element

Element is a leader in secure communications

FEATURING RESEARCH FROM FORRESTER

The Forrester Wave™: Secure Communications, Q3 2022

IN THIS DOCUMENT

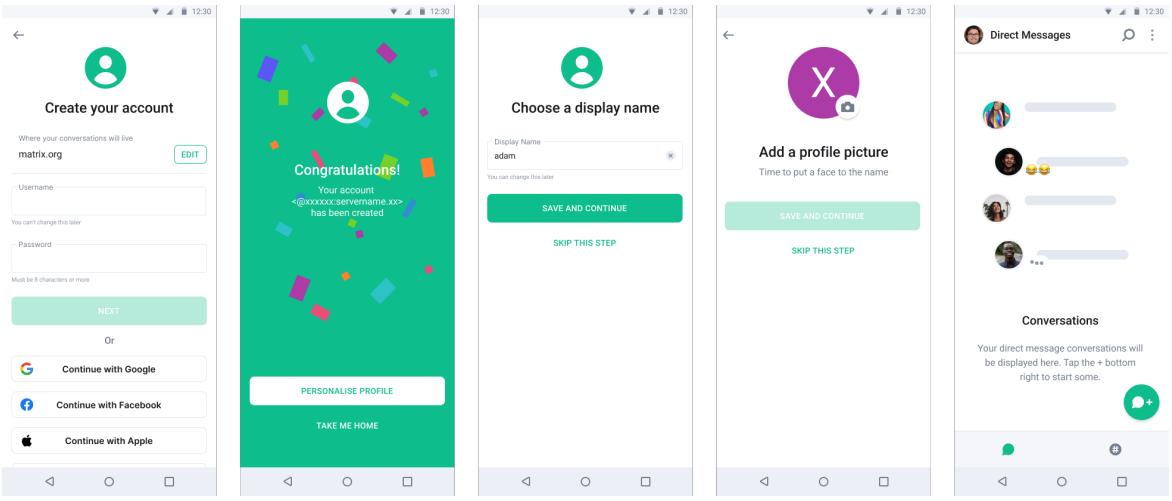
SECURITY IS FUNDAMENTAL

Being **recognised as a leader in secure communications by Forrester** is a powerful validation to many of Element's customers. The report notes that Element is a great fit for "...organizations that prioritize flexibility, federation, and data sovereignty". Yet 'secure communications' is just the beginning, a foundation. From there Element has built a leading enterprise communication app. It may come as a surprise that many of the incumbent/omnipresent communication apps aren't secure. All vendors in this Wave report use end-to-end encryption because communication can't be truly secure without it. Element goes above and beyond by making the most of the Matrix open standard.

The Forrester report states: "Element delivers on a vision for **open, secure, and self-sovereign** communications". Successfully achieving this paradigm shift requires careful balance. Element puts the customer experience at the center of everything. This, twinned with an impressive range of features, means Element's ideal customers range from start-ups (scaling quickly) to large multinational enterprises and governments (numerous entities with differing needs).

FUNCTIONALITY AND FLEXIBILITY

Element provides **instant messaging, video calls, virtual meetings, team/project rooms, live location sharing and many more features** that end users have come to expect today. If these are now commonplace, what differentiates Element?

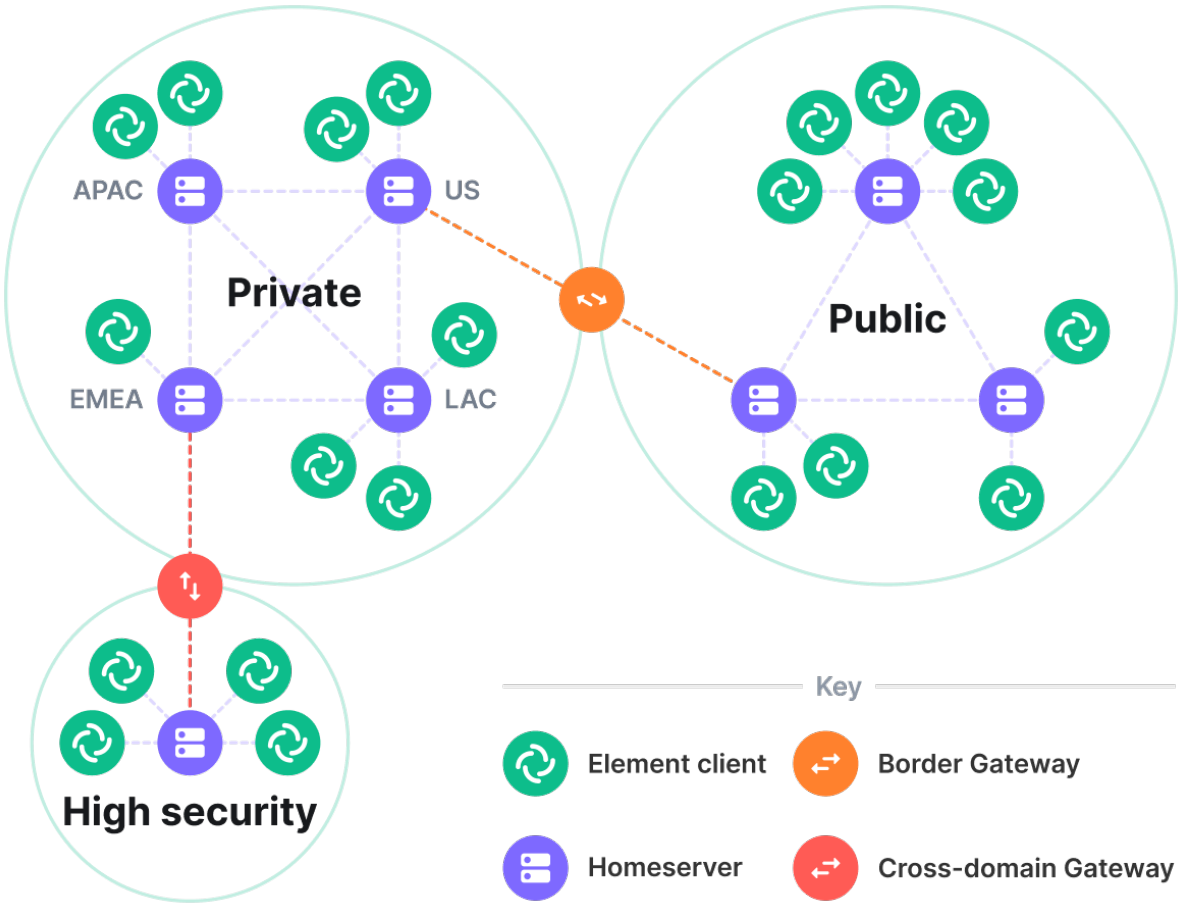


Screenshot showing the mobile sign up experience on Android and iOS

Element combines the usability of consumer-grade apps like WhatsApp and Signal with enterprise functionality typically associated with apps like Microsoft Teams and Slack. This means coworkers and customers like using it. Usability also increases productivity. Frontline workers often need to communicate 'on the go' via mobile/cell phones. Often they need to interface with desk-based tasking managers who a) can have differing levels of computer literacy and b) are using a desktop/laptop not a phone. Some companies target 'mobile-first' but Element has prioritized mobile and desktop user experience.

Ease of use drives adoption but organizations must also have the tools required to meet their compliance obligations e.g. GDPR, ISO270001, CCPA, HIPAA, GovCloud, etc. End-to-end encryption can pose challenges here. Through **enterprise-grade auditing, retention and archiving capabilities** Element overcomes this.

Unlike other well-known communication apps, Element offers **flexible cloud and on-premises hosting** options. Some larger customers self-host in their private cloud with an ongoing support contract. With hosting in place, organizations **choose how 'open' or 'closed'** they want their network to be. Users can either communicate with everyone on the network much like email (a.k.a. open federation) or only with users within their organization or on specific domains more similar to Slack (a.k.a. closed federation).



A private, public and high-security network showing federated communication while preserving security and data sovereignty

Users can access their accounts easily by using existing ‘single sign-on’ credentials. In other words: no new passwords to remember. Also, staff details (job roles, departments, interests, etc.) can be mapped across to predefined permissions within Element. This saves time when **synchronizing all new joiners, movers and leavers** and reduces admin burden.

OPEN ROAD AHEAD

Underpinning all the features and benefits described above is **the Matrix protocol**, an open standard for decentralized, end-to-end encrypted communications. An open standard like Matrix has the potential to **set real-time communications free** just like SMTP did for asynchronous communications via email: both are ‘common languages’ enabling users to communicate between vendors. Someone using Gmail or Hotmail can message someone with a Yahoo or mybusiness.com email address. And every email inbox can be accessed from applications developed by different vendors. In much the same way, Matrix-based apps aren’t locked into a provider’s proprietary ecosystem.

Native interoperability also means organizations are **never locked into a vendor** creating healthy competition which drives innovation: survival of the fittest not the biggest.

Matrix is decentralized and today this is often heralded as the future of computing, but why? In communication at least, it migrates the risks associated with a single point of failure. If one node on the network goes offline, all the messages/calls continue going through the other nodes which are still communicating. It is a **highly resilient** design. Decentralization is not only resilient it also supports a **zero trust** approach to cybersecurity and enables **data sovereignty**. Enterprises can retain ownership of their data, choose which country it is stored in, and have absolute certainty that the data isn’t being mined and sold to advertisers.

In keeping with this ethos of openness, Element and Matrix are both **open source**. This puts customers in control of their collaboration platform and the data within it. Organizations can trust open source products. Code is publicly available. This transparency is necessary. Reputational damage is a huge risk to organizations so using a product where the code is openly available makes it more accessible and decreases the likelihood of potential vulnerabilities.

As this Wave report is going out Element has just: revamped its mobile sign up experience and its cloud hosting self-serve journey; implemented new versions of video calling (including video rooms); updated its embedded live chat website plug-in; redeveloped its on-premise installer; and added customisable ‘space mapping’ to make managing instances easier. Element’s new decentralized, end-to-end encrypted video conferencing capability will also be released shortly. Products and user experience are evolving quickly.

In short, Element is: built on Matrix; part of the open source moment; flexible to organizational needs; a combination of user-friendly layouts and powerful collaboration functionality; suitable for a range of use cases (e.g. frontline workers); highly secure whilst able to meet compliance obligations; and already used by UK, US, French and German governments and enterprises around the world. It’s an exciting time for Element and a great fit for “organizations that prioritize flexibility, federation, and data sovereignty”.

Element partners with the French government (DINUM) to support 300K users.

Element works with Dataport to support 500K users across the states of Hamburg and Schleswig-Holstein.

Mozilla uses Element for secure team collaboration and community discussion.

WAVE REPORT

The Forrester Wave™: Secure Communications, Q3 2022

The 12 Providers That Matter Most And How They Stack Up

August 29, 2022

By Heidi Shey with Amy DeMartine, Lok Sze Sung, Peggy Dostie

FORRESTER®

Summary

In our 26-criterion evaluation of secure communications providers, we identified the 12 most significant ones — ArmorText, Armour Communications, Element, HighSide, RealTyme, Salt Communications, SpiderOak, Stashcat, Teamwire, Threema,Wickr, and Wire — and researched, analyzed, and scored them. This report shows how each provider measures up and helps security and risk professionals select the right one for their needs.

Additional resources are available in the online version of this report.

The Range Of Uses For Secure Communications Mirror Market Offerings

Security and privacy concerns and controls exist on a spectrum, so the use cases for secure communications can vary greatly. One organization's requirements might be focused on enabling a remote workforce to handle sensitive data in compliance with regulations, while another's might be rooted in personal safety, with life and death of individuals at stake. For some organizations, these two use cases are not mutually exclusive. As a consequence, technology offerings in this space span a wide range in how they meet customer requirements for secure communications. The heritage of a secure communications offering provides insight into its philosophy and approach, the key industries and geographies it aims to serve, and the types of innovation it focuses on. One thing is clear across all providers in this market: Offerings are expanding in use and becoming more embedded in everyday workflows within customer organizations as secure communications proves its value.

As a result of these trends, look for providers that:

- **Have views and capabilities for user privacy and use of metadata that align with yours.** User privacy can mean fully anonymous enrollment and use of the secure communications app where required, as well as individual users' ability to control what information from their user profile is visible to other users of the app. In an enterprise setting, you may prefer that individuals are not anonymous, with profile information reflecting corporate directory details. The degree of anonymity required depends on your use case. Likewise, while limited metadata collection is typically preferred for privacy purposes, you may want use of metadata for monitoring user app activity for event logging purposes. The way a secure communications offering is designed to optimize for privacy naturally invokes trade-offs for other capabilities like metadata collection and use.
- **Support customization fit for your purposes.** None of these solutions require customization for you to use them. You may want a corporate-branded version of the secure communications app, and this is a standard customization capability across offerings. Organizations requiring more extensive, nonstandard customization to create a bespoke solution can choose providers equipped to provide that particular type of support. Examples include swapping out encryption libraries and modules or modifying the ringtone a user hears while waiting for a secure connection to be established.
- **Enable data retention suitable for your business and compliance requirements.** Not every organization or use case will require data retention, and the design of

secure communications tools typically prioritizes ephemeral messages and handling of privileged content over retention. However, for regulated industries subject to compliance requirements for data retention and organizations that have a business requirement to retain messages — such as for forensic purposes — data retention is a critical capability. How secure communications offerings enable this varies a great deal, from policy settings, to integrating with an archiving solution, to offering their own value-added service or built-in functionality.

- **Offer the necessary assurances for your procurement process requirements.** Organizations must assess the third-party risk of their technology vendors. Secure communications providers will assist you here with their approach to addressing your security and risk requirements, such as allowing for penetration testing, providing results of independent audits, and more. Note that all of the providers in this Forrester Wave™ are experienced with supporting government entities with proven deployments. The differences lie in whether a provider holds specific government certification, such as Germany BSI or US FedRAMP. In many countries, there may be no equivalent government-level certification scheme and individual governments may have their own vetting processes. Not every provider will hold such certifications, based on where they operate and their current customer base; it also takes time for those that are in process of certification, so this is worth asking about in RFIs if it's relevant.

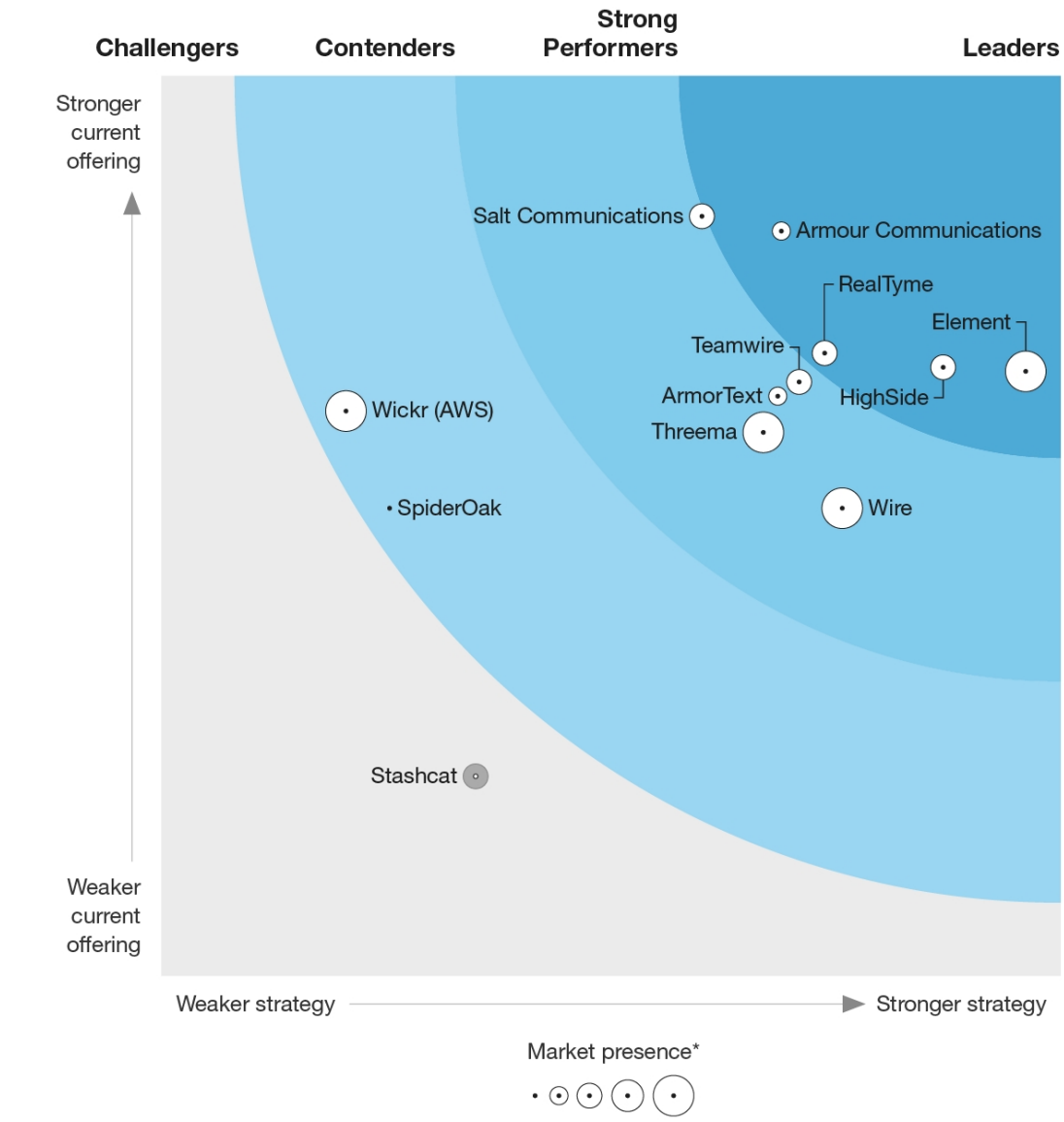
Evaluation Summary

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 our reports on secure communications.

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 Figure 1 and see Figure 2). Click the link at the beginning of this report on Forrester.com to download the tool.

Figure 1

Forrester Wave™: Secure Communications, Q3 2022



*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 Scorecard, Q3 2022

	Forrester's weighting	ArmorText	Armour Communications	Element	HighSide	RealTyme	Salt Communications
Current offering	50%	3.22	4.14	3.36	3.38	3.46	4.22
Assurance and control	10%	3.00	5.00	3.00	5.00	5.00	5.00
User privacy	10%	3.00	5.00	5.00	1.00	5.00	5.00
Metadata security and privacy	10%	3.00	5.00	1.00	3.00	5.00	5.00
Retention	12%	5.00	5.00	1.00	3.00	1.00	3.00
Flexibility	10%	1.00	5.00	5.00	3.00	3.00	5.00
Scalability	4%	5.00	5.00	3.00	1.00	1.00	1.00
Performance and resiliency	8%	3.00	1.00	5.00	3.00	3.00	5.00
Integrations	12%	3.00	3.00	5.00	5.00	3.00	3.00
Enhanced functionality	2%	5.00	3.00	3.00	5.00	3.00	3.00
Customization	8%	1.00	3.00	5.00	5.00	5.00	5.00
Deployment	2%	4.00	4.00	3.00	4.00	2.00	2.00
Administration	10%	5.00	4.60	1.40	3.00	3.40	5.00
Security and risk requirements	2%	3.00	3.00	3.00	3.00	3.00	3.00

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

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

	Forrester's weighting	ArmorText	Armour Communications	Element	HighSide	RealTyme	Salt Communications
Strategy	50%	3.42	3.44	4.80	4.34	3.68	3.00
Product vision	20%	3.00	3.00	5.00	5.00	3.00	3.00
Execution roadmap	22%	3.00	3.00	5.00	5.00	5.00	3.00
Market approach	10%	5.00	3.00	5.00	3.00	3.00	5.00
Performance	15%	3.00	3.00	5.00	5.00	3.00	3.00
Planned enhancements	12%	3.00	5.00	5.00	3.00	5.00	3.00
Innovation roadmap	10%	3.00	3.00	5.00	3.00	3.00	1.00
Partner ecosystem	10%	5.00	5.00	3.00	5.00	3.00	3.00
Commercial model	1%	5.00	3.00	5.00	3.00	3.00	3.00
Market presence	0%	1.33	1.66	4.33	2.65	2.33	2.32
Revenue	33%	1.00	1.00	5.00	2.00	2.00	2.00
Average deal size	33%	2.00	3.00	4.00	5.00	3.00	4.00
Number of users	34%	1.00	1.00	4.00	1.00	2.00	1.00

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

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

	Forrester's weighting	SpiderOak	Stashcat*	Teamwire	Threema	Wickr (AWS)	Wire
Current offering	50%	2.60	1.11	3.30	3.02	3.14	2.60
Assurance and control	10%	5.00	0.00	3.00	5.00	5.00	3.00
User privacy	10%	5.00	1.00	3.00	5.00	3.00	1.00
Metadata security and privacy	10%	1.00	0.00	3.00	3.00	1.00	1.00
Retention	12%	5.00	1.00	3.00	0.00	3.00	3.00
Flexibility	10%	1.00	3.00	5.00	3.00	5.00	3.00
Scalability	4%	1.00	3.00	3.00	3.00	3.00	3.00
Performance and resiliency	8%	1.00	1.00	3.00	3.00	5.00	3.00
Integrations	12%	0.00	1.00	3.00	3.00	5.00	3.00
Enhanced functionality	2%	1.00	3.00	5.00	3.00	3.00	1.00
Customization	8%	1.00	1.00	3.00	3.00	0.00	5.00
Deployment	2%	3.00	0.50	4.00	2.00	2.00	3.00
Administration	10%	4.60	1.00	3.00	3.00	1.00	1.40
Security and risk requirements	2%	3.00	1.00	5.00	3.00	3.00	5.00

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	SpiderOak	Stashcat*	Teamwire	Threema	Wickr (AWS)	Wire
Strategy	50%	1.26	1.74	3.54	3.34	1.02	3.78
Product vision	20%	1.00	1.00	3.00	1.00	1.00	5.00
Execution roadmap	22%	1.00	0.00	5.00	3.00	1.00	5.00
Market approach	10%	1.00	3.00	3.00	5.00	1.00	5.00
Performance	15%	1.00	3.00	5.00	5.00	1.00	1.00
Planned enhancements	12%	3.00	3.00	3.00	5.00	1.00	5.00
Innovation roadmap	10%	1.00	1.00	1.00	3.00	1.00	3.00
Partner ecosystem	10%	1.00	3.00	3.00	3.00	1.00	1.00
Commercial model	1%	3.00	3.00	3.00	3.00	3.00	3.00
Market presence	0%	1.00	2.02	3.00	4.01	5.00	4.34
Revenue	33%	1.00	1.00	2.00	5.00	5.00	5.00
Average deal size	33%	1.00	1.00	4.00	2.00	5.00	3.00
Number of users	34%	1.00	4.00	3.00	5.00	5.00	5.00

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.

Vendor Offerings

Forrester included 12 vendors in this assessment: ArmorText, Armour Communications, Element, HighSide, RealTyme, Salt Communications, SpiderOak, Stashcat, Teamwire, Threema, Wickr, and Wire (see Figure 3).

Figure 3

Evaluated Vendors And Product Information

Vendor	Product evaluated
ArmorText	ArmorText
Armour Communications	Armour Mobile
Element	Element Enterprise
HighSide	HighSide One
RealTyme	RealTyme Pro, Enterprise and Defense
Salt Communications	SaltIM
SpiderOak	CrossClave
Stashcat	Stashcat
Teamwire	Teamwire
Threema	Threema Work (SaaS and on-premises versions)
Wickr (AWS)	Wickr Enterprise
Wire	Wire

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

Vendor Profiles

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

Leaders

- **Element delivers on a vision for open, secure, and self-sovereign communications.** Element offers the flagship application for the Matrix open standard, an open protocol for decentralized and end-to-end encrypted (E2EE) communications. Matrix has the potential to do for secure communications what SMTP did for email; become the common language, enabling those using one communications platform to communicate with those on another communication platform, much like how someone using Gmail can send an email to someone using Outlook. Element's approach is to create an ecosystem for Matrix. This focus and its offering have fueled grassroots-driven adoption among technologists and developers in addition to government and enterprise deployments. Its roadmap is

publicly available on GitHub, encouraging input from both open source community participants and customers. Element also has a dedicated team focused on future innovation for the product, experimenting with innovations like collaboration in spatial web.

Element's key strengths are its flexibility in supporting various use cases for secure communications, data sovereignty, and performance and resiliency in challenging environments. Reference customers also mentioned these strengths. However, there is still room for improvement for more widespread general enterprise use, particularly with the user interface, to support ease of use, administrator experience, iOS user experience, and inclusion of more features within the chat. Element is a great fit for tech enthusiasts and their organizations that prioritize flexibility, federation, and data sovereignty.

- **HighSide pairs secure and segmented communications with robust data management.** HighSide's platform is built on the notion of decentralized encryption and trust systems while maintaining centralized control. Its platform aims to mitigate the risk of data loss from communications, data storage, and file sharing. HighSide tightly couples secure data management with its communications functionality. Its approach is to start secure by default, with options to reduce controls where necessary. It has built a diverse sales and delivery partner ecosystem, in addition to a Microsoft partnership that brings HighSide into Microsoft Teams environments. This ecosystem, in addition to the vendor's compliance focus, has helped HighSide gain traction within government, defense, and enterprises concerned with intellectual property protection. Its innovations are focused on delivering features for security enhancements and compliance controls, particularly as it relates to file management for productivity.

  HighSide's strengths are in assurance and control, customization, and compliance with requirements such as export administration regulations (EAR) and international traffic in arms regulations (ITAR). Key trade-offs associated with delivering on these include metadata privacy, user privacy, and scalability. Customer references noted HighSide's audit trail capabilities, fast time to value, user profile restrictions, and vendor support. Areas of improvement that customers wished to see are features related to more integrations and the user interface. HighSide is a great fit for organizations requiring controlled file sharing and secure data management alongside secure communications functionality.

- **Armour Communications enables high assurance, primarily for government and defense.** Armour's NATO IA and FIPS 140-2 certified offering is designed with mission-critical use cases in mind. Its intelligence community relationships underpin their perspective on the threat landscape, while its partner-led approach

enables it to deliver a compelling solution for government and defense customers. This focus has resulted in less traction outside of the defense community. Its innovation vision was established seven years ago, and Armour has continued to populate it based on customer needs. While Armour is innovating to meet the requirements of other verticals such as financial services, healthcare, and legal, it will require allocating additional commitment to do so.

Armour provides robust user privacy protections and high scalability. However, it needs to improve on performance and resiliency in challenging environments. Reference customers also had mixed experiences with this, in addition to integrations and customizations. They wished to see further improvements to videoconferencing functionality and easier transfer of data to new devices. Armour Communications is a strong fit for organizations that could also benefit from its partners for consultancy services (including engineering for OEMs and white labeling) and secure devices to offer a holistic secure communications solution.

- **RealTyme boasts strong metadata protections, with minor scalability limitations.** RealTyme's offering combines secure collaboration with privacy in communications, the result of a merger of two Swiss companies: RealTyme, focused on collaboration, and Adeya, bringing encrypted secure communications technology. RealTyme's superior execution roadmap supports not just the technology requirements of customers but differentiates through support of customer values such as sustainability through reduced data storage and net zero carbon emissions. While its planned enhancements are well-defined, many areas of focus for innovation are capabilities already found in competitors' offerings, with some forward-looking features in the mix.

  RealTyme has strong metadata security and privacy protections as well as customization support, and its variety of enhanced functionality for productivity and security enable flexibility for many different types of business use cases for secure communications. Its current limitations on number of users for a group chat and videoconferencing calls are an issue for some customers and their use cases. Reference customers are generally positive about the offering, its features, and flexibility. However, they have mixed experiences relating to scalability as well as performance and reliability; they also wished for visibility into future releases and faster vendor support response times. RealTyme is a strong fit for organizations in need of an easy-to-manage, user-friendly, secure communications app for data control and collaboration.

Strong Performers

- **Salt Communications excels in enabling bespoke use cases but can be complicated.** Salt's platform aims to protect the mobile workforce, enabling productivity, compliance, and physical safety for an organization's employees. It also 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 these customers will use the platform for. As a result, the sales process and establishing a proof-of-concept could be seen as onerous by some organizations. Salt Communications' approach to planned enhancements and innovation is also heavily customer-driven and less future-forward relative to others evaluated, primarily reflecting the needs of its existing customer base concentrated in legal, wealth management, government, law enforcement, and military and defense.

  Salt Communications has strong capabilities across multiple areas, including assurance and control, user privacy, metadata security and privacy, and customization. Reference customers also praise its flexibility in addressing multiple use cases within the organization and integrations. With customization in particular, customers noted the strength of the codesign and development process with the Salt Communications team. While the capabilities are robust, customers wish the administrator experience for user management could be simplified and offer even more granularity, in addition to broader integrations. Salt Communications is a strong fit for organizations operating in high-security environments seeking a truly customized solution for their business and threat model.

- **Teamwire is an all-around solid offering but has an incremental focus on innovation.** Teamwire's offering is designed to facilitate secure communications between a mobile workforce and desktop workers, with a strong focus on enabling police and first responders. Its multifaceted execution roadmap and disciplined approach to planned enhancements enable it to consistently deliver improvements for its customers. As a result, multiyear deals followed by multiyear renewals are common. While there is a specific focus on new market features, much of its innovation roadmap is focused on incremental and typically customer-led product features, which will offer less differentiation over time.

  Teamwire's options for data sovereignty is a strength, in addition to its rich enhanced functionality for productivity for specific customer segments like police and first responders. This enhanced functionality could also be used for enterprises. While it meets requirements necessary for government deployments, it currently does not hold a specific named government certification; however, BSI certifications are underway and will take time to complete. Reference customers

are generally satisfied; in particular, they note the product's ease of use and Teamwire's responsiveness to feedback. They would still like to see more integrations and greater interoperability with other applications. Teamwire is a strong fit for organizations requiring a secure, feature-rich alternative to consumer apps such as WhatsApp.

- **ArmorText excels at enabling out-of-band communications but has narrow focus.** ArmorText's platform is purpose-built for out-of-band collaboration to meet the needs of security operations teams while providing granular governance and retention capabilities. ArmorText has notable adoption in the energy and utilities sectors, and ISACs for information sharing. This is partly the result of having investors with security operations and incident response experience, strong partnerships with service providers, and adapting to customer feature requests. ArmorText's innovation roadmap also reflects this focus, which may be too specific for some organizations' needs.

  While ArmorText offers rich, enhanced functionality with incident responder needs in mind, it sacrifices some flexibility and integrations by design for addressing wider enterprise communication use cases. Reference customers praised its ease of use and E2EE archiving capabilities, noting its segmented data retention lifecycles and data reviewer controls. However, they expressed a desire for more provisioning and calendar integrations. ArmorText is a great fit for security operations and incident response communications and collaboration, as well as multiorganization threat intelligence sharing.

- **Wire brings a strong platform but lacks added functionality for specific use cases.** Wire's offering is designed to enable secure and private collaboration for any type of organization. Its focus on open standards and interoperability underpins its fast development cycles and flexible architecture, creating an offering with compelling capabilities. Wire's flexible architecture enables organizations to integrate Wire into a wide range of workflows. It has a highly disciplined approach to its execution roadmap and planned enhancements; this approach has been assessed and rated by an independent auditor as within the top 5% of audited firms for software delivery performance and operations. While it has many enterprise and government customers already, Wire could stand to expand its partnership ecosystem to further its reach. Its innovation focus continues to support its vision for open standards for secure communications with a general-purpose, secure collaboration platform for a range of business scenarios.

  Wire support for customization is a key strength, stemming in particular from its role in codeveloping messaging layer security (MLS), an E2EE protocol with crypto

agility as one of its properties. Its focus on serving any type of organization means a lack of enhanced functionality around security or productivity for any particular vertical or use case. Wire was the only participating vendor that did not provide reference customers for this evaluation. Wire is a strong fit for any organization seeking an easy-to-use and full-featured platform for secure communications, for both internal use and external-facing collaboration with business partners and customers.

- **Threema Work is privacy-first with many built-ins but lacks data retention.** Threema's business offering includes Threema Work and Threema OnPrem; the consumer app and the company are both called Threema. Its business offerings are full-featured apps with many built-ins on top, such as its own mobile device management capabilities to support BYOD, work-life balance "off hours" policies, and protection against location tracking and phishing. Threema's disciplined approach to planned enhancements enables it to quickly bring new functionality to market. It also has a recognizable brand with its consumer app; its expertise in the consumer market is reflected in its user experience and user interface — helpful when it comes to employee adoption within the enterprise. While prioritization of customer needs is a strength, this approach overlooks future demands that customers have yet to identify for its innovation roadmap.

  Threema's strength in user privacy enables anonymous use of its product and gives the user full control over their profile information. A trade-off of its privacy focus is a lack of support for data retention for archiving, which some customers require for compliance or legal purposes. Reference customers are generally satisfied with its ease of use, response to feature requests, and impact on employee experience, specifically highlighting Threema's broadcast functionality, corporate directory, and user identification tagging. They wish for smoother user onboarding and account switching processes, as well as more back-end features via Threema Gateway. Threema Work is a strong fit for companies of all sizes looking for an all-in-one app for protection of user privacy and sensitive corporate information.

Contenders

- **Wickr shines with its flexibility and integrations but lags in manageability and features.** Wickr's platform is a hub for secure collaboration across messaging, meetings, file sharing, and workflows. Wickr offers flexible pricing with different plans to meet the needs of a variety of customers of all sizes, along with a multitude of hosting and deployment options. Acquired by AWS in 2021, it is currently undergoing a transition period; planned enhancements and innovation

continue to be based on customer needs, including US government and public sector. Notable areas of continued innovation include working with industry partners in the development of the MLS encryption standard and building an E2EE SDK to enable customers to secure products and workflows.

Wickr's strength is with integrations and its flexibility to support a wide range of business use cases, from small businesses to government and defense. Its Open Access feature is notable for helping maintain connectivity in network environments that try to block certain communications, such as for censorship purposes. It lags in customization and deployment support; administrator experience and restrictions could be improved. Reference customers highlight Wickr's security capabilities. However, they noted challenges and wished to see improvements to customization, manageability, content of user profiles, effort required to enable data retention, and response to feature requests to name a few. Wickr is a good fit for organizations seeking a secure collaboration suite with reliable, no-frills communication functionality.

- **SpiderOak is highly agile, with room to further develop features and functionality.** SpiderOak's offering enables secure collaboration and communications as a productivity suite based on a flexible core platform that enables fast implementation of new features and customization (such as for the space industry). Its security philosophy is security without compromise; its vision is to strive to meet and match competitor feature sets that align with this perspective. SpiderOak has its roots in secure backup; it is a newer market entrant for secure communications and one to watch. It is continuing to develop its market approach and growing its partnership ecosystem but adapting quickly to customer requests from a diverse base ranging from design firms to government. With innovation, SpiderOak currently prioritizes near-term agility over a clearly defined long-term roadmap.

  SpiderOak's focus on user privacy and its data retention capabilities are key strengths; data retention is notable, based on blockchain technology to be tamperproof and immutable. It does currently lag across many features and lacks integrations, all of which are on the roadmap. Reference customers praised its ease of use and Zero Trust standards. Areas of desired improvement are primarily feature-related, such as the mobile experience, workflow options, and video improvements. SpiderOak is a good fit for organizations that could benefit from a secure, agile platform for file collaboration with communications features, where they have a say in influencing new feature and integration requests.

Challengers

- **Stashcat enables granular messaging controls but lacks communications assurance.** Its offering is a multipurpose, easy-to-use business messenger with a full suite of communications and collaboration functionality. Stashcat's market approach and partnership ecosystem have helped it establish a foothold in Germany, with limited presence elsewhere. Acquired by secunet in 2021, Stashcat is undergoing a transition period; its product vision and innovation roadmap are changing and will primarily fit the needs of digital public authorities in the future and e-government in the near term. However, it does have its sights on further geographic and vertical expansion for its offering, although the specific timeline and focus are not clear.

  Stashcat's enhanced functionality for security and privacy, such as disabling of features, and modules that can be activated and deactivated by the organization is a strength; the most privacy-friendly setting is the default. However, it lacks capabilities for communications assurance and control, metadata security, and support for government requirements outside of their core market focus of Germany and Europe. Stashcat is a good fit for organizations seeking a simple platform for collaboration and messaging with flexibility to address a range of business use cases for secure communications. Stashcat declined to participate in the full Forrester Wave evaluation process.

Evaluation Overview

We evaluated vendors against 26 criteria, which we grouped 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. Key criteria for these solutions include assurance and control, user privacy, metadata security and privacy, retention, flexibility, scalability, performance and resiliency, integrations, enhanced functionality, customization, deployment, administration, and security and risk requirements.
- **Strategy.** Placement on the horizontal axis indicates the strength of the vendors' strategies. We evaluated product vision, execution roadmap, market approach, performance, planned enhancements, innovation roadmap, partner ecosystem, and commercial model.
- **Market presence.** Represented by the size of the markers on the graphic, our market presence scores reflect each vendor's revenue, average deal size, and number of users.

Vendor Inclusion Criteria

Forrester included 12 vendors in the assessment: ArmorText, Armour Communications, Element, HighSide, RealTyme, Salt Communications, SpiderOak, Stashcat, Teamwire, Threema, Wickr, and Wire. Each of these vendors has:

- **A broad set of supported features.** This includes a suite of communications capabilities to support business collaboration, including text/chat, voice calls, videoconferencing, and file sharing.
- **An experienced user base.** More than 50 organizations have deployed and are using the solution across multiple industries such as government, financial services, manufacturing, energy, education, legal, and more. Some vendors may have hundreds of organizations or more that have deployed their solution.
- **Interest from and/or relevance to Forrester clients.** Forrester clients ask about the participating vendors and products during inquiries and interviews or have use cases that these vendors are well-suited to support. Alternatively, in Forrester's judgment, participating 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 Guide 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 6, 2022 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 The Forrester Wave™ And New Wave™ 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 The Forrester Wave™ And The Forrester New Wave™ Nonparticipating And Incomplete Participation Vendor 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.

FORRESTER®

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.

FOLLOW FORRESTER 

Contact Us

Contact Forrester at www.forrester.com/contactus. For information on hard-copy or electronic reprints, please contact your Account Team or 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

ABOUT ELEMENT

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.