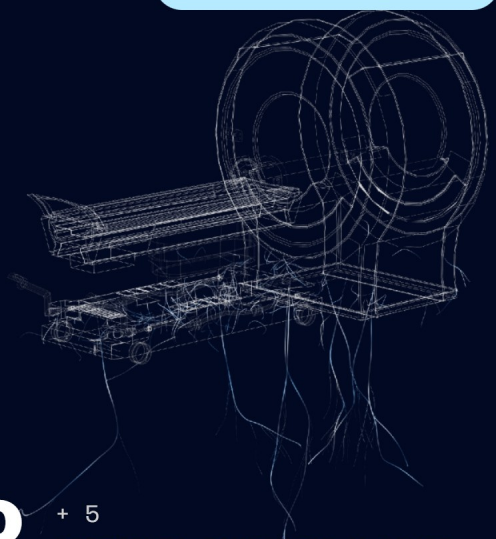
PRIVATE EQUITY

EveryCloud
AI & Data Security

Beyond the questionnaire: evidence-based cyber assurance across a private equity portfolio



+ 5
PORTFOLIO COMPANIES X-RAYED

+ CASE STUDY

Industry: Private Equity

Portfolio: 5 companies assessed

Sectors: Facilities services, healthcare, fuel retail, trade and building materials distribution

Service: EveryCloud X-Ray Assessment

Overview

A global private equity investor wanted a clear, comparable view of cyber risk across its portfolio, one that went further than self-reported answers.

EveryCloud ran its X-Ray Assessment across five portfolio companies. Rather than asking whether controls existed, the X-Ray measured how security tools were deployed, configured and performing, and what each business was spending to run them.

The result was board-ready evidence for every company, benchmarked side by side against the portfolio average.

THE CHALLENGE

The PE firm needed to understand cyber risk consistently across very different businesses, and questionnaires weren't giving it the full picture.

Questionnaire-based assessments ask whether a control exists, not whether it works. Answers depend on who completes them and how each question is read, so two companies giving the same "yes" can carry very different levels of risk. With no supporting evidence, results were hard to compare, prioritise or present to the board with confidence.

Key challenges included:

+ Subjective, self-reported answers with no evidence behind them
+ Binary yes/no responses that hide partial deployment and misconfiguration
+ No like-for-like comparison between portfolio companies
+ Little insight into whether security spend was delivering value
+ Difficulty articulating cyber risk to the board and investment committee

+ 11,086
PAYLOADS TESTED

+ 1,854
PAYLOADS ARRIVED

+ 83%
XDR MISCONFIGURED

+ 177
IMPROVEMENTS AVAILABLE

THE SOLUTION

EveryCloud replaced self-attestation with independent, evidence-based measurement.

The X-Ray connects to the tools each company already runs and safely tests them against real-world attack techniques mapped to the MITRE ATT&CK framework. Findings are measured, not declared, so every company is assessed to the same standard and the results compare like for like.

What a questionnaire records vs what the X-Ray shows

EXAMPLE FINDINGS FROM ONE PORTFOLIO COMPANY

● Measured score (reality) ● Self-assessed score (perception)

Is endpoint protection deployed across the estate?

SURVEY

Yes

1 **2** 3 **4** 5

→

X-RAY EVIDENCE

95% of devices are enrolled in at least one control, but 20% are missing one or more of the minimum required controls.

Are security tools configured correctly?

SURVEY

Yes

1 2 3 **4** 5

→

X-RAY EVIDENCE

XDR is deployed on 90% of devices, yet 83% of those deployments are configured incorrectly.

Is web filtering in place?

SURVEY

Yes

1 **2** 3 **4** 5

→

X-RAY EVIDENCE

37 of 76 command-and-control sites and 2,443 phishing sites were reachable during testing.

Is sensitive data protected from leaving the business?

SURVEY

Yes

1 2 **3** 4 5

→

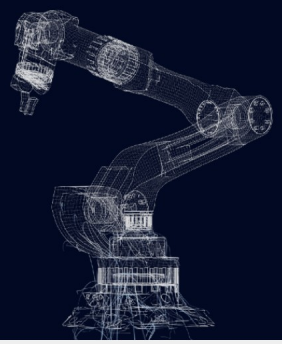
X-RAY EVIDENCE

100% of simulated data was exfiltrated, with no data loss prevention controls in evidence.

Each answer becomes a measured position rather than a tick box, showing not just whether a control exists but how well it performs.

THE DELIVERY

Three modules. One consistent standard.



The X-Ray combines Value, Visibility and Validate modules, giving the PE firm one evidence-based view of each company's security posture.

Every portfolio company was assessed with the same methodology and scoring, creating a consistent baseline the investor could compare, prioritise and act on.

+ 01 Value

Security, cost, utilisation and optimisation

Licence, cost and utilisation analysis across Microsoft 365 and the wider security stack, with tool overlap mapped against the NIST Cybersecurity Framework.

£365k–£770k
potential annual saving at a single company

£130k
from recategorising E3 licences to F3

46.5%
Microsoft Secure Score, against an E5 potential of 81%

+ 02 Visibility

Cyber asset management of deployed tools

Every device was checked for the minimum required controls, confirming whether each tool was deployed, functioning and configured correctly.

95%
of devices enrolled in at least one security control

20%
missing one or more minimum required controls

37%
of Microsoft Defender deployments configured incorrectly

+ 03 Validation

Security tool validation against MITRE ATT&CK

Safe breach and attack simulation tested endpoint, email, web gateway and data loss prevention controls with 11,086 real-world payloads.

98/100
endpoint protection, stopping all ransomware, Trojan and worm tests

43/100
web gateway, identified as the highest-priority gap

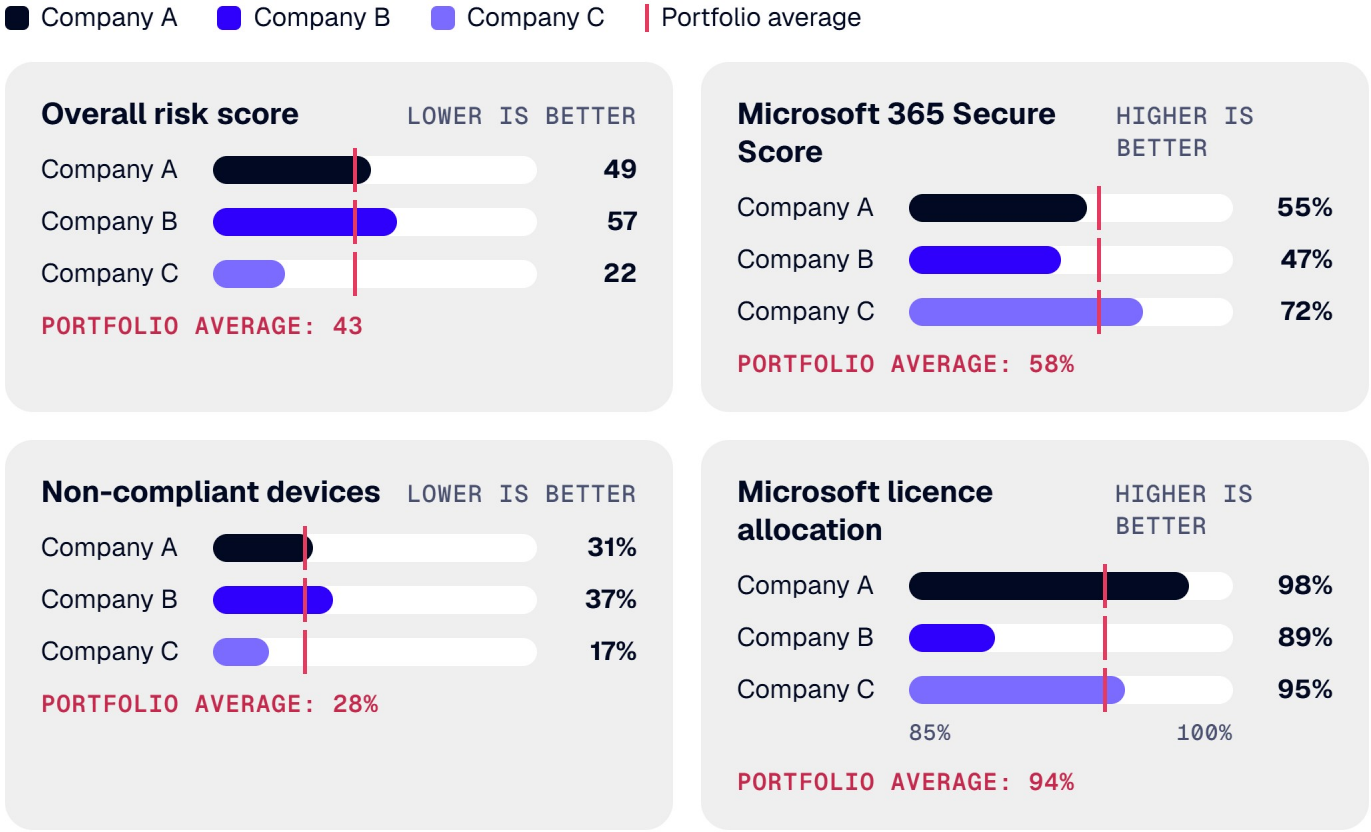
0/100
data loss prevention, with no egress controls in evidence

MODULE FINDINGS SHOWN ARE FROM ONE PORTFOLIO COMPANY

PORTFOLIO BENCHMARKING

Every company, side by side

Because every company is measured the same way, results sit side by side and against the portfolio average, showing which businesses lead, which need support and where to invest first.



Three of the five assessed companies shown. Portfolio average is calculated across the companies shown. Figures rounded.

The outcome

The PE firm now has one evidence-based view of cyber risk across its portfolio. Every company was measured to the same standard, so results compare like for like and priorities are clear.

The engagement surfaced 177 available improvements and a potential £365k–£770k annual saving at a single company, giving the PE firm board-ready evidence to direct investment where it reduces risk most.