, implementing enhanced security practices or providing end users with really efficient and friendly 24 hour IT support, ramsac manages IT on your behalf, so that you can focus on achieving your organisation's goals, safe in the knowledge that IT is secure, staff are working efficiently, and the IT investment is delivering tangible benefits to the business.

More information

For more information on **secure+** please contact ramsac on **01483 412040**, **email info@ramsac.com** or visit **ramsac.com**

ramsac
the secure choice

ramsac Limited

www.ramsac.com
01483 412 040

ramsac
the secure choice