FORRESTER®

The Future Of Secure Communications

Data Sovereignty, End-To-End Encryption, And Interoperability Will Revolutionize Internal And External Workplace Discussion

A FORRESTER CONSULTING THOUGHT LEADERSHIP PAPER COMMISSIONED BY ELEMENT, SEPTEMBER 2023

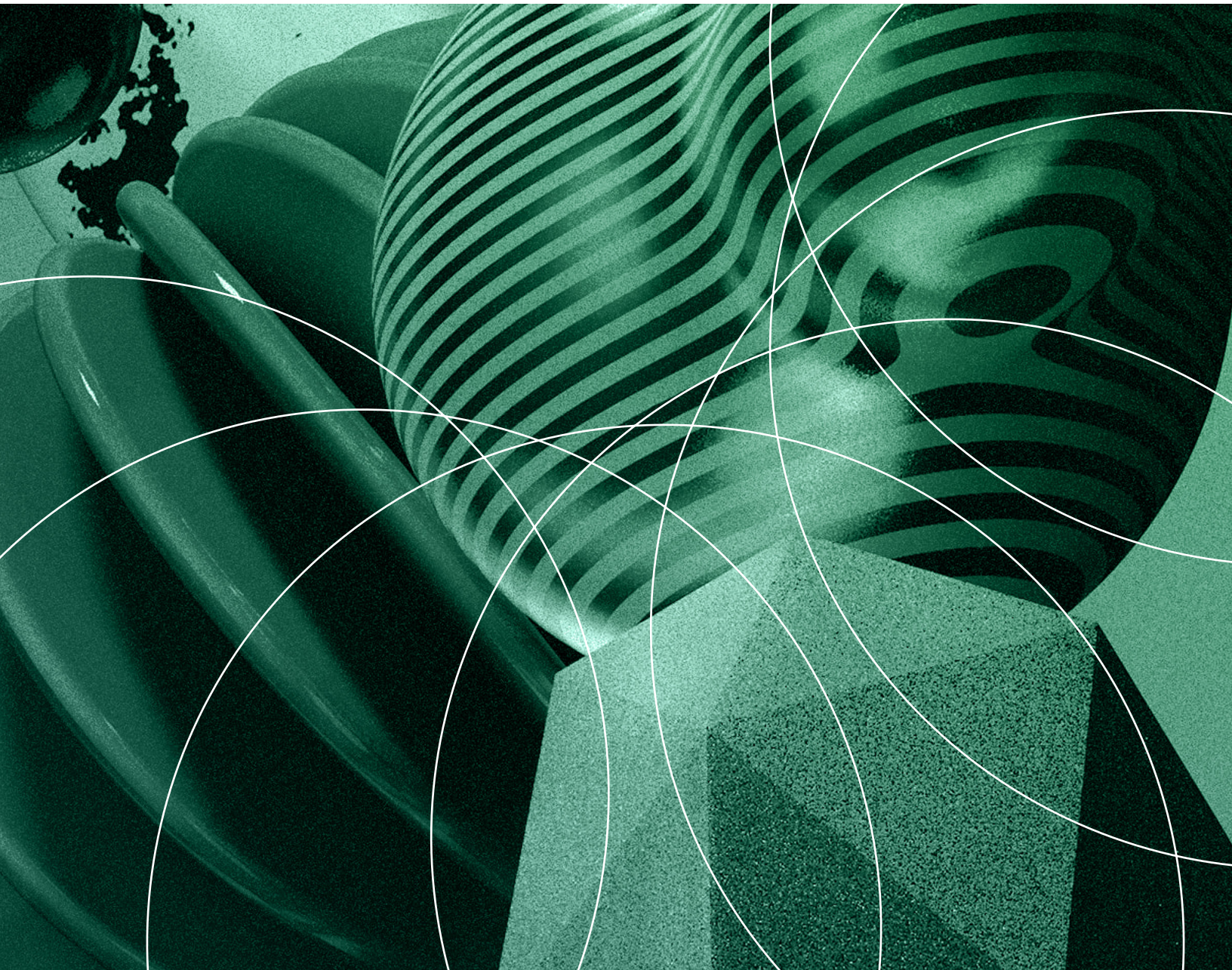


Table Of Contents

Project Team:

Sophia Christakis,

Market Impact Consultant

Alex Martini,

Associate Market Impact Consultant

Contributing Research:

Forrester's Security & Risk research group

ABOUT FORRESTER CONSULTING

Forrester provides independent and objective research-based consulting to help leaders deliver key outcomes. Fueled by our customer-obsessed research, Forrester's seasoned consultants partner with leaders to execute their specific priorities using a unique engagement model that ensures lasting impact. For more information, visit forrester.com/consulting.

Executive Summary

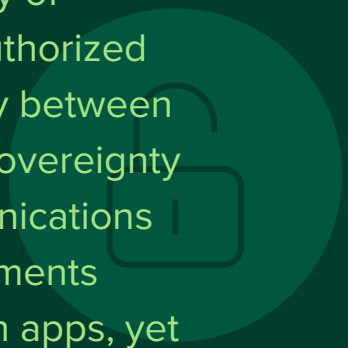
In today's fast-moving, digital workplaces, an organization's communication technologies (e.g., messaging/chat, voice, videoconferencing tools) are fundamental to bridging the distance between workers and their colleagues, customers, and partners. However, leaders are finding that traditional communication approaches often fall short as security threats, compliance requirements, interoperability challenges, and the need for more controls continue to rise.

In the spring of 2023, Element commissioned Forrester Consulting to explore the value leaders see in secure communications platforms for addressing these issues. Forrester conducted an online survey with 217 global leaders with authority over their organization's communication technology decisions from government, healthcare, energy/utilities, and transportation/logistics sectors to explore this topic. The study uncovered that there's a large and growing need for secure communications to improve real-time connections within and beyond the organization without sacrificing security and compliance goals.

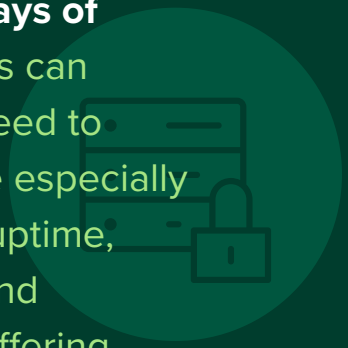
Key Findings

Leaders are paying particular attention to partner communications. The ability to funnel the capabilities of external partners is now vital.[1] However, external communications introduce security concerns, and a lack of common technology standards presents compatibility issues. Because of this, 63% of leaders note securing communications along supply chains as a top near-term priority.

A lack of control is a common obstacle to success. Tech leaders must optimize the security and reliability of real-time communications, but face challenges. Unauthorized apps, inflexible systems, and a lack of interoperability between tools are common. Inadequate capabilities for data sovereignty means that leaders have limited control over communications data, making adherence to data governance requirements difficult. Many also are using different communication apps, yet still face concentration risk due to a reliance on large vendors.



A secure communications platform enables new ways of working and specific use cases. Dedicated platforms can bridge the gap between existing solutions and the need to support different workers and scenarios. Leaders are especially interested in platforms that support high availability/uptime, end-to-end encryption, reliability, data sovereignty, and federation. A majority of leaders believe a platform offering these and other high-value capabilities would allow them to realize meaningful security, user experience, compliance, and productivity improvements.



Real-Time Communications Underpin Business Operations

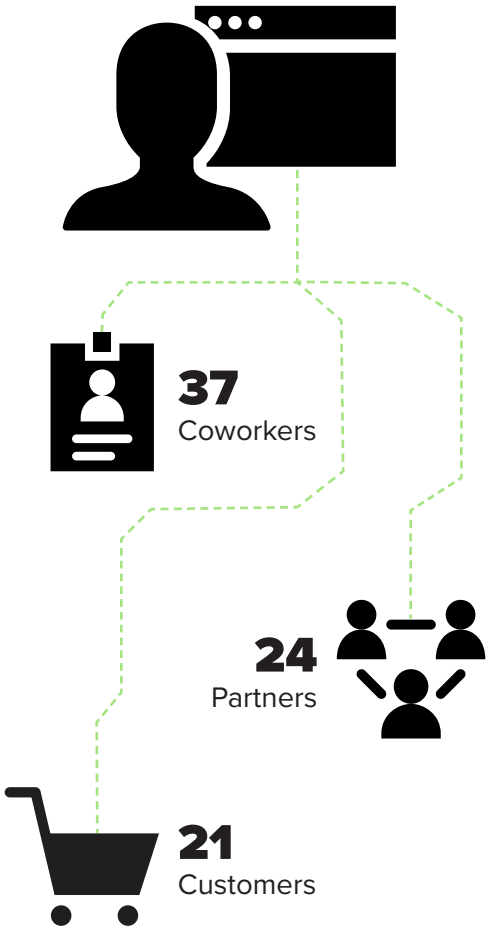
An organization's communication tools are a key part of workers' daily collaboration with internal and external stakeholders. They also often transmit customers' personal information, insights about business operations, confidential documents, or other highly sensitive material.[2] Ensuring that these tools operate without interruption, delay, or compromise under all circumstances is now business critical. However, it's also more complicated in today's interconnected world where systemic risks, compliance requirements, security threats, and user experience expectations continue to evolve.[3]

Seventy-five percent of leaders say that the reliability and security of their organization's communications are critical to ensuring trust in their services. Yet many of them are concerned about the security and reliability of internal and external communications. In a typical week, communication tools connect each employee to many colleagues, customers, and partners (see Figure 1).[4] Changes in employee work patterns, customer expectations, and the way value chains operate are adding complexity to these interactions and putting new demands on tools. For example, 74% of leaders have experienced challenges securing internal communications due to the rise of hybrid work, and 66% are finding that customers increasingly expect transparency and control over the information they share.

FIGURE 1

Employee Communications Span A Wide Network

Average number of people each employee communicates with in a typical work week:



Base: 217 global communications technology decision-makers
Source: A commissioned study conducted by Forrester Consulting on behalf of Element, May 2023

COMMUNICATION FRICTION WITH EXTERNAL PARTNERS CAN LEAD TO RISKY WORKAROUNDS

Fifty-six percent of respondents acknowledge that their organization is but one piece of a larger value chain of partners working together to deliver critical services to customers. Thus, fast, secure, and effective partner communications are essential. Employees are using a range of traditional tools with partners, with 88% reporting that email is used often or very frequently. Email's popularity is expected given that it operates on a common standard, making it the common denominator between organizations.

While email and other frequently used tools like audio and videoconferencing tools are important, each also has compatibility, user experience, and/or security limitations when used with partners; most respondents agree that they are not very well suited for enabling secure and reliable real-time communications in this context (see Figure 2). For example, a lack of end-to-end encryption makes email messages less secure. Respondents speak of viruses that can easily spread through email attachments and links and a lack of real-time interaction.

Siloed communications platforms, time delays, and collaboration friction can no longer keep up with market realities and experience expectations. Employees accustomed to using more seamless, instant communication methods internally and in their personal lives may resort to consumer messaging apps if organizational tools are not up to the task. In fact, 52% of leaders say their employees are commonly using unsanctioned, real-time messaging apps with partners. Unsanctioned communication tools introduce a host of serious risks, including noncompliance, eavesdropping, data loss or exposure, lack of admin controls, and reputational concerns.[5]

> Unsanctioned apps creep into the enterprise when organization-provided tools are not up to the task.

FIGURE 2

Traditional Tools Fall Short In Adequately Supporting Secure And Reliable Partner Communications

(Showing "Not very well suited")

Sanctioned/work email — 66%

"Viruses can be easily spread through email attachments or links"
— Manager at a healthcare organization in the US

"Lower collaboration capacities"
— Director at a transportation and logistics company in France

"Real-time interaction is not there"
— Director at a defense/national security agency in the US

Sanctioned voice tools — 76%

"Makes it difficult to streamline workflows or automate certain processes"
— Manager at an energy generation company in the US

"Less scope for documentation"
— C-level executive at a transportation and logistics company in the UK

"Not easily accessible from anywhere"
— Manager at a regional government agency in Germany

Sanctioned video conferencing tools — 79%

"Less smooth communication and higher downtime"
— Director at a healthcare organization in Canada

"Difficulties with [technology] compatibility and collaboration"
— Director at a defense/national security agency in the UK

"There is a huge risk when sharing sensitive information"
— Director at a defense/national security agency in France

Base: 217 global communications technology decision-makers
Note: Showing three responses
Source: A commissioned study conducted by Forrester Consulting on behalf of Element, May 2023

THE IMPORTANCE OF SECURE AND RELIABLE PARTNER COMMUNICATIONS IS GROWING

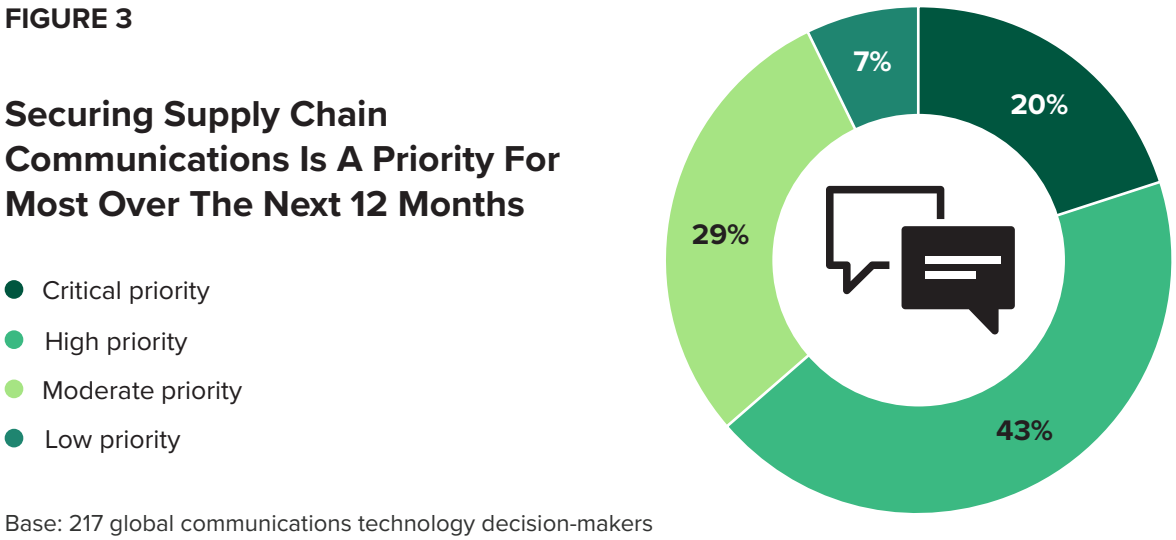
Fifty-three percent of leaders expect the number of partners in their supply chain to grow over the next two to three years. As reliance on partners increases, so does the importance of securing partner communications. Sixty-three percent of leaders state that securing communications along their supply chains is a high or critical priority for their organization over the next year (see Figure 3.)

77%

say that security vulnerabilities in communication tools used with partners pose a significant risk to their organization.

FIGURE 3

Securing Supply Chain Communications Is A Priority For Most Over The Next 12 Months



Base: 217 global communications technology decision-makers
Note: Percentages may not total 100 due to rounding.
Source: A commissioned study conducted by Forrester Consulting on behalf of Element, May 2023

Existing Communication Approaches Reveal Capability Gaps And Present Risks

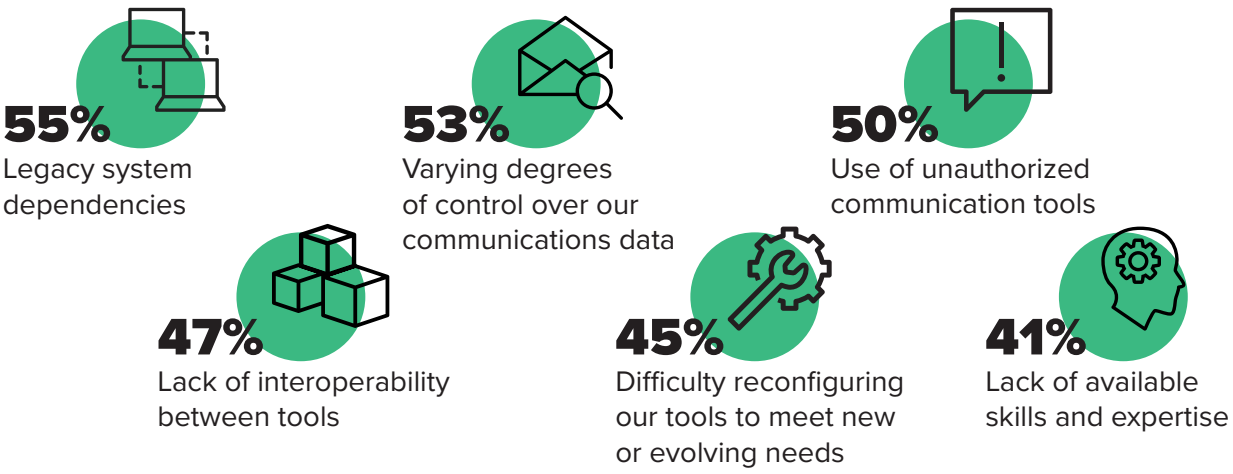
Beyond the use of unauthorized communication tools, which 50% of respondents describe as a significant challenge, a number of other obstacles stand in the way of leaders' ability to improve the security and reliability of real-time communications (see Figure 4).

Among the most common are legacy and other inflexible systems that cannot easily be reconfigured to meet new or evolving needs. Another is varying degrees of control over communications data, depending on available configurations and options for data hosting and capabilities to support data sovereignty. A lack of interoperability between tools means that most apps are not talking to each other, contributing to communication silos as well as frequent app/context switching, which zaps workers' focus and productivity.

> As the number of apps workers need continues to grow, interoperability becomes even more important to prevent context-switching and time loss.[6]

FIGURE 4

Significant Obstacles To Improving The Security And Reliability Of Real-Time Communications



Base: 217 global communications technology decision-makers
Note: Showing top 6 responses
Source: A commissioned study conducted by Forrester Consulting on behalf of Element, May 2023

On average, surveyed leaders manage five unique communication apps, while 21% have seven or more. While leaders are grappling with a plethora of communication tools, their organizations still face concentration risk. In early 2020, standalone apps for chat, videoconferencing, or document-sharing began to give way to broader bundles from large vendors as work-from-home mandates forced enterprises into a digital-first mode of work.[7] Signaling the reliance on these "mega vendors," 85% say disruption from just one of their large communication technology vendors is enough to pose significant risk to their organizations.

"SAFE ENOUGH" COMMUNICATIONS ARE INSUFFICIENT

Organizations must consider how well their communications technologies stand up to various scenarios and stress tests. Even sanctioned apps pose a risk in certain use cases.[8] One example is incident response: 75% of decision-makers are concerned about the compromise of their communications technologies during a cyberattack, which may lead to attackers monitoring workers' and incident responders' real-time communications. Traditional tools may also lack certain controls, such as more granular access controls for external collaboration or data protection.[9]

Sixty-five percent of decision-makers say the potential direct (e.g., fines, revenue losses due to system downtime) and indirect (e.g., lost employee productivity) costs of a security breach involving their communications would be significant. Most are speaking from first-hand experience: 66% come from organizations that have suffered a communications-specific breach or compromise in the last three years, while 25% have had multiple incidents in that period. These incidents led to several negative consequences, including additional security/audit requirements, regulatory investigations, and lost productivity, with diminished customer (ranked first) and partner (ranked fourth) trust among the most common outcomes.

72%

say that disruptive events have highlighted the strategic importance of their communications technologies.

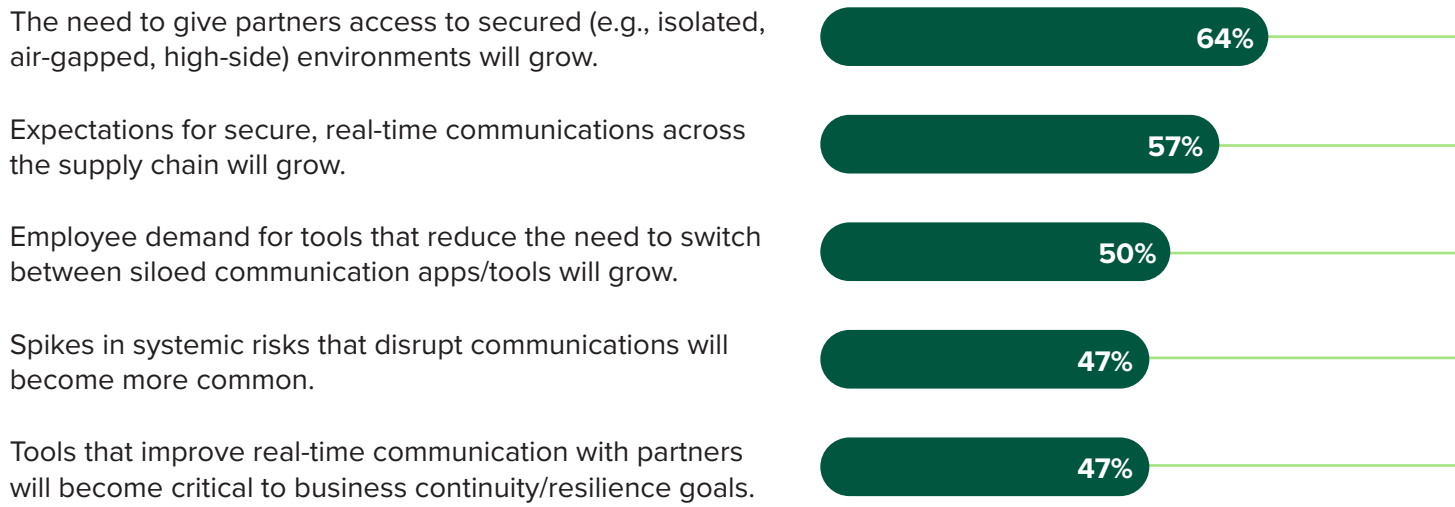
A Secure Communications Platform Supports A Future Fit Organization

Decision-makers predict that communication within and beyond the organization will need to evolve to be even more secure, seamless, and resilient (see Figure 5). To prepare, organizations must become future fit. A key part of future fitness is being ecosystem driven, i.e., adept at capturing the value available in the organization's internal and external ecosystems at scale.[10]

Optimizing communications between all players brings organizations one step closer to this vision and opens up opportunities for greater collaboration and innovation. However, security and dependability must be front and center to prevent these opportunities from turning into threats. Respondents believe that efforts focused on strengthening the security and reliability of real-time communications would lead to a significant reduction in their organizations' overall regulatory (78%), security (75%), operational (70%), and reputational (68%) risk exposure.

FIGURE 5

Internal And External Communications Will See Transformation In The Future



Base: 217 global communications technology decision-makers
Note: Showing top 5 responses
Source: A commissioned study conducted by Forrester Consulting on behalf of Element, May 2023

DEDICATED PLATFORMS PROVIDE SECURITY AT SCALE

Certain scenarios (e.g., response to a data security incident or disruption to critical infrastructure) and users (e.g., frontline workers, senior executives) have specific communication requirements that demand more care. This is where a secondary platform that delivers secure communications plays a critical role. For example, they can enable a channel for:

- **Out-of-band communications.** Out-of-band communication channels are those that are separate from the organization's primary communications infrastructure. These channels are particularly useful in situations supporting business continuity (e.g., if the organization's main servers go down), executive conversations around sensitive topics (e.g., hiring, bonuses, mergers/acquisitions), and incident response (e.g., when a cyberattack impacts or compromises primary channels).
- **Air-gapped communications.** Air-gapped communication channels refer to highly secure networks that are physically separated from other networks and systems. These channels are useful in situations supporting a high-side environment in government, intelligence, or defense for classified information. They are also useful in strongly regulated environments (e.g., stock exchanges) and industrial control environments (e.g., critical systems like controls for nuclear power plants, aviation) requiring this level of separation for security and privacy.

Fifty-two percent of leaders say that their organization has a large or significant need for real-time communications within secure (e.g., air-gapped, isolated, high-side) environments like these for a variety of scenarios, and most expect this need to grow (see Figure 6).

64%

expect their organization's need to provide their partners with access to air-gapped or isolated environments to grow over the next two to three years.

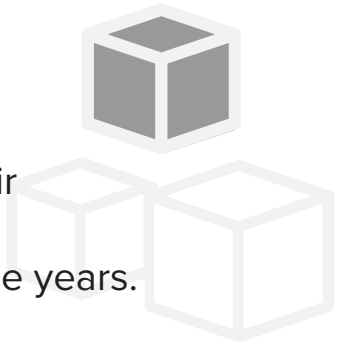
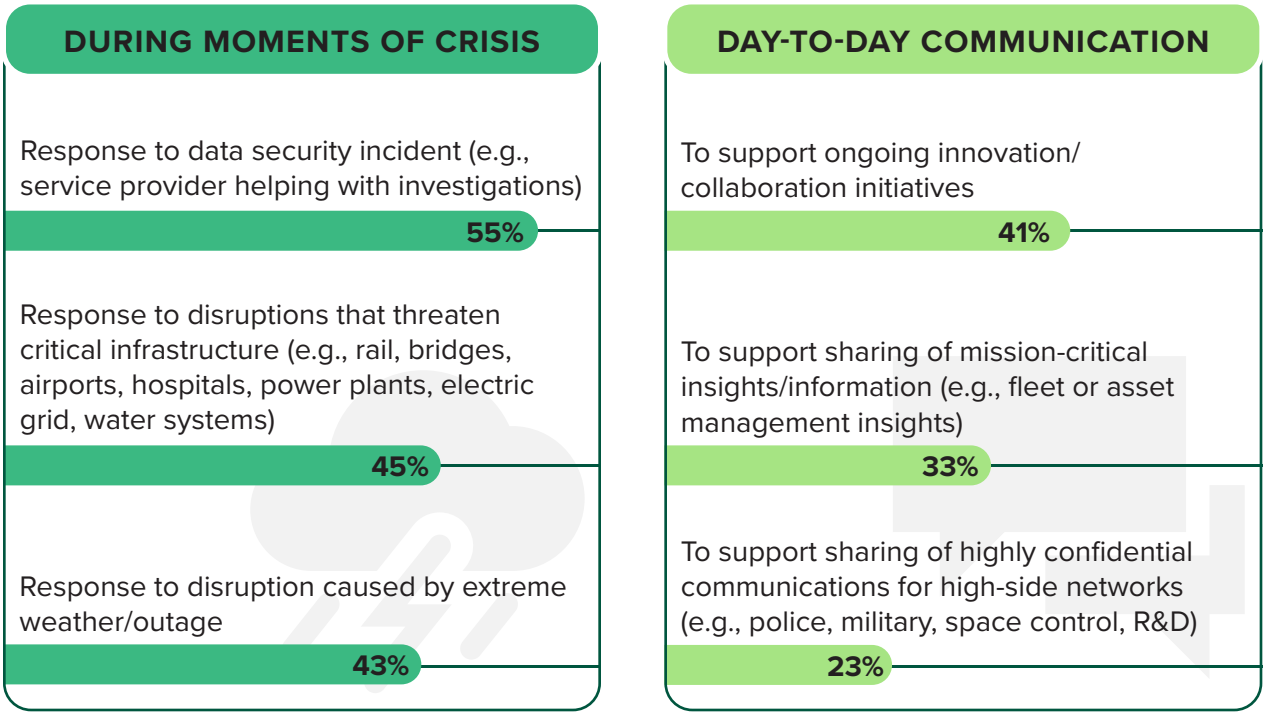


FIGURE 6

Secured, Real-Time Communications Are Needed In Crisis And Day-To-Day Scenarios



Base: 212 global communications technology decision-makers at organizations with need for real-time communications within secured environments
Note: Showing top responses
Source: A commissioned study conducted by Forrester Consulting on behalf of Element, May 2023

LEADERS SEEK PLATFORM CAPABILITIES THAT OFFER DIFFERENTIATED VALUE

Seventy-seven percent of leaders agree that the market environment demands that they keep up with leading capabilities for securing their communications. In the case of secure communications platforms, this means prioritizing solutions that provide (see Figure 7):

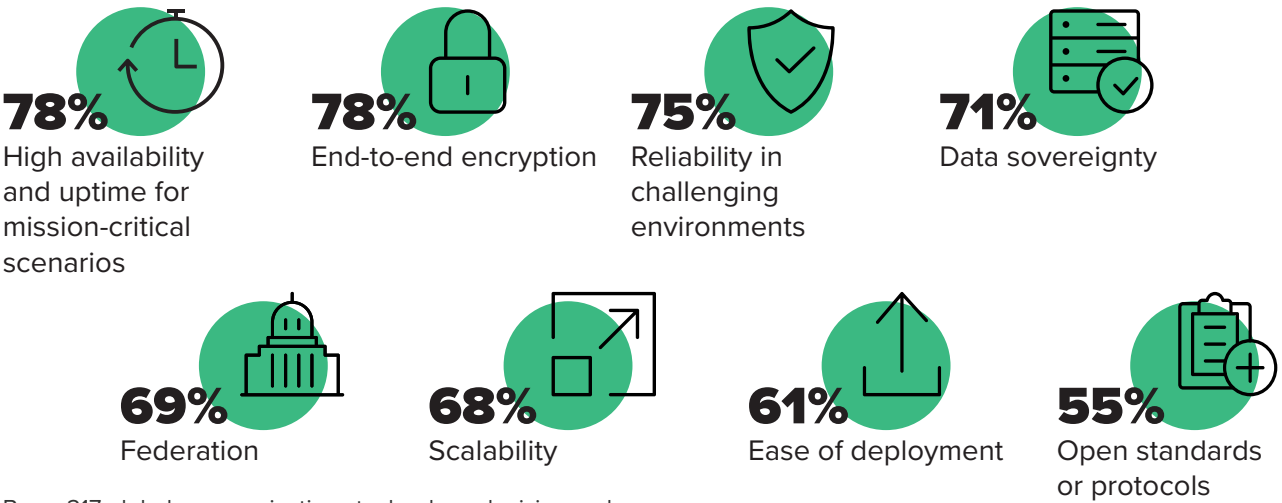
- High-availability and uptime for mission-critical scenarios, especially those found in critical infrastructure sectors. Indeed, this is a top-three capability for those in healthcare, and the number one most-valued capability for those in government and energy/utilities sectors.

- End-to-end encryption to protect data, such that even the technology provider and platform itself cannot see the content of the communications. The data is encrypted at the endpoint prior to its transmission — a measure to ensure data security, privacy, and mitigation against data tampering. Only the sender and receiver have access to the data.
- Reliability in challenging environments, such as in areas with low bandwidth or connectivity, to support an organization's operational and business resilience.
- Data sovereignty through capabilities that provide ownership and control of communications data (including where and how it's hosted and managed) so it remains subject to the organization's governance structure.
- Federation, which brings separate communication technology deployments together, enabling easy connectivity between different organizations across the supply chain or within one large organization.

FIGURE 7

Leading Capabilities Have The Power To Optimize Real-Time Communications

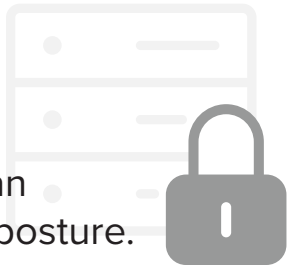
(Showing "Considerable value" and "Transformational value")



Base: 217 global communications technology decision-makers
Note: Showing eight responses
Source: A commissioned study conducted by Forrester Consulting on behalf of Element, May 2023

Seventy-seven percent of leaders report that their organization struggles to maintain privacy and control of data shared via communications technologies. Between this obstacle and the need to juggle regulatory and organizational requirements for data governance and control, the value that leaders place on data sovereignty becomes clear. Beyond strengthening their organizations' security posture, other top benefits of data sovereignty cited include greater protection against vendor lock-in (e.g., because the organization's data isn't in a proprietary vendor's system) and compromise stemming from a third-party vendor or tool.

> **64%**
>
> associate data sovereignty capabilities with an improvement to their organization's security posture.



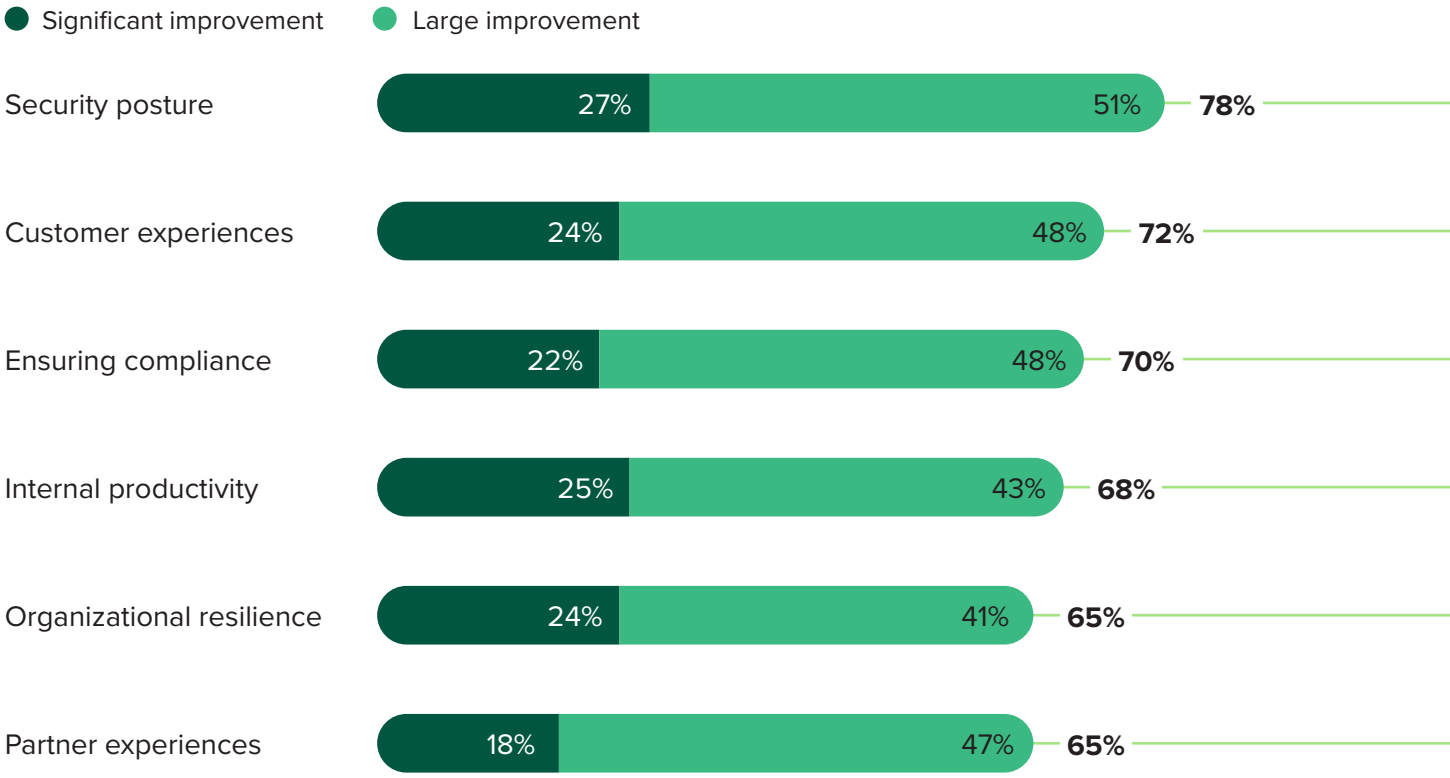
Leaders are likely to consider several other factors when evaluating secure communications platforms. Among these is support for open standards. Open standards help solve interoperability needs by providing formalized protocols accepted by multiple players (much like the common standards used for email) that allow for greater interconnectedness between an organization and its industry ecosystems. They also reduce the organization's dependence on any single vendor, making it possible to link to any number of vendors offering a vibrant range of products, fostering innovation across the ecosystem.

SECURE COMMUNICATION PLATFORMS ELEVATE SECURITY AND USER EXPERIENCES

Fewer than 45% of leaders say that their company's current tools can support any of these leading capabilities very well. However, they believe that access to a secure communications platform with these capabilities would deliver considerable value. Among the benefits they'd expect to realize is a meaningful improvement to their security posture, customer and partner experiences, compliance (e.g., data retention, privacy), and productivity (see Figure 8).

FIGURE 8

Secure Communications Platforms That Offer Leading Capabilities Deliver Numerous Benefits



Base: 217 global communications technology decision-makers
Note: Showing the impact respondents expect to realize from adopting a secure communications platform with the capabilities previously identified as valuable (e.g., high availability, end-to-end encryption, reliability, data sovereignty, federation, among others)
Source: A commissioned study conducted by Forrester Consulting on behalf of Element, May 2023

Key Recommendations

Forrester's in-depth survey of over 200 technology decision-makers about secure communications yielded five important recommendations:

Ease of use is non-negotiable.

If employees and partners don't see the value in a solution, they won't use it. As organizations map their requirements and desired capabilities for secure communications technology, ease of use will be a key consideration. With so many available — and unsanctioned — options, people will do what they need to do to get their job done.

Secure your organization's communication data via flexible hosting options and end-to-end encryption to achieve true data sovereignty.

Additional granular controls and security features include bring your own key for encryption, crypto agility, and vendor transparency with software bill of materials (SBOM) reports. Robust security functionality can also help tremendously with various security and privacy compliance requirements by enabling control over your organization's data.

Look for added functionality to support compliance requirements beyond security and privacy.

Depending on the specific compliance requirement that you are trying to meet, such as sector-specific regulations or contractual requirements from business partners, security functionality may not be enough. For example, you may have requirements for data deletion or retention.

Address the outage and cybersecurity risks coming from centralized solutions.

Communications are the backbone of business operations, and secure communications matter both for everyday communications and in moments of crisis. Hybrid work practices will ebb and flow as organizations adapt to a host

of externalities from extreme weather to competitive hiring practices. Systemic risk events, disruptions and outages, and issues with critical infrastructure also fuel the need for operational and business resilience. These tools must work where your employees and partners need them to work.

Embed interoperability into your firm's communications solution to meet regulatory demands and evolving requirements.

The use of open standards for interoperability will enable users of one platform to communicate with users of another platform. In the EU, the Digital Markets Act (DMA) adopted in May 2022 requires interoperability for messaging platforms; such platforms have until March 2024 to comply.[11] Messaging Layer Security (MLS) Protocol, an interoperable standard in development for years by the Internet Engineering Task Force (IETF), is published as an RFC as of July 2023.[12] Other open standards include Web Real-Time Communication (WebRTC), Session Initiation Protocol (SIP), Extensible Messaging and Presence Protocol (XMPP), and Matrix. For messaging platforms, interoperability will be a requirement to help support a future fit organization.

Appendix A: Methodology

For this study, Forrester conducted an online survey of 217 decision-makers at government (central and regional), energy/utility, healthcare, and transportation/logistics organizations in North America and Europe to evaluate current and future communication technology needs. Questions provided to the participants asked about the frequency with which employees are using various tools for communications; obstacles to improving the security, reliability, and experience of these interactions; and the value a secure communications platform may provide in mitigating common challenges and driving new value. Respondents were offered a small incentive as a thank-you for time spent on the survey. The study fielding began and was completed in May 2023.

Appendix B: Demographics

COUNTRY	
United States	**32%**
Canada	**19%**
United Kingdom	**18%**
Germany	**16%**
France	**15%**

INDUSTRY	
Federal/central government	**30%**
Energy and utilities	**21%**
Healthcare	**20%**
State/regional government	**16%**
Transportation and logistics	**13%**

DEPARTMENT	
IT	**55%**
Security	**30%**
Compliance/risk	**16%**

NUMBER OF EMPLOYEES	
2,500 to 4,999	**11%**
5,000 to 9,999	**65%**
10,000 to 19,999	**18%**
20,000 or more	**7%**

SENIORITY	
C-level executive	**7%**
Vice president	**15%**
Director	**30%**
Manager	**47%**

Note: Percentages may not total 100 due to rounding.

Appendix C: Endnotes

[1] Source: "The Future Fit Practices Strategy," Forrester Research, Inc., September 23, 2022.

[2] Source: "Now Tech: Secure Communications, Q2 2022," Forrester Research, Inc., May 2, 2022.

[3] Experience in this context refers to the perceptions an individual (be it a customer, employee, or partner) has about their interactions with a company. For example, the employee experience represents the perceptions employees have about their interactions with their employer, including their perceptions of the technology they are provided to complete their daily work.

[4] For the purposes of this study, "customer" refers to any individual or entity the organization exists to serve (e.g., citizens, patients, clients).

[5] Source: "Now Tech: Secure Communications, Q2 2022," Forrester Research, Inc., May 2, 2022.

[6] Source: "Make Digital Employee Experience The Centerpiece Of Your Digital Workplace Strategy," Forrester Research, Inc., November 15, 2022.

[7] Source: "The Forrester Tech Tide™: Enterprise Collaboration Technologies, Q3 2022," Forrester Research, Inc., September 19, 2022.

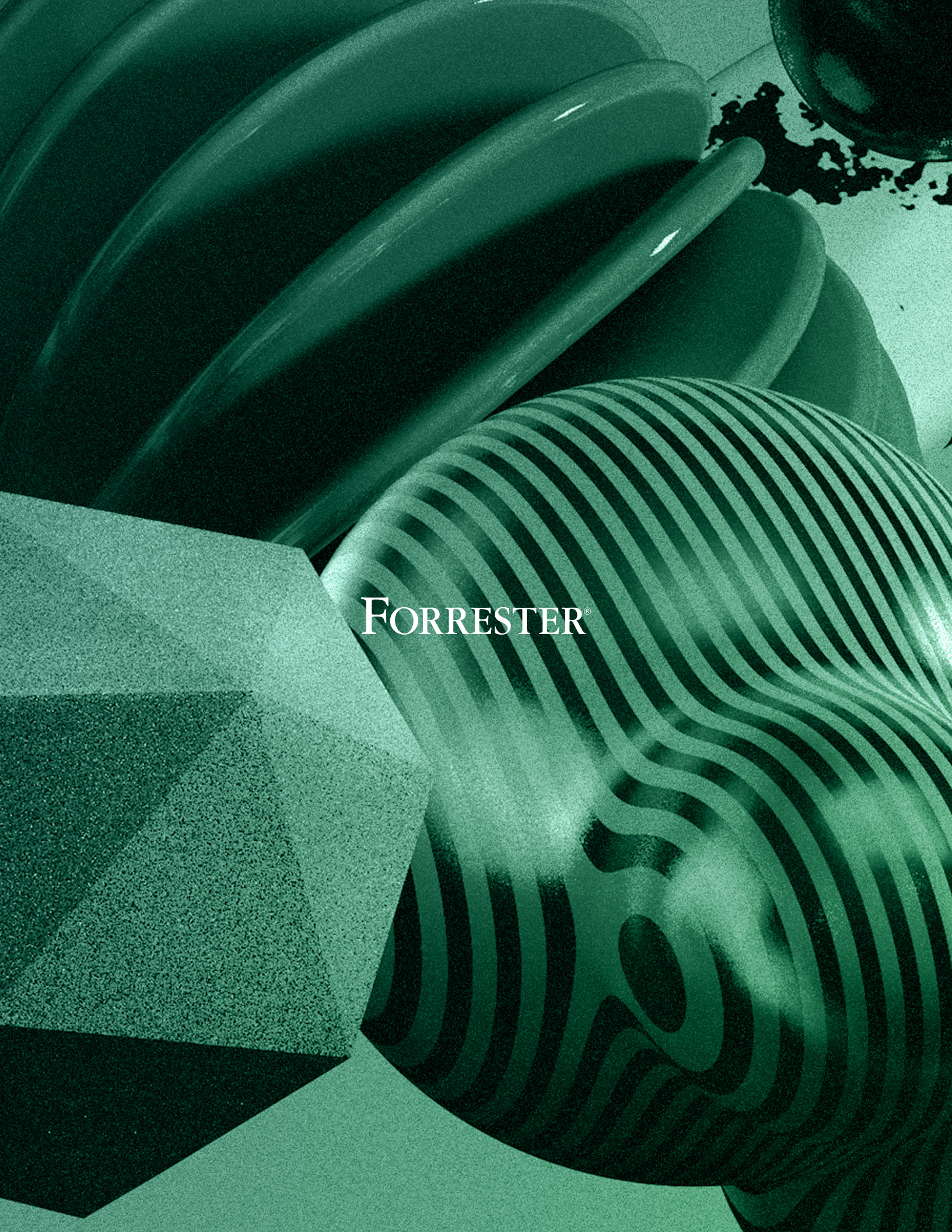
[8] Source: "Now Tech: Secure Communications, Q2 2022," Forrester Research, Inc., May 2, 2022.

[9] Ibid.

[10] Source: "The Future Fit Practices Strategy," Forrester Research, Inc., September 23, 2022.

[11] Source: "Digital Markets Act: rules for digital gatekeepers to ensure open markets enter into force," European Commission press release, October 31, 2022.

[12] Source: "New MLS protocol provides groups better and more efficient security at Internet scale," Internet Engineering Task Force, July 19, 2023.


FORRESTER®