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+ is the watchful eye over your IT estate.

secure+ is a proactive cybersecurity monitoring service designed to hunt for signs of malicious activity or potential cyberbreach. ramsac 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 as a result of human error and compromised accounts.

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 client address, or a supplier complains that a payment has never been received, but on investigating further they discover the bank details were changed and the payment was sent to a fraudulent account.

secure+ is a ramsac managed service, run by our dedicated in-house Cybersecurity team that allows us to detect a breach the moment it happens and to take action to prevent damage from being done.

What is secure+

secure+ is a 24/7 eye on your IT security, helping you to protect your data and prevent cyber breaches. secure+ uses Microsoft Sentinel, which is a security monitoring and management tool created by Microsoft specifically for the analysis and investigation of security events. Sentinel ingests millions of events a day across an organisation's IT estate, and using artificial intelligence looks for signs and behaviours that seem unusual, risky or potentially malicious.

Microsoft Sentinel

Sentinel then highlights these to the ramsac Cybersecurity team, who manually investigate them and determine what action may be required to safeguard your organisation. Sentinel can also ingest event data from other systems, such as Anti-Virus, firewall, and physical, virtual, or cloud servers. We continuously review and tweak the monitors we use in Sentinel to improve our effectiveness at detecting suspicious events.

What does secure+ comprise of

secure+
from ramsac

Ongoing threat intelligence

We continuously review current threat and vulnerability trends, updating processes and procedures to incorporate them.

Ingest

Event data is gathered from a variety of sources.

Detect

Our tools look for suspicious or potentially malicious behaviour.

Assess

Our Cybersecurity team assess any perceived threats.

Respond

Action is taken to stop the threat & prevent further impact.

Resolve

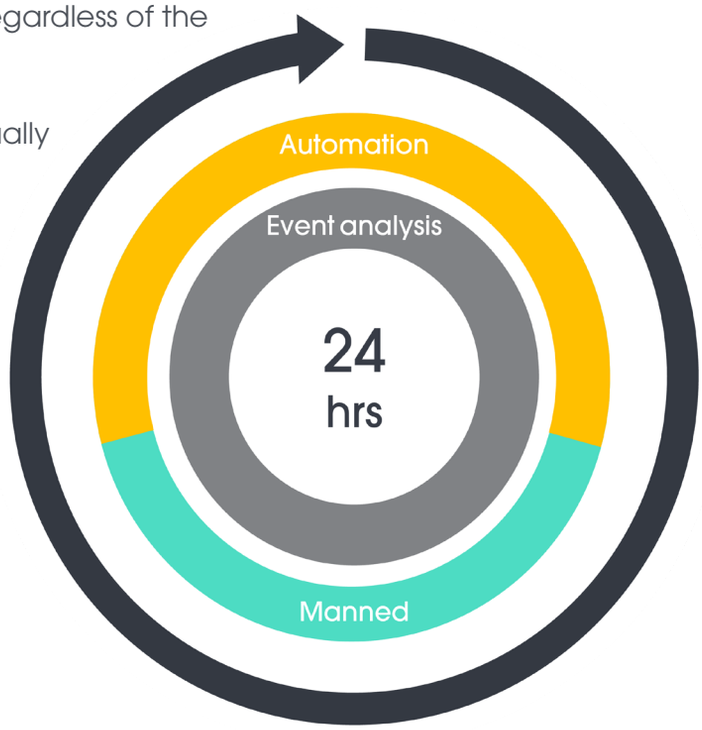
We clear up the impact of the breach and mitigate future occurrences.

24/7 cybersecurity response

secure+ from ramsac

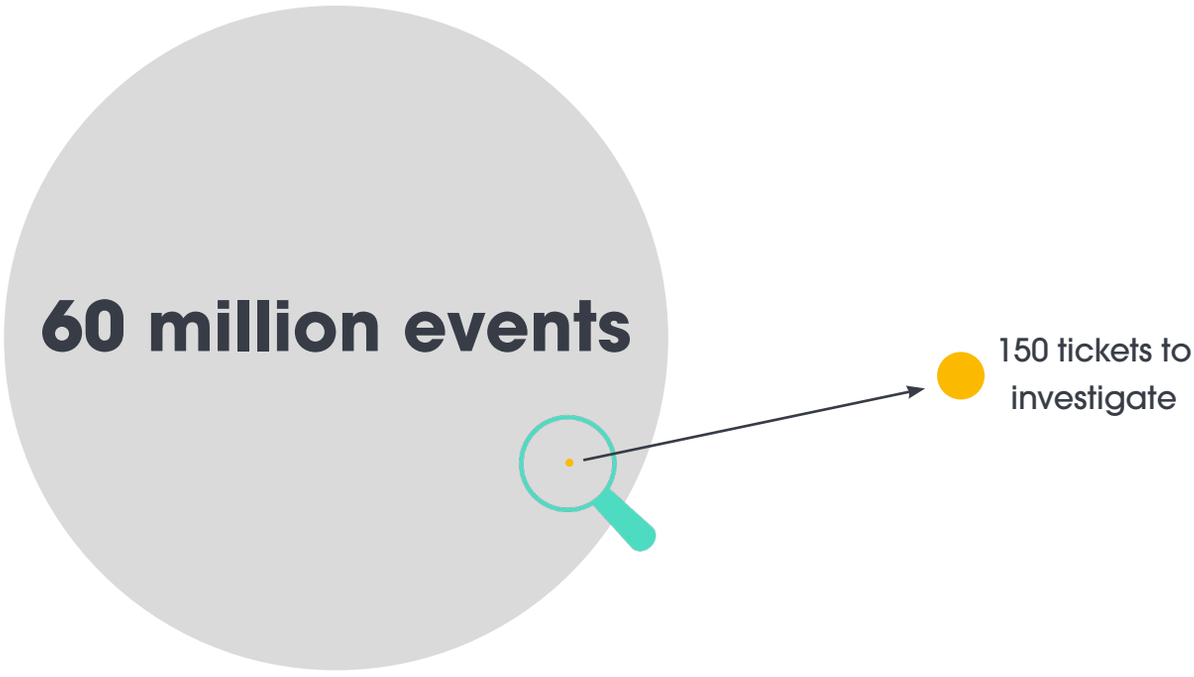
secure+ monitoring runs 24/7, ingesting event data, analysing and hunting for potential threats and generating alerts as required, If it detects something that could be malicious, it will log an alert for investigation, regardless of the time of day.

Alerts triggered during business hours will be manually investigated by our Cybersecurity team. During non-working hours and at weekends, critical alerts can be responded to using intelligent automation. For example, for alerts where there is a high probability that an event is malicious, we can automatically lockout an end user's account to prevent an account compromise. This would then be investigated and remediated during business hours. Clients of our 24-hour support service can also call to speak to a consultant day or night.



Detecting what matters

Our monitoring software will receive millions of pieces of data from your network every month. We used advanced AI to work out what's just noise and what alerts require investigation. A typical SME can generate around 60 million pieces of data, which might result in 150 tickets. We assign each of these tickets a severity level and our cyber analysts will investigate, closing down anything which can be ruled out. and taking urgent action against any ticket that indicates a threat.



secure+ in action

An example of secure+ in action would be the detection of a malicious login to an account through credential theft. Phishing attacks result in tens of thousands of account credentials being stolen every day, which are then sold on the dark web for use by threat actors to gain illegitimate access to organisations, to attempt to steal their data and hold them to ransom.

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 Severity 1 alert is generated for our Cybersecurity team who immediately investigate the incident.

Alex's account is locked

Through interaction with Alex and our primary contact, we quickly establish that this is an illegitimate login and lock out Alex's account and 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.

Preventing reoccurrence

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

Additional benefits of secure+

secure+
from ramsac

Monthly report

Each month you will get a comprehensive report of your secure+ service, where we call out significant events and recommendations to improve your security.

Vulnerability scanning

We periodically run scans against your external facing infrastructure to look for vulnerabilities or gaps in your security.

Priority patching

As a secure+ customer, you will get priority status for emergency or critical patches that get announced.

Quarterly audits

Every quarter we will run an audit of critical accounts, mailboxes and other services to check that privileges are as expected across your estate.

secure+ from ramsac

Security events secure+ will detect

Secure+ runs 24/7 looking for potential signs of malicious activity or cyber breach. Secure+ runs several hundred monitors every day looking for these suspicious events, but some of the key ones include:

Login activity

- Login or attempted login from an unexpected location
- Unfamiliar sign-ins or atypical travel, for example logging in from the UK and then Spain in a 10-minute period.
- Multiple failed login attempts followed by successful login.
- A brute force login attempt to a user account (trying multiple passwords).
- An attempt to login to a previously disabled user account
- A login to a rarely used Remote Desktop Connection

Changes to user accounts or permissions

- New user added to a SharePoint group or folder that you've told us is sensitive (such as HR or Finance)
- New user added to privileged access group (such as Directors or Finance Users)
- New accounts created with elevated or administrator permissions
- New delegation or access permissions being applied to a users email account or OneDrive

Multi-Factor authentication

- A change being made to your MFA policies
- MFA being disabled for a user account
- An MFA request being denied by an end user, suggesting it was unexpected

Data management

- Creation of a new rule to forward a users email to another account
- A download of a large amount of information to a USB device
- A bulk download of SharePoint data to a secondary location

Passwords

- A change to a password policy, such as changing settings to use non expiring passwords
- Multiple password resets in a short space of time

Integration with other systems

- Alerts generated by your enterprise Anti-Virus solution, such as failed attempts to remove or quarantine malware.
- Firewall alerts such as configuration or rule changes, and intrusion attempts.

secure+
from ramsac

Tailorable to your organisation

A key feature of **secure+** is that it's completely tailorable to your organisation, based on your priorities and sensitivities. During set up, we will discuss with you what is particularly important for your organisation and advise how we can better monitor for threats against these priorities.

As a **secure+** client, you will receive priority deployments of patches or fixes issued in light of critical service vulnerabilities, ensuring that your organisation is protected before threat actors can exploit them.

Pre-requisites for secure+

- Licenses – your core users will need one of the following Microsoft licenses or combination of licenses in order for us to be able to run secure+ for your organisation:
    - Microsoft Business premium or
    - Microsoft 365 E3 or
    - Office 365 E3 and EM+S E3.
- Environment – secure+ is based on the Microsoft Sentinel product, as such your primary office suite should be Microsoft/Windows based.

secure+
from ramsac

EDR, MDR, XDR, SIEM, SOC

Understanding the jargon in cybersecurity monitoring

The cybersecurity product market is full of acronyms which can make it hard to determine what security monitoring services you need, and what benefits you get from them. Here we explain the meaning behind these acronyms and what you need for your organisation's safety.

What is SIEM?

At the core of **secure+** is the powerful Microsoft Sentinel platform, which is an internationally recognised "Security Information & Event management" (SIEM) system. Sentinel ingests user activity and event data from a raft of different sources, applying Machine Learning and Artificial Intelligence on these events to determine if they are suspicious or unusual, passing them to our Cybersecurity Analysts for further investigation.

What is a SOC?

A "Security Operations Centre" (SOC) is a team of qualified people who are responsible for managing all security aspects for your organisation, including preparation & prevention, monitoring & response, incident recovery, and compliance management. Full SOC services are aimed at large enterprises with complex networks where there is a need to be performing real-time detailed analysis of every packet of information crossing their network, looking for obscure new threats, which obviously is extremely expensive. Our **secure+** service is far more cost effective than a traditional SOC as it has been developed to identify and act upon the real-world threats that we see day-in-day-out. We also continuously review emerging threats to ensure our services keep up to date with current security trends.

What is EDR, XDR and MDR?

"Endpoint Detection & Response" (EDR) is commonly performed by most modern enterprise-grade Anti-Virus solutions, such as Sophos Intercept X and Microsoft Defender for Endpoint. Your anti-virus will automatically respond to certain key events, such as quarantining suspected malware. Some AV services now offer what is called "Extended Detection & Response" (XDR) which detects events across more than just endpoints. secure+ integrates your Anti-Virus solution into our cybersecurity monitoring services, meaning that ramsac can provide a complete "Managed Detection & Response" (MDR) service for your organisation.

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