HORIZON

EXECUTIVE CYBER ASSURANCE

WHAT IS HORIZON

Proprietary software designed, built and operated by former senior Government cyber experts as an essential first line of cyber assurance for Microsoft office 365 and Google G suite cloud computing environments

WHAT IT DOES

Provides indicators of invoice fraud and e-mail compromise by alerting users if there has been an attempted or successful login to your cloud network, outside of your organisation.

HOW IT WORKS

Accounts remotely monitored 24 x 7 x 365 by Horizon operations centre providing live threat alerts when a compromise is detected.

WHO IT'S FOR

Designed for non-cyber experts with an uncomplicated and easy to navigate interface supported by intuitively displayed dashboards for rapid insights.

Maps organisation's IT network and displays current operating systems and software that maybe out of date and not supported.

Horizon will work alongside additional cyber security products.

Unrestricted by scale providing cyber assurance to small, medium and large organisations.

Cuts through the noise to focus on threats that really matter to your organisations.

Typical on-boarding in less than 1 hour and no installations required.

Compatible with Microsoft Office 365 and Google G Suite

Horizon's automated detection supports manual event creation and investigation within the GUI environment. Simple visuals allow for quick identification of geographic spread of logins as well as operating systems and software in use. More granular breakdowns of all login events are also tabulated, accompanied by further information to support event investigation.

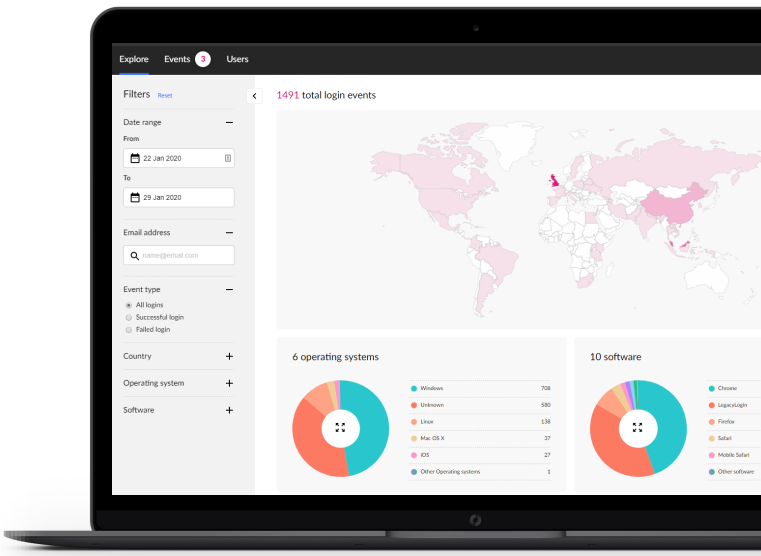
AUTOMATICALLY DETECT AND IDENTIFY:

- Suspicious login activity including:
  a. Malicious software and operating systems
  b. Malicious IP addresses
  c. Abnormal IP behaviour
  d. Impossible travel

- Software and operating system version number for compliance purposes
- Highly exposed accounts due to use of weak passwords appearing in dark web data
- Auto-forwarding rules from internal company accounts to external email accounts
- Blacklisted indicators across entire community of clients from initial identification of 'patient zero'
- Company email used for B2B and third-party services, such as LinkedIn (dark web data)

HORIZON SUPPORTS THE USER BY:

- Grouping detected events by signature to reduce event fatigue
- Allowing for dynamic white-listing of detected suspicious activity event indicators
- Providing user information to add context to investigations



TRIAL

To undertake a 30 day Horizon trial please email:
hello@clearwaterdigital.io

clearwaterdigital.io

Clearwater DIGITAL