

Threat Detection for Financial Services:

Rejuvenating Cyber Defence Strategies for an Experienced and Fast-Moving Sector.



Table of contents

<u>Foreword</u>	3
<u>Introduction</u>	4
<u>Suppliers are underperforming and failing to alleviate CISO burn-out</u>	5
<u>Why are providers unfit for purpose?</u>	7
<u>Hybrid teams are the most effective</u>	9
<u>Navigating the challenges of locked-in cyber contracts</u>	11
<u>Looking ahead</u>	13
<u>Research Methodology</u>	15
<u>Why e2e-assure?</u>	16

The life of the CISO isn't going to get any easier in 2024, as organisations across all sectors contend with rapidly evolving extortion techniques such as phishing, ransomware, and supply chain attacks to invade internal networks. e2e-assure's recent study* shows there is a genuine cause for concern for the Financial Services industry, as nearly half (44%) of organisations in the sector believe their current set-up is underperforming, making it one of the highest underperforming industries when compared to Healthcare, Professional Services and Manufacturing.



Given its access to sensitive information, the industry will always be highly vulnerable to cyber attacks. A strong relationship with providers is integral to cyber resilience, especially for fast-moving Financial Services organisations that rely on technology such as online banking, apps, and electronic trading systems. When an incident or breach occurs, collaborating with providers can enhance an organisation's response capabilities, offering rapid assistance and plugging gaps that could be missed by an in-house team working alone.

As an industry that has been under threat from cyber attacks for a long time, many Financial Services organisations will have access to the cutting edge of technology and, therefore, stronger internal cyber security postures than organisations operating in other sectors. Providers need to be offering genuine value if these well-prepared Financial Services organisations are going to keep operations with them, rather than move security in-house.

At e2e-assure, we have been working with Financial Services firms to shore up their cyber defences for the past ten years and are repeatedly called upon to help in the aftermath of an attack. But we need to consider the provider's role before an attack, to prevent it completely. Particularly those that are using legacy technology, which is more difficult to protect.

So, how are providers failing Financial Services organisations? And what questions should the industry be asking of their providers, to drive better resilience for an industry forever vulnerable?

Rob Demain
CEO e2e-assure

Introduction

33% of Financial Services organisations that outsource do not feel confident in their organisation's ability to act and respond to security incidences within 30 minutes of detection.

33%

of Financial Services organisations that outsource do not feel confident in their organisation's ability to act and respond to security incidences within 30 minutes of detection.

Only
14%

said that their provider was exceeding their expectations. 39% said their provider was performing ok but that there was room for improvement.

For Financial Services organisations, there are no signs that cyber security attacks will relent in 2024.

According to ICO data breach reports, cyber security breaches for UK Financial Services organisations have tripled since 2021. Digital transformation has led to increased cyber security issues as organisations push forward with technological solutions but fail to consider the cyber security implications of these tools.

Our survey reflects this too, revealing that the majority (77%) of Financial Services

organisations have experienced a cyber attack, which is higher than the average across industries at 75%. Only 26% of the CISOs and cyber security decision-makers in the Financial Services sector who took part in this study describe their organisation as resilient.

Those that fully outsource their cyber operations in the Financial Services sector are faring the worst compared with other sectors, with almost half (44%) stating that they are underperforming and looking to make changes. This compares with an average of 37% across all industries.

In this paper we explore the key areas for improvement and how Financial Services organisations can challenge their security provider to create more resilience and provide greater ROI.

Chapter 1

Suppliers are underperforming and failing to alleviate CISO burn-out



For Financial Services organisations, the key reason they outsource is speed (46%). A rapid response to cyber threats for this sector is integral. If they fail to protect their customers' data and information, this can result in mistrust from both existing and prospective clients, ultimately leading to a loss of business.



28%

organisations saying their provider is escalating too many false positives

33%

stating that they do not feel confident in their current cyber security operations' ability to act and respond to alerts within 30-minutes

A provider that can rapidly respond to cyber threats can also help to alleviate the burnout that is prevalent among CISOs. But with 44% of those in the Financial Services sector saying that their providers are underperforming and are looking to make changes, it seems there is more to do before they are properly supporting overstretched teams.

Providers are lacking accuracy, with 28% of organisations saying their provider is escalating too many false positives.

This lack of control is being compounded by the fact that 40% said they don't have but desire real-time visibility of reporting dashboards which show up-to-date cyber posture.

As a result, organisations are lacking in confidence, with over a third (33%) stating that they do not feel confident in their current cyber security operations' ability to act and respond to alerts within 30-minutes. As a result, only 30% of Financial Services organisations that fully outsource feel resilient.

Chapter 2

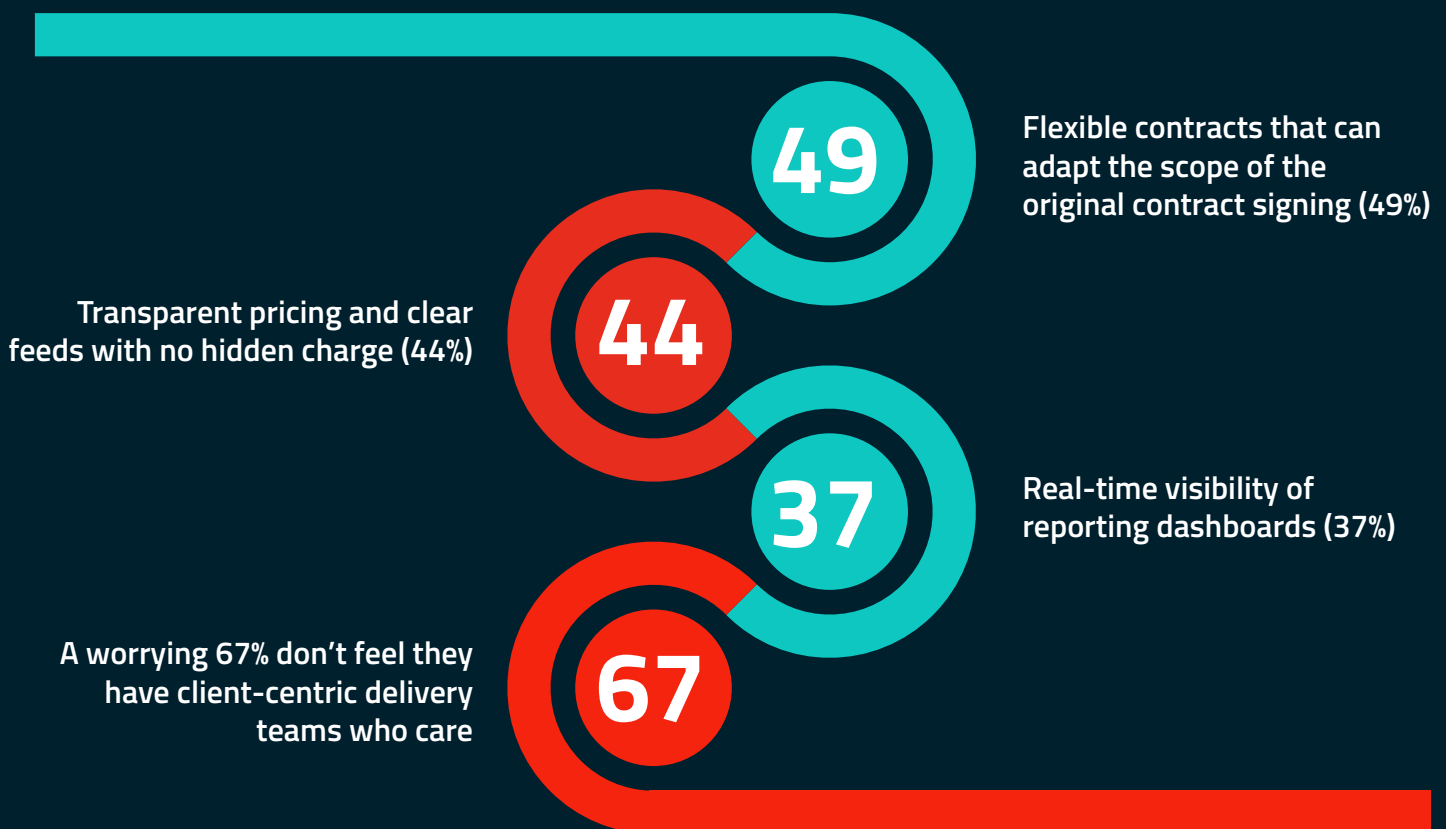
Why are providers unfit for purpose?



A cyber security provider should be able to reduce risk using tactics such as threat intelligence, to pre-empt and disrupt attackers prior to execution.

Our survey revealed, however, that Financial Services organisations that fully outsource their cyber security operations are unconfident because although threat intelligence is being used, it has had no measurable positive impact (42%) or that threat intelligence has simply not been implemented (7%).

The majority of those that fully outsource don't have but desire:



Contracts are also not covering the full scope of needs, and clients are continuously having to bolt on extras (40% of those that fully outsource) meaning it's difficult for them to scale and leaves organisations vulnerable to security threats as they evolve and advance.

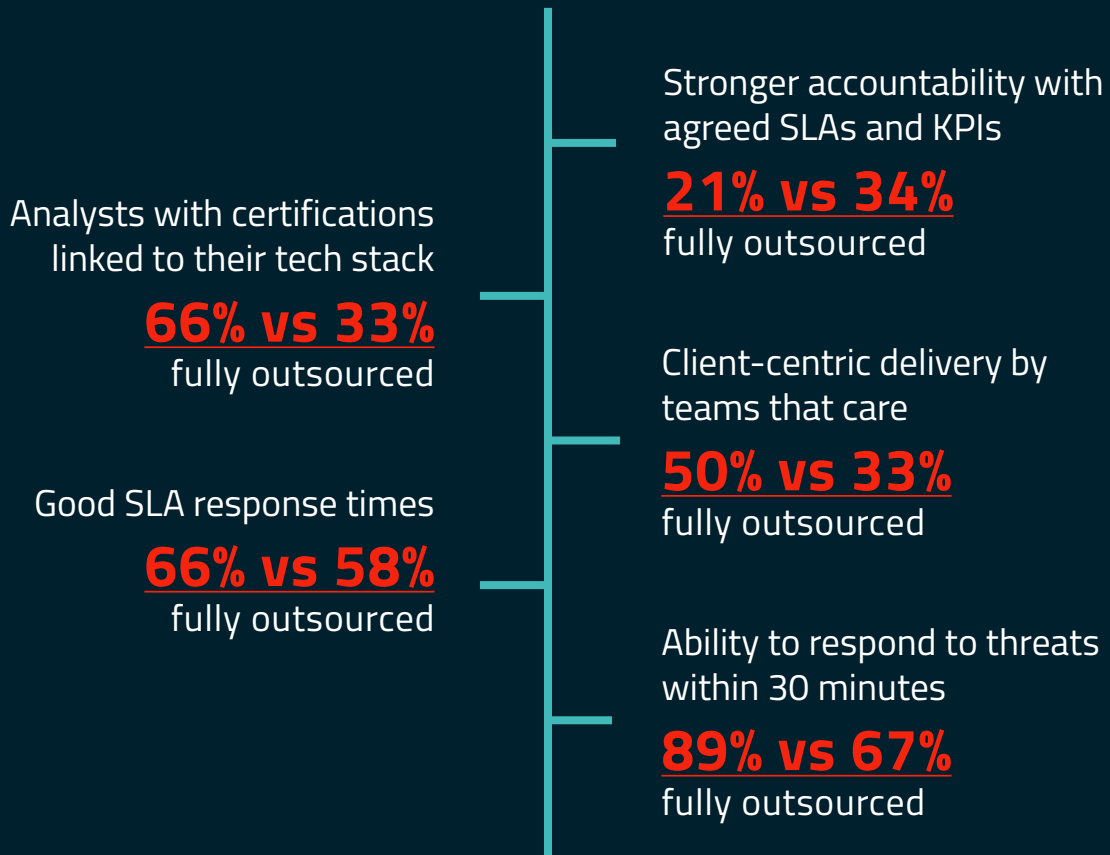
Chapter 3

Hybrid teams are the most effective






The Financial Services sector is the second most likely industry to outsource (45%) but when asked 'When next procuring cyber security operations what will you be looking for?' over a third (32%) said they'll be going hybrid, while more than one in five (21%) said they will be looking for specialist expertise in specific areas.

Why? Hybrid teams already provide:



When we asked about their specific priorities, CISOs in Financial Services organisations are looking for:

-  Speed (46%)
-  Control (40%)
-  Resilience (34%)

But the results of our survey suggest that outsourced providers are lagging behind hybrid teams in providing CISOs in the Financial Services sector with the clarity, precision and control they need.

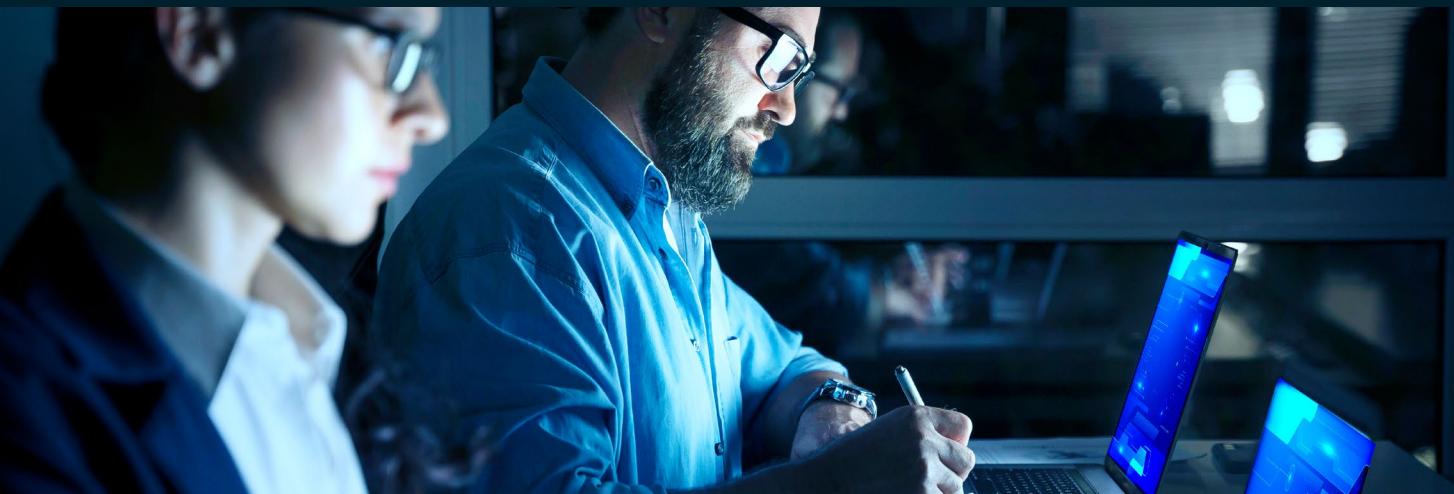
Chapter 4

Navigating the challenges of locked-in cyber contracts



Security moves fast. While long contracts allow for predictable costs, they can also tie teams into a set of terms that do not adapt to their changing cyber security needs over time. The result is often the need to bolt on new security options. This is not ideal as the process of onboarding can be expensive and clunky, therefore restricting their agility.

The fact that providers are not implementing proactive measures such as threat hunting, is also problematic. In the face of rapidly evolving cyber threats, teams need to implement proactive measure and be able to act fast.



Despite disappointment in the performance of their providers, the majority of Financial Services organisations that outsource said they would be happy to relinquish more control in return for



quicker decisions (67%),



faster response times (60%),



less reliance on in-house skills (72%).

This suggests that factors such as proactivity and ownership play a key role in CISO disappointment and highlights a missed opportunity for providers who could be doing more to support their clients.

It's clear that there is a need for a critical shift to ensure cyber defence quality meets the needs of Financial Services organisations in 2024. So, what are the key provider attributes organisations should be looking for when they next procure, to create resilience and drive greater ROI?

Chapter 5

Looking Ahead

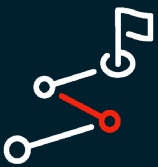


The form and sophistication of today's cyber threats are changing from moment-to-moment. This means Financial Services organisations need to be monitoring and ready to respond, moment-to-moment. This report shows a real desire and need for Financial Services organisations to work collaboratively with their providers, to achieve this.

There are three clear initial steps organisations can take to drive greater performance from their providers; opening an honest conversation about more flexible contracts, pushing for closer integration so providers can better understand an organisation's environment and spearhead plans, and making proactive and demanding more up-to-date, accurate reports to drive quick decision making.



Moving forward, flexibility will play an integral part in a company's cyber defences. Long fixed contract terms without a clear road map will cause organisations to become increasingly vulnerable as threat tactics evolve. It's important to have frank conversations with providers at the start of the contract to determine if they will be willing to adapt the contract based on a company's needs as they change and evolve.



Providers need to integrate more closely with internal teams, take on more responsibility and accountability, and make the time to truly understand customers' environments. Providers should spearhead cyber defence roadmaps and lead CISOs in the Financial Services sector through the evolving landscape. Providers should be able to provide clear road maps to evolve the security posture of an organisation rather than pushing continuous bolt-ons.



Quick decision making on alerts will be a key priority for Financial Services firms going into 2024. As one of Financial Services organisations' key frustrations, a lack of threat hunting capabilities will mean organisations fall behind in their cyber defences as cyber attacks continue to advance. Key processes that providers should be carrying out include continually validating analytics to ensure that threat data is accurate and tracking emerging threats and vulnerabilities using proactive measures such as **Attack Disruption**.

What are the key, critical questions Financial Services organisations should be asking their security providers today, to drive improved performance?



How will you demonstrate that you've made our organisation's cyber security provision more resilient?

By tracking emerging threats utilising an Attack Disruption approach while deploying threat intelligence and alert tuning, your provider should be able to eliminate false positives and improve detection and response times.



Can you measure how long it will take to contain a compromised account?

Your provider should be able to give clear KPIs including the mean time to detect and contain, and how long it takes to neutralise an incident when threat intelligence is utilised.



How will you provide more visibility of our security stance?

Your provider should be able to provide clear reports that allow you to document, respond and learn from attempted breaches.

Research methodology*

The research was conducted by Censuswide, on behalf of e2e-assure, surveying 95 CISOs and cyber security decision-makers from within Financial Services companies with between 500-5,000 employees. Censuswide abides by and employ members of the Market Research Society which is based on the ESOMAR principles.

Why e2e-assure?

e2e-assure is a UK based Threat Detection and Response company that gives you the advantage in protecting your business against cyber threats.

We abstract away unnecessary complexity from the communication channels and empower your teams with clear, understandable and actionable knowledge.

Our drive for innovation is focussed on continually reducing the friction, time and cost of protecting your business against cyber criminals. We are meticulous in applying cutting edge technology capabilities to solve real business problems and ensuring that only high value signals gain attention and distracting noise is eliminated.

We give you back time, budget and headspace to reflect and plan security improvements in a careful and considered manner.

During the 10 years that e2e-assure has been protecting businesses of all types and sizes, we have observed the challenges that Security and IT teams face in addressing competing demands with overstretched budgets, resources and time.

Our response to that challenge is not to overlay more tools, processes and contracts over your existing security operation. Instead, we inject value into what you already have, and reveal the benefits of your security investments in a manner that is understandable to your business peers.

Our commitment to customer excellence is not just about ensuring your business is protected to the highest standards, it is also about giving you a clear and simple path to getting the basics right without creating additional complexity or unnecessary overhead. We offer you three simple promises: **Clarity. Precision. Control.**

[Contact Us](#)