



FEATURING RESEARCH FROM FORRESTER

# The Forrester Wave™: Secure Communications Solutions, Q3 2024

## INNOVATION SHINES IN THE FORRESTER WAVE

### The top twelve vendors

The Forrester Wave™: Secure Communications Solutions is “...an assessment of the top vendors in the market”. Of the 12 vendors, Forrester states: “Each of the vendors we included in this assessment has ... interest from and/or relevance to Forrester clients.”

Element emerged as a ‘strong performer’ and is described as delivering:

***“...leading innovation and functionality...”***

This underscores Element’s commitment to innovative technology and functionality in areas such as security and customisation. These qualities are increasingly vital in today’s complex communication landscape.

### The situation is escalating

As digital threats increase in volume and sophistication, the demand for secure communication platforms also grows. Organisations across sectors - from government entities to IT solutions providers - are under increasing pressure to protect their communications from interception, unauthorised access, exfiltration, ransomware attacks and data breaches. Element’s secure communication solution directly addresses these challenges, offering a platform that meets and exceeds industry standards for security, privacy, and compliance.

### Offer usability to avoid shadow IT

A key value underpinning Element’s innovation is, on top of providing organisations with the ability to achieve a previously unobtainable level of digital sovereignty, end-users must experience feature parity with the best consumer-grade messaging apps. Users’ experiences must be effortless and feature-rich.

The result: a solution IT leaders can provide (as an alternative to the likes of WhatsApp, Telegram and Signal) to address the use of non-compliant IT products in the workplace.

## KEY STRENGTHS

The following three sections highlight how Element meets the evolving needs of modern organisations.

### IN THIS DOCUMENT

Innovation Shines in The Forrester Wave

Research From Forrester: The Forrester Wave™: Secure Communications Solutions, Q3 2024

About Element

## Setting the standard for innovation

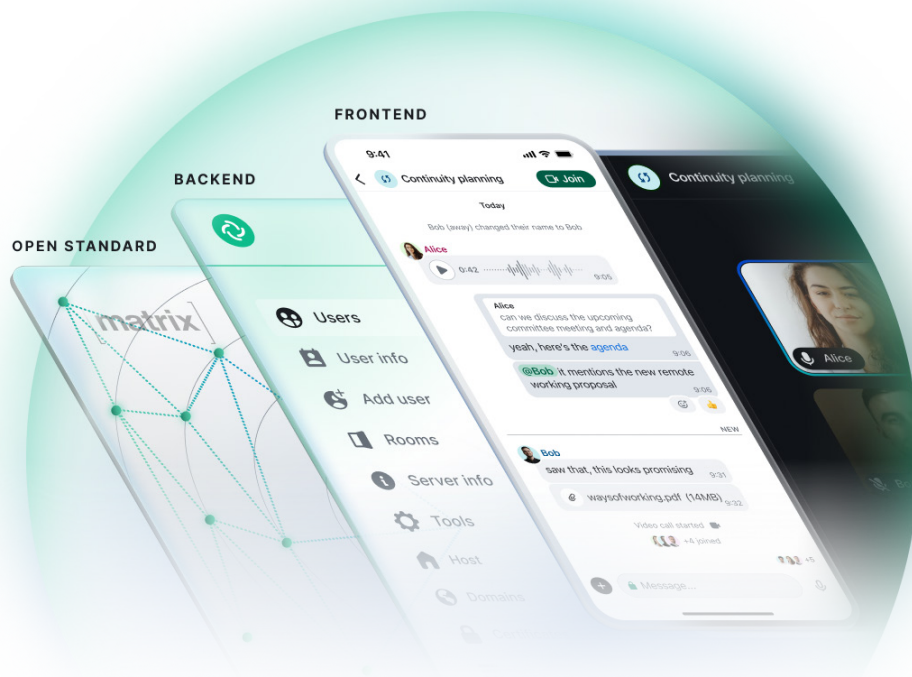
Element's success is rooted in its unwavering pursuit of innovation. In an environment where anticipating future threats is notoriously difficult, Element excels.

Element received the highest possible score in the innovation criterion (5 out of 5). Element's vendor profile in the Forrester report states:

***"Its approach to innovation enables it to cover a blend of thoughtful near-term capabilities for differentiation and market-disrupting functionality for both its current customer base and a wider range of enterprise organizations in the future."***

The Forrester report states that Element's cryptographic agility is "a core competency" which supports a forward-thinking approach. Element also scored 5 out of 5 in the post-quantum cryptography criterion. Being able to adapt its encryption methods to emerging threats means Element ensures its customers are not only secure today but also prepared for the challenges of tomorrow.

For the first time the report includes two Matrix-based communications solutions: a sign of the growing importance of Matrix. Of the Matrix-based vendors, Element had the highest score in the current offering category.



***Caption: The layers of Element's value - open standard (Matrix), back end (Element Server Suite), and front end (the Element app) - each contributes to security and customisation.***

## Customisation and interoperability

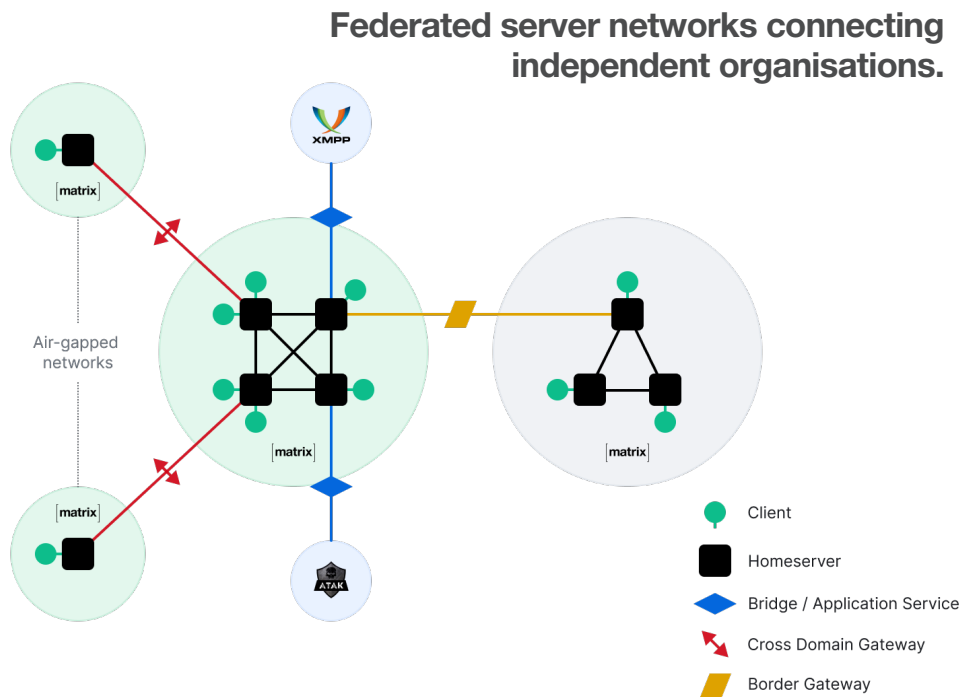
Element excels in the areas of customisation and interoperability. Unlike platforms that offer a one-size-fits-all approach, Element is built on an open protocol and has a strong emphasis on federation. Many vendors offer proprietary federation but, being built on the Matrix open standard, Element enables federations on sovereign infrastructure and absolute autonomy whilst not limiting interoperability between entities. Element is highly customisable, able to meet unique needs, particularly suited to organisations with strict security and data sovereignty requirements.

In the report, Element received the highest possible score in the customisation criterion (5 out of 5), which is defined as “vendors who offer in-house, hands-on custom development of a bespoke app to be a core part of its value proposition.”


Federation is a key feature of Element, enabling different instances to communicate seamlessly across organisations without compromising security. The Forrester report noted:

***“Organizations with requirements for interoperability, federation, and data sovereignty should consider Element.”***

This combination of features makes Element potentially the right choice for complex organisations that need data sovereignty in order to meet regulatory requirements and adhere to industry-specific security standards.



***Caption: A visual representation of the constituent components of a federated network, demonstrating how Element enables secure communication across different entities while maintaining data sovereignty.***



Also note that Element scored 5 out of 5 in the assurance criterion. Forrester describes this as how well the solution verifies and authenticates users and devices, and provides assurance that users are communicating with the correct individuals. It considers how well the solution addresses eavesdropping concerns (e.g. man-in-the-middle attacks). In the short time since Element received this score, further work has been done to enhance the way users are notified if a verified identity changes ([source](#)). Progress is a constant at Element.

### **Performance and resilience**

Robust performance and resilience are key tenets at Element. Dependability is non-negotiable. Receiving a 5 out of 5 in the performance and resilience criterion reinforces this. Organisations need to be confident that their communications are secure and operational, even in the most challenging conditions. Given the inherent complexity of building software using an open standard, this is a really noteworthy score.

Where networks are physically isolated from the internet such as air-gapped networks, Element is capable of providing uninterrupted, secure communications. Forrester carried out customer interviews in which Element's customer references reported they were:

***“...happy with its use in air-gapped environments...”***

Element is a viable choice for customers who require certainty of operational continuity, where security of their communication is mission critical (e.g. national security, public infrastructure and global banking systems). Whether it's during a cyber attack, or in situations where network connectivity is restricted, Element's resilience ensures communications can continue uninterrupted.

The report also notes:

***“Element's approach is to create an ecosystem for Matrix. This focus and its offering have primarily fueled grassroots-driven adoption among technologists and developers in addition to government, healthcare, and tech services deployments.”***


Many large enterprises and government agencies manage vast (ever-growing?) amounts of sensitive information. Element's architecture inherently supports scalability. It scored 5 out of 5 in the scalability criterion, one of only 2 vendors to do so. The platform grows alongside an organisation's needs.

### **WHY ALL OF THIS MATTERS**

This recognition by Forrester should provide large organisations with the confidence to invest in a communications solution that not only meets but exceeds industry expectations for security and compliance, while also offering the flexibility and transparency needed to address future challenges.

### **Controllable communication**

Being consistently recognised in the industry as a leader among secure communications vendors supports Element's strong position in this market. This recognition in such an established category is particularly important



for organisations in regulated industries where digital integrity, privacy and compliance are fundamental. By choosing Element, customers invest in a solution that aligns with the highest security standards while offering the flexibility to integrate seamlessly with existing IT infrastructure. This dual capability (security and flexibility) is often promised but seldom delivered. Element is unusual in that respect.

### **Open-source models provide transparency**

Open-source code offers an additional layer of transparency and security. This is valued by organisations who seriously consider their exposure to cybersecurity risks. Even on the rare occasion when a vulnerability is discovered, this is preferable to relying on a black box of closed-source code. Customers can inspect the code, verify the security implementations to satisfy their risk profile, and contribute to the platform's development.

### **Highest standards of security**

The importance of Matrix as a technology in this category is reinforced by the Forrester Wave, with Element being one of two Matrix-based secure communications solutions included. Having contributed more than 90% of Matrix's open-source codebase, Element is leading the development of this interoperable communication technology making it a strong choice for large public and private sector enterprises.

As a 'strong performer' in the Wave with the highest scores possible in six criteria (assurance, scalability, performance and resilience, customisation, post-quantum cryptography, and innovation criteria) Element delivers a secure communications platform that organisations rely on today, and will continue to do so long into the future.

WAVE REPORT

# The Forrester Wave™: Secure Communications Solutions, Q3 2024

The 12 Providers That Matter Most And How They  
Stack Up

August 29, 2024

By Heidi Shey with Amy DeMartine, Pippin Evarts, Peter Harrison

FORRESTER®

## Summary

In our 21-criterion evaluation of secure communications solution providers, we identified the most significant ones and researched, analyzed, and scored them. This report shows how each provider measures up and helps security professionals select the right one for their needs.

**Not Licensed For Distribution.**

© 2024 Forrester Research, Inc. All trademarks are property of their respective owners.

For more information, see the [Citation Policy](#), contact [citations@forrester.com](mailto:citations@forrester.com), or call +1 866-367-7378.

# Secure Communications Solutions Showcase Their Unique Fit

Secure communications solutions enable the flow of necessary and mission-critical communications and collaboration for varied use cases. These range from workforce collaboration and external partner collaboration to out-of-band communications for incident response to military and defense mission operations. As buyers struggle to establish a business case against common and existing enterprise communication tools, the value of a secure communications solution becomes clearer when it is aligned with a clear use case and its corresponding security and privacy requirements. Organizations highly concerned about targeted attacks on and surveillance of their communications will have different requirements than organizations primarily concerned with regulatory compliance.

As a result of these trends, secure communications customers should look for providers that:

- **Are fit to enable the use case.** There are differences in how vendors handle assurance that users are communicating with the correct person, such as using cryptographically backed verification for users and their devices. For high-assurance or government use cases, this may mean additional mechanisms for user verification and countering surveillance. However, the biggest differentiators include integrations with the enterprise applications that you care about for enabling desired workflows, and if required, hands-on customization to develop a truly bespoke secure communications solution for your organization to meet very specific requirements for app functionality and features.
- **Fulfill communication data retention requirements.** Secure communications solutions vary in how they enable data retention — and for good reason. For some use cases, ephemeral — disappearing — messages are a requirement, while for other use cases, there is a regulatory or business requirement to retain the data. If there is retention capability, the controls for retained data and how admins may interact with the archive can also vary. As a result, vendor approaches to retention can range from limited capability to integration with common enterprise archiving solutions to separate environments for retention with different degrees of control for retained data.
- **Meet procurement process requirements for the appropriate security and risk.** Organizations must assess the third-party risk of their technology vendors. The intended use of a secure communications solution raises the stakes to ensure that



a given solution is securely developed and, if required for procurement, validated and certified for specific uses. This can include whether a solution holds a specific government security certification and approval for use, though in many countries, where no certification exists, there is often a government-specific vetting process. It's also common for such solutions to regularly submit to independent audits and penetration testing and to take a proactive approach to identifying and remediating vulnerabilities. Some buyers will go a step further and ask for source code reviews as well as software composition analysis and software bills of materials.

- **Align with the organization's requirements and timeline for PQC capabilities.**

The National Institute of Standards and Technology (NIST) released the first three finalized postquantum encryption [standards](#) as this Forrester Wave™ evaluation entered its final stages. However, secure communications solution vendors clearly recognized the relevant risks — and importance of cryptoagility and postquantum readiness — prior to the release of finalized standards. All vendors we evaluated in this report have an established approach and timeline for use of postquantum cryptography (PQC) and a view on how they will proceed. In some cases, their solution architecture may currently allow for cryptoagility and enable customers to specify preferred algorithms for use. What may make the difference is whether their timeline and approach satisfy your requirements. Buyers in government are typically the most demanding in terms of this criterion.

## Evaluation Summary

The Forrester Wave evaluation highlights Leaders, Strong Performers, Contenders, and Challengers. It's an assessment of the top vendors in the market; it doesn't represent the entire vendor landscape. You'll find more information about this market in [The Secure Communications Solutions Landscape, Q2 2024](#).

We intend this evaluation to be a starting point only and encourage clients to view product evaluations and adapt criteria weightings using the Excel-based vendor comparison tool (see Figures 1 and 2). Click the link at the beginning of this report on [Forrester.com](#) to download the tool.

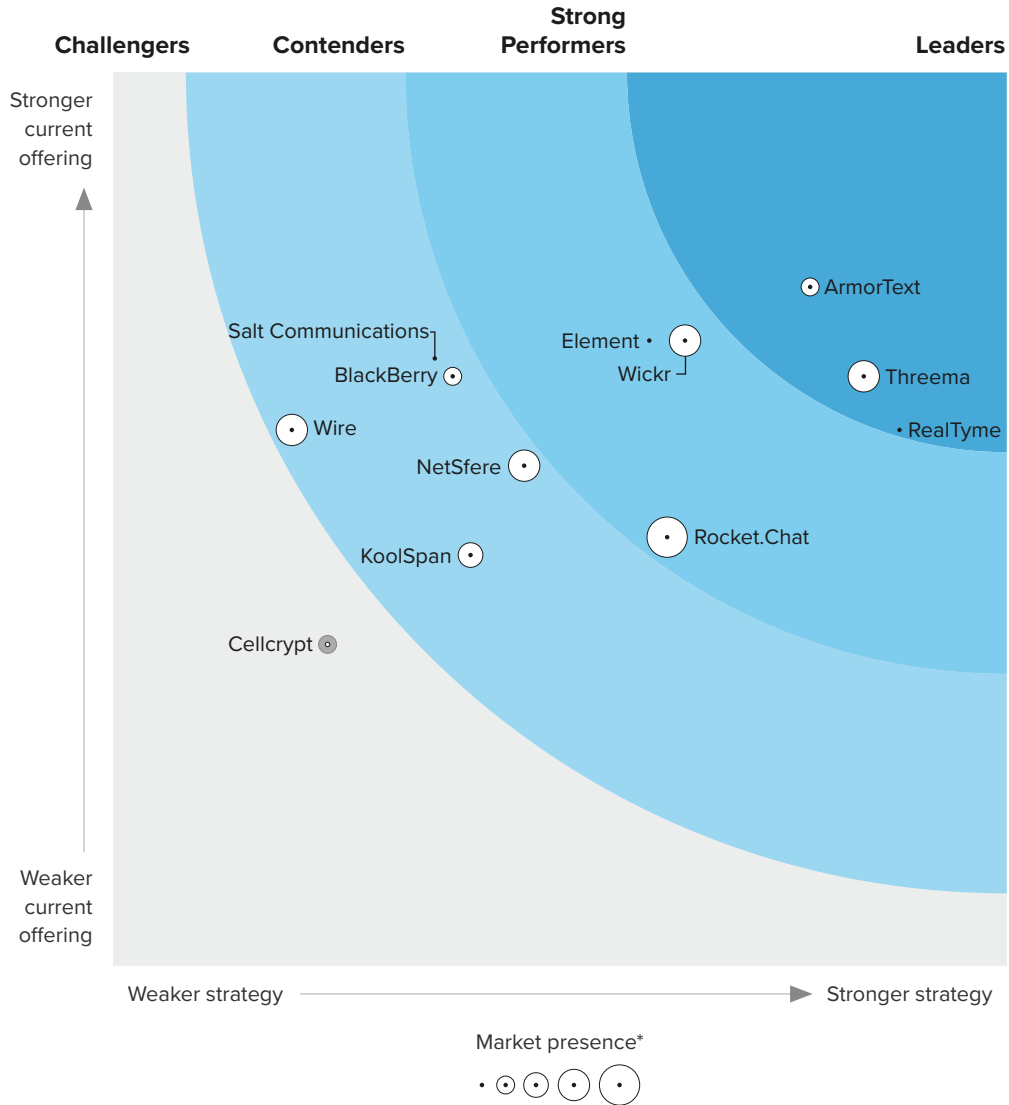
Figure 1

Forrester Wave™: Secure Communications Solutions, Q3 2024

# THE FORRESTER WAVE™

## Secure Communications Solutions

Q3 2024



\*A gray bubble or open dot indicates a nonparticipating vendor.

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Figure 2

Forrester Wave™: Secure Communications Solutions Scorecard, Q3 2024

	Forrester's weighting	ArmorText	BlackBerry	Cellcrypt*	Element	KooSpan	NetSfere
<b>Current offering</b>		3.80	3.30	1.80	3.50	2.30	2.80
Assurance	15%	3.00	3.00	3.00	5.00	1.00	3.00
Metadata security, privacy, management	10%	5.00	3.00	1.00	3.00	3.00	5.00
Retention	10%	5.00	3.00	1.00	3.00	1.00	3.00
Scalability	5%	3.00	3.00	1.00	5.00	3.00	1.00
Performance and resilience	5%	5.00	5.00	3.00	5.00	3.00	1.00
Integrations	5%	3.00	3.00	1.00	3.00	1.00	3.00
Customization	5%	1.00	3.00	1.00	5.00	3.00	3.00
Postquantum cryptography	5%	3.00	1.00	3.00	5.00	1.00	1.00
Government requirements	5%	1.00	5.00	3.00	3.00	1.00	1.00
Manageability	10%	3.00	5.00	3.00	3.00	3.00	3.00
Administrator restrictions	10%	5.00	3.00	1.00	1.00	1.00	3.00
Supplier risk	15%	5.00	3.00	1.00	3.00	5.00	3.00
<b>Strategy</b>		3.90	1.90	1.20	3.00	2.00	2.30
Vision	20%	3.00	1.00	1.00	3.00	1.00	1.00
Innovation	15%	5.00	1.00	1.00	5.00	3.00	3.00
Roadmap	20%	3.00	3.00	1.00	3.00	3.00	3.00
Partner ecosystem	15%	5.00	1.00	1.00	3.00	3.00	3.00
Adoption	15%	3.00	3.00	1.00	1.00	1.00	1.00
Pricing flexibility and transparency	10%	5.00	1.00	3.00	3.00	1.00	3.00
Community	5%	5.00	5.00	1.00	3.00	1.00	3.00
<b>Market presence</b>		2.00	2.00	2.00	1.00	3.00	4.00
Revenue	50%	1.00	3.00	3.00	1.00	3.00	5.00
Number of customers	50%	3.00	1.00	1.00	1.00	3.00	3.00

All scores are based on a scale of 0 (weak) to 5 (strong).

\*Indicates a nonparticipating vendor

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

		Forrester's weighting	RealTyme	Rocket.Chat	Salt	Communications	Threema	Wickr	Wire
<b>Current offering</b>			3.00	2.40	3.40	3.30	3.50	3.00	
Assurance	15%	5.00	1.00	5.00	3.00	5.00	3.00	5.00	3.00
Metadata security, privacy, management	10%	3.00	3.00	5.00	5.00	3.00	3.00	5.00	5.00
Retention	10%	1.00	3.00	3.00	3.00	3.00	3.00	3.00	3.00
Scalability	5%	1.00	3.00	3.00	3.00	3.00	3.00	3.00	5.00
Performance and resilience	5%	3.00	1.00	1.00	5.00	5.00	5.00	3.00	3.00
Integrations	5%	1.00	5.00	3.00	5.00	3.00	3.00	3.00	1.00
Customization	5%	3.00	5.00	5.00	1.00	1.00	1.00	1.00	1.00
Postquantum cryptography	5%	1.00	1.00	3.00	5.00	5.00	5.00	5.00	5.00
Government requirements	5%	3.00	3.00	1.00	3.00	5.00	5.00	3.00	3.00
Manageability	10%	5.00	3.00	3.00	3.00	3.00	3.00	3.00	1.00
Administrator restrictions	10%	3.00	3.00	3.00	5.00	3.00	3.00	3.00	3.00
Supplier risk	15%	3.00	1.00	3.00	1.00	3.00	3.00	3.00	3.00
<b>Strategy</b>			4.40	3.10	1.80	4.20	3.20	1.00	
Vision	20%	5.00	5.00	1.00	3.00	1.00	1.00	1.00	1.00
Innovation	15%	3.00	3.00	5.00	5.00	3.00	3.00	1.00	1.00
Roadmap	20%	5.00	5.00	1.00	3.00	3.00	3.00	1.00	1.00
Partner ecosystem	15%	5.00	1.00	1.00	5.00	5.00	5.00	1.00	1.00
Adoption	15%	5.00	1.00	1.00	5.00	5.00	5.00	1.00	1.00
Pricing flexibility and transparency	10%	3.00	3.00	3.00	5.00	3.00	3.00	1.00	1.00
Community	5%	3.00	1.00	1.00	5.00	3.00	3.00	1.00	1.00
<b>Market presence</b>			1.00	5.00	1.00	4.00	4.00	4.00	4.00
Revenue	50%	1.00	5.00	1.00	3.00	5.00	3.00	5.00	3.00
Number of customers	50%	1.00	5.00	1.00	5.00	3.00	3.00	5.00	5.00

All scores are based on a scale of 0 (weak) to 5 (strong).

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

## Vendor Offerings

Forrester evaluated the offerings listed below (see Figure 3).

**Figure 3**

**Evaluated Vendors And Product Information**

Vendor	Product evaluated
ArmorText	ArmorText 0.35.x
BlackBerry	SecuSUITE
Cellcrypt	Cellcrypt Server
Element	Element (ESS 24.05)
KoolSpan	TrustCall 10.13
NetSfere	NetSfere 6.4
RealTyme	RealTyme Government, Business and Pro versions
Rocket.Chat	Rocket.Chat 6.5 or higher
Salt Communications	Salt Communications
Threema	Threema Work (Android 5.2.4k; iOS 5.9.3k; Threema Work 2.0 Desktop Beta 32 for macOS), Management Cockpit 2.1.0, Threema OnPrem 2.2.2
Wickr	AWS Wickr and Wickr Enterprise
Wire	Wire Secure Messenger (Web 3.34.482; iOS 3.111.9; Android 4.6.3)

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

## Vendor Profiles

Our analysis uncovered the following strengths and weaknesses of individual vendors.

### Leaders

- **ArmorText outclasses for SecOps, incident response, and threat-intel-sharing use cases.** ArmorText’s platform is purpose-built for out-of-band collaboration to meet the unique needs of security operations (SecOps) teams. It also offers a secure gateway for enabling end-to-end encryption (E2EE) integrations and crisis-response reserve capacity as an add-on. Firms can use it to support business continuity, disaster recovery, board communications, and more. Headquartered in the US, its customers are concentrated in North America, but there is also a sizeable contingent in Europe. It has notable use in the energy and utilities sectors and Information Sharing and Analysis Centers (ISACs) for information sharing. Law firm and incident-response provider partnerships further enhance customer value. ArmorText’s approaches to innovation, partner ecosystem, and pricing flexibility are

well aligned with its vision, and enabling the core use cases is where it currently excels. Integrations could help it further expand its use cases.

ArmorText's key strengths are in retention, performance and resilience, administrator restrictions, and meeting customers' supplier risk requirements. There are granular settings to enable different types of retention and data access, including use in a federated environment, and retention settings customizable by group and user. Its deficiencies are in customization and government certifications. Reference customers lauded ArmorText's auditability, ease of use and administration, robust calling features, and reserved capacity offering, but they wanted to see improvement in scalability for enabling organizationwide calling for hundreds of users and user onboarding. Organizations that require out-of-band communications for incident response, security operations, or threat-intel sharing should consider ArmorText.

View [ArmorText's detailed scorecard](#).

- **Threema dominates as a privacy-first and flexible business communications app.**

Threema's business offering includes Work, OnPrem, Broadcast, and Gateway; the consumer app and the company are both called Threema. A varied roster of organizations uses Threema, including those in hospitality, education, financial services, retail, healthcare, and government. Headquartered in Switzerland, Threema delivers on its vision for setting a standard for business communication rooted in security and privacy for all, with user privacy and control as a key principle. To continue to drive growth, it fosters a robust customer community and introduced a new approach to innovation two years ago. Threema also revamped its partner model in 2023; the diversity of its partner ecosystem, which spans secure phone providers to reinsurance brokers, is a key strategic asset for enabling broad applicability and reach for its solution.

Threema's strengths center on metadata controls, administrator restrictions, integrations, and its approach to postquantum cryptography. Its privacy-first strategy is evident not only in its thoughtful approach to metadata and administrator restrictions but also in its ability to put various privacy choices and controls in the hands of users for their profiles. It lags in customization for a highly bespoke app and addressing supplier risk concerns. Reference customers highlight Threema's focus on privacy, manageability, broadcast capabilities, and user profiles, but they felt that it could improve its desktop version for macOS, multidevice use and device-switching process, and data retention. Organizations seeking a privacy-oriented secure communications solution to integrate with their

enterprise apps and business workflows should consider Threema.

View [Threema's detailed scorecard](#).

- **RealTyme excels in manageability and enabling and supporting customers.**

RealTyme's Swiss heritage heavily influences the privacy focus of its offering for trusted collaboration. Its customers span government and defense, finance, energy and utilities, and frontline and first responders. It also has a sizable presence in and focus on serving customers located in the Middle East and Africa. RealTyme's differentiating vision and roadmap not only support the current and anticipated technology requirements of customers but also take a forward-looking view of enabling sustainability through reduced data storage and net-zero carbon emissions. It provides extensive support and resources to customers to enable successful adoption and use of the solution, including tailored materials for customer use cases and hands-on, on-site workshops at RealTyme's headquarters.

RealTyme's outstanding manageability is its top strength. It employs a sophisticated and holistic customer experience framework across stages prior to, during, and after deployment in addition to ongoing customer success processes. It falls short in the areas of retention and scalability for specific communications functionality like group chat and conference calls. It also has room to improve its integrations and postquantum cryptography. Reference customers praised RealTyme's ability to meet their country-specific cybersecurity standards for government use, usability, assurance capabilities, and deployment options. They wanted to see RealTyme improve at interface language support (particularly Arabic), file sharing and editing, and app branding and design. Organizations that require a highly customer-focused and forward-looking technology partner should consider RealTyme.

View [RealTyme's detailed scorecard](#).

## Strong Performers

- **Wickr thrives in high-stakes, high-assurance use cases and sticks to this lane.**

Amazon Web Services (AWS) Wickr provides a straightforward communication and collaboration app that is especially well suited to scenarios where users' personal safety is at stake and where monitoring of communications is a concern. Acquired by AWS in 2021, Wickr continues its steadfast focus on the US government and public sector. It has a robust partner ecosystem and deep engagement to help with customer adoption and maximizing use of the app. Its very targeted focus and vision make it a less-desirable option for organizations looking for a more general-purpose secure communications application. It will need to continue to accelerate

and push its approach to innovation and roadmap to adapt to organizations' future needs for secure communications, maintain its edge, and meet the demands of its current customer base.

Wickr's key strengths — meeting government certifications, supplier risk requirements, and customization — align with its focus on government and defense use. It also boasts impressive assurance capabilities, including measures like account takeover protection and anticensorship capabilities through Wickr Open Access. Reference customers praised Wickr for its support, suitability, and approval for government and military use; low-bandwidth performance; and flexibility of configuration. However, they expressed the desire for continued improvement of custom user interfaces, a move from on-premises to SaaS deployment, and operational security. Organizations with demands for compliance, flexible deployment, and high assurance — and those concerned with securely and privately communicating on restricted or monitored network environments — should consider Wickr.

View [Wickr's detailed scorecard](#).

- **Element delivers leading innovation and functionality but has gaps enabling adoption.** Element offers the flagship application for the Matrix open standard, an open protocol for decentralized and E2EE communications. Element's approach is to create an ecosystem for Matrix. This focus and its offering have primarily fueled grassroots-driven adoption among technologists and developers in addition to government, healthcare, and tech services deployments. Headquartered in the UK, its customer base is primarily situated in Europe. Its approach to innovation enables it to cover a blend of thoughtful near-term capabilities for differentiation and market-disrupting functionality for both its current customer base and a wider range of enterprise organizations in the future. Reliance on top-down-mandated use in organizations will only go so far, and Element must do more to enable customer success and adoption to fuel growth among a broader enterprise population.

Element's strengths span its capabilities for assurance, scalability, performance and resilience, and customization as well as its approach to postquantum cryptography and addressing supplier risk concerns. Cryptographic agility is a core competency. Options for enabling administrator restrictions are a limitation. Reference customers were enthusiastic about Element's open protocol and federation but wished for improvements to the admin interface, usability (finding users, custom presence features, and general ease of use), and integrations. While references were happy with its use in air-gapped environments, they also



desired improvements to the deployment process to get there. Organizations with requirements for interoperability, federation, and data sovereignty should consider Element.

View [Element's detailed scorecard](#).

- **Rocket.Chat delivers solid manageability and integrations but needs to bolster usability.** Rocket.Chat's offering enables a wide array of use cases for secure communications. Headquartered in the US, it boasts a large open-source community of users in more than 150 countries, and many organizations that use its commercial product start with the Community version of the platform, which is offered for free under the MIT Open Source License. Rocket.Chat has a differentiated vision and roadmap for secure collaboration and communication, in service of key themes, like enabling government-citizen communications as well as self-managed, secure AI for augmenting workflows while maintaining privacy. While it has key strategic partners to fulfill specific customer needs, and joint roadmaps, the scope of its partner ecosystem is relatively narrow today; it could improve efforts and resources to facilitate adoption within customer organizations.

Rocket.Chat provides solid capabilities for manageability, integrations, government requirements (notably Iron Bank certification and verification for use under the US Department of Defense Platform One DevSecOps Initiative), and addressing the supplier risk concerns of its customers. Professional services are also available to help with customization. It lags in assurance, performance and resilience, and postquantum cryptography. Reference customers applauded Rocket.Chat's manageability, security controls for data privacy, stability, and high availability. Their challenges were with its usability and UI, integration capabilities, and scalability. Organizations that require a unified collaboration experience, task management, and interoperability (it runs on the Matrix protocol) from a developer-friendly solution should consider Rocket.Chat.

View [Rocket.Chat's detailed scorecard](#).

## Contenders

- **Salt Communications is tops for a bespoke app, but it has some performance hurdles.** Salt's platform offers a wealth of security configurations and controls, enabling great flexibility for use cases ranging from attorney-client communications to hostage negotiations. Headquartered in the UK, it serves high-assurance use cases in defense, government, law firms, wealth management, financial services, telecom, and law enforcement. It adheres to an upfront, know-your-customer

process to prevent use of the platform for nefarious purposes; in other words, it does due diligence to identify who its customers are and what they will use the platform for. While Salt's vision and customer selectivity limit its mass-market use, it still punches above its weight with a presence in 52 countries due to its tailored innovation and pricing. The impact of this vision feeds into shortcomings in its nascent community efforts and narrow use of its partner ecosystem.

Salt offers noteworthy assurance, metadata controls, and customization. It doesn't flinch at developing capabilities unique to a customer's deployment. It falls short in performance and resilience in challenging environments and for specific certifications for government requirements. Reference customers liked its assurance capabilities, ease of onboarding and use, broadcast and mass-messaging functionality, and reliability. However, they noted challenges with its ability to operate in low-data-coverage areas and wanted features like emojis and integrations with industry-specific applications. Firms that require strong assurance capabilities for verifying users and their devices, metadata controls, and customization for bespoke use cases should consider Salt Communications.

View [Salt Communications' detailed scorecard](#).

- **BlackBerry shines for government use but lags in postquantum cryptography.**

BlackBerry SecuSUITE delivers a high-assurance secure communications platform. Customers have additional complementary options like UEM from BlackBerry and secure devices through its partner ecosystem. Headquartered in Canada, BlackBerry's cybersecurity offerings have global presence and reach. Its SecuSUITE product is suited to audiences like government and defense and therefore has a smaller, yet still global, market presence. BlackBerry's roadmap process and well-developed customer community give it a strategic edge with its target market in government and defense. However, tailoring to the stringent needs of these customers results in a narrow focus for vision and innovation and complexity in pricing.

BlackBerry's strengths coalesce around performance and resilience, customization, manageability, and meeting government requirements. It boasts an impressive number of government certifications and approvals for use across the US, Canada, Germany, and Australia as well as NATO Restricted use. However, it stands to improve when it comes to enabling the transition to postquantum cryptography. Reference customers highlighted BlackBerry's ease of deployment and excellence in support. However, they wanted to see improvements to call handling in poor network conditions, integrations with enterprise applications, white labeling,

bring your own encryption, and measures for enabling a transition to use of postquantum cryptography, including capabilities to coexist and transition from existing cryptologic methods to newer ones. Organizations with requirements for government security certifications and customization for use should consider BlackBerry.

View [BlackBerry's detailed scorecard](#).

- **NetSfere excels in collaboration but lacks key government security certifications.**

NetSfere's offering combines messaging, voice, video, and screen sharing. A notable strength is that engagement is one of four key pillars of its vision, alongside security, control, and compliance. This focus on engagement permeates the product and innovation strategy, which is beneficial for adoption and use among its current customer base but also an area where competitors are vying to close the gap. While many competitors tailor controls for high-assurance use cases in defense and government before expanding to other industries, NetSfere builds from a foundation of secure messaging to serve business and compliance needs across industries. NetSfere is headquartered in the US, and its customers span the globe. It has a wide market presence and diverse customer community. However, it will face increasing headwinds for continued differentiation despite a thoughtful approach to innovation and roadmap.

NetSfere shines when it comes to metadata controls and enabling industry-specific collaboration workflows, such as its integration with Nuance for healthcare speech to text. It has examples of customizations for customers across transportation and logistics, healthcare, banking, and more. Key areas where it falls short are advanced capabilities for scalability, performance and resilience in challenging environments, government security certifications, and postquantum cryptography. Reference customers praised NetSfere's ease of use and versatility but wished to see further improvement in retention, integrations, advanced features like AI-powered assistance, and the UI. Businesses that need secure collaboration and communications with tight integrations and customization for workflows should consider NetSfere.

View [NetSfere's detailed scorecard](#).

- **KoolSpan offers a hardened, isolated solution but lags in data retention and integration.** KoolSpan renewed and relaunched its TrustCall and TrustCall Dome (on-premises) offerings in 2023. It offers voice, messaging, video, conference calling, file transfer, and a secure device bundle for use cases across government, highly regulated industries, and education. KoolSpan is headquartered in the

US. Its customers span the globe, supported by strategic partners that give it a presence across more than 28 countries. KoolSpan's vision for a secure mobile communications platform deployed within a customer's hardened environment, independent of public internet access, is narrow. It maintains a solid approach to innovation and roadmap to deliver on this vision. It can improve by streamlining pricing models and developing its community beyond its current customer advisory board and roundtable discussions.

KoolSpan's offerings are solid across multiple key areas, including metadata security, privacy, and management as well as performance and resilience, and it's notable for its approach to addressing supplier risk concerns. Its deployment options contribute to these strengths. For example, it can be deployed onto portable systems, such as in a van or backpack. A key weakness is its approach to enabling retention, with no default option to do so. Although customers that require further customization can ask KoolSpan developers for support, the vendor lags in out-of-the-box integration with common enterprise applications, primarily supporting mobile device management and enterprise mobility management today. It could also benefit from additional certifications for government requirements. KoolSpan's reference customers did not respond to Forrester's outreach for this evaluation. Global organizations in need of a mobile-first and robust secure calling solution should consider KoolSpan.

View [KoolSpan's detailed scorecard](#).

- **Wire offers robust metadata controls and features alongside manageability obstacles.** Wire offers a secure communications platform built on open standards; it codeveloped Messaging Layer Security (MLS), an open protocol for E2EE in real time. Headquartered in Germany, Wire is well versed in strict data protection standards and the needs of organizations with such requirements. It is one to watch; it is now gearing up to expand and do more with the backing of a new investor, new management team, and revamped partner ecosystem. With a transformation to better serve the needs of B2B and government customers, Wire must improve the clarity of its vision to differentiate and transparency of its roadmap to entice customers. It also needs to continue to build on its customer community and refine and formalize its approach to supporting adoption within customer environments, particularly within industries like government, where it aims to expand its reach.

Wire stands out for its assurance; scalability; and robust metadata security, privacy, and management capabilities. Its approach to cryptoagility and preparing for

postquantum cryptography is another notable strength. Key weaknesses include manageability, integrations, and customizations. Reference customers commended Wire's rich feature set, reliability and availability across OSes, and commitment to MLS and E2EE. However, they expressed a desire for Wire to improve its usability, interoperability, and product dependability (fewer bugs); speed up development of feature requests; and offer multifactor authentication. Organizations that prioritize scalability, control of metadata, and cryptoagility should consider Wire.

View [Wire's detailed scorecard](#).

## Challengers

- **Cellcrypt commits on encryption but delivers value mainly via secure calls and video.** Cellcrypt offers "Cellcrypt" and "Cellcrypt Federal" products that enable secure voice, video and conference calling, messaging, and large file transfer. While Cellcrypt has a global presence, it is headquartered in the US, and its customer base is largely concentrated in North America. It primarily serves the needs of enterprise organizations (more than 1,000 employees), but it does have midmarket (500 to 1,000 employees) organizations as customers. Cellcrypt's pricing flexibility and transparency are notable strategic strengths, but its overall vision and focus may limit broader growth at this time. Cellcrypt has invested in developing a solution that primarily serves the needs of government, with heavy attention on the US federal sector as a National Information Assurance Partnership (NIAP)-validated solution. This commitment can provide the foundation for expanding its government certifications and approvals for use by other governments.

Cellcrypt's focus on the requirements of US federal customers is demonstrated through prioritization of capabilities like postquantum protections, data retention, and a gateway that can extend connections to physical office spaces so users can also securely join PBX-hosted conference calls. While it has file-sharing capabilities, it currently lacks functionality like document collaboration, workflow orchestration and automation, and federation. Organizations in government that require a NIAP-certified, CSfC solution for voice- and video-over-IP calling should consider Cellcrypt. Cellcrypt declined to participate in the full Forrester Wave evaluation process.

View [Cellcrypt's detailed scorecard](#).

# Evaluation Overview

We grouped our evaluation criteria into three high-level categories:

- **Current offering.** Each vendor's position on the vertical axis of the Forrester Wave graphic indicates the strength of its current offering.
- **Strategy.** Placement on the horizontal axis indicates the strength of the vendors' strategies, including elements such as vision and innovation.
- **Market presence.** The size of each vendor's marker on the graphic reflects Forrester's assessment of its market presence.

## Vendor Inclusion Criteria

Each of the vendors we included in this assessment has:

- **A broad set of communication capabilities for collaboration.** These include text/chat, voice calls, videoconferencing, file sharing, and more.
- **Experience with enterprise security requirements.** Vendors have a customer base that consists of at least 70% enterprise organizations (more than 1,000 employees).
- **Interest from and/or relevance to Forrester clients.** Forrester clients ask about the evaluated vendors and products during inquiries and interviews or have use cases that these vendors are well suited to support. Alternatively, in Forrester's judgment, evaluated vendors may have warranted inclusion because of their capabilities and market presence.

# Supplemental Material

## Online Resource

We publish all our Forrester Wave scores and weightings in an Excel file that provides detailed product evaluations and customizable rankings; download this tool by clicking the link at the beginning of this report on Forrester.com. We intend these scores and default weightings to serve only as a starting point and encourage readers to adapt the weightings to fit their individual needs.

## The Forrester Wave Methodology

A Forrester Wave is a guide for buyers considering their purchasing options in a technology marketplace. To offer an equitable process for all participants, Forrester

follows [The Forrester Wave™ Methodology](#) to evaluate participating vendors.

In our review, we conduct primary research to develop a list of vendors to consider for the evaluation. From that initial pool of vendors, we narrow our final list based on the inclusion criteria. We then gather details of product and strategy through a detailed questionnaire, demos/briefings, and customer reference surveys/interviews. We use those inputs, along with the analyst's experience and expertise in the marketplace, to score vendors, using a relative rating system that compares each vendor against the others in the evaluation.

We include the Forrester Wave publishing date (quarter and year) clearly in the title of each Forrester Wave report. We evaluated the vendors participating in this Forrester Wave using materials they provided to us by June 14, 2024, and did not allow additional information after that point. We encourage readers to evaluate how the market and vendor offerings change over time.

In accordance with [our vendor review policy](#), Forrester asks vendors to review our findings prior to publishing to check for accuracy. Vendors marked as nonparticipating vendors in the Forrester Wave graphic met our defined inclusion criteria but declined to participate in or contributed only partially to the evaluation. We score these vendors in accordance with [our vendor participation policy](#) and publish their positioning along with those of the participating vendors.

## **Integrity Policy**

We conduct all our research, including Forrester Wave evaluations, in accordance with the [integrity policy](#) posted on our website.

# We help business and technology leaders use customer obsession to accelerate growth.

FORRESTER.COM

## Obsessed With Customer Obsession

At Forrester, customer obsession is at the core of everything we do. We're on your side and by your side to help you become more customer obsessed.

### Research

Accelerate your impact on the market with a proven path to growth.

- Customer and market dynamics
- Curated tools and frameworks
- Objective advice
- Hands-on guidance

[Learn more.](#)

### Consulting

Implement modern strategies that align and empower teams.

- In-depth strategic projects
- Webinars, speeches, and workshops
- Custom content

[Learn more.](#)

### Events

Develop fresh perspectives, draw inspiration from leaders, and network with peers.

- Thought leadership, frameworks, and models
- One-on-ones with peers and analysts
- In-person and virtual experiences

[Learn more.](#)

## Contact Us

Contact Forrester at [www.forrester.com/contactus](http://www.forrester.com/contactus). For information on hard-copy or electronic reprints, please contact your Account Team or [reprints@forrester.com](mailto:reprints@forrester.com). We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA  
Tel: +1 617-613-6000 | Fax: +1 617-613-5000 | [forrester.com](http://forrester.com)

### Not Licensed For Distribution.

© 2024 Forrester Research, Inc. All trademarks are property of their respective owners.  
For more information, see the [Citation Policy](#), contact [citations@forrester.com](mailto:citations@forrester.com), or call +1 866-367-7378.





Element offers a new and unique type of collaboration (such as Microsoft Teams or Slack) and messaging (think WhatsApp or Signal). It combines a consumer style messenger interface with the power of a collaboration tool, encouraging fast adoption in the office and across the frontline. Element's enterprise customers benefit from data sovereignty (whether deployed on-premise, or as a hosted service), end-to-end encryption and easy interoperable connections via the Matrix open standard for real time communication. The result is a secure platform for collaboration, messaging and VoIP with enterprise-grade functionality and the flexibility to match a wide range of use cases and risk profiles.