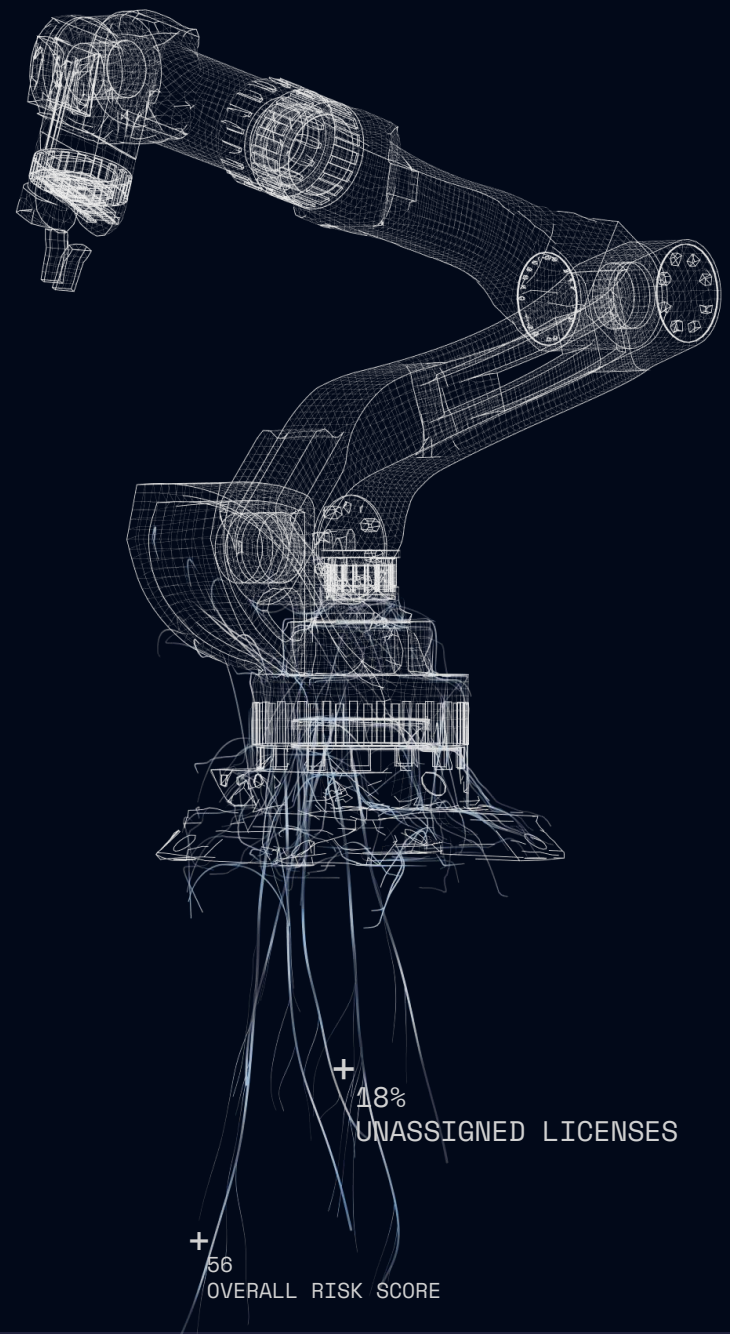
EveryCloud

EVC X-Ray Assessment

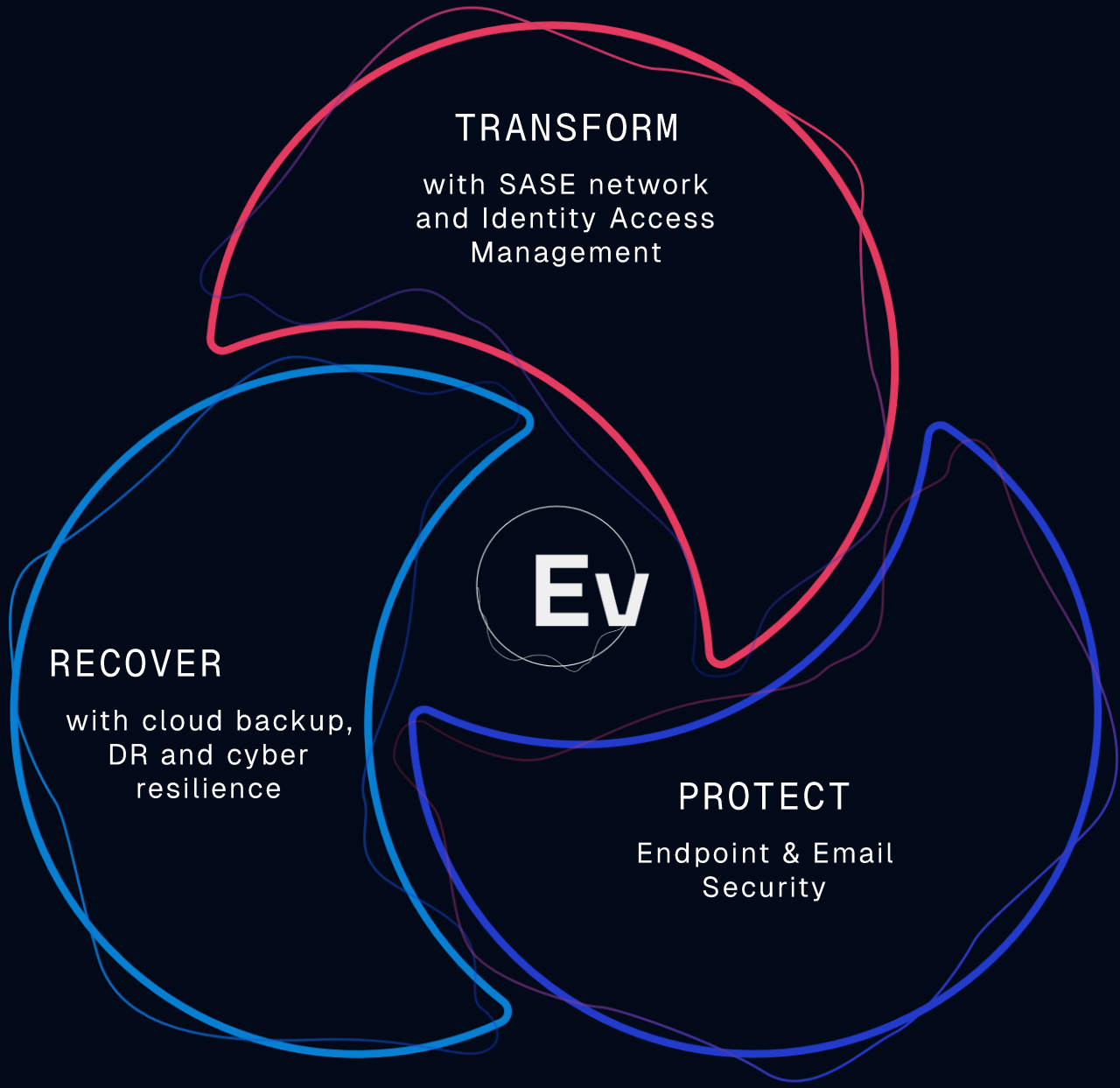


EveryCloud Who are we?

+
Securing 300,000+ End Users

+
10 Years Specialising in Cloud Security

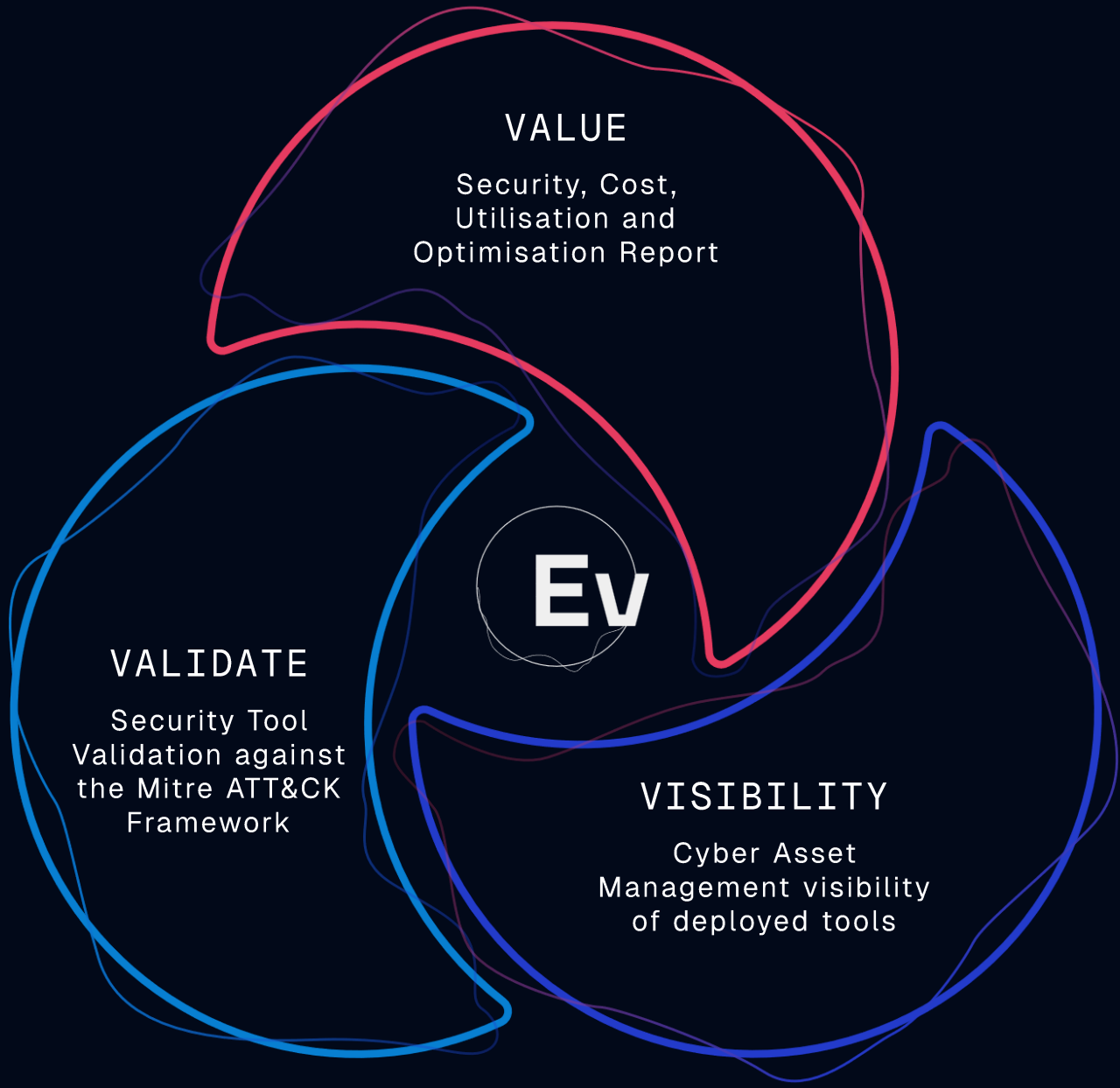
+
Zero Trust Network Access and Identity Access Management Experts



+ EveryCloud X-Ray Assessment

X-Ray Cyber Assessment 3Vs

EveryCloud has provided a consultative review of the baseline security of your organisation. This is based on best security practices, cyber hygiene, tool validation and optimisation of spend.



Portfolio
Expectations vs Reality

VISIBILITY

Expectation:

Devices are protected

Reality:

20% devices missing critical tools

VALIDATE

Expectation:

Tools deployed and configured

Reality:

50% of phishing sites accessed

VALUE

Expectation:

Great Licence Allocation

Reality:

Potential saving of 24%

We show what is beneath the surface

+ Highlight positives

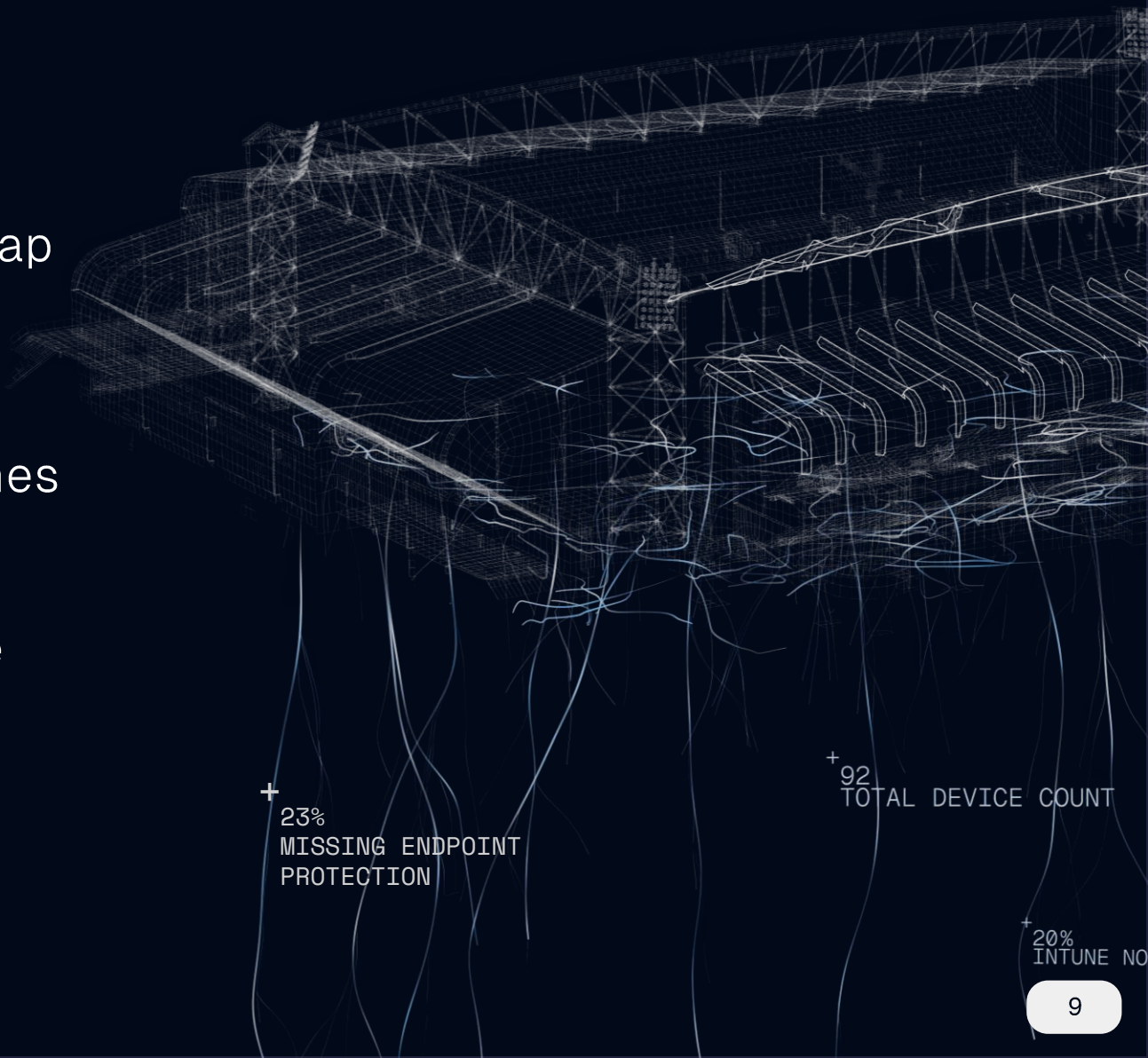
+ Highlight wastage/overlap

+ Provide clarity into best practice

+ Help protect against breaches

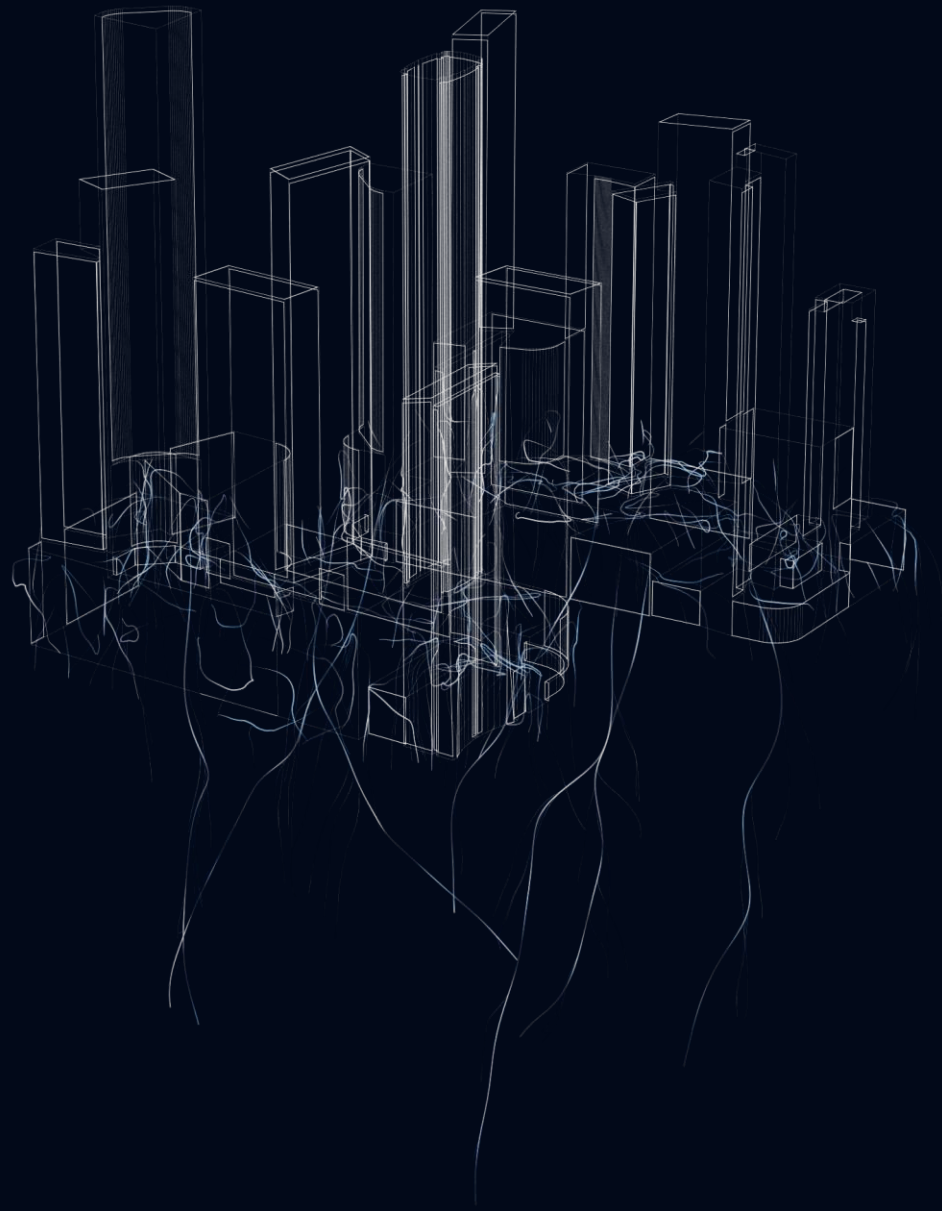
+ Provide evidence-based recommendations

+ Help articulate to the board



+

Value



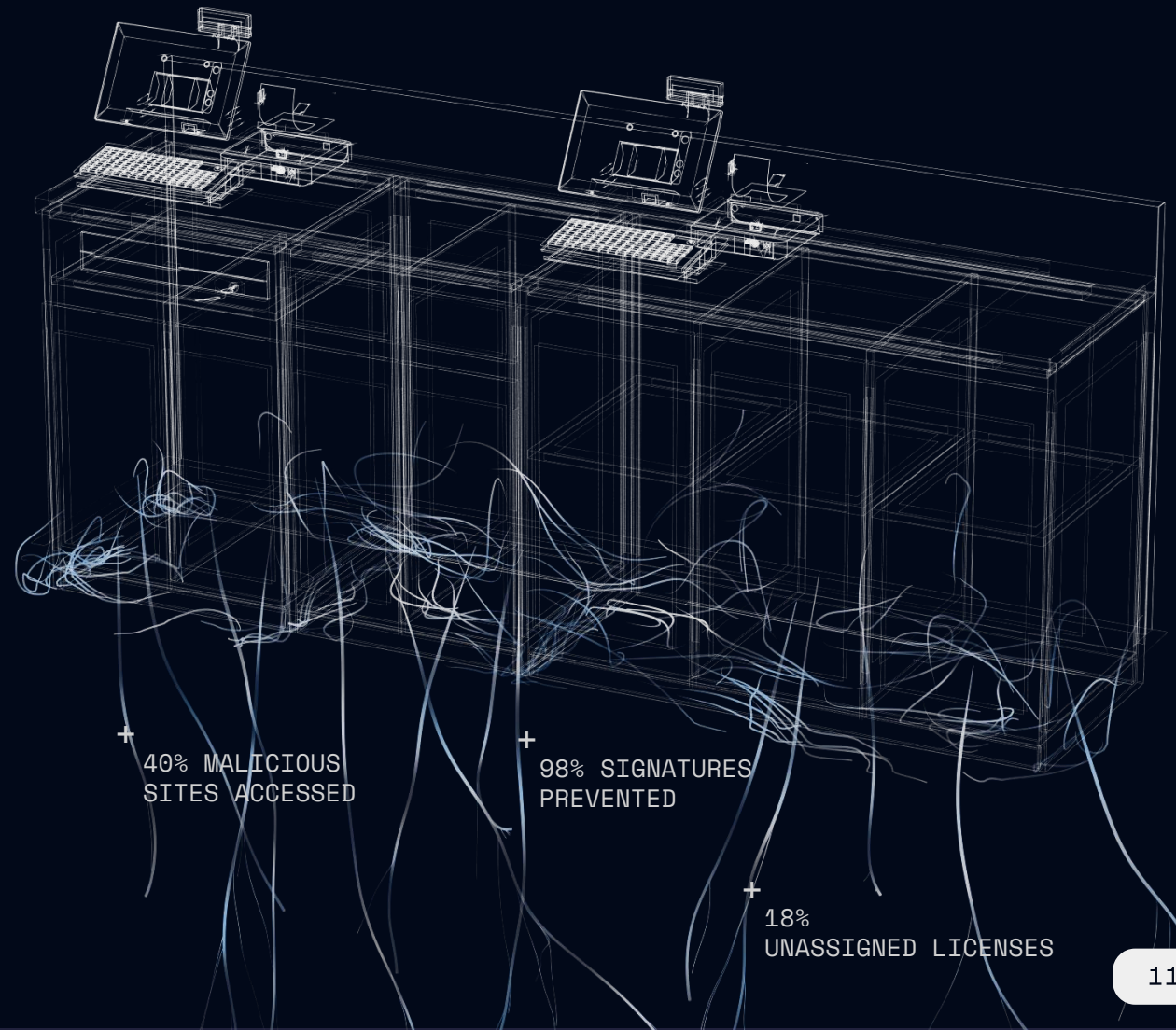
EveryCloud

Looking beneath the surface of license spending

+ Uncover license wastage

+ Overlapping technology

+ Gaps in security scores



+ EveryCloud X-Ray Assessment

Understanding Product
Overlap and Coverage

Security Coverage Map

Threat detection 4	XDR 3	Endpoint Detection and Response 3	Asset Management 3
Vulnerability Management 2	Sandbox 2	Containment/Isolation 2	Network Security 2
Cloud Security 2	Remediation 2	Zero Trust Architecture 2	Web filtering 2

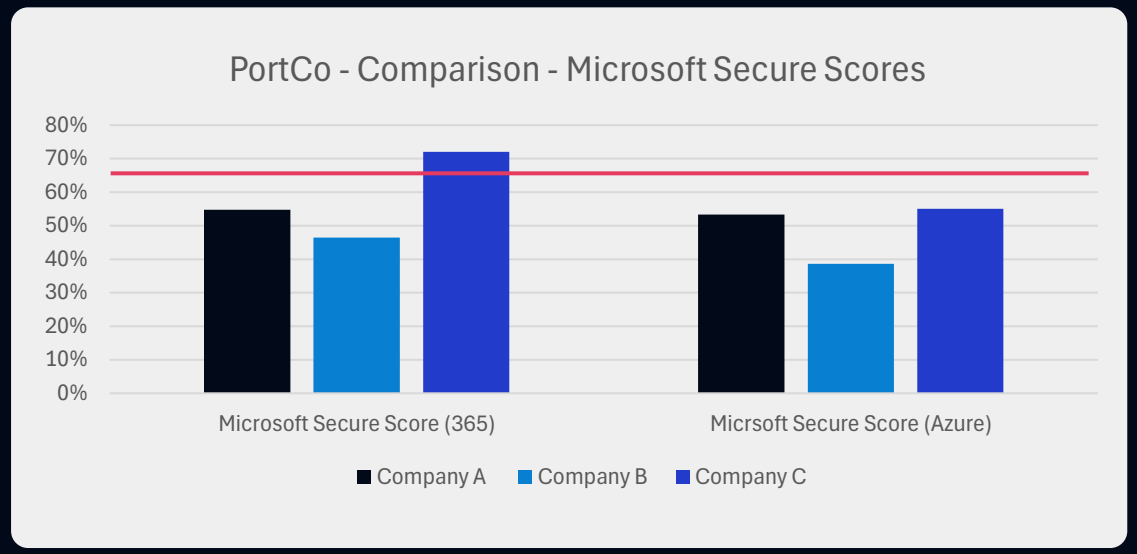
NIST CSF Mapping

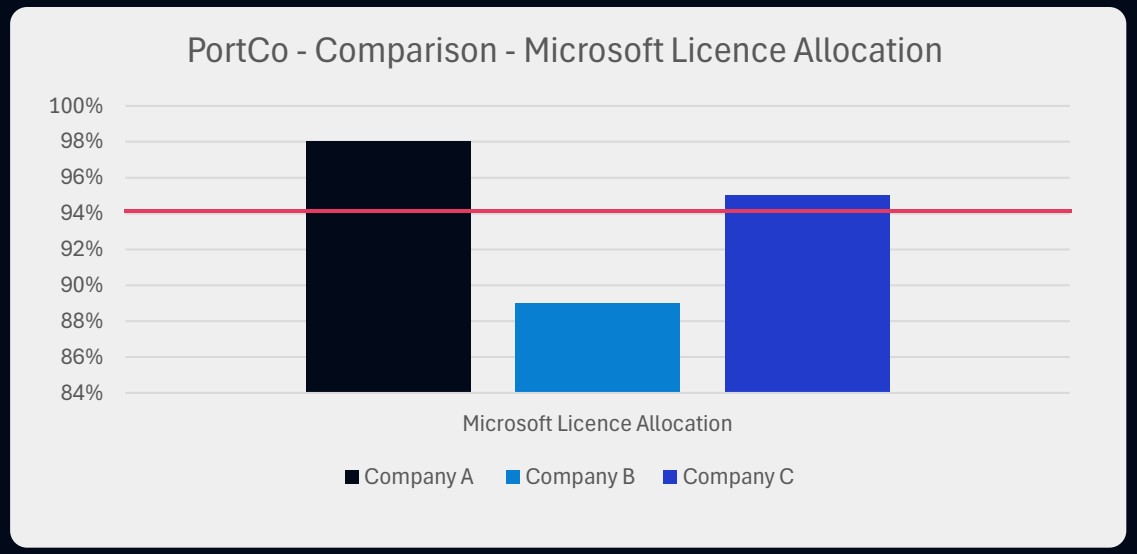
Protect — Coverage: 64% — Mapped: 4

PR.AA	PR.AT	PR.DS	PR.IR	PR.PS
85% | Mapped: 5	0% | Mapped: 0	53% | Mapped: 2	31% | Mapped: 1	87% | Mapped: 5
PR.AA-01	PR.AT-01	PR.DS-01	PR.IR-01	PR.PS-01
PR.AA-02	PR.AT-02	PR.DS-02	PR.IR-02	PR.PS-02
PR.AA-03		PR.DS-10	PR.IR-03	PR.PS-03
PR.AA-04		PR.DS-11	PR.IR-04	PR.PS-04
PR.AA-05				PR.PS-05
PR.AA-06				PR.PS-06

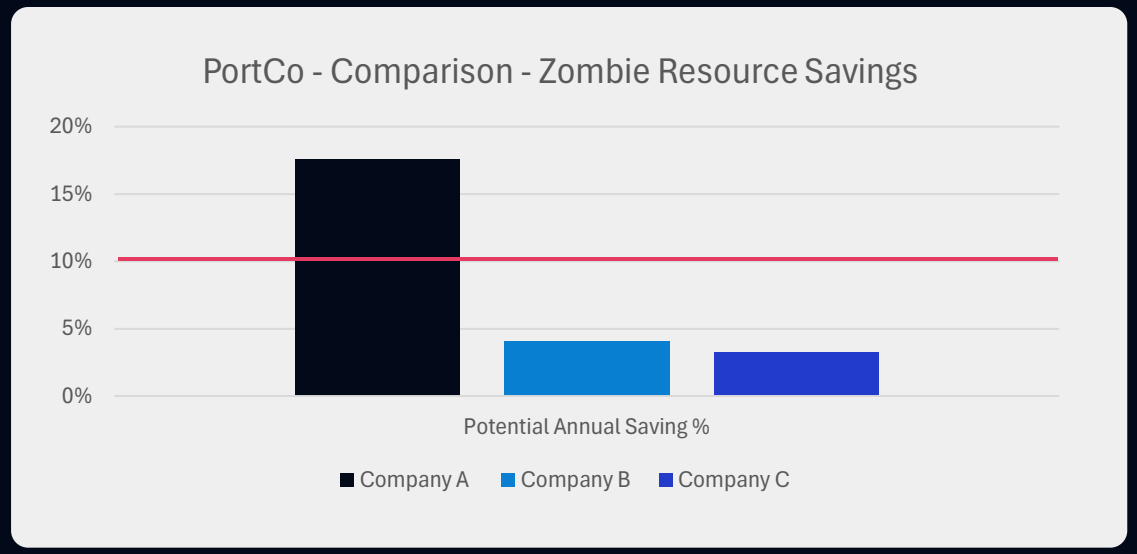
EVC 365 license and security

+ EVC Average: 57





+ EVC Avg: 94%



+ EVC Avg: 17%

Microsoft 365 license and security audit

EveryCloud

Total Cost	License Allocation	Recategorize savings	Secure Score
£4,000,000	**90%**	**£130,000**	**46.5%**
Monthly Investment £340,000	10% licences not allocated	Recategorise E3 licences into F3	Below industry standard

Total Saving per year

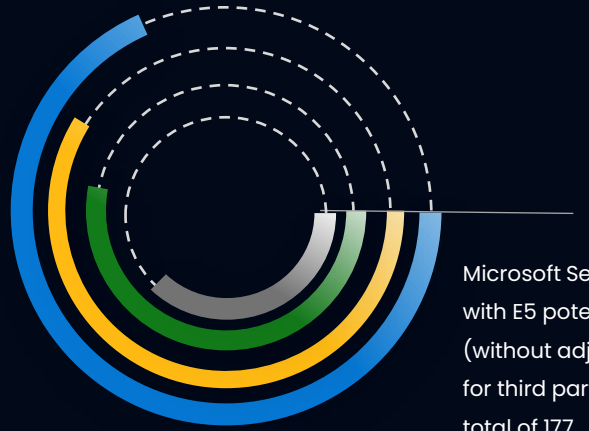
£365,000 – £770,000

Dynamic 365 Finance (12% allocation) — **£38,880/£324,000**

Power BI Pro (60.5% allocation) — **£20,589/£34,032**

Dynamic 365 for supply chain management (45% allocation) — **£14,785/£32,856**

Secure Score Summary



Microsoft Secure Score with E5 potential of 81% (without adjustments for third party tools). A total of 177 improvements available.

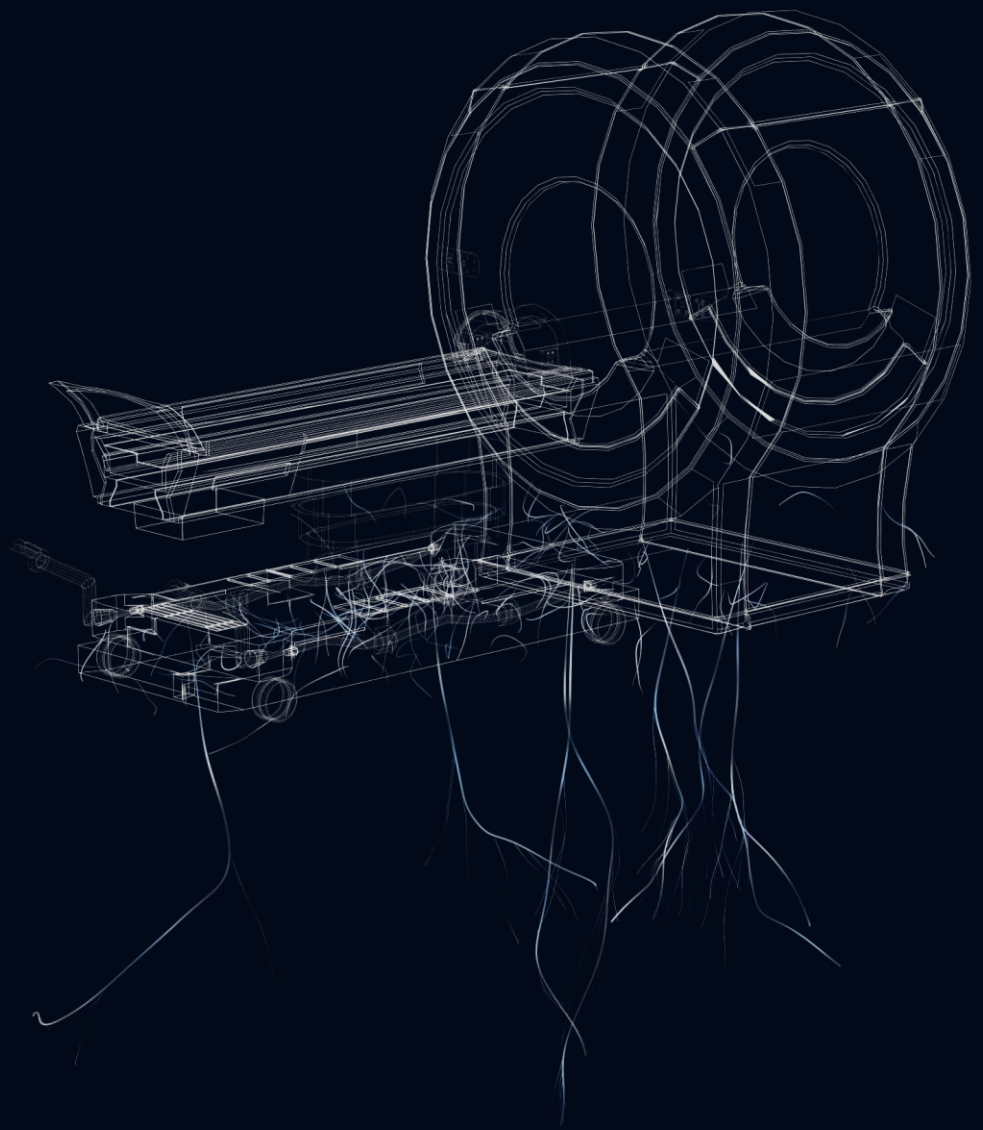
Identity (65%) **Data (56%)**

Device (45%) **Apps (36%)**

+ EveryCloud X-Ray Assessment

+

Visibility



+ Visibility

EveryCloud

95% of devices enrolled into at least 1 security control

20% of devices are missing 1 or more of the minimum required controls

MS Defender

Configured Incorrectly	**37%**
Functioning	94%
Deployed	95%

MS Intune

Configured Incorrectly	**17%**
Functioning	91%
Deployed	94%

EDR

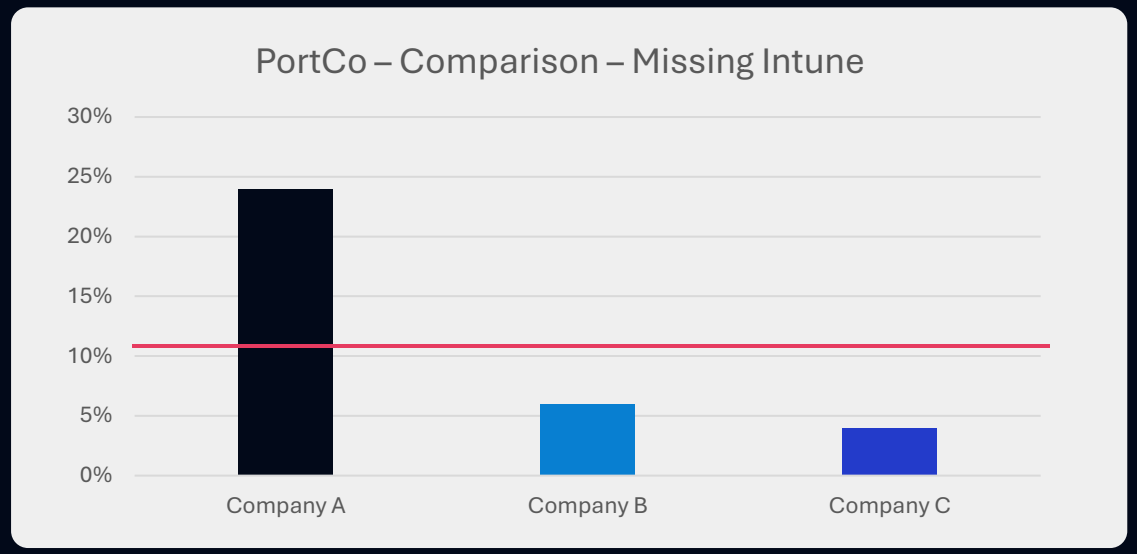
Configured Incorrectly	**10%**
Functioning	94%
Deployed	95%

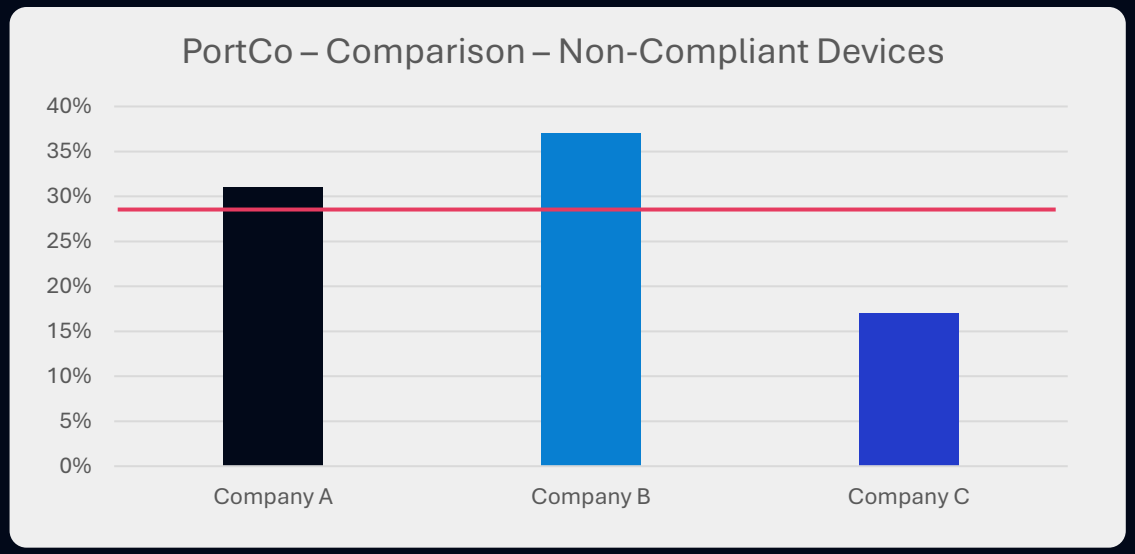
XDR

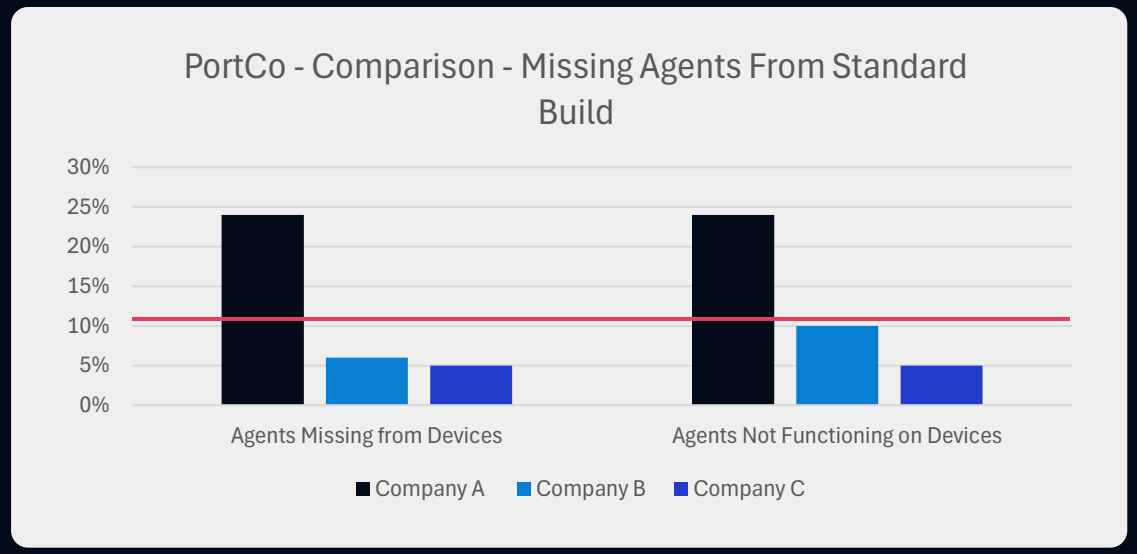
Configured Incorrectly	**83%**
Functioning	90%
Deployed	90%

EVC – Cyber Hygiene

+ EVC Avg: 10%







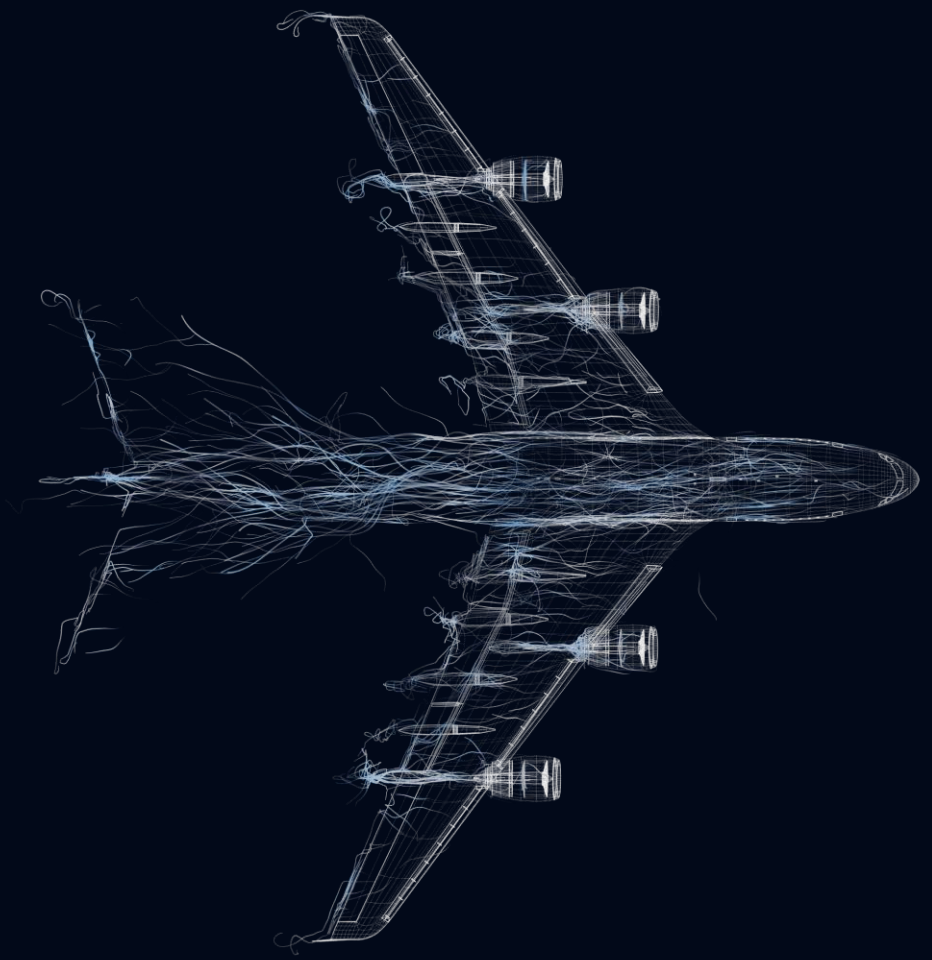
+ EVC Avg: 25%

+ EVC Avg: 9%

+ EveryCloud X-Ray Assessment

+

Validation



Security Tool Risk

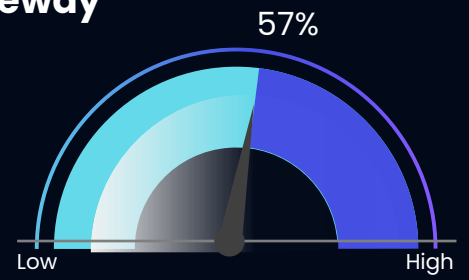
EveryCloud

Overall Risk Score: Medium

Low | Medium | High

Highest Priority: Web Gateway

The assessment was **completed**, achieving a risk score of **57**, indicating moderate vulnerabilities. During the simulation, **4,295 payloads** were sent, out of which **1,854 arrived successfully**, from a total of **11,086 payloads** tested.



Endpoint Protection

High performing endpoint controls based on a series of tests around Ransomware, worms and Trojans.

Email

Moderate Risk with measures in place to shield recipients from harmful emails.

Web Gateway

Large gaps discovered during testing of the web gateway, showing significant risk. Areas of concern around access to known phishing and C&C sites.

Data Loss Prevention

No evidence of any DLP and controls to stop data egressing the organisation.

Security Tool Performance

EveryCloud

Endpoint Controls

Ransomware Protection	100%
Trojan Protection	100%
Worm Protection	100%
Signature Based Detection	85%

Tested

Application Layer Protocol
Obfuscated Files or Information
System Information Discovery
Process Injection
Hijack Execution Flow

Web Gateway Controls

Phishing Sites Accessed	2443/14411
Command & Control	37/76
Malicious Files inbound	1336/1339
Blocked file types	1/154

Outbound Traffic to Malicious URLs: 64.4%

Download of code execution from trusted source 31%

Data Loss Prevention

Data exfiltrated	100%
Protection in place	None

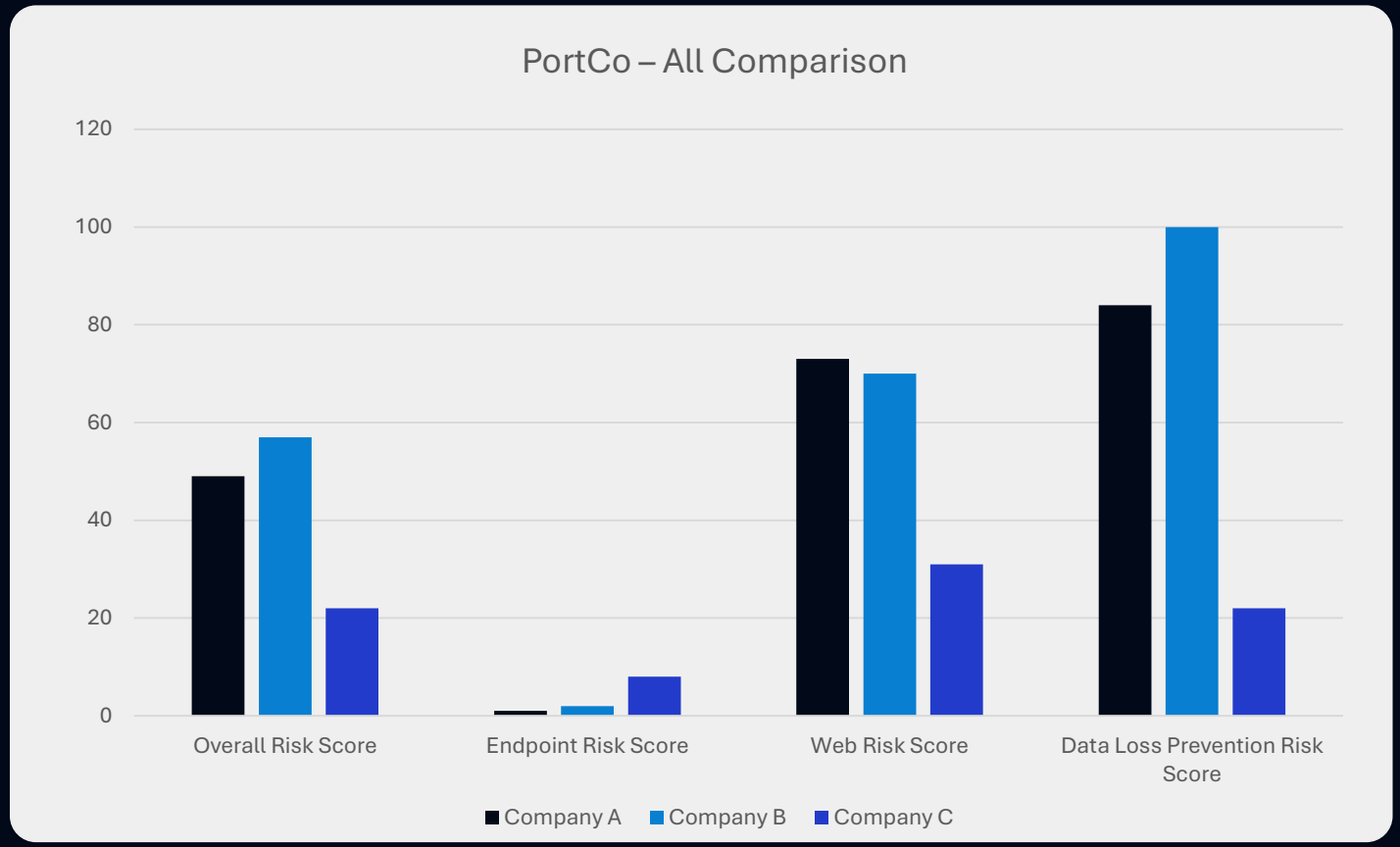
+ EveryCloud X-Ray Assessment


Initial Access
10 techniques
Content Injection
Drive-by Compromise
25%
Exploit Public-Facing Application
26%
External Remote Services
31%
Hardware Additions
Phishing
32%
Replication Through Removable Media
Supply Chain Compromise
Trusted Relationship
40%
Execution
16 techniques
Cloud Administration Command
Command and Scripting Interpreter
8%
Component Object Model and Distributed COM
0%
Container Administration Command
Deploy Container
Exploitation for Client Execution
100%
Inter-Process Communication
Native API
1%
Scheduled Task/ Job
Persistence
21 techniques
Account Manipulation
0%
BITS Jobs
Boot or Logon Autostart Execution
12%
Boot or Logon Initialization Scripts
0%
Browser Extensions
Compromise Client Software Binary
57%
Create Account
0%
Create or Modify System Process
9%
Privilege Escalation
15 techniques
Abuse Elevation Control Mechanism
30%
Access Token Manipulation
0%
Account Manipulation
0%
Boot or Logon Autostart Execution
12%
Boot or Logon Initialization Scripts
0%
Create or Modify System Process
9%
Domain Policy Modification
20%
Defense Evasion
44 techniques
Abuse Elevation Control Mechanism
30%
Access Token Manipulation
0%
BITS Jobs
Build Image on Host
Debugger Evasion
Deobfuscate/ Decode Files or Information
18%
Deploy Container
Direct Volume Access
Domain Policy Modification
Credential Access
17 techniques
Adversary-in-the-Middle
100%
Brute Force
Credentials from Password Stores
0%
Exploitation for Credential Access
Forced Authentication
Forge Web Credentials
Input Capture
9%
Modify Authentication Process
Multi-Factor Authentication Interception
Discovery
32 techniques
Account Discovery
23%
Application Window Discovery
0%
Browser Information Discovery
Cloud Infrastructure Discovery
18%
Cloud Service Dashboard
50%
Cloud Service Discovery
0%
Cloud Storage Object Discovery
0%
Container and Resource Discovery
Lateral Movement
10 techniques
Component Object Model and Distributed COM
0%
Exploitation of Remote Services
0%
Internal Spearphishing
Lateral Tool Transfer
14%
Remote Service Session Hijacking
0%
Remote Services
2%
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content
Collection
17 techniques
Adversary-in-the-Middle
100%
Archive Collected Data
4%
Audio Capture
25%
Automated Collection
Browser Session Hijacking
0%
Clipboard Data
0%
Data Staged
100%
Data from Cloud Storage
Data from Configuration Repository
Exfiltration
9 techniques
Automated Exfiltration
Data Transfer Size Limits
57%
Exfiltration Over Alternative Protocol
96%
Exfiltration Over C2 Channel
0%
Exfiltration Over Other Network Medium
0%
Exfiltration Over Physical Medium
0%
Exfiltration Over Web Service
0%
Scheduled Transfer
Command and Control
18 techniques
Application Layer Protocol
30%
Commonly Used Port
Communication Through Removable Media
Content Injection
Data Encoding
17%
Data Obfuscation
Dynamic Resolution
Encrypted Channel
32%
Fallback Channels
Impact
14 techniques
Account Access Removal
33%
Data Destruction
5%
Data Encrypted for Impact
1%
Data Manipulation
67%
Defacement
0%
Disk Wipe
0%
Endpoint Denial of Service
16%
Financial Theft
Firmware Corruption

EVC – Tool Validation

+ 100% DATA EXFILTRATED

+ MODERATE RISK SCORE



+ EVC Avg: 42

+ EveryCloud X-Ray Assessment

HSS Hire

BLAKE MORGAN

BDO

Funding Circle

Fred.Olsen & Co.

EVERYCLOUD IS TRUSTED BY

hcrg Care Group

International Personal Finance

Everton 1878 NIL SATIS NISI OPTIMUM

ao


EveryCloud
AI & Data Security