Cloud Security+ from the Cyber Security Expert

From theft and data loss to untold reputational damage - the costs of cyber-attack are escalating

If your business is one of the 68%[1] that now store commercially confidential or personal data in the cloud, then you cannot afford not to protect it, and technology alone cannot make it secure.

The PLUS in Cloud Security+ from The Cyber Security Expert is the virtual addition of world-class cyber security consultants to your existing IT team. Armed with the knowledge of the latest threats and trends, our experts will be “eyes on” to keep your data secure.

Cloud Security+ is designed to arm start-ups, scale-ups and SMEs with cost-effective cyber security for their cloud data.

WHY CHOOSE THE CYBER SECURITY EXPERT

Our priority is to arm start-ups, scale-ups and SMEs with cost-effective, proportionate and flexible systems to keep them cyber safe. We’ve deployed our extensive knowledge to create a best of both worlds solution in Cloud Security+: monitoring and security technology watched by our world class cyber security experts. We have up to the minute understanding of the latest threats and deliver clear, concise and practical advice to help you combat them.

Cloud Security+ HUMAN ERROR, THREATS AND MITIGATION

The continued escalation phishing and social engineering attacks underpins the fact that humans are still the weakest link in cyber security protection. Two in five[2] businesses reported security breaches, identifying 75%[3] of those as a result of fraudulent email sent to staff.

The primary protection for your data is the credentials used to access it. Usually a username and password, it is those credentials that hackers target. If staff respond to fraudulent emails and reveal passwords, financial data or open dangerous attachments, then your business is vulnerable to cyber criminals impersonating your business online.

The advantage of cloud services is that they offer robust security - the companies that provide them have large teams dedicated to protecting your data and making it available as you need it.

Cloud service providers cannot legislate for human error however and ultimately ensuring that only authorised staff have access to cloud data storage depends on your business and its staff.

Determined hackers can still find a way!

[1/2/3]Cyber Security Breaches Survey 2018 from Department of Media Culture & Sport

Cloud Security+ delivers visibility on who is accessing your data, from where, when, on what devices and what they are doing.

We help protect confidential business and personal data by monitoring the data we receive and issuing Cloud Security+ Alerts as needed for:

- Access from known bad locations
- Suspicious patterns of use (e.g. impossible travel)
- Access from unusual or potentially malicious IP addresses
- Evidence of unauthorised access attempts
- Unusual password change activity
- Potentially insecure, or unauthorised, behaviour by staff (e.g. automated email forwarding to third parties)

Monitoring coupled with our expert knowledge and pattern visualisations, enhance those results enabling us to spot other potentially malicious activity.

You can take steps today to start securing the data you store in the cloud by:

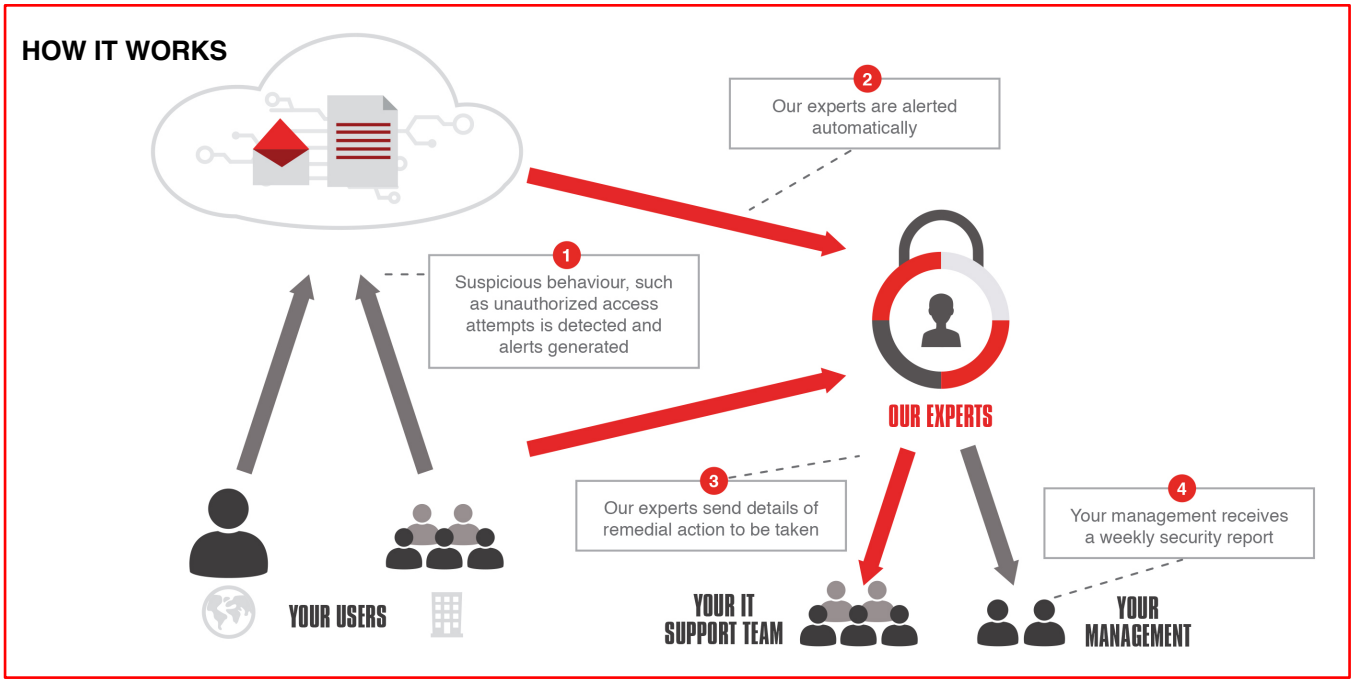
- Putting in place the security tools available directly from your cloud service providers, such as two factor authentication, (which requires you to enter a number in addition to a password).
- Training your staff on how to spot, and avoid being taken in by, phishing emails.

Cloud Security+ THE BENEFITS

There is no replacement for having expert cyber security specialist monitor and analyse security data. Cloud Security+ promises:

- The addition of world-class cyber security experts to your IT team without the need to add to headcount
- Rapid detection of potential data breaches enabling swift mitigation of impact, legally, reputationally and financially
- Confidence that your business can demonstrate GDPR compliant policies and procedures
- A cost-effective service achieved by monitoring for suspicious activity using the built-in functions of the cloud services you use, including Google, Microsoft Office 365, Dropbox
- Reassurance for your customers that their data and your services are cyber-safe
- Cloud Security+ Alerts delivered directly to your inbox when threats are detected together with impact assessments and remediation advice from our experts

HOW IT WORKS



Preparation
There is nothing to install - the precise steps will depend on the service provider(s) you are using. We will work with you to take the steps necessary to give us access to the data we need.

Operation
We require the contact details of the individuals or groups that should receive our Cloud Security+ Alerts. It is important that any changes to these details are notified immediately as incorrect, or out of date contact details will undermine our ability to delivery timely alerts.

During the initial period of service delivery, we will need to work closely with you to understand how your staff legitimately access and use your cloud services. You can provide some of this information by answering the questions we provide. To ensure we are properly attuned to the patterns of your business, and don't miss something we should alert on, we will be in touch more frequently in the early stages. For example, if you have a very mobile workforce (e.g. do you have staff in China this week?), then we will need your assistance in differentiating between legitimate and potentially malicious access.

There will always be some activity that is obviously suspicious, and we will issue immediate Cyber Security+ Alerts accordingly.

SERVICE PROMISE

Our Cloud Security+ monitoring tools operate 24 hours a day, seven days a week. Our expert analysts are on hand between the hours of 0800–1800 UK, Monday to Friday. Security events will be notified in accordance with the response times outlined in the table below].

Cloud Security+ Alerts will include details of the security event, our assessment of the impact and our remediation advice. Your weekly report will highlight all relevant activity requiring review and other security related events that are appropriate for your business.

ALERT LEVEL	DESCRIPTION	RESPONSE TIME
High	An actual or potential breach of the cloud service.	4 hours
Medium	A suspicious event which has had no immediate impact, but is indicative of a potential security issue, or may in the long term cause a security issue	8 hours
Low	Failed brute force attempts, failed accesses from unusual or suspicious locations	Summarised weekly

PRICING

From £500 per month, depending on the size of your organisation

CONTACT US

The Cyber Security Expert Ltd.

info@thecybersecurityexpert.com

+44 (0)20 3290 4065/+33 (0)9 70 462662