Internet of Things Integration

Technology Snapshot

Second Front Systems (2F)
is a public benefit, venture-backed software company dedicated to fast-tracking government access to emerging technology for national security missions.

EXECUTIVE SUMMARY

Though the number of Internet of Things (IoT) devices online today continues to fall below what experts predicted just a half decade ago, IoT use cases are maturing across varied industries, including retail, logistics, and transportation. As organizations consider IoT solutions - either as initial pilots or follow-on projects - ensuring smooth integration with existing hardware and software systems remains a key challenge. A diverse set of vendors aim to address this challenge, as well as complementary concerns, particularly IoT cybersecurity.

Published August 2021.

TABLE OF CONTENTS

ABOUT

Atlas Fulcrum is Second Front System's subscription-based technology research and innovation scouting platform to help government users discover and engage Venture Capital (VC)-backed, commercially-developed technologies for national security missions. Specifically designed to access "dual-use" (commercial and government) technologies, Atlas Fulcrum is supported by a research team that combines deep understanding of national security mission requirements and US Government customers with VC best practices. This custom support is combined with best-of-breed commercial tools to enable users to more quickly and easily identify, assess, and access these technologies.

Second Front Systems, Inc. is a lightweight systems integrator and public benefit corporation committed to bringing emerging technology to bear on pressing national security missions. Second Front has operations in Washington, D.C. and San Francisco. More information can be found at secondfront.com.

INTERNET OF THINGS INTEGRATION

> "New and old machines rarely integrate as well as one might hope… If your chosen [Internet of Things] project will require technological heroism, or the digital equivalent of duct tape solutions for tricky integration challenges, consider a different project instead. Come back to your favorite project when reliable connectors become available or when new generations of equipment are more compatible."
>
> - George Westerman
> Sloan School of Management
> Massachusetts Institute of Technology[1]

PROMPT

This report examines key challenges and considerations for implementing Internet of Things (IoT) solutions in enterprise environments, with a particular emphasis on the integration between IoT devices and legacy software.

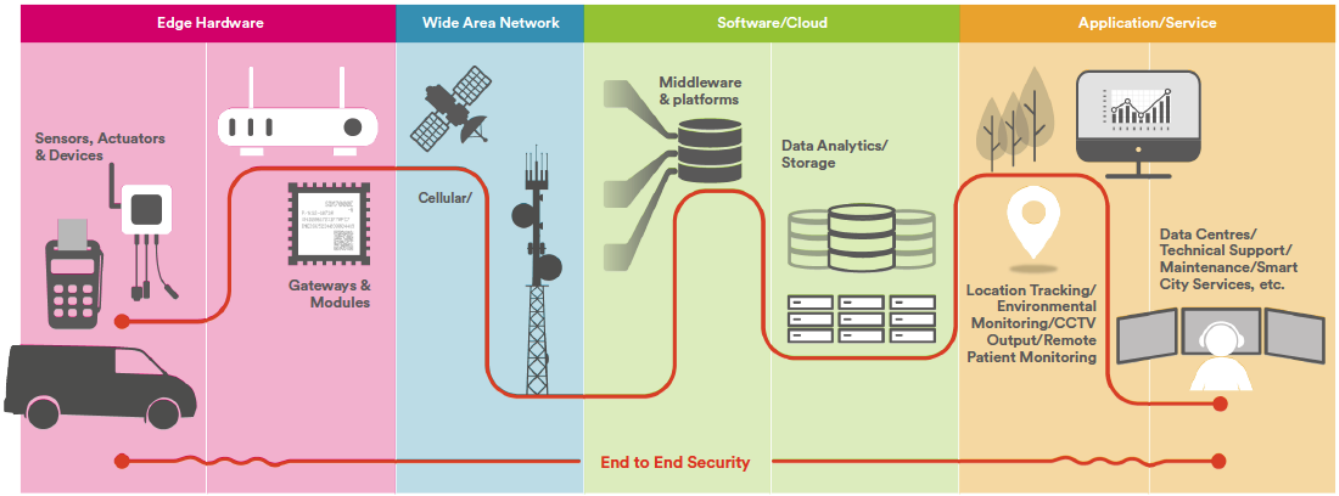
BACKGROUND

IoT encompasses billions of internet-connected devices around the world deployed at the edge to collect and share data.[2] The way these "smart" devices - which can include objects as diverse as wearable fitness trackers, home thermostats, Radio-Frequency Identification (RFID) tags, and infrastructure sensors - communicate with one another, data analytics and storage tools, and the humans they are designed to inform, make up the broader IoT solution stack (see Graphic 1. below). In general, IoT, an admittedly amorphous label, is only applied to objects that until recently would not have had an internet connection, leaving laptops, desktops, and mobile phones out from underneath the IoT umbrella.[3]

Distinct from consumer-focused applications, the growing maturation of "IoT-enabled industrial assets" - autonomous robots with IoT sensors, for example - has spurred some enterprises to experiment with or fully embrace smart factories, smart warehouses, smart grids, and smart

[1] Brian Gilmore and George Westerman. "Realizing IoT's Potential: How to Overcome Challenges to Enterprise Implementation." *MIT Sloan Management Review*. January 2020. https://sloanreview.mit.edu/sponsors-content/realizing-iots-potential-how-to-overcome-challenges-to-enterprise-implementation/.
[2] Lionel Sujay Vailshery. "Internet of Things (IoT) and Non-IoT Active Device Connections Worldwide from 2010 to 2025." *Statista*. March 2021. https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/.
[3] Steve Ranger. "What Is the IoT? Everything You Need to Know About the Internet of Things Right Now." *ZDNet*. February 2020. https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/.

plants.[4] The industrial IoT (IIoT), as this subsector of the wider IoT market is commonly known, is often associated with broader digital transformation efforts underway as part of the fourth industrial revolution, or Industry 4.0.[5]



Graphic 1. - Typical elements of an IoT solution. Source: Beecham Research.[6]

PRIMARY FINDINGS

IoT solutions are maturing across a wide range of industries, including consumer electronics, retail, industrial manufacturing, logistics, and transportation. Findings from a 2020 study of the Australian retail sector highlight several advantages of IoT adoption for organizations involved in supply chain management, in particular. By providing enterprises with real-time asset tracking and ecosystem visibility, IoT projects can save money, time, and energy; improve warehouse productivity and safety; and reduce inventory-related waste, among other benefits.[7] It is important to note, however, that successful implementation is not a given. IoT project failures are common, often due to the complexity and cost of integration across the IoT solution stack and with non-IoT systems and software.[8]

---

[4] "Industry 4.0 and the Fourth Industrial Revolution Explained." *i-SCOOP*. Accessed August 2021. https://www.i-scoop.eu/industry-4-0/.
[5] Ibid.
[6] "Why IoT Projects Fail." *Beecham Research*. 2020. https://www.whyiotprojectsfail.com/?cs=r1brpfh.
[7] Shah J. Miah, Himanshu Shee, and Tharaka de Vass. "IoT in Supply Chain Management: A Narrative on Retail Sector Sustainability." *International Journal of Logistics Research and Applications*. June 2020. https://www.researchgate.net/publication/342578541_Iot_in_supply_chain_management_a_narrative_on_retail_sector_sustainability.
[8] Kyle Wiggers. "Microsoft: 30% of IoT Projects Fail in the Proof-of-Concept Stage." *Venture Beat*. July 2019. https://venturebeat.com/2019/07/30/microsoft-30-of-iot-projects-fail-in-the-proof-of-concept-stage/.

In order to optimize chances of successful implementation, enterprises must first decide whether to build a custom IoT platform, buy one ready-made, or pursue a combination of the two. Each option has its own benefits and drawbacks:

- **Build.** Enterprises that choose to build an IoT platform can exert more control over its functionality. This is especially useful when the solution must integrate with legacy systems already in the environment, or manage a mix of IoT sensors with varying connectivity needs and other requirements.[9]

  However, this route requires a high level of in-house expertise, not just during the initial build process, but throughout the lifecycle of the project via continuous maintenance, platform management, and security testing.[10] Over time, accumulated costs (including the resources required to hire and retain developers) can sometimes surpass the sticker price of a new off-the-shelf platform.[11]

- **Buy.** Though vendors often develop IoT platforms with diverse devices, connectivity methods, power needs, and security requirements in mind, enterprises looking to adopt a ready-made solution may face tradeoffs for their particular use case.

  Should an enterprise go the "buy" route, they must choose outside partners carefully, according to the head of global IoT research for Frost & Sullivan, a Texas-based market research firm. Out of the roughly 500 vendors advertising an IoT platform, he cautions, "only 30-40 offer true platform capabilities."[12] As this comment suggests, definitions of platform capabilities vary, though they are often thought to include "device and endpoint management, connectivity and network management, data management, processing and analysis, application development, security, access control, monitoring, event processing and interfacing/integration."[13]

- **Hybrid.** A hybrid path entails partnering with outside experts in a "building block" approach that mixes and matches capabilities to address specific use cases.[14] Though this approach offers flexibility, it also adds complexity. Since IoT solution deployments often include numerous partners across different layers of the technology stack, from device makers to data analytics software providers, engaging with multiple vendors at the

[9] Crystal Bedell. "Build or Buy? An Executive's Guide to IoT Platforms." *IoT World Today*. April 2019. https://www.iotworldtoday.com/2019/04/24/build-or-buy-an-executives-guide-to-iot-platforms/.
[10] Walter Haydock. "IIoT Cybersecurity: Why Building Your Own Platform Comes with Risk." *PTC*. May 2021. https://www.ptc.com/en/blogs/corporate/iiot-cybersecurity-risks.
[11] Bedell.
[12] Ibid.
[13] "IoT Platforms – IoT Platform Definitions, Capabilities, Selection Advice and Market." *i-SCOOP*. Accessed August 2021. https://www.i-scoop.eu/internet-of-things-iot/iot-platform-market-2017-2025/.
[14] Ibid.

middleware or platform level can heighten management-related challenges and also require some of the in-house expertise required for the "build" approach.[15]

As organizations weigh their options, the pool of potential industry partners is diverse. Big name cloud vendors like **Amazon Web Services** (https://aws.amazon.com/), **Google Cloud** (https://cloud.google.com/solutions/iot), and **Microsoft Azure** (https://azure.microsoft.com/en-us/overview/iot/) are popular choices for enterprises interested in the hybrid approach, while **PTC** (https://www.ptc.com/) and Germany's **Software AG** (https://www.softwareag.com/) have emerged as market leaders for IIoT platforms.[16] Smaller shops have also entered the IoT platform market with custom platform developers, like **Cloudastructure** (https://cloudastructure.com/) and **Losant** (https://www.losant.com/), as well as ready-made solution providers like **Particle** (https://www.particle.io/) and **Tulip Interfaces** (https://tulip.co/).

George Westerman, a senior lecturer at Massachusetts Institute of Technology's (MIT's) Sloan School of Management, recommends selecting a partner that has experience relevant to the proposed project and is willing to shoulder at least some of the risk inherent in complicated integrations.[17] To realize an IoT solution's full potential, such integrations with existing legacy and proprietary systems - like enterprise resource planning (ERP) software, customer relationship management (CRM) tools, or manufacturing execution systems (MES) - are critical.[18]

Despite the benefits of a complementary approach, integration between these tools and IoT devices is often challenging. A 2017 survey of two hundred North American IIoT decision makers, conducted by Swedish enterprise asset management and vendor in this space **IFS** (https://www.ifs.com/), found that only about a fifth of organizations feed data from IoT devices and sensors into their organization's ERP software.[19] Responses from those surveyed suggest the inability of ERP systems to ingest and understand IoT data in real-time (or, in some cases, at all) as the largest obstacle to integration.[20] Though some legacy or proprietary systems were originally designed to read bar codes, RFID tags, and other specific pieces of information, many are not automatically equipped to ingest the more diverse datasets generated by IoT sensors.[21]

---

[15] "David Gustovich. "Integrating IoT and ERP Data to Achieve Performance Excellence." *TechTarget*. September 2018. https://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/Integrating-IoT-and-ERP-data-to-achieve-performance-excellence.

[16] Eric Goodness, et al. "Magic Quadrant for Industrial IoT Platforms." *Gartner*. October 2020. https://www.gartner.com/doc/reprints?id=1-24KDTTSL&ct=201109&st=sb.

[17] Gilmore and Westermen.

[18] Mary Shacklett. "Can IoT Eliminate the Need for ERP and MES in Manufacturing?" *TechRepublic*. July 2021. https://www.techrepublic.com/article/can-iot-eliminate-the-need-for-erp-and-mes-in-manufacturing/.

[19] "IFS Study: 84% of Industrial Companies Face Gap between IoT and ERP." *IFS*. September 2017. https://www.ifs.com/news-and-events/newsroom/2017/09/27/ifs-study-84-of-industrial-companies-face-gap-between-iot-and-erp/.

[20] Ibid.

[21] Mary Shacklett. "Can ERP and MES Systems Keep Up with IIoT?" *IoT World Today*. August 2021. https://www.iotworldtoday.com/2021/08/02/can-erp-and-mes-systems-keep-up-with-iiot/.

A more recent global survey conducted by Microsoft shows integration remains a persistent inhibitor of IoT adoption. According to the 2020 report, 25% of participating companies described IoT solutions as too difficult or time-consuming to implement, while 28% reported they did not have the budget or human capital to adopt one.[22]

In response to these integration challenges, companies are developing tools to streamline flows of information between IoT sensors and systems already deployed in an enterprise environment. In partnership with Microsoft Azure, the IFS' IoT Business Connector tool, for example, purports to open lines of communication and translate IoT data into actionable insights within ERP systems.[23] **Bridgera** (https://bridgera.com/), a custom IoT solution provider, uses an application programming interface (API) based approach also intended to integrate IoT devices and data with a variety of legacy systems, including CRM and ERP software. In addition, several companies offer ERP solutions explicitly designed with IoT integration in mind, like one from **Aptean** (https://www.aptean.com/).

Analytics platforms have also proven useful for helping organizations transform vast amounts of IoT-generated data into more ingestible and actionable formats, for both legacy systems and their human operators.[24] While established big names, including **IBM** (https://www.ibm.com/) and **SAP** (https://www.sap.com/), are key players in this market, younger venture-backed companies, like **Cloudera** (https://www.cloudera.com/) and **DataStax** (https://www.datastax.com/), have also gained recognition.[25]

ADDITIONAL FINDINGS

SECURITY CONSIDERATIONS

As the exploration, adoption, and maturation of IoT solutions expands across diverse industries and ecosystems, related security risks have skyrocketed. According to recent data from cloud security company **Zscaler** (https://www.zscaler.com/), malicious cyber activity directed at IoT devices has jumped a whopping 700% since the start of the COVID-19 pandemic.[26] Some of this rise is attributed to the uptick in work-from-home policies, which increased the number of vulnerable consumer home-based IoT devices connecting to corporate networks. However, "most

[22] "IoT Signals." *Microsoft*. October 2020. Available for download: https://azure.microsoft.com/mediahandler/files/resourcefiles/iot-signals/IoT%20Signals_Edition%202_English.pdf.
[23] "IFS IoT Business Connector Fact Sheet." *IFS*. Accessed August 2021. Available for download: https://www.ifs.com/-/media/assets/2016/10/19/ifs-iot-business-connector-factsheet.pdf.
[24] Jack Vaughan. "BI Dashboards Integrate Smart Factory Data for Meaningful Analytics." *IoT World Today.* August 2021. https://www.iotworldtoday.com/2021/08/26/bi-dashboards-integrate-smart-factory-data-for-meaningful-analytics/.
[25] Ibid.
[26] "IoT-Specific Malware Infections Jumped 700% Amid Pandemic." *Dark Reading*. July 2021. https://www.darkreading.com/endpoint/iot-specific-malware-infections-jumped-700--amid-pandemic/d/d-id/1341537.

of the risky IoT traffic [reported by Zscaler] came from manufacturing and retail devices, including 3D printers, barcode readers, and payment terminal devices."[27]

Looking at the IoT security landscape more broadly, the Open Web Application Security Project (OWASP), a nonprofit foundation with tens of thousands of members worldwide, has highlighted the most concerning vulnerabilities. These "top 10 things to avoid when building, deploying, or managing IoT systems" include "weak, guessable, or hardcoded passwords; insecure network services; insecure ecosystem interfaces; lack of secure update mechanism; use of insecure or outdated components; insufficient privacy protection; insecure data transfer and storage; lack of device management; insecure default settings; and lack of physical hardening."[28]

As awareness of such risk grows, some companies are developing IoT-specific security solutions. **Threat9** (https://www.threat9.com/), a New York-based startup funded by London's CyLon cybersecurity accelerator, for example, is building software intended to scan an organization's IoT network and provide real-time vulnerability alerts. Others, like asset tracking and management platform provider **Axonius** (https://www.axonius.com/), have adapted existing solutions in an effort to holistically address IoT-related concerns in concert with non-IoT vulnerabilities.

NETWORK CONSIDERATIONS

Determining smart devices' optimal mode of internet access is another key consideration for any organization onboarding an IoT solution. Numerous connectivity options exist, including WiFi, Ethernet, satellite, cellular, and Low Power Wide Area Networks (LPWAN).[29] The growing adoption of fifth generation (5G) networks stands to significantly impact the IoT market by providing increased capacity for a large influx of both smart devices and the traffic they generate, faster data transfer speeds, lower latency, and heightened reliability over fourth generation (4G) cellular networks and other methods of connectivity.[30]

Large commercial retailers with relatively mature IoT solutions have already begun incorporating 5G into their logistics environments. Home appliance company **Whirlpool** (https://www.whirlpool.com/), for example, is switching one of its factories from WiFi to 5G,

---

[27] Ibid.

[28] "OWASP Top 10: Internet of Things." *Open Web Application Security Project (OWASP)*. 2018. Available for download: https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf.

[29] Alicia Asin. "IoT Survey: Key Concerns and Barriers to Develop Successful Projects." *Libelium*. June 2019. https://www.libelium.com/libeliumworld/iot-survey-key-concerns-and-barriers-to-develop-successful-projects/.

[30] Rishi Vaish and Sky Matthews. "5G Will Accelerate a New Wave of IoT Applications?" *IBM*. Accessed August 2021. https://newsroom.ibm.com/5G-accelerate-IOT;
"What's the Difference Between Speed and Latency?" *Phoenix Internet*. 2019. https://www.phoenixinternet.com/whats-the-difference-between-speed-and-latency/;
"Critical Capabilities for Private 5G Networks." *Ericsson*. Accessed August 2021. https://www.ericsson.com/en/reports-and-papers/white-papers/private-5g-networks.

allowing for the introduction of automated forklifts and other vehicles.[31] This innovation was not feasible under the factory's previous setup, because of the way WiFi reflected off the metal in the factory.[32]

With the continued expansion of 5G networks and 5G-IoT integration, however, come compounded security challenges. For many IoT companies, pressure to be first to market has pushed device security to the backburner during the design and development process.[33] As the number of vulnerable connected devices climbs in accordance with 5G's extended capacity, hackers and other bad actors have access to an ever-growing attack surface. Cybersecurity risks are further amplified in environments with legacy or proprietary systems and software, which are often difficult (or even impossible, depending on the situation) to patch with security updates.[34]

FORECAST AND CONCLUSION

In 2015, Gartner predicted there would be 25 billion IoT objects online by 2020; though experts' calculations for last year vary, most agree the actual number of devices fell at least ten billion short of that hypothesis.[35] To Stacey Higginbotham, a thought leader in the IoT space, this missed target does not imply IoT's days are numbered. Rather, it indicates developers and sellers are "tapping the brakes as they find ways to… ensur[e] vendor control and profits."[36]

Others posit the slow down in device onboarding has to do with data compute and analysis, interoperability, and complexity challenges.[37] As the 2020 Microsoft survey referenced above demonstrates, enterprises continue to identify integration concerns and costs as key roadblocks to IoT adoption.[38] Though these findings identify real challenges for IoT implementation in the years to come, the report also highlights the continued maturation of IoT integration with enabling technologies, including artificial intelligence, edge computing, and digital twinning.[39] Advances in these areas - as well as 5G, IoT cybersecurity, and data analytics - will significantly impact the IoT's own growth trajectory and potential.

---

[31] Maria Korolov. "8 Ways 5G Mobile Networks Will Change IoT Security, and How to Prepare." *CSO Online*. June 2020. https://www.csoonline.com/article/3442939/how-5g-mobile-networks-will-change-iot-security-and-how-to-prepare.html
[32] Ibid.
[33] Esther Shein. "5G and IoT Security: Why Cybersecurity Experts Are Sounding an Alarm." *TechRepublic*. March 2020. https://www.techrepublic.com/article/5g-and-iot-security-why-cybersecurity-experts-are-sounding-an-alarm/.
[34] Ibid.
[35] Stacey Higginbotham. "2020 Was a Year of Reckoning for the IoT." *Stacey on IoT*. January 2021. https://staceyoniot.com/2020-was-a-year-of-reckoning-for-the-iot/.
[36] Ibid.
[37] Alicia Asin. "Where Does IoT Go from Here?" *Libelium*. December 2020. https://www.libelium.com/libeliumworld/where-does-iot-go-from-here/.
[38] "IoT Signals."
[39] Ibid.

In particular, the enabling infrastructure provided by 5G's rollout is predicted to spur an explosion of IoT devices, with such networks becoming "the underlying fabric of an entire ecosystem of fully connected intelligent sensors and devices."[40] This projected surge may be hampered, however, by a continuation of today's global semiconductor shortage. For more information on the state of the semiconductor sector in general, please see our Microelectronics Sector Overview, and for a deeper examination of the global chip shortage, please see our complementary Microelectronics Sector Update.[41]

POTENTIAL AREAS FOR FURTHER STUDY

- Map and assess potentially applicable IoT solutions for a given use case;
- Conduct a deeper examination of one or more levels of the IoT technology stack (see Graphic 1., above). Focus areas could include edge hardware, data analytics and storage, or applications/services;
- Examine US government use cases, regulations, and published guidance relating to IoT;
- Explore the intersection between IoT and 5G connectivity in the context of a given use case;
- Examine IoT-related cybersecurity concerns and relevant industry solutions;
- Explore IoT's interplay with other complementary or enabling technologies. Areas for particular consideration include edge computing, digital twinning, big data analytics, artificial intelligence and machine learning, and blockchain.

[40] Randal Kenworthy. "The 5G And IoT Revolution Is Coming: Here's What To Expect." *Forbes*. November 2019. https://www.forbes.com/sites/forbestechcouncil/2019/11/18/the-5g-iot-revolution-is-coming-heres-what-to-expect/?sh=67c0d8946abf.

[41] "Microelectronics Sector Overview." *Second Front Systems*. June 2021. https://app.kitesrm.com/share/179309c61b034bb6f47dace537e775c2/reports/2940/views/12293-sector-overview; "Microelectronics Sector Update." *Second Front Systems*. July 2021. https://app.kitesrm.com/share/179309c61b034bb6f47dace537e775c2/reports/2940/views/17588-sector-update.

METHODOLOGY

In producing this study, our research team reviewed industry reports, market research products, and trade-specific professional commentary. We also consulted industry experts and reviewed marketing materials produced by individual companies. Our team continuously monitors technology news and trade publications related to the subject of this study.

NOTABLE RESOURCES

Brian Gilmore and George Westerman. "Realizing IoT's Potential: How to Overcome Challenges to Enterprise Implementation." *MIT Sloan Management Review*. January 2020. https://sloanreview.mit.edu/sponsors-content/realizing-iots-potential-how-to-overcome-challenges-to-enterprise-implementation/.

"IoT Signals." *Microsoft*. October 2020. Available for download: https://azure.microsoft.com/mediahandler/files/resourcefiles/iot-signals/IoT%20Signals_Edition%202_English.pdf.

Shah J. Miah, Himanshu Shee, and Tharaka de Vass. "IoT in Supply Chain Management: A Narrative on Retail Sector Sustainability." *International Journal of Logistics Research and Applications*. June 2020. https://www.researchgate.net/publication/342578541_Iot_in_supply_chain_management_a_narrative_on_retail_sector_sustainability.

Stacey Higginbotham. "2020 Was a Year of Reckoning for the IoT." *Stacey on IoT*. January 2021. https://staceyoniot.com/2020-was-a-year-of-reckoning-for-the-iot/.

Maria Korolov. "8 Ways 5G Mobile Networks Will Change IoT Security, and How to Prepare." *CSO Online*. June 2020. https://www.csoonline.com/article/3442939/how-5g-mobile-networks-will-change-iot-security-and-how-to-prepare.html.

Alicia Asin. "Where Does IoT Go from Here?" *Libelium*. December 2020. https://www.libelium.com/libeliumworld/where-does-iot-go-from-here/.

MORE INFORMATION

For more information about this report; our methodology, capabilities, and portfolio of offerings; the Atlas Fulcrum platform; or any other comments or inquiries, please contact us at research@secondfront.com.