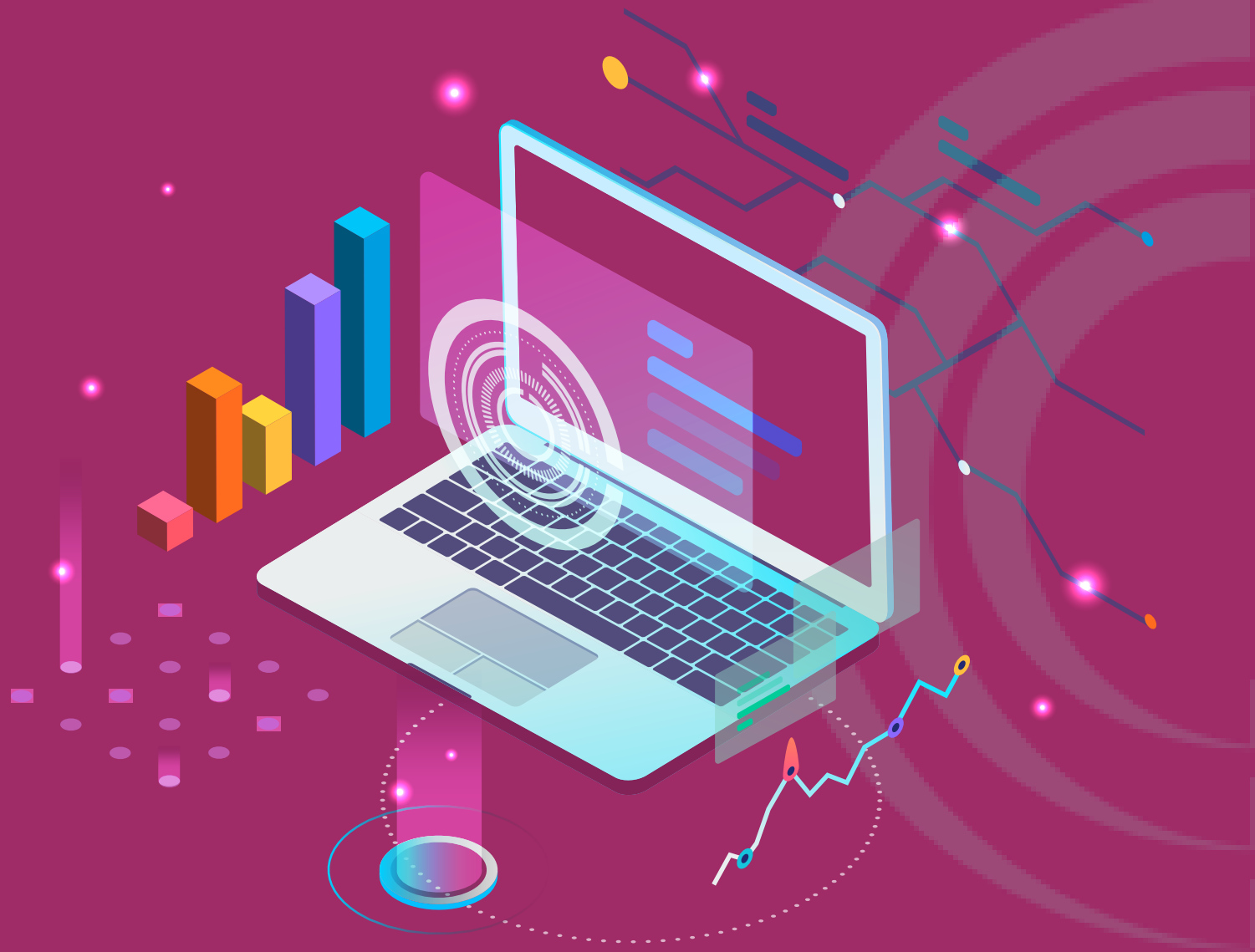
Clearwater Digital

Horizon

Smart Threat Detection for
Microsoft SaaS applications



The Science

Horizon's automated detection is complemented by 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 operating systems
- Suspicious software
- Suspicious IP addresses
- Anomalous travel patterns
- External auto-forwarding rules
- Weak passwords
- Software and operating system version number for compliance purposes
- User accounts with compromised credentials
- Threats to the community
- Company email used for b2b and 3rd-party services, such as LinkedIn

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

Clearwater Digital

Automated Password Assurance

Horizon

Password creation

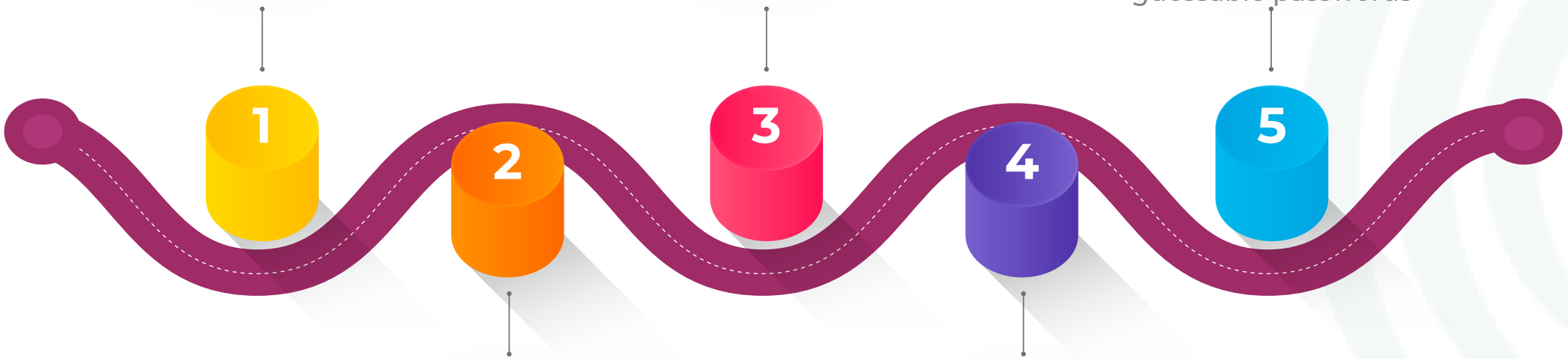
In days gone by, user passwords were: “password”

Password - Completed

Password1
Password123
Pa55w0rd
$password1

Logged activity

Horizon can automatically emulate an attacker attempting to login to your user accounts with weak or easily guessable passwords



New rules

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

Not secure

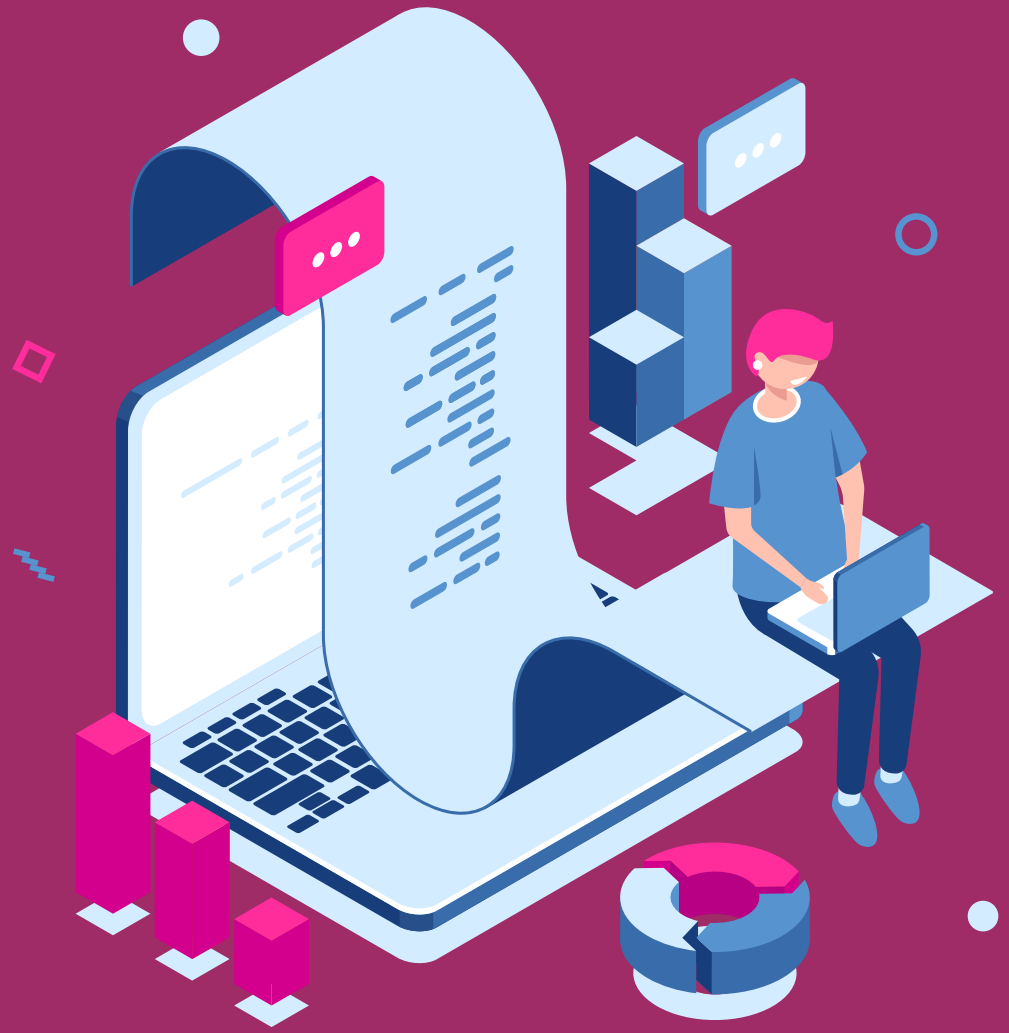
Malicious actors regularly try easy to guess passwords to gain access a target’s emails

Energy and Industrial Conglomerate

Horizon detected over 160 compromised accounts within a multibillion-dollar company undergoing an (M&A) Merger and Acquisition 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. Additionally, 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. The valuable insights provided by Horizon highlighted a previously overlooked aspect of IT security within the group, resulting in a specialist internal unit being established to use Horizon to detect and respond to threats, on an active basis.

Clearwater Digital

Horizon CASE STUDY

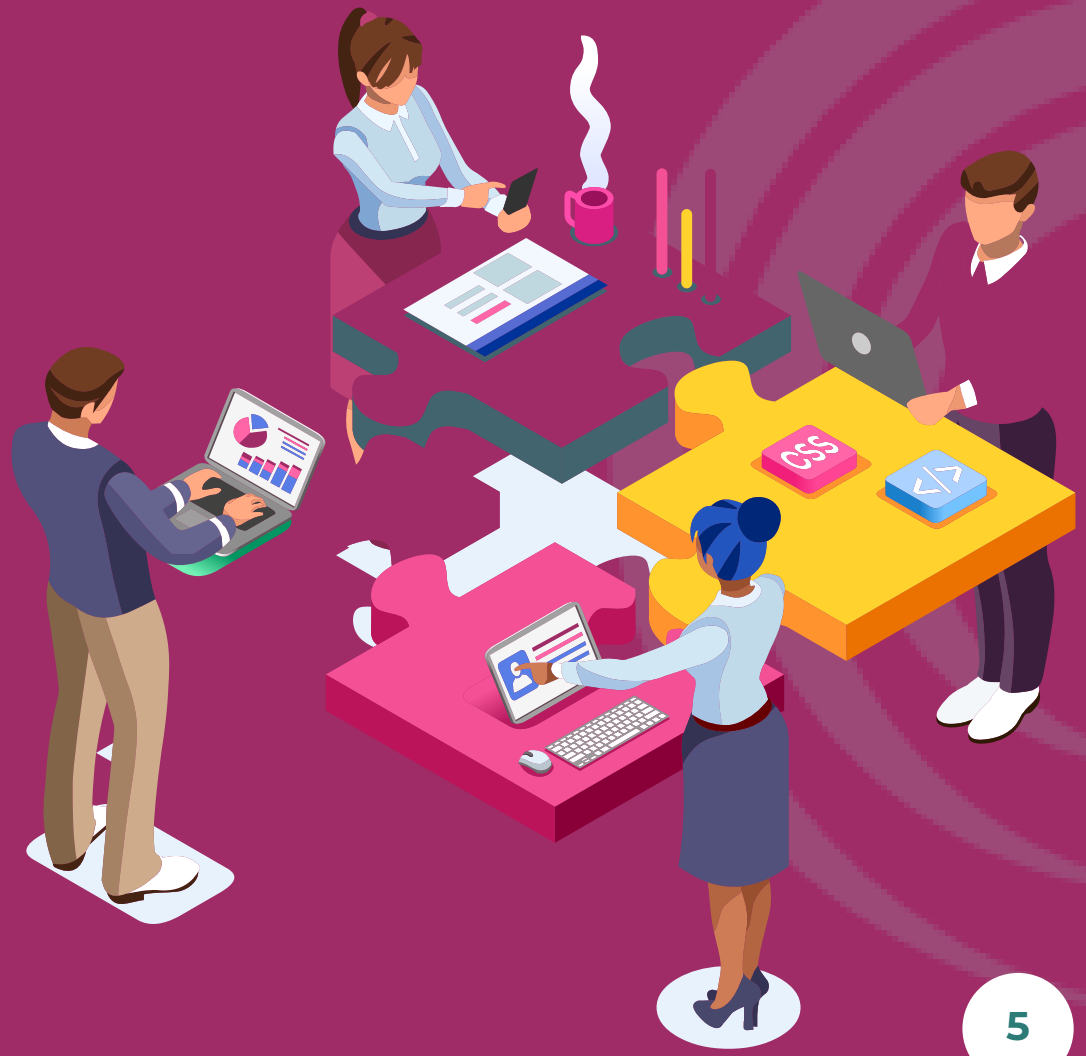


Finance

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.

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.



Clearwater Digital

Horizon CASE STUDY

Maritime

Following an identified breach of a financial analyst'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 member's email using outdated Operating Systems (OS), which could be vulnerable to the suspected malware employed 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 3rd-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.

Clearwater Digital

Email Address
horizon@cwdynamics.com

Phone Number
(00 44 (0) 1202 804 140)