

Web Security+ from the Cyber Security Expert

Securing your business from data thefts, costly disruption and reputational damage



The headlines may focus on website breaches of high-profile businesses like British Airways, but did you know that, whatever you might think, your website is coming under attack on a daily basis – a software change, update or configuration mistake could mean you are unexpectedly vulnerable.

Technology and tools alone aren't enough to keep your business secure. Web Security+ is specifically designed to arm start-ups, scale-ups and SMEs with cost-effective website security monitoring and to stop them becoming a statistic.

The PLUS in Web Security+ is the addition of our world-class cyber security consultants to your existing IT team. They will be “eyes on”, monitoring reports from the security tools we use, analysing incidents, alerting you to potential or actual breaches and delivering the guidance you need to keep your website and its data safe.

Web Security+ is suitable for all single-hosted websites. If you need to clarify your hosting position, please don't hesitate to call us.

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 Web 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.

Web Security+ IDENTIFYING THREATS AND MITIGATING THEM

The absolute best defence against any type of attack is to eliminate all vulnerabilities from your website by ensuring your developers consider security, running security testing and ensuring software is kept up-to-date. In reality, that rarely happens!

The latest statistics show a 14% increase in website attacks from Q4 2017 to Q1 2018 and it's a trend that's set to continue.

There is a growing array of individuals and groups operating on the internet who are intent on trying to hack your business website – sometimes to hold you to ransom, sometimes to steal private or sensitive information, sometimes to steal credit card details and sometimes just for fun or to prove that they can.

Web Security+ is designed to help prevent any of this happening and the software we install can detect and block attacks as they happen. Not only are attacks blocked, but the hackers are temporarily barred from accessing your website completely preventing them attempting variations of technique and reducing the load on your website. They are also simultaneously blocked from access to any website under our protection.

In addition, all the data reported by our monitoring tools is analysed by our cyber security experts. They will issue **Web Security+ Alerts** which include clear guidance on any action that needs to be taken by you or your webservice provider.

Web Security+ tools also report on administrative access made to your website, and any changes to key webpages or changes to system files. This gives you real time protection and assurance that any unauthorised changes will be detected.

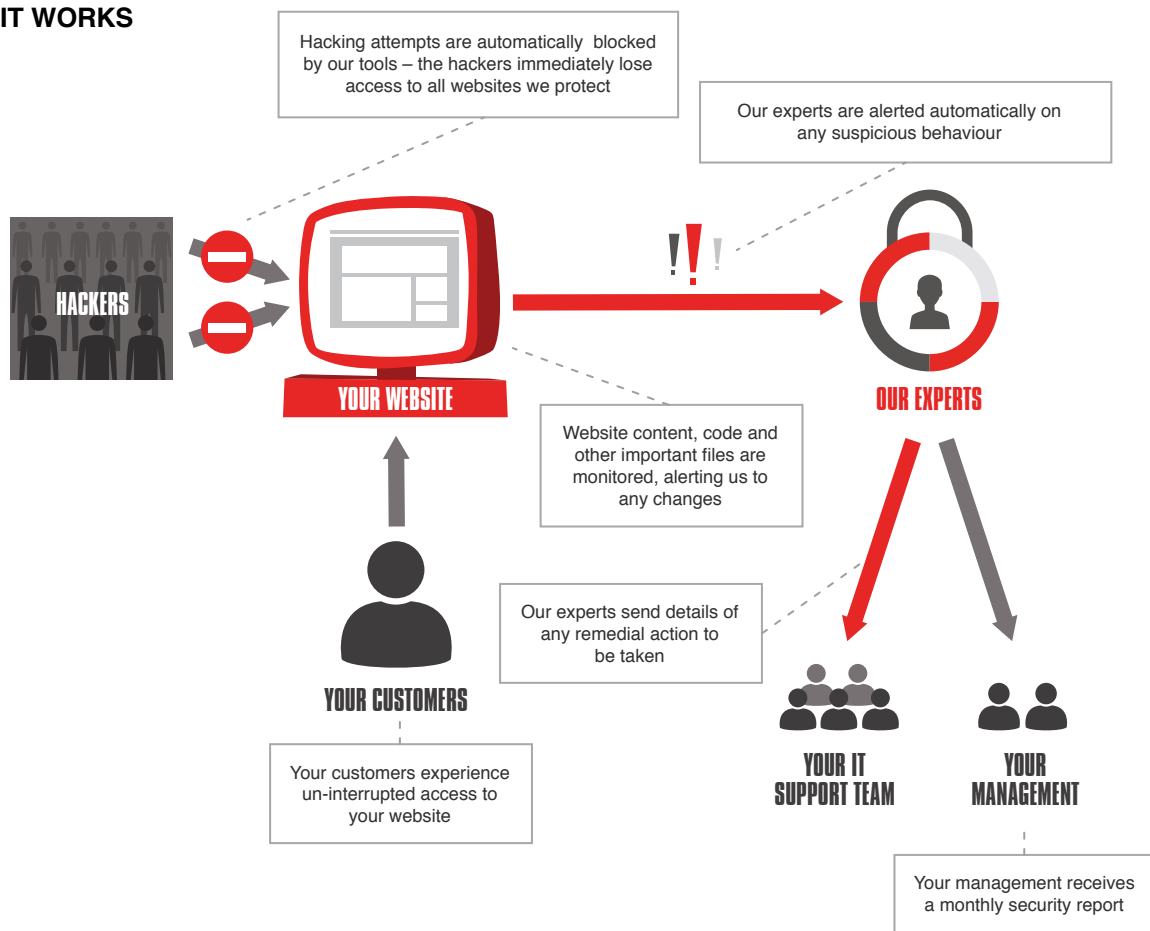
In addition to Alerts, our Web Security+ service also includes a monthly summary report giving visibility on any trends in attempted attacks and recommendations from The Cyber Security Expert to help you continuously improve your website security.

Web Security+ THE BENEFITS

There is no replacement for having cyber security experts “eyes on” to monitor and analyse website security data. **Web Security+ promises:**

- The addition of world-class cyber security experts to your IT team without the need to add to headcount
- Website monitoring for attacks and security breaches 24 hours a day, 7 days a week, 365 days a year
- Web Security+ Alerts delivered directly to your inbox when threats are detected together with impact assessments and remediation advice from our experts
- Automated prevention of a range of cyber-attack techniques
- Avoidance of costly data breaches, loss of valuable management time and untold reputational damage
- The ability to demonstrate GDPR compliant policies and procedures
- Reassurance for your customers that their data and your services are cyber-safe

HOW IT WORKS



Preparation

We will need:

- to understand your website configuration and which platforms you are using
- to know about any other security measures, such as security testing, you have already taken
- to install our monitoring tools on your webserver (which means we are unable to provide this service if you are using a shared hosting platform)

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 deliver timely alerts.

Installation

We will require remote root access to your webserver in order to install our monitoring tools, or to work alongside someone from your team who can do this for us. This access does not need to be permanent, it is not needed for day-to-day monitoring and can be rescinded once installation and testing is complete.

We will require you to make the configuration changes to your firewall that we recommend so that our monitoring tools are able to talk to our monitoring server in the Amazon cloud. We will provide you with specific IP addresses for our end points, so the rules are as restrictive as possible.

Operation

We will periodically require remote root access to the web server in order to upgrade our tools - or access to someone from your team who can do this under our guidance. It may also occasionally be necessary to restart the web server software, or reboot the server itself, for changes to take effect.

We will always: request access in advance; make any changes in accordance with your change management policy; run upgrades at a time that is acceptable to you.

SERVICE PROMISE

Our Web 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.

Web Security+ Alerts will include details of the security event, our assessment of the impact and our remediation advice. Your monthly 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 your website, or the underlying operating system.	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		Summarised monthly

PRICING

£500 +VAT per website per month
Minimum term 1 year

CONTACT US

The Cyber Security Expert Ltd.

 info@thecybersecurityexpert.com

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