HORIZON

Your email compromise
and fraud detection solution

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

- ✓ Cuts through the noise to focus on threats that really matter to your organisation's.
- ✓ 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.
- ✓ Displays current operating systems and software that maybe out of date and not supported.

How it works

- ✓ Horizon scans and collects external threats to a customer's network through proprietary algorithms and prioritises and visualises them for remedial action.
- ✓ Horizon will work alongside any other Cyber security products.
- ✓ Typical on-boarding in less than 1 hour and no installation of hardware or software on the network is required.

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.
- ✓ Unrestricted by scale providing cyber assurance to small, medium and large organisation's.
- ✓ Compatible with Microsoft Office 365 and Google G Suite

The Horizon Competitive Advantage

Benefits

- ✓ Uniquely identifies non authorised attempted and successful cloud login's, files being viewed, and mails being accessed. Displays compromised e-mails and passwords on a persistent basis.
- ✓ Faster identification of cyber threats enables quicker response, reduced down time and financial losses.
- ✓ Maps IT infrastructure highlighting out of date and non-supported software improving operations and compliance.
- ✓ Identifies cyber threats not detected by competitive products.
- ✓ Non-intrusive, no hardware or software installed on the network.
- ✓ Accelerated onboarding delivering 90 days of data analysis within an hour of deployment.
- ✓ Future proofed road map integrating monthly Horizon upgrades and features.

Expertise

- ✓ Delivers expert cyber security without the expert.
- ✓ Optional monitoring and in-depth forensics available 24 x 7 by expert analysts.
- ✓ Circumvents the industry challenges of skills shortages and event fatigue.
- ✓ Tools and monitoring services developed and supported by most senior UK Government hackers.

Methodology

- ✓ Competitively priced for any size customer.
- ✓ Built from the ground up integrating proprietery code and data bases and extensively tested on large global corporate networks.
- ✓ Designed to mitigate the most prevalent Cyber risks namely e-mail compromise and the growing $300Million dollar a month invoice fraud crisis.
- ✓ Consolidates and complements existing cyber security products.
- ✓ Un-restricted markets by industry, sector and organisation size.

HORIZON TECH

The Science

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 users 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

AUTOMATED PASSWORD STRENGTH CHECKING

The monitoring of cyber hygiene for companies remains of critical importance. No matter the level of sophistication with network monitoring systems and employed security teams, the weakest link to cyber security is human behaviour, and users are very difficult to monitor.

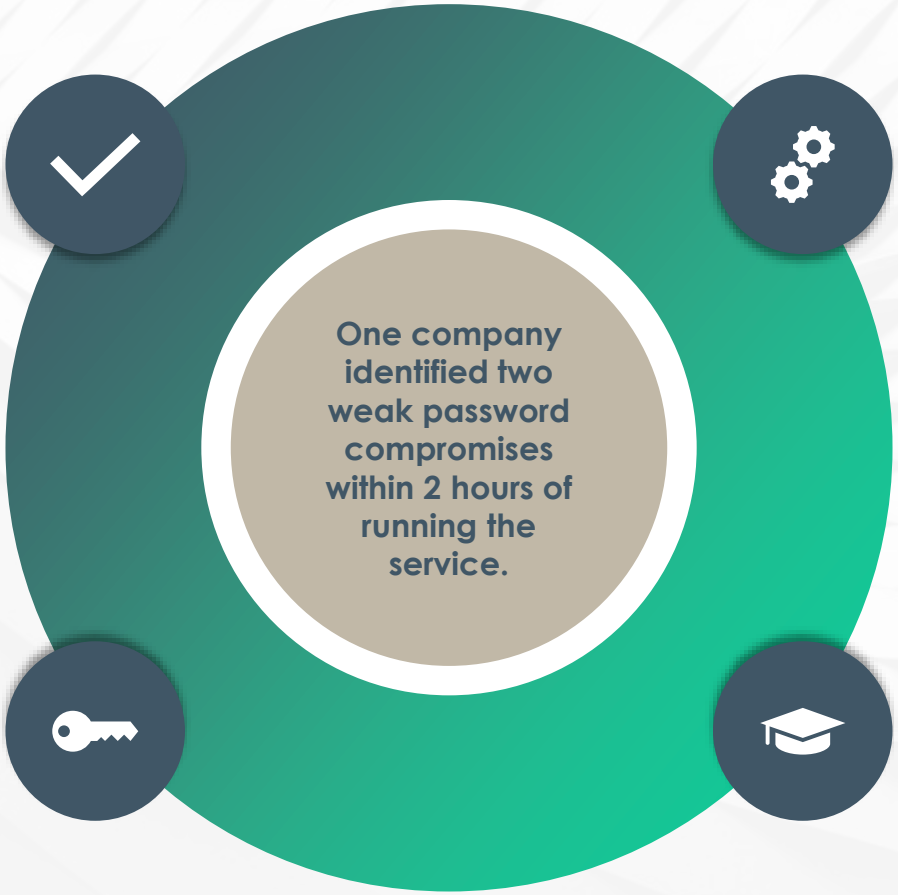
The use of weak or repetitive passwords is the single most frequent cause of network penetration. There is a growing divide between what users believe is a safe operating mode and what hackers are able to do with minimal information or access to a corporate network. As databases and businesses software migrate to the cloud, vulnerability rises exponentially.

Opt-In

As an opt-in service for Horizon subscribers the organisation's Microsoft365 accounts will be scanned on a live 24/7 basis by a propriety automated tool searching for weak passwords.

Assess password policy

If people can use a weak password, you may need to re-assess password policy for the organisation.



Runs in the background

This tool runs in the background and sends an alert to Horizon when a weak password is detected.

No training needed

The tool requires no additional training or software and alerts you when something is wrong.

HOW SECURE IS YOUR ORGANISATION?

In days gone by, user passwords were:
"password"

Password1
Password123
Pa55w0rd
$password1

One solution is to require a second stage to complete login, such as a response from mobile.

Microsoft introduced rules that passwords must contain at least one of the three categories:
A to Z
a to z
0 to 9
~!@#$%^&*_-+='|\(){}[]:;"<>,.?/

Hackers regularly try passwords like these to break into an organisations emails, usually targeting CEOs/CFOs

Office 365 provides admins with information for all user login activity. Horizon can automatically login using a database of likely passwords and examine the results.

HORIZON CASE STUDY

Energy and Industrial Conglomerate

Horizon detected over 160 compromised accounts within a multibillion-dollar company undergoing an M&A process with the possibility of a new listing. Further investigation by the Horizon threat intelligence team identified unauthorised external file sharing and access to commercially sensitive cloud folders and documents. In addition, Horizon detected a significant number of system vulnerabilities caused by employees using out of date or unsupported IT operating systems and software, resulting in a cross-group review of assurance budget and resources. Valuable insights delivered by Horizon have resulted in the formation of a specialist security and investigation division. Horizon continues to be employed across the group to provide ongoing assurance and threat detection in parallel with the group's IT and cyber transformation programme.

HORIZON CASE STUDY

Finance

Following a previous breach of the company's cloud email platform, Horizon was deployed to conduct a vulnerability assessment of newly introduced IT security measures. On initial deployment Horizon identified several users operating legacy software, unable to apply the Two Factor Authentication (2FA) policy. During the second week of monitoring Horizon detected a breach of the CEO's email, as a result of an IT permissions request. Horizon supported an immediate post incident risk assessment and monitoring of further attempted account breaches and or email rule/policy exploitation.

HORIZON CASE STUDY

Media, Communications and Telecoms

The CEO of a large media, communications and telecoms group in South East Asia requested an assessment of its cloud security integrity, following a vulnerability assessment of its internet facing assets and infrastructure by Clearwater Digital. Horizon detected unusual access to the Clients cloud emails from high risk geographic locations and auto forwarding policy violations to non corporate email accounts. Horizon further identified 'at risk' Operating Systems (OS), one of which was associated with a broadcast engineer, who would have posed a significant risk to the client's infrastructure, should the identified engineer's laptop have been infected or compromised by cyber criminals.

HORIZON CASE STUDY

Maritime

Following an identified breach of a finance staff's email account, Horizon was deployed to identify further account compromises and provide a risk assessment to the client's key risk holders. The Horizon team identified that there were a proportionally large number of staff using outdated Operating Systems (OS), which could be vulnerable to the suspected malware used in the original breach. Horizon supported an independent IT security transformation process, ensuring baseline security measures were updated across the company. Horizon data analysts identified that the third-party IT managed service company was unable to support requested and timely access to historic log data, commensurate to post Cyber incident triage requirements. Furthermore, the comparison of the company's attack profile, was not consistent to that of other Horizon clients. This inconsistency is currently under review and has prompted a legal discussion regarding 3rd party managed service liability and due diligence.

Frequently Asked Questions

What data do we hold?

We access the Azure Active Directory Audit Log data (Azure Active Directory powers access and authentication for all Office 365 systems).

A typical record contains:

- User Details (name and email)
- Time of Access
- IP Address
- Software details (e.g. Chrome on Windows 10)

We also capture additional data such as user profile data. This is so we can compare login events against the users' job title and typical work patterns. This includes:

- Users' names
- Job title & team details
- Email forwarding rules

When Horizon collects data, it is done under two controlled and restricted access methods; neither of which can view the content of emails or documents. In limited instances, the Microsoft APIs may present us the 'Subject Line' (but not the content) of an email for events that we do not subscribe to or process. We immediately blacklist these events, do not process or store them and ensure the data does not end up in any of our logging.

How will we hold your data?

We use the Amazon EC2 infrastructure. We follow security best practices to secure and monitor this infrastructure. All data at rest or in transit is secured to meet the United Kingdom, European Union and United States data assurance standards and privacy regulations. For European clients, we host our data inside the Amazon European Union data centres.

Who has access?

As part of the monitoring service, vetted Clearwater analysts will have access to the data to perform the security monitoring service. Access distribution within your organisation is up to you as the client. We highly recommend that you use the two-factor authentication option to secure access to the Horizon application.

Why are we asking for API access and PowerShell?

Ideally, we could access all the data we need for security monitoring using the Microsoft APIs. However, there is still some key data that is only available from Microsoft using PowerShell.

Our PowerShell access method does support Multi-Factor Authentication and conditional access policies.

How do we revoke access later?

Removing the PowerShell access is simple. Simply disable or delete the account you setup in the "Creating a limited account for Horizon PowerShell" section in the 'Onboarding Process' document.