In the Shadows

Poor visibility of complex IT infrastructure leaves businesses vulnerable

QUOD ORBIS

Contents

Foreword

The biggest challenge facing every security team is the unpredictable nature of the industry. Hours are spent implementing a solid security strategy, only for it to be completely disrupted by unprecedented events. This forces businesses to take somewhat of a reactive approach, which leads to greater investments.

As a result, businesses have added layer upon layer of technology to address every evolving security threat. This piecemeal approach however, while seemingly pragmatic, has created an unwieldy and opaque tech stack. The burden of this complexity falls squarely on the shoulders of Chief Information Security Officers (CISOs) and their teams, who fight on the front lines.

Their challenges are seemingly endless; as well as maintaining 360-degree defence for the organisation, CISOs are also responsible for reporting back to the board, translating security into an accessible language for non-technical individuals. But one of the major concerns is a lack of visibility across their infrastructure.

Quod Orbis' independent research study shines a light on the true challenges that CISOs face in maintaining a robust security strategy, and reveals that a greater focus needs to be on functionality, rather than simply technology in order to keep up with the rigorous demands of the environment.

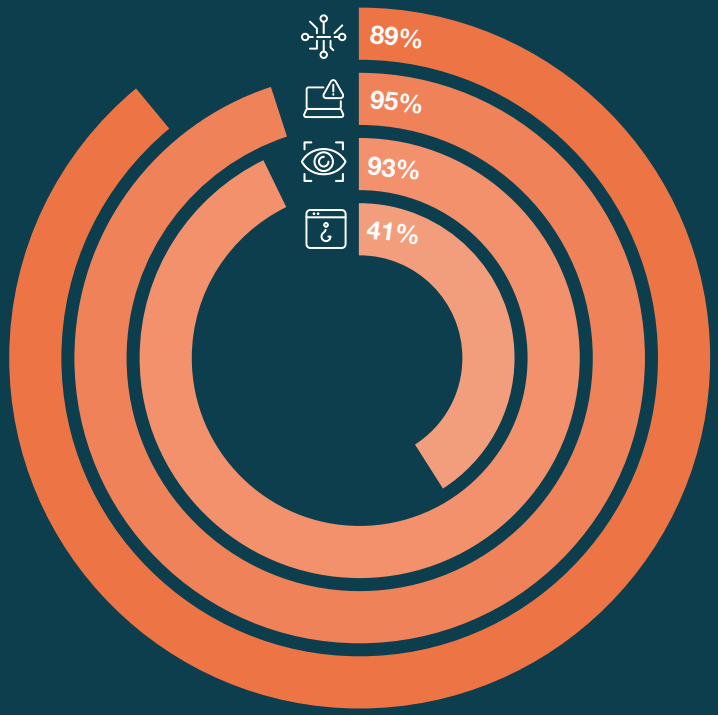
Martin Greenfield
CEO at Quod Orbis

Executive Summary

Quod Orbis commissioned a research study with international research house, Censuswide, to poll 500 board executives and IT decision makers across enterprises of 500+ employees in the UK.

The lack, or false impression of consistent visibility of all assets, controls and technology is leaving organisations unnecessarily exposed.

Exposure is lurking in the shadows.



89% of security professionals are familiar with Continuous Controls Monitoring

95% of businesses have not been able to easily access a specific digital asset* in the last year

However, 93% are confident they have clear visibility of assets despite admitting to not being able to access them easily

Lack of technology is the biggest challenge of maintaining a robust security posture, according to 41% of IT teams

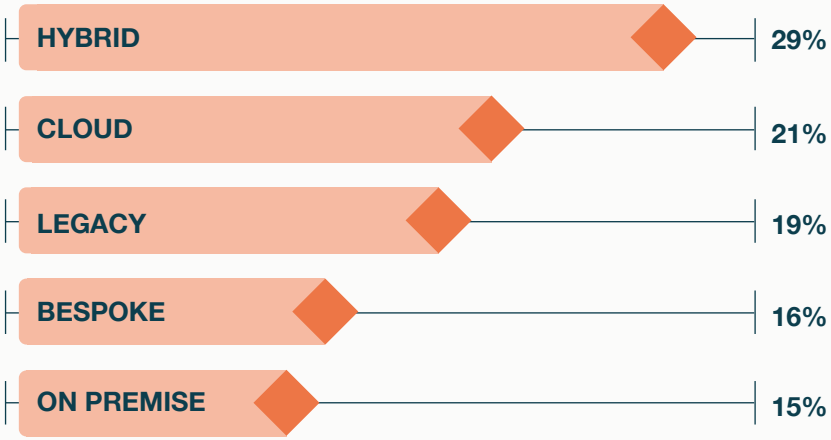
Through greater visibility and assurance, organisations have an opportunity to improve their operational resilience

Defined for the purpose of this report as any type of data that is stored electronically and has value.

\\ 01 Battling with Complexity

Modern business infrastructure is a complex labyrinth of critical assets, connections and endpoints. We've come a long way since the days of massive, cumbersome mainframe computers, but this transformation brings with it equally substantial security challenges.

Modern IT environments



19 **The average IT team manages 19 security solutions at any one time.**

Of the businesses polled, the average IT team now manages 31 endpoints* per person across the entire organisation. For a 1,000-person company, that's over 30,000 devices. To put that in perspective, imagine being responsible for the security of a building that has 30,000 lockable windows. That means checking roughly 100 windows across 300 floors.

The speed at which new threats emerge results in rapid investments to upgrade security systems. In this instance, speed often outweighs strategy. Thousands of pounds have since been invested in 'state of the art' security solutions, however these were often sold to businesses on empty promises. Now the average team manages 19 security solutions at any one time.

**Defined for the purpose of this report as any digital device connected to the company's network.*

41%

Despite businesses housing so many solutions, 41% still report a lack of technology as being their biggest challenge when it comes to maintaining a robust security posture. Existing solutions are clearly not doing the job businesses need them to do.

With existing solutions clearly so ineffective, businesses shouldn't be looking to expand their tech stack, but instead need to replace obselete technology.

"This is a clear example of how rash investment in technology has not done the trick. Businesses report an unwieldy number of tools, yet 39% still lack actionable data. Why: because the technology isn't doing what these teams need it to. To truly extract value from the insights derived from their systems, businesses need a tool that contextualises the data."

Martin Greenfield, CEO

Almost half (47%) of larger organisations report a lack of technology as a serious issue. However, given they face greater budgetary constraints than smaller businesses, the issue remains unaddressed.

All technology investments should provide teams with real-time insights that fuel ongoing and future strategies.

However, 39% of businesses currently report a lack of actionable data.

CISOs in particular struggle with this challenge (40%) due to limited visibility over digital infrastructure. While the majority of IT decision makers (93%) feel confident they have the necessary tools to address this, 95% have not been able to easily access specific digital assets in the last year.

Are IT teams settling for the degree of visibility they currently have, or should they be striving for more?

Organisations with more than 1250 employees have less confidence in their existing tools (88%). It's therefore unsurprising that the same respondents struggled the most to access their critical assets (97%). Larger organisations are more likely to have bespoke and legacy technology, leaving them with the lowest visibility of their systems (79%) compared to other business sizes.

Inaccessible assets, limited system visibility and declining confidence in their tools: the perfect storm is brewing for security teams.

95%

95% of businesses have not been able to access a specific digital asset in the last year.

Across all businesses, nearly four in 10 (38%) rank a lack of visibility as a big challenge.

>1250

Organisations with more than 1250 employees express the least confidence in their existing tools.

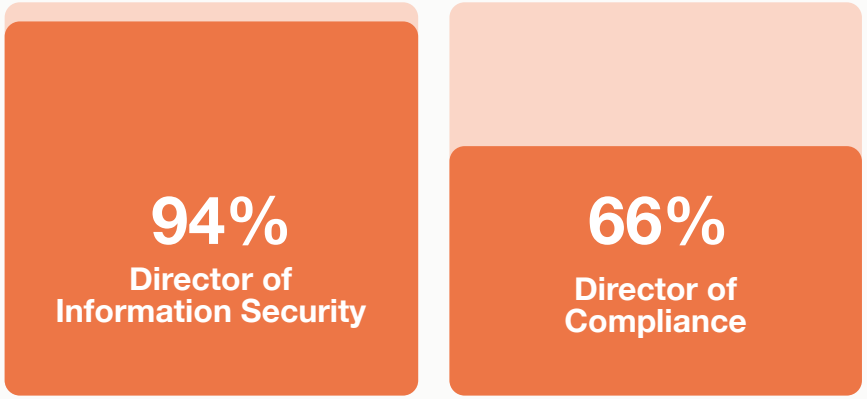
18%

Collectively, 18% of IT decision makers do not believe that visibility will improve their processes.

"Businesses are suffering from a blind spot that's leaving them exposed. Misplaced confidence in existing security tools means these organisations are susceptible to data breaches and non-compliance fallout with potentially crippling financial and reputational consequences. The disconnect between confidence and tangible output signifies a need for a paradigm shift."

Martin Greenfield, CEO

Research also shows that senior compliance staff tend to have less confidence in their system visibility than technically orientated employees.



The enormous gap between respondents' perceptions and the reality of their situation is staggering. Teams lack actionable data, they're frequently unable to find critical assets and some even admit to not having the right level of visibility. Yet nearly all of them are confident they have the tools to overcome this challenge.

\\ 02 The CISO-Boardroom Gap

Establishing smooth communication channels between the technical and non-technical individuals within an organisation is a long-standing issue. The two sides quite literally speak different languages, and in absence of a Google Translate equivalent, misalignment often occurs.

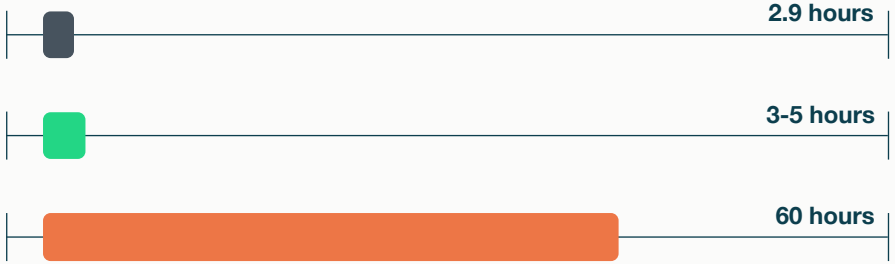
CISOs are tasked with reporting the business' security status to the board as frequently as deemed necessary – sometimes quarterly, sometimes monthly.

85%

85% agree that the time it takes to prepare a board pack is a drain on a team's resources.

The larger the organisation, the more they feel the resource drain from creating board packs.

Time investment per person



\\ It takes the average IT decision maker 2.9 hours to prepare a report for the board.

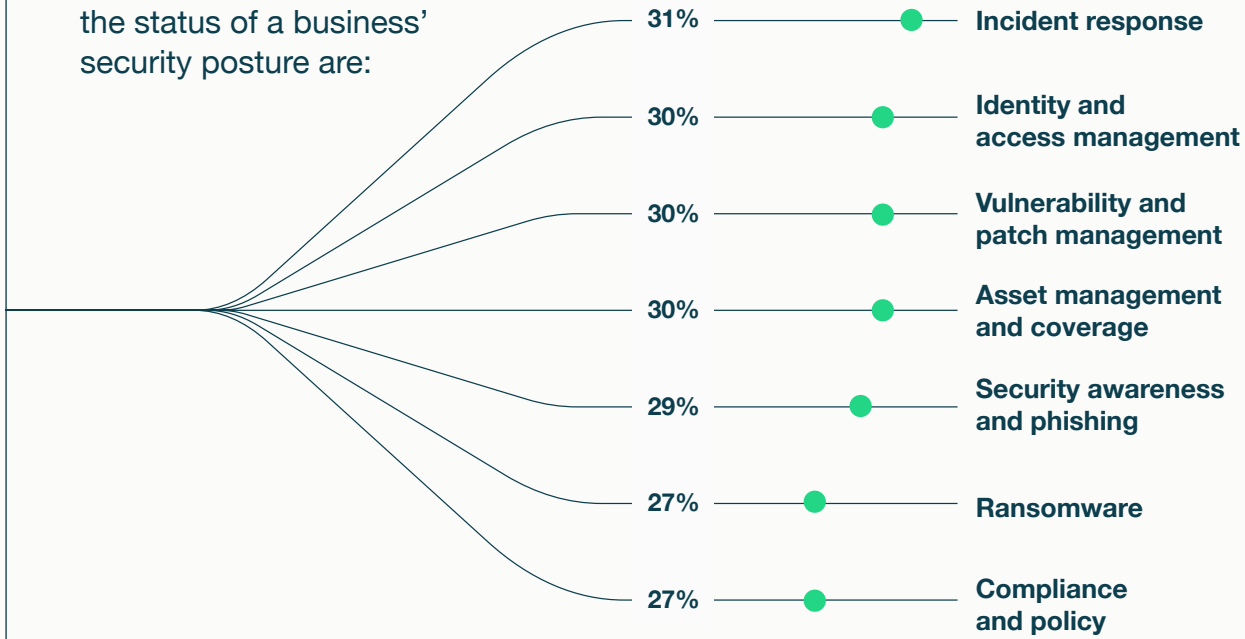
\\ Over a third (35%) spend anywhere between 3 and 5 hours

\\ Based on monthly board meetings, this equates to as much as 60 hours in a year

How many people help create your board reports? Based on these numbers, how might this time be better spent if the process became more efficient?

Once organisations define the metrics required to measure their security posture, operational teams must then gather the relevant data from varying technologies across the business. However, more technology causes convoluted systems and data, resulting in greater challenges for CISOs when reporting to the board.

The metrics used to report the status of a business' security posture are:



*Regardless of company size, all metrics are reported on evenly.
**Respondents were able to select all that apply.

Every organisation faces the same threats – be it ransomware, phishing or DDOS to name a few – yet we see a huge difference in the approaches taken by businesses to monitor these threats.

33%

All metrics are used by less than a third of organisations.

44% **38%**

Larger organisations favour identity and access management (44%), and smaller organisations favour asset management and coverage (38%).

31%

CISOs themselves rank asset management and coverage metrics and incident response as joint top (30%).

Boardroom Blunders

Despite 89% of security professionals stating they get satisfaction and clarity from board feedback regarding their IT security strategies and initiatives, some still receive worrying comments from executives:

That it is just about protecting financial information but not personal and sensitive data.

Our employees are smart, they won't fall for phishing scams.

'Cyber security': isn't that just a fancy world for antivirus software.

Why do we need to invest in cyber security when our company doesn't have anything worth stealing?

I heard that hackers only target big corporations so we should be aware but no need to invest much in this kind of security.

Can we just install some antivirus software and we're good to go?

Can't we just tell our employees not to click on suspicious links?

Miscommunication is deadly. It leads to inadequate security budgets, delayed response times to threats, and ultimately, a higher chance of costly data breaches. CISOs are often trapped within a toxic cycle.

They need business buy-in to support cyber security strategies, which means investing in technology. However, in order to sufficiently demonstrate the current security posture to highlight the need for that investment, they must be able to extract insights and translate cyber risk into business objectives – for which they need tools to do so.

\\ 03 Making the *Right* Investment

CISOs and their teams are crying out for more visibility across business infrastructure and the critical assets that reside within. More than eight in 10 (82%) agree that greater visibility over digital assets will significantly improve business security – and the larger the organisation, the more they believe this to be true. However, 93% of respondents claim their businesses already provide them with the necessary tools to do so.

Are IT teams settling for less than complete visibility? Or is there a better way?

Budgets are a common impediment to innovation. Despite 86% of IT decision makers claiming they are 'completely satisfied' with the budget allocated to cyber security, over a third (37%) report budget as one of the biggest challenges that they face. Perhaps there is an underlying acceptance of current budgets, rather than pushing for more.

There is a significant perception gap yet again across organisations, and a general lack of awareness at play, of what other options are available when it comes to investing in security solutions.

82%

agree that greater visibility over digital assets will significantly improve business security.

93%

believe their businesses already provide them with the necessary tools

The confidence felt by organisations in their tools is hugely undermined by their desire for greater visibility. It's time to stop settling, and start facing reality.

Promisingly, almost three quarters (72%) of IT teams have had their IT budget increased in the past 3 years. However, businesses need to break free from the typical cycle of throwing money at a problem and hoping something sticks.

It's not about the biggest investment, it's about the right investment.

While it's clear that upcoming investments are fairly evenly spread across different areas of security, there are a few red flags.

26% **26% of IT decision makers are yet to allocate budget to basic security tools like asset visibility technology.**

At the same time, businesses clearly recognise the advantage of implementing the right technology. Automation in particular is widely adopted for its numerous use cases; for IT decision makers, this technology will help accelerate document creation (38%), pull together board packs (37%), and free up time to assess other aspects of the business' security posture (36%).

Other areas of improvement include reducing the risk of human error (35%) and enhancing confidence in the accuracy of data (35%).

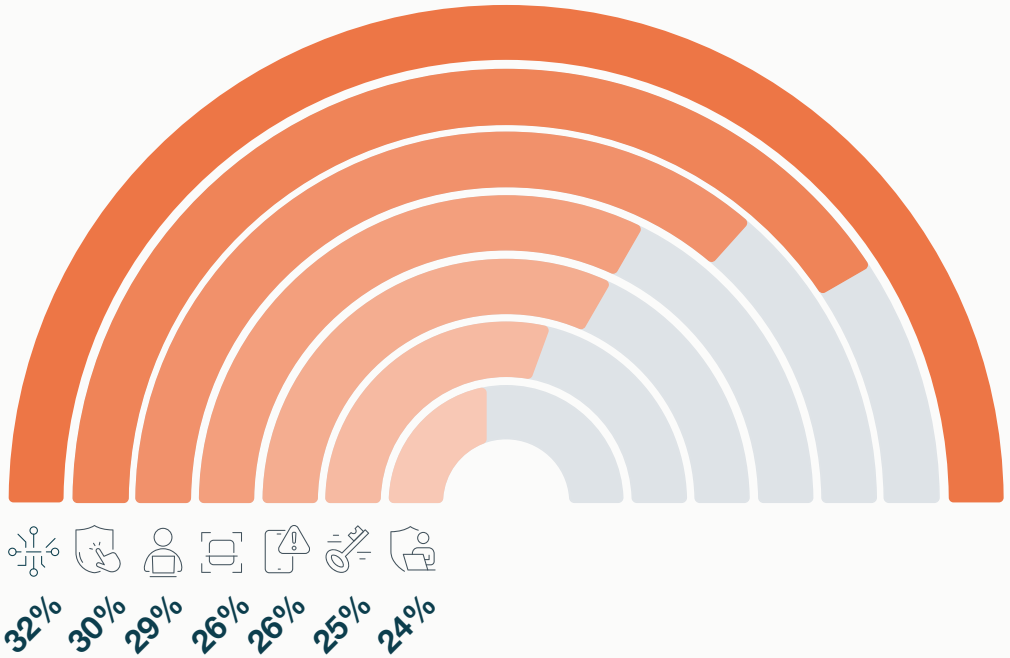
Automation use cases for IT decision makers:

35% **Enhance confidence in the accuracy of data**

37% **Pull together board packs**

36% **Free up time**

Where will increased budgets be allocated in the next year?

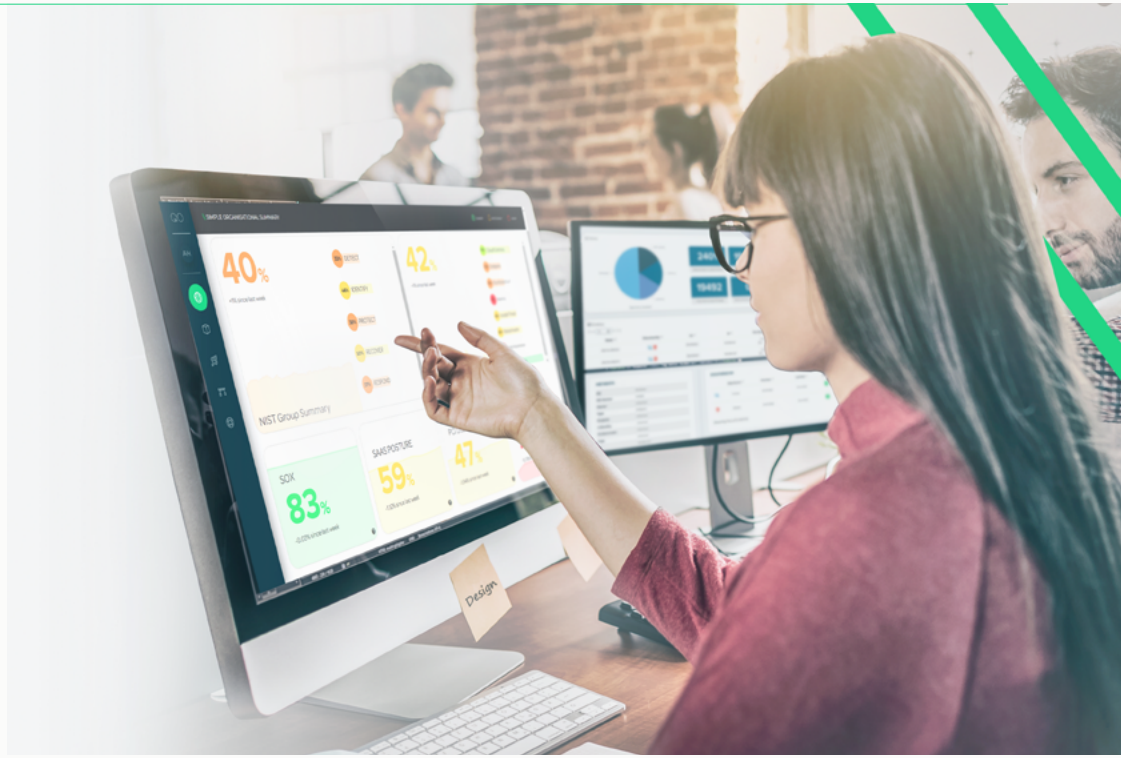


- **Continuous Controls Monitoring**
- **Privileged and identity access management**
- **Zero trust**
- **Asset visibility technology**
- **Disaster recovery solutions**
- **SOC compliance**
- **GRC**

With such a small discrepancy among the solutions being explored, it's clear that there's no consistency as to where the gaps lie from one organisation to another. Perhaps that's why Continuous Controls Monitoring came out on top.

\\04 The Rise of Continuous Controls Monitoring

Sitting at the top of organisations' investment strategies is CCM (32%). Powered by AI and automation, CCM allows you to connect to your business ecosystem and see and understand your security risk and compliance posture in near real time - it unites the disparate tools within an ecosystem.



Gartner's Hype Cycle for Cyber-Risk Management 2024 reported CCM's market penetration as 1% to 5%. Since then our research has revealed that 32% of IT teams would allocate increased budget to CCM in the next twelve months.

The strong value proposition of CCM suggests that with the right resources, its market penetration could grow significantly.

Businesses of all sizes believe automation will reduce the risk of human error. With it, businesses can continuously monitor key systems and data in real time, which in turn increases operational resilience and effectiveness, automates compliance assurance and helps mitigate cyber risks.

CCM platforms adapt with your organisation, allowing you to track assets, measure KPI's, manage a set of controls, and align with regulatory frameworks. This is the level of performance and visibility that organisations should be striving to achieve – anything less is not sufficient for today's threat landscape. It's this proactive approach that increases operational efficiency at reduced cost.

"CCM delivers a single source of truth. It helps teams see and understand their security and risk posture in real time, giving them peace of mind that all of their data is relevant and up-to-date. This level of insight provides early awareness of potential problems and empowers teams to take a proactive approach to security, instead of being forced back into the same reactive position they've been in for years. After all, now is not the time to gamble with your company's security."

Martin Greenfield, CEO

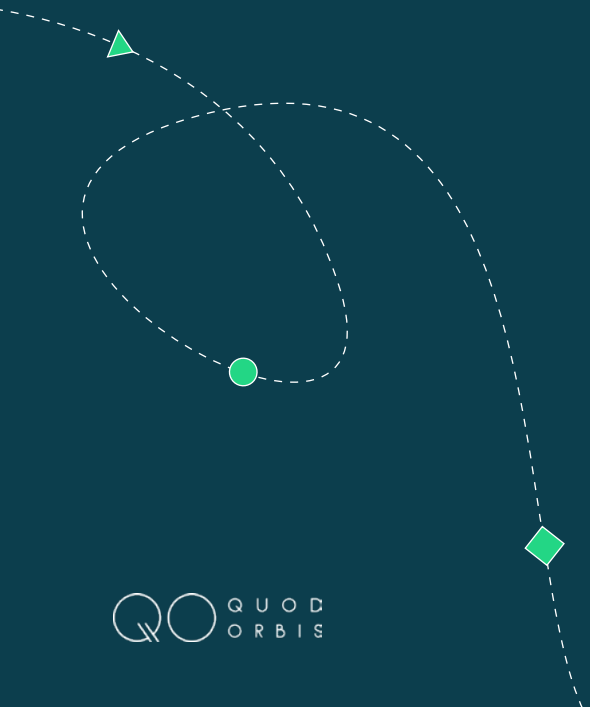
Strengthening cyber security posture is an ongoing process that demands continuous adaptation and improvement. As the scale and sophistication of cyber threats continue to grow, it is imperative that businesses prioritise visibility and real-time insight as a critical component of their overall security strategy.

For almost all businesses (95%), digital assets are left hidden in the shadows. Tools like CCM are built to provide comprehensive, real-time visibility, bringing them back into the light.

About Quod Orbis

Quod Orbis is the single source of truth across security, risk and compliance, providing an orchestration layer for the entire tech stack whether in the cloud, on-premise, legacy or bespoke. Founded in 2018, Quod Orbis became part of Dedagroup, one of the leading Italian IT players, in 2024.

A pioneer in Continuous Controls Monitoring (CCM), Quod Orbis provides complete and constant visibility into a company's cyber security, compliance and risk posture. Quod Orbis' ability to connect with every piece of technology within a business, unrivalled automation capabilities and continual support enables the company to serve a global client base across a wide variety of industries.



QUOD ORBIS

Contact Details
www.quodorbis.com
contact@quodorbis.com

Tel:
+44 (0)203 9622206

Office Address:
5th Floor,
72 King William Street,
London,
EC4N 7HR

Registered Office:
5 Technology Park,
Colindeep Lane,
Colindale,
London,
United Kingdom,
NW9 6BX