RATEYOURCYBER

Your Cyber Posture. Precisely Rated.

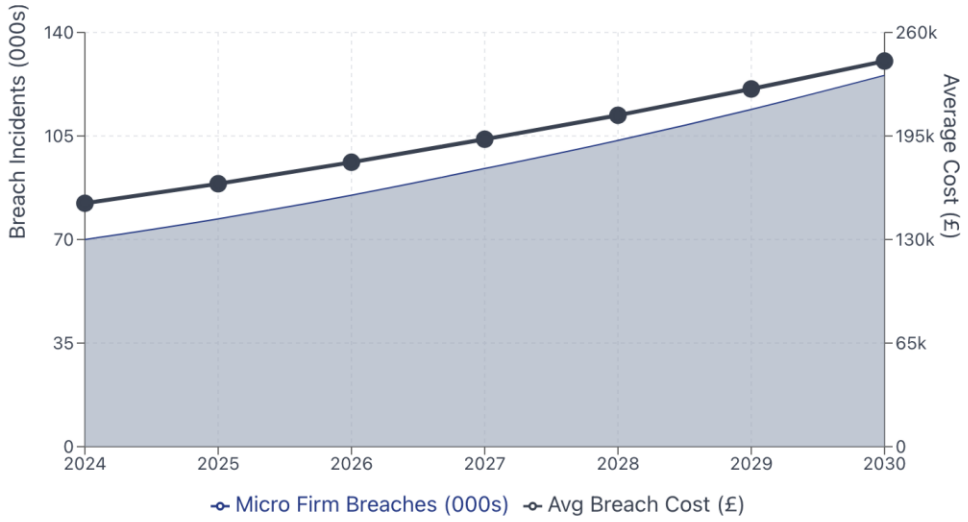
HaloPSA - RateYourCyber Webinar Presentation

November 18th, 2025

Why cybersecurity matters more than ever in today's AI-driven landscape

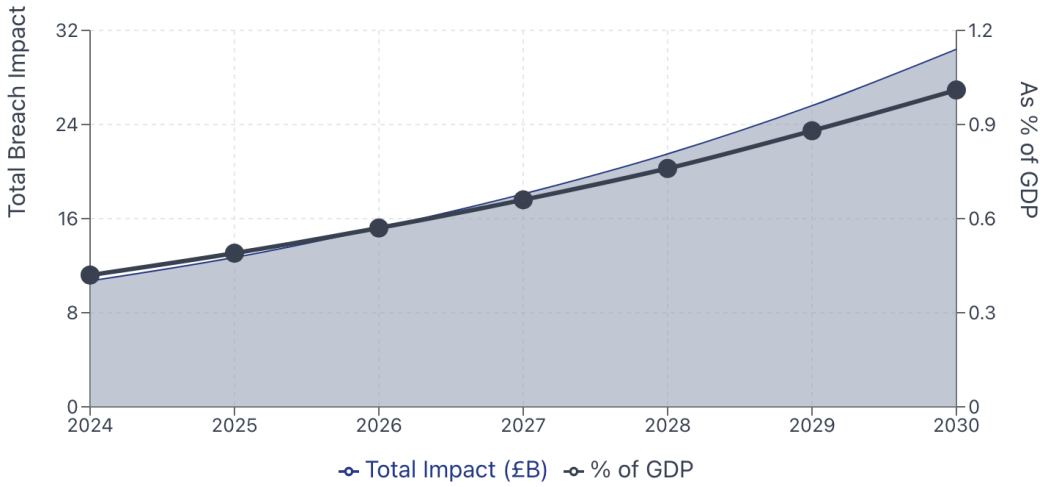
Threat Landscape Projections (2024-2030)

Accelerating breach frequency and costs driven by digitalization and targeted SME attacks



Breach Economic Impact Trajectory

Annual SME breach costs in billions and as percentage of UK GDP



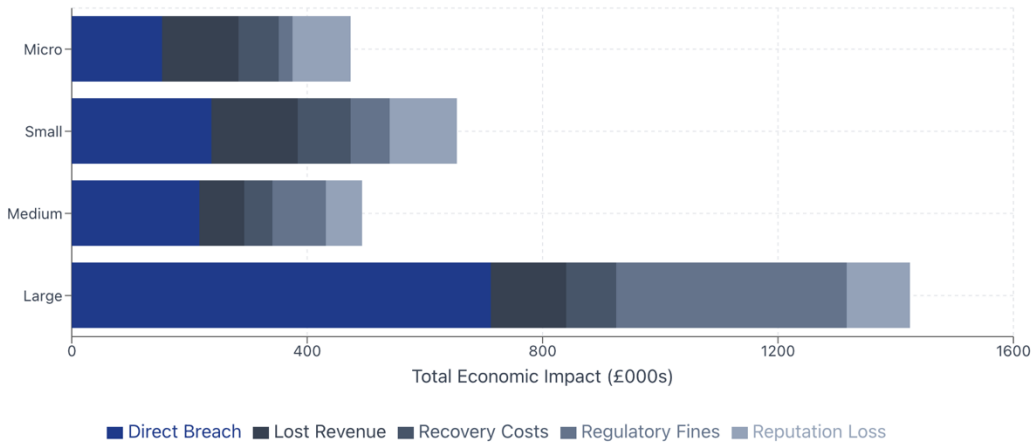
What 1% of GDP means:

- 80% of the UK's entire defence budget
- £454 taken from every person in the UK annually

Sources:
https://www.gov.uk/government/publications/independent-research-on-the-economic-impact-of-cyber-attacks-on-the-uk
https://www.gov.uk/government/statistics/business-population-estimates-2024
https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024
https://www.ons.gov.uk/economy/grossdomesticproductgdp

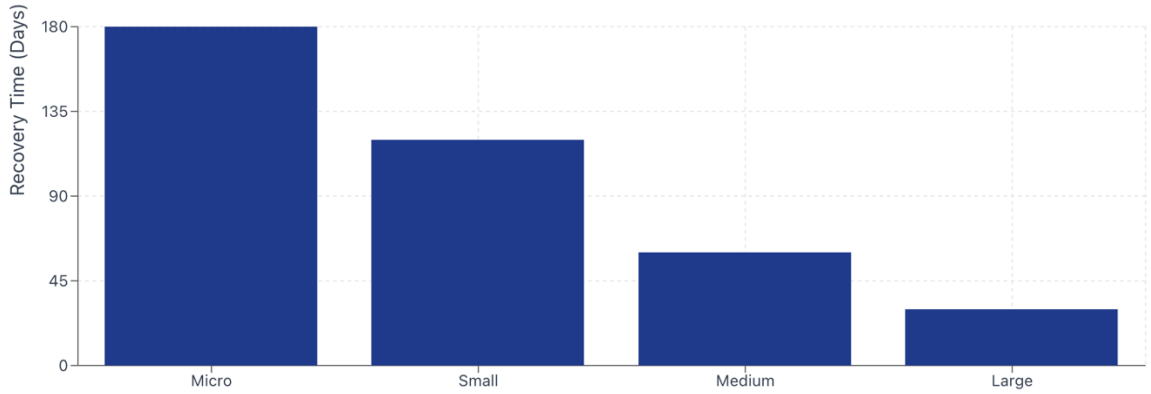
Cumulative Economic Impact by Firm Size

Total breach costs including cascading effects (£000s)



Time-to-Recovery Analysis

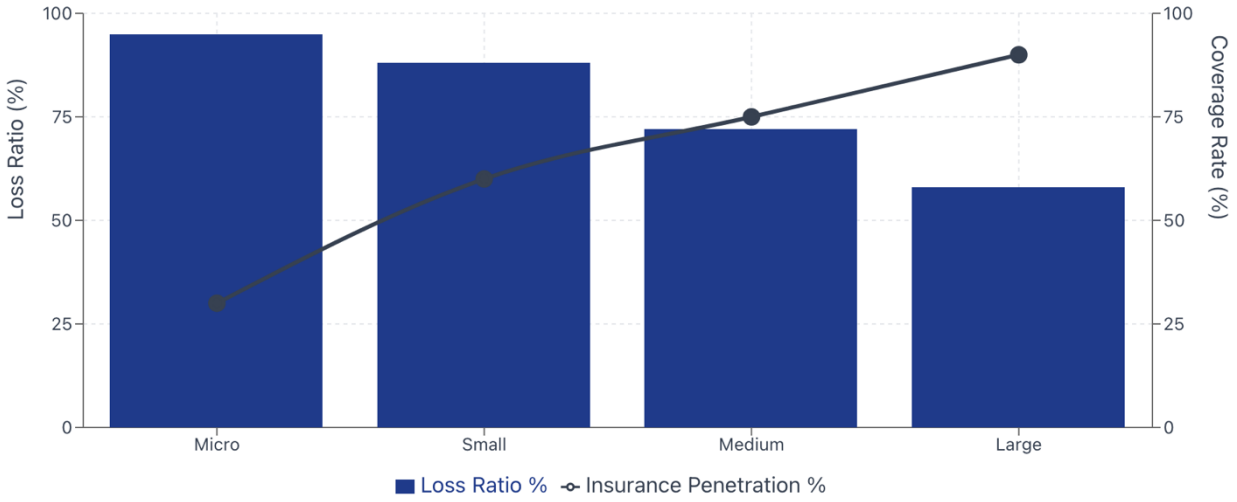
Operational recovery timelines and business impact duration



- The total economic impact for small and micro firms from a cyber breach averages at 280% of direct breach cost which for enterprise is “only” 200%.
- Time to recovery for SME is around 120 days with average of 30 days for large enterprise.
- Large enterprise have systems and processes in place and can spend money and resources on cyber and business continuity protection that helps them with fast recovery and minimization of a breach impact cost

Insurance Market Sustainability

Loss ratios and coverage gaps reveal fundamental market instability for SME cyber insurance



Firm Size	Premium	Loss Ratio	vs. Sustainable Benchmark (60-70%)
Micro	£1,200	95%	25-35 points ABOVE (underpaying)
Small	£3,500	88%	18-28 points ABOVE (underpaying)
Medium	£12,000	72%	2-12 points above (slight underpay)
Large	£45,000	58%	2-12 points BELOW (overpaying)

Micro/Small Firms are underpaying for their cyber insurance:
- Insurers pay out £95/£88 for every £100 in premiums collected
- Only 5%/12% margin vs. needed 30-40% for sustainability

Large Firms are overpaying:
- Insurers pay out £58 for every £100 in premiums collected
- 42% margin vs. standard 30-40%
- Insurers making excess profit on large firm policies

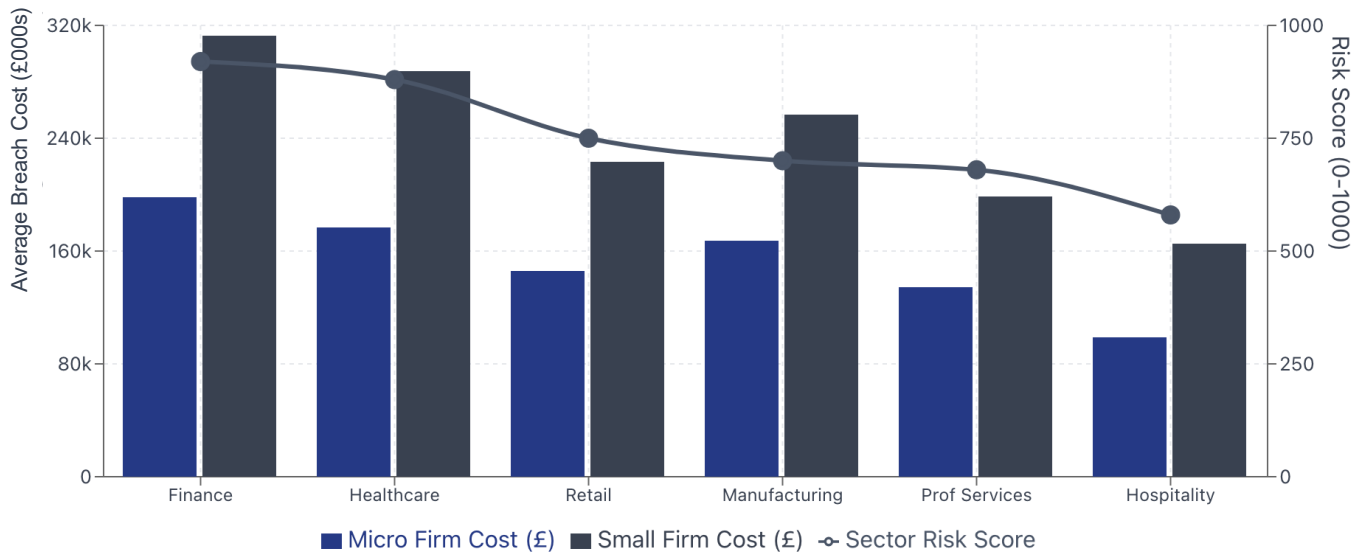
Medium Firms are OK:
- 72% loss ratio - roughly at market, slight underpayment

The truth is, micro/small firms literally cannot afford actuarially sound premiums, creating the protection gap.

909k SMEs (64%) have their cyber risks uninsured

Sector-Specific Risks

Breach costs and risk scores vary significantly by industry sector



HIGHEST RISK

Finance (920/1000)

High-value targets, regulatory exposure, data sensitivity. Micro firm avg: £198k breach cost.

ELEVATED RISK

Healthcare (880/1000)

Patient data breach penalties, ransomware targeting. Micro firm avg: £177k breach cost.

MODERATE RISK

Hospitality (580/1000)

Payment card data, lower digitalization. Micro firm avg: £99k breach cost.

- **One size fits all does not really work** - Cyber Essentials certifications government spends money and resources on helps but the magnitude of help varies in different industries
- Moreover, **not a single "big" certification** (ISO, SOC2) **is objectively considering a true context of industry and size** of organization (it is a checkbox).
- **CE and CE+** is great initiative however; it is **badly designed and realistically almost impossible for pass** without external help.
- When a business puts a CE (CE+) badge on their website and abandons cyber till next certification cycle the cyber risk does not go anywhere and they still suffer breaches.

The Now:

- With moving to “all digital” and becoming cloud-native and remote work enabled, the possible number of infliction points for SMEs goes through the roof.

- AI is complicating things for SMEs - a prohibitive cost of a targeted attacks that previously covered only large enterprise is going down to a cost of an AI tool monthly subscription and with lack of protection - SMEs become even more obvious targets.

- SMEs are targeted as entry points to larger enterprise. More than half of breaches in enterprise defences in 2023-24 were initiated through SME firms - and all of this - before the age of AI.

- Regulatory fines are escalating at 12% p.a., and, as we have seen on slide number 2, they are still going to lag behind the damage poor cyber defences do to the economy, to SME businesses and to each and every one of us.

The (not-so-distant) Future

- Regulatory pressure will increase: faster, machine-readable evidence to put a blame on a specific business that did not enable proper protection and automated enforcement (read- fines).
- Attackers will use everything AI-assisted. Attacks will be highly automated and hyper targeted.
- Automation in enforcement of reporting will be in place: regulators & insurers will expect continuous evidence of protection and compliance.
- Humans move up the stack: decision-making, exceptions, strategy - these will remain in the hands of humans. There will be extensive use of AI assistants in cyber (fight fire with fire).
- AI-enabled SaaS tools helping businesses tackle rising pressures from hostile external environment, government and regulators will dominate in cyber space.

- **It is not yet a "Terminator" but probably close to "Fight Club" and "Minority Report"**
- The EU's NIS2, DORA, and AI Act all explicitly require machine-readable evidence and continuous compliance demonstration. The UK's proposed cyber governance code follows the same pattern. SEC cybersecurity disclosure rules in the US are pointing in the same direction.
- We would argue that from what we see the only uncertainty is **pace**, not direction.

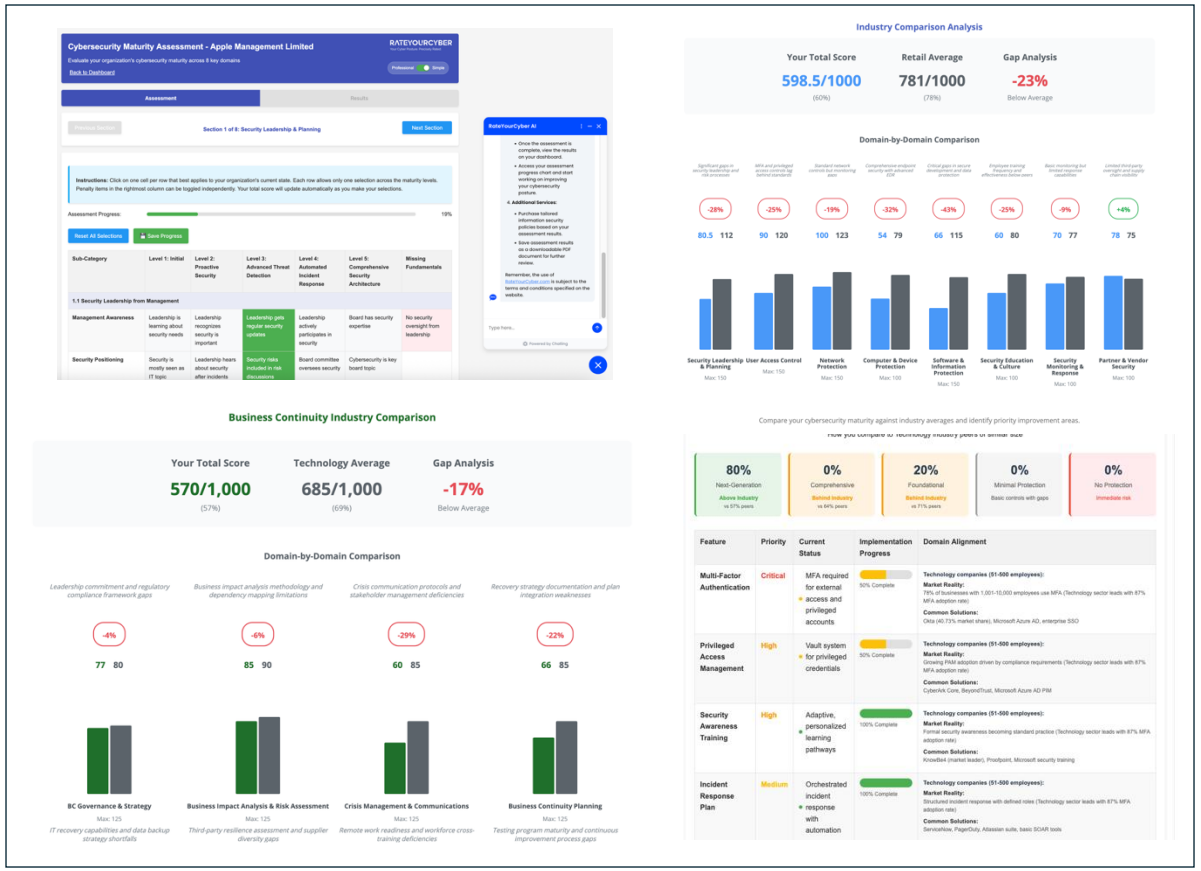
How RateYourCyber delivers fast, board-ready cybersecurity and continuity assessments

- **Patent-pending analysis**.
- **AI-assisted** assessments
- Scoring out of 1000 with **peer benchmarking** (same industry, infrastructure, size, regulatory regime - all together more than 10 factors considered)
- **Business case formulation**, ROI calculations and budget scenarios, success metrics and KPIs, governance structures suggestions.
- **Strategies and implementation guidance** with immediate steps, 90 days, 6 months and 3-year roadmaps developed
- **Dynamic, board-ready visuals and scorecards,** board-ready reports
- **Policies tailored to specific assessment results**, industry, size, governance and compliance requirements, and specific goals of organisations.
- **Plain-English toggle** for non-technical users.
- **Vulnerability scanner** for asset security monitoring.
- **Send to MSP functionality** for immediate implementation of proposed improvements.

- **N.B. Why have we added "Plain English" Toggle:**
- Medical Dictionary: 125,000 words
- Finance Glossary: 5,000-8,000 words
- Aircraft Manufacturing Glossary: 7,000-10,000 words
- **Cyber Security Glossary: 10,000+ words**

This is **RateYourCyber**

Risk Assessment Method/Size of the Firm	Data Points Considered, on Average	Cost	Average Time to Report
Traditional Consultants			
Small	550	£8k-£16k	1.5-2 weeks
Medium	850	£10k-£15k	2-3 weeks
Large	4,500	£50k-£150k	6-8 weeks
Enterprise-grade GRC tools			
Small	950	£6k-£10k p.a.	24-48 hours, tools require dedicated internal resources
Medium	1,400	£12k-£31k p.a.	
Large	1,850	£31k-£79k p.a.	
RateYourCyber			
Small	1,800	£3k p.a.	2-5 hours for complete assessment of all security and business continuity domains
Medium	2,300	£3k p.a.	
Large	Currently N/A	Currently N/A	Currently N/A



Fast, Easy to Understand, Board-Ready, Enterprise-Grade

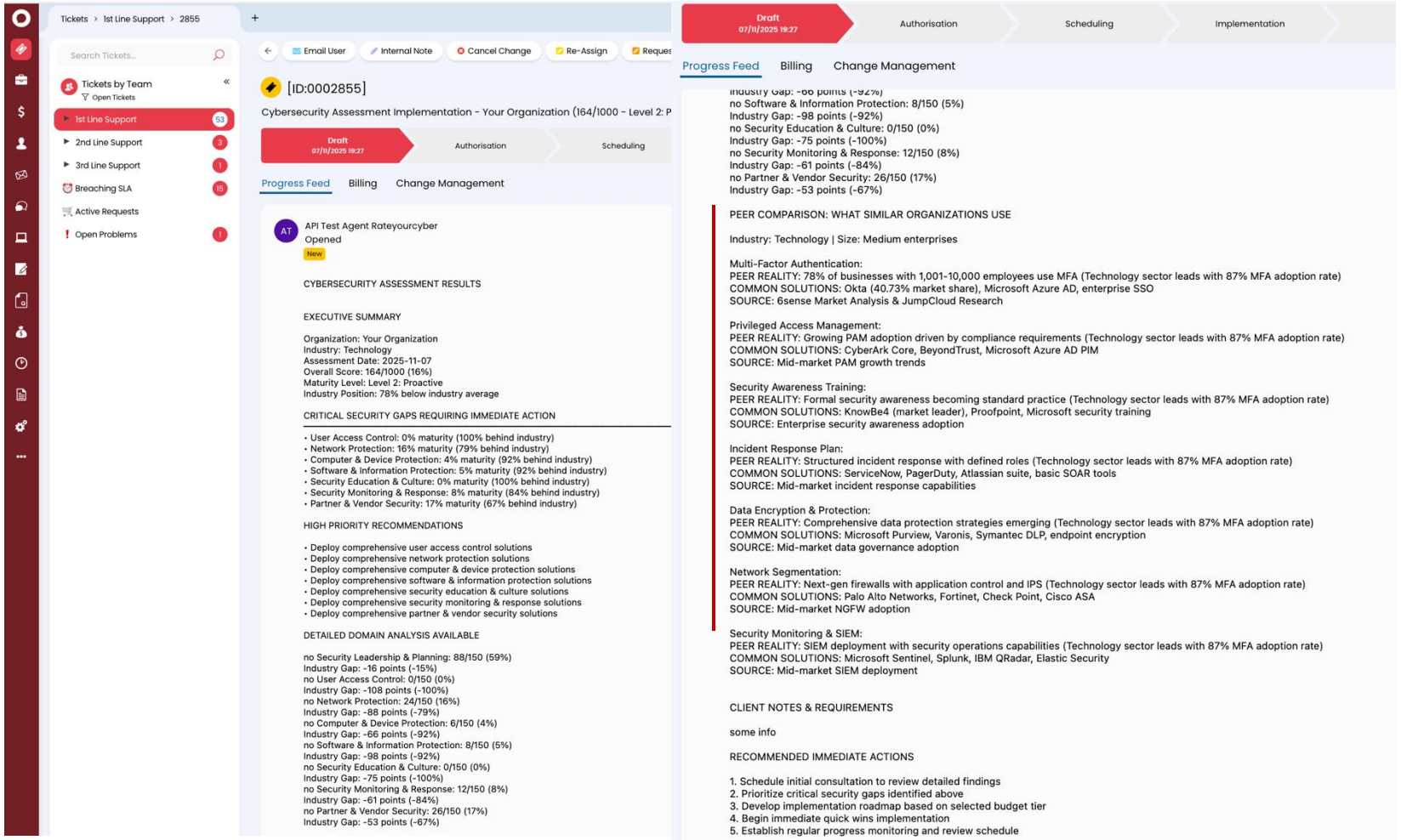
RATEYOURCYBER

Your Cyber Posture. Precisely Rated.

AI context | RYC | Halo+ RYC

Measurement and Analysis	Strategy	Governance	Policy Generation	Implementation	Integrations & Reporting
Cyber Security Assessments	Cyber and Business Continuity Security Strategy	Industry Average Maturity Score	Core Cyber and Business Continuity Policies	Journey to Industry Average	HALO PSA integration
Business Continuity Assessments		ISO 27001	Comprehensive set of 20+ policies covering major governance frameworks	Journey to ISO, SOC2, NIS, DORA Compliance	Automated Third-Party Reporting (Audits, Questionnaires), Integration and Automated Response on Data from Security Software and Data Sources (Dark-Web Monitoring, Threat Feeds).
Third-party Security Assessments		SOC2			
Vulnerability Assessments		DORA			
Physical Security Assessments	Infrastructure Security Strategy	NIS2			
HR Security Assessments					
Data Privacy Assessments	Data Security Strategy				

The new RateYourCyber + HaloPSA integration, enabling MSPs to instantly identify client gaps and recommend the right tools



- We are sharing with MSPs exactly the same information as we give to users when assessing their feature maturity against industry peers.
- MSPs will also be aware of what is the approximate budget that users would like to allocate to improve their cyber security posture and reach industry standard levels.
- It is a tool that allows users to get professional help from companies that can do that most efficiently. It also helps MSPs with increasing the share of the wallet of a customer and reducing headache from dealing with cyber incidents.

Thank you.

Contact:
Website: https://rateyourcyber.com

Looking forward to working with you.