



Qwil Messenger

Convenient, compliant, and secure chat between the business, its clients, and partners



Table of Contents

.....	1
About this report.....	3
Highlights:	3
• Qwil Messenger now has over 2,000 firms using Qwil with their clients, with the majority in financial services.....	3
The business context for Qwil Messenger	4
Key drivers – Security, privacy, financial risk, and client convenience drive the need for Qwil Messenger.	4
The convenience of instant messaging comes with risk.....	5
Qwil Messenger - the story so far.....	5
Three co-founders established Qwil Messenger in 2017	5
Qwil Messenger - a platform by design to provide client convenience, privacy, and security	6
The market for Qwil Messenger has expanded beyond large financial institutions.	6
Solution overview.....	6
Security goes beyond the technology and is core to the way the organization is managed	7
Current position	8
Qwil Messenger now has over 2,000 customers, with the majority in financial services ..	8
Pricing is attractive irrespective of company size.	8
Future direction.....	9
What to expect	9
Oracle Cloud Infrastructure and Oracle support program prove their value to Qwil Messenger.	9
CX-Create's viewpoint.....	9
Customer experience and security are critical concerns.....	9
Summary details	9
Appendix	10
Further reading.....	10

About this report

Based on interviews with the company director and Chief Revenue & Financial Officer Laurent Guyot and additional secondary research sources, this report provides an overview of [Qwil Messenger](#), its genesis, and its current position in the secure, compliant messaging field between businesses, their clients, and partner ecosystems.

The company, founded in 2017 by three individuals steeped in financial services, has developed a secure and compliant messaging platform used by many wealth managers and professional firms concerned about delivering a positive client experience without compromising security or regulatory compliance.

The theme for this month is around startups in the finance sector and how they are innovating and changing the competitive landscape. Qwil Messenger, headquartered in London, has made rapid progress in a relatively short time. Not just in the financial sector but wherever there is a need for proven secure, compliant, and confidential business-to-client communications.

CX-Create is an independent IT industry analyst and advisory firm, and [Oracle](#) sponsors this report.

Highlights:

- Key drivers – security, privacy, financial risk, and client convenience drive the need for Qwil Messenger
- Qwil Messenger - a platform by design to provide security and convenience
- Qwil Messenger now has over 2,000 firms using Qwil with their clients, with the majority in financial services
- Oracle Cloud Infrastructure and Oracle support prove their value to Qwil Messenger

The business context for Qwil Messenger

Key drivers – Security, privacy, financial risk, and client convenience drive the need for Qwil Messenger.

Cybercrime impacts every type of business and potentially any individual with internet access, and it is increasing.

According to Alessandro Profumo (CEO of defense industry company Leonardo S.p.a.), opening the Cybertech Europe 2022 conference in Rome, the global cost of cybercrime in 2021 exceeded \$6trillion, double the 2015 estimate. In a Cybercrime Magazine report in November 2020 by Steve Morgan, its editor-in-chief, cybercrime is expected to reach around \$10.5 trillion by 2025. The World Economic Forum's Partnership Against Cybercrime (PAC) launched the Cybercrime ATLAS project in September 2021 to help pool knowledge and understanding of cyber threats and how to deal with them, sharing information and expertise with law enforcement agencies and senior executives of large companies. Cybercrime is big business. The Verizon 2021 Data Breach Investigations Report found that organized crime was responsible for 80% of attacks, and sophisticated criminal organizations disproportionately impact financial services companies. Why is this?

The biggest reason is the time-honored one in that banks manage the money. The difference is that today's bank robbers use different methods involving unauthorized access to customer and financial data to get at the money. However, additional digital vulnerabilities exist accelerated by the Covid-19 pandemic.

IT systems consultants Atos observed that financial services companies, spurred on by the Covid-19 pandemic and emerging fintech competitors, have accelerated their digital transformations creating new routes for attack by cybercriminals. Another pandemic impact has been a significant shift to remote and hybrid work patterns, likely to persist. The home-working environment is generally less resilient to cybercrime than the typical bank office. IBM's [Cost of Data Breach Report 2021](#) found that data breach costs rose 10% over the year from \$3.86M to \$4.24M, and the average cost difference where remote work was involved was \$1.07M.

However, even if all employees were behind their bank's firewalls, they have clients to serve, and this often involves the most significant vulnerability – email.

Email and messaging are major vulnerabilities because of the human-in-the-loop

According to a January 2020 article by [Deloitte](#), 91% of cyber-attacks begin with a phishing email, but cybercrime via smartphones is also a growing problem. The identity and access management company RSA stated that 60% of fraud online is accomplished through mobile platforms, and [80% of mobile fraud](#) is achieved through mobile apps instead of mobile web browsers.

Popular instant messaging apps, despite end-to-end encryption, are still a source of vulnerability. An article in the Mexican edition of [El País](#), January 2022, highlighted the vulnerability of messaging apps to SIM swapping. This practice enables criminals to steal

identities by cloning phone numbers, assigning the stolen identity to another device, and gaining access to passwords and account details. They can then pose as a WhatsApp friend or relative and send requests for money, claiming some spoof emergency. Cybersecurity firm Kaspersky claimed account theft through this method had increased 120% in Latin America. Lloyds Bank in the UK warned customers in March 2022 to be wary of WhatsApp messages asking for money posing as a family member in distress. The bank estimated such scams had risen by over 2,000%. Research cited by Qwil Messenger showed that SMS scams globally had increased by 328%. An additional weakness of instant messaging is that the recipient is unverified. If the intended recipient's identity has been compromised, the sender can inadvertently breach client confidentiality with potentially disastrous consequences, not least reputation damage to the company.

The convenience of instant messaging comes with risk.

The advantage of instant messaging apps is their immediacy as a communications mechanism. Customers or clients expect communications between them and their financial services organizations to be convenient and friction-free. Attempts to mitigate these potential vulnerabilities and ensure verified identities and sensitive information security are often cumbersome, inconvenient, and time-consuming. But the downside of client convenience can be exposed to substantial financial risk, as JP Morgan discovered its cost in December 2021. Its brokerage arm was fined \$200M as it failed to monitor employees' use of personal messaging apps, falling foul of strict record-keeping regulations.

It's this dilemma of total security, compliance, and employee, client, or partner convenience and privacy that Qwil Messenger resolves.

Qwil Messenger - the story so far

Three co-founders established Qwil Messenger in 2017

Network Platform Technologies Limited, trading as Qwil Messenger, was founded in March 2017 by co-founders: Laurent Guyot, Nicolas Georges (Chief Technology Officer), and Peter Reading (CEO). All three have extensive experience within the financial sector. Guyot, a trusted partner to treasurers and CFOs in some of the largest banks and insurers, enjoyed fifteen years of senior-level experience with Citigroup, UBS, and Bank of America Merrill Lynch. Georges is a technology leader developing sophisticated solutions for major financial services firms such as Société Générale, BBVA, Nomura, and Bank of America. Reading has almost twenty years of designing and delivering significant digital projects in the financial sector, including delivery of Barclays Wealth online banking and cloud-based CRM solutions.

Qwil Messenger - a platform by design to provide client convenience, privacy, and security

Rather than focus on a single app for messaging, the team took a cloud-based platform approach enabling employees to use secure messaging from desktops or smartphones as required. API-based connectors and workflow capabilities would also allow ingestion of essential documents and data from CRM or financial systems.

After an initial trial and proof of concept as part of the asset and wealth manager's in-residence startup program to bring Qwil from product to enterprise-ready, Cobalt, Schroders became the first major customer in 2018, describing Qwil Messenger as the WhatsApp for financial services. Since then, Qwil Messenger has seen a rapidly growing roster of financial services companies signing up as customers, resulting as much from word-of-mouth as direct connections.

'Our vision was to create a walled garden for secure and confidential conversations between the business, its clients, and partners'

Laurent Guyot, Chief Revenue & Finance Officer

The market for Qwil Messenger has expanded beyond large financial institutions.

Today, Qwil Messenger serves customers in multiple industries and sectors, wherever confidential, secure, and convenient messaging communication is a priority. This includes healthcare, professional services, and small and medium enterprises (SMEs) across various industries where confidentiality and security are critical. As well as meeting GDPR and industry-specific regulatory requirements, Qwil Messenger is ISO-27001 and Cyber Essentials Plus* certified. (*A UK government-backed certification from the [National Cyber Security Centre](#). Cyber Essentials Plus includes hands-on technical verification).

Solution overview

Qwil Messenger was designed from the ground up to be a highly secure messaging platform that would meet the strictest security and compliance requirements without sacrificing simplicity of use. Figure 1 highlights the application's main features, which can be used on desktop or smart mobile devices for staff and clients.

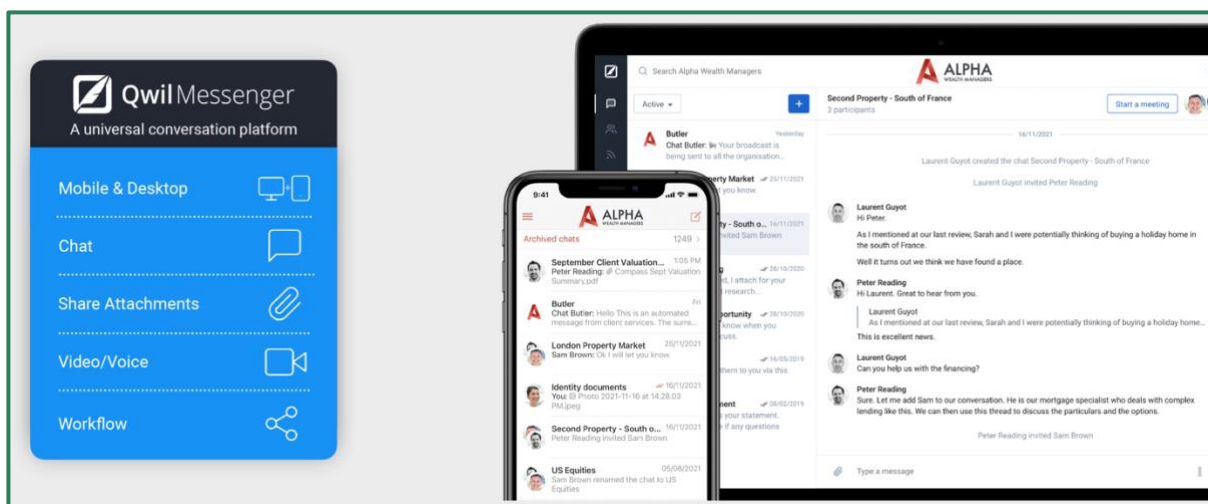


FIGURE 1: OUTLINE OF THE QWIL MESSENGER MOBILE AND DESKTOP VIEW

A fundamental weakness of most messaging apps is that the recipient cannot be verified. Qwil Messenger overcomes this in several ways. Built on Amazon Web Services, an employee must first prove their credentials before they gain access to the application. It is an invitation-only platform, and the client address book is defined by the organization and not harvested by Qwil or any third party. Before a client can access the app to read a message, they must verify their identity with Face ID or via a PIN, ensuring 2FA at all times. Users can also invite additional participants from their organization or partner to provide additional expertise to the conversation with a view of the history of the conversation. Attachments up to 50MB can be sent to the client, such as KYC documents, proposals, valuation summaries, or other documents relevant to the discussion. The organization captures the entire conversation audit trail to meet FCA regulations or similar in other jurisdictions. A PDF transcript can be generated for the whole messaging conversation.

Voice and video can enrich communication and enhance the client experience. As Guyot said, 'this is a conversation, not correspondence.'

Qwil Messenger has over fifty API connectors, so the application can be embedded within CRM and other systems and become part of an automated workflow, boosting productivity and timeliness.

Security goes beyond the technology and is core to how the organization is managed.

Every direct and indirect employee at Qwil Messenger is bound by strict terms and conditions and subject to background checks. They must also attend security training and confirm their understanding of the company's procedures and policies.

Their service is monitored 24 hours a day, seven days a week, with guaranteed uptime. Accounts and resources are kept safe from unauthorized use. Credentials are employed for

access control, secured network connections, separate user accounts, user activity logging for security monitoring, alerts, and various automated security checks.

Security experts lead development teams to ensure that future developments adhere to security best practices. Qwil is also hosted by the best cloud providers benefiting from the highest level of protection, and performs annual penetration testing of all its software (ethical hacking).

Qwil Messenger operates all access control activities based upon the principle that default permissions are set as "deny all," and specific permission is needed to enable access to be granted, in line with the individual's role and legitimate business needs. This rule applies to their premises, IT systems and networks, cloud servers, and services.

In terms of managing environments, everything is kept separate. Development, Test, and Production environments are entirely segregated, using different cloud accounts for each of these environments.

See the security [white paper](#).

Current position

Qwil Messenger now has over 2,000 customers, with the majority in financial services.

Along with the co-founders' credentials, its early backing and use by Schrodgers gave the vendor immediate credibility. It has over 2,000 customers, mainly in financial services and private banking. Significant customers include Capital Union Bank, Fidelity International, Global Block Digital Asset Trading, Nedbank Private Wealth, and FTSE 100 wealth management services company St James's, representing over 10% of the market alone.

Qwil caters for the whole client journey, from prospects to clients and internal staff interactions. Everyday use cases include identity verification and KYC (know your customer/client), account inquiries, onboarding and investment advice, managing instructions, statement delivery, and trading, among others.

Pricing is attractive irrespective of company size.

The vendor offers a fourteen-day free trial without a credit card and a professional and enterprise subscription option. The professional version costs US\$34 per month for each staff member; clients are free, making this a realistic solution for every SME, independent of size. This includes chat, document sharing, full video and screen sharing ability, APIs for integration and automation, and centralized security administration. For larger organizations, the enterprise edition provides a choice of public or private cloud deployments and a customized fee depending on the type of deployment required. A white-label version for enterprise will be made available in the second half of 2022.

Future direction

What to expect

In January 2022, PIMFA, a trade association for wealth management and investment services, announced a partnership with Qwil Messenger that will likely accelerate take-up by its membership and the broader financial services community.

Given the international nature of financial services and a growing number of international banking customers, we can expect growth from other regions.

Oracle Cloud Infrastructure and Oracle support program prove their value to Qwil Messenger.

In March 2021, Qwil Messenger joined the Oracle for Startups program and used Oracle Cloud Infrastructure (OCI) to build and deploy its audio, video, and screen sharing capability, Qwil Meet, which was a crucial part of fulfilling their customer demand for an entire business to client communication channel. This has lowered its costs, but the main benefit to Qwil Messenger has been to leverage Oracles' expertise in this field, the support of the startup team, and introductions to Oracle's extensive global enterprise customer base.

CX-Create's viewpoint

Customer experience and security are critical concerns.

Minimizing friction without sacrificing security is a universal challenge in every industry. Qwil Messenger provides a solution that manages to balance these two objectives in the field of business-to-customer communications. For smaller businesses, the vendor already has APIs that enable integration with the leading CRM provider, Salesforce, and other CRM applications are in the works, including Microsoft Dynamics 365 and Zoho. Qwil Messenger is well-positioned to support businesses of all sizes across any industry where there is a pressing need for customer/client communication confidentiality and security.

We also expect the Oracle for Startup relationship to boost Qwil Messenger recognition in other regions and industries to accelerate growth.

Summary details

Table 1: Fact sheet

Solution name	Qwil Messenger	Solution category	Business-to-customer/client
----------------------	----------------	--------------------------	-----------------------------

			secure messaging
Key industries	Financial services, professional services	Geographies	Europe & Global
Deployment model	SaaS	Licensing basis	Subscription
Size of organizations served	Any size	Go-to-market model	Direct & Channel
Number of employees	10	Key partnerships	Oracle for Startups Salesforce FNZ Linktank (SA)
URL	https://www.qwilmessenger.com/	HQ	London, UK

Appendix

Further reading

[Security Whitepaper](#)

[Cyber security: Proactive vs. Reactive](#)

[Professional firms have nothing to hide. So why are secret social chat apps still being used?](#)

For more reports sponsored by Oracle on innovative startups, visit the CX-Create [blog](#) and select the category: 'Startups and Scaleups'.

