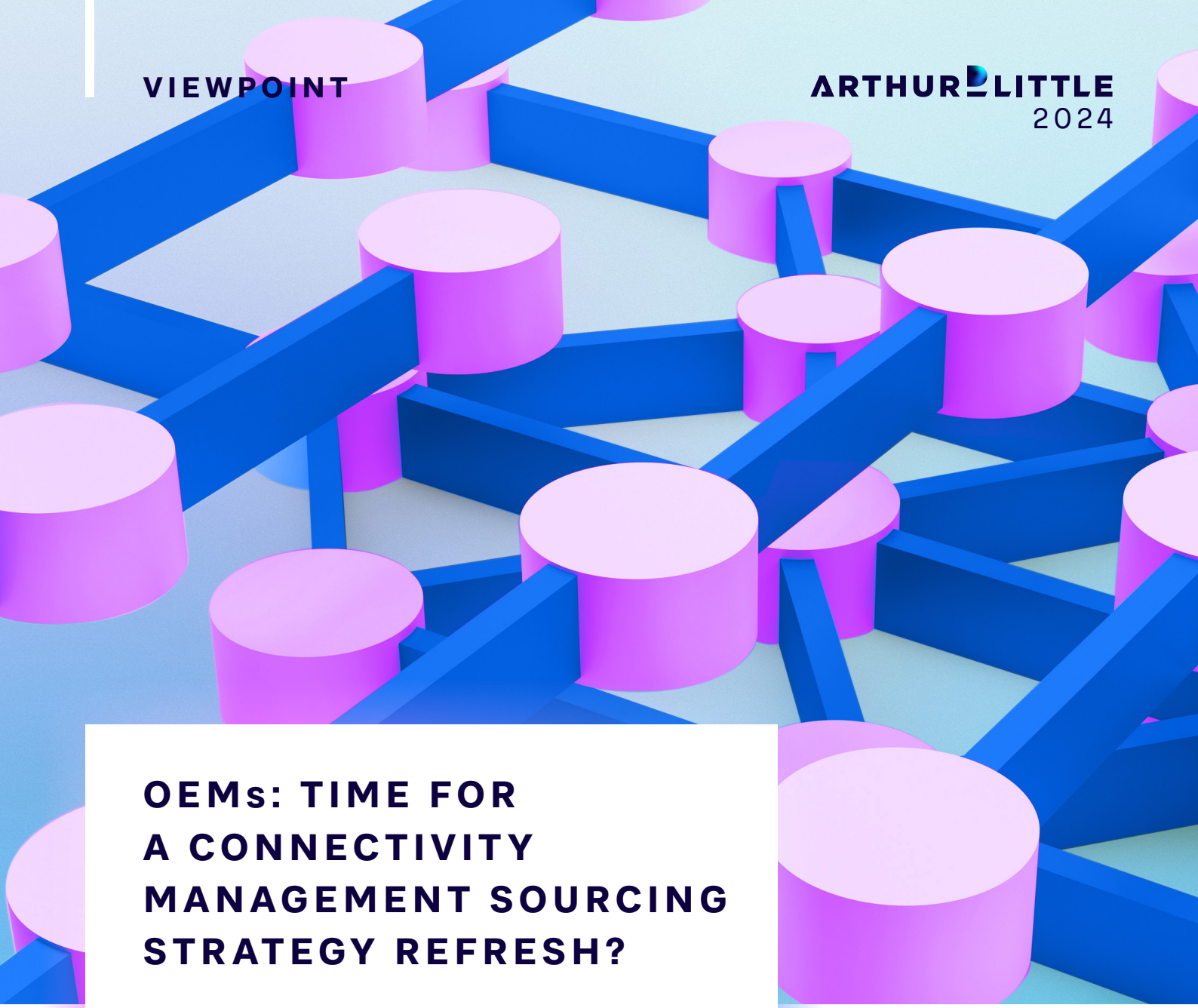
VIEWPOINT

ARTHUR D LITTLE
2024



OEMs: TIME FOR A CONNECTIVITY MANAGEMENT SOURCING STRATEGY REFRESH?

The transition to eSIMs is affecting IoT value chain

In this Viewpoint, we discuss the impact that the transition from classic subscriber identity module (SIM) cards to embedded SIM (eSIM) cards will have on the Internet of Things (IoT) value chain. The eSIM is changing the roles of a variety of players in the IoT ecosystem. With the cellular IoT landscape at an inflection point, we believe IoT OEMs should rethink their connectivity management sourcing strategies to offer more competitive value propositions.

AUTHORS

Makram Chehayeb

Julien Duvaud-Schelnast

Matteo Ainardi

Agron Lasku

Bela Virag

A SHIFT IN THE INDUSTRIAL IoT CELLULAR LANDSCAPE

According to Gartner, the shipment of IoT devices in the industrial sector is forecasted to grow at a CAGR of 6% between 2022 and 2030, with volumes increasing from around 1.7 billion to approximately 2.9 billion endpoints shipped annually. The verticals responsible for the largest industrial IoT volumes include automotive, energy and utilities, government, manufacturing and agriculture, smart buildings, retail, and connected health, which together represent more than 95% of annual industrial IoT shipments by 2030.

IoT solutions are being leveraged to increase automation and optimize processes. For example:

- Caterpillar, a US machinery company, leverages IoT for tasks such as monitoring fuel levels, providing real-time equipment information to dealers, optimizing operations, and improving customer satisfaction. Caterpillar claims to have improved production efficiency by 45% thanks to its IoT solutions.
- ABB, a Swiss-Swedish multinational corporation specializing in robotics, leverages connected sensors to monitor robot maintenance and proactively schedule repairs.

The rise of cellular penetration in IoT devices

Wireless connectivity for IoT devices can be provided through short-range solutions, such as Wi-Fi, Zigbee, and Bluetooth, and long-range solutions, such as cellular, non-cellular low-power wide-area networks solutions, satellite, and proprietary radio-frequency solutions. The choice of connectivity solution depends on requirements, such as coverage, throughput, latency, battery life, cost, security, mobility, availability, and security (see Table 1). Cellular, across its standards, typically offers the best performance when compared to other solutions. However, it typically comes with a larger total cost of ownership (TCO) driven by higher module costs and higher connectivity subscription fees.

Cellular penetration in IoT devices is expected to increase, driven by decreasing costs of cellular IoT modules and new IoT use cases requiring increasing connectivity performance. Gartner forecasts that cellular penetration in installed IoT devices will increase from 19% in 2022 to 35% in 2030. In this Viewpoint, we focus on cellular as a wireless IoT connectivity solution and explore how innovative cellular products and services are disrupting this ecosystem.

Table 1. Performance comparison of selected long-range IoT connectivity solutions

	LoRaWAN	Sigfox	NB-IoT	LTE-M	4G/5G
Coverage (estimate)	<10 km	<15 km	<15 km	<10 km	100 m-5 km
Peak data rates	<10 kbit/s	<0.1 kbit/s	<150 kbit/s	<1 Mbit/s	10-100 s of Mbit/s
Maximum messages/day	Unlimited	140 uplink & 4 downlink	Unlimited	Unlimited	Unlimited
Latency	1-2 seconds	In order of seconds	1-10 seconds	100-150 ms in normal coverage mode	Tens of ms for 4G Few ms with 5G
Battery life	High	High	Medium	Medium	Low
Radio module cost	$5	$2-$3	$2-$5	$7-$8	$30-$80 for 4G & $150-$200 for 5G
Voice support	No	No	No	Yes	Yes
Roaming	Requires roaming agreements	In footprint of Sigfox networks	Requires roaming agreements	Requires roaming agreements	Requires roaming agreements
SIM card/cellular IPsec security	No	No	Yes	Yes	Yes

Source: Arthur D. Little

Tracking cellular-connectivity enablement

Until recently, the removable SIM (rSIM) was the most deployed SIM product. Although the rSIM has evolved in form factor (micro SIM, nano SIM) it lacks remote management capabilities, forcing one to change SIMs to change connectivity provider. The introduction of the eSIM and its successor the integrated SIM (iSIM) has changed this (see Figure 1). The remote provisioning and remote management feature of e/iSIMs enables:

1. The ability to dynamically multisource connectivity from multiple providers and switch providers without sending technicians to replace the SIM in IoT endpoints (most eSIMs and iSIMs can be remotely provisioned and managed)
2. The ability to simplify the manufacturing process by relying on a single stockkeeping unit (SKU) that can be used in multiple geographies

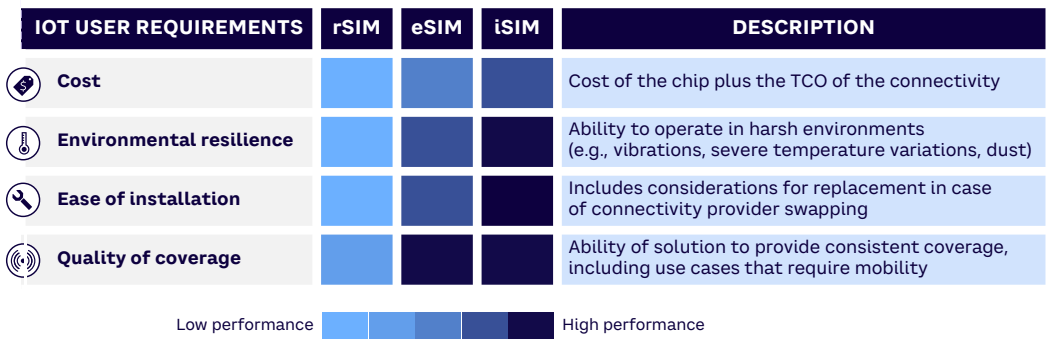
Mobile network operators (MNOs) have been reticent to push next-gen SIM products to their customers, fearing they would decrease customer stickiness and facilitate churn. Despite resistance from MNOs, the adoption of remote service module (RSM)-capable eSIM and iSIM in industrial cellular IoT devices shipments is forecasted by Counterpoint Research to increase from 11% in 2022 to 28% in 2026.

NEXT-GEN SIMs ENABLE ADVANCED DEPLOYMENTS

Many IoT use cases rely on a scattered deployment of numerous endpoints that have a device lifetime of seven to 15 years. With traditional rSIMs, solution providers could not easily switch between connectivity providers because sending technicians into the field to switch SIMs was prohibitively expensive. e/iSIM uses over-the-air provisioning to remove this complexity, giving solution providers more flexibility in switching connectivity providers. This enables multiple use cases that can reduce TCO and/or improve quality of service. Examples include:

- Connecting to the network with which the business has the best roaming agreement to minimize roaming costs and reduce connectivity TCO
- Connecting to the network that has the best signal strength to optimize network quality of service for each IoT device on the network

Figure 1. Performance of SIM products



Source: Arthur D. Little

Next-gen SIMs address security threats & regulatory intervention

With the rapid growth of connected devices and increasing cyberattacks and security breaches, IoT security has become a critical issue. Regulators are taking action to set security standards for IoT solutions, with the Federal Office for Information Security (BSI) in Germany leading the way. BSI has imposed strict security requirements on utility companies deploying IoT solutions, including the need for preapproved embedded security elements (eSEs) to be incorporated in smart meters for device authentication and encryption. Regulators in the EU, US, and Singapore are also defining regulated security requirements for IoT deployments.

Next-gen SIM products help address these security challenges. On the product side, eSIMs are sometimes sold in combination with an eSE, saving space and cost. On the service side, standards body GSMA developed a standard called IoT SIM Applet for Secure End-2-End Communication (IoT SAFE for short). The standard allows the SIM to be used as root of trust, instead of a dedicated eSE, to generate keys and certificates that can be used to encrypt end-to-end communication over the IoT network.

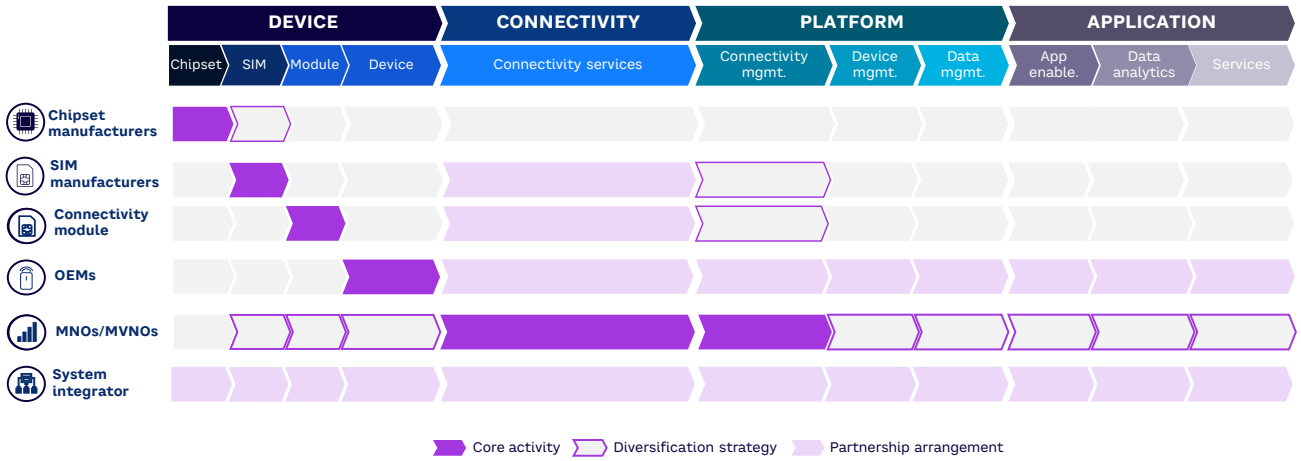
IoT PLAYERS ADAPT POSITIONING

Numerous players moving toward connectivity services

Driven by next-gen SIM products, players in the IoT ecosystem are evolving (see Figure 2). Chipset manufacturers such as Qualcomm traditionally focused on designing and producing core components, such as microprocessors and communication chips for IoT devices. With the emergence of iSIMs, they are playing a critical role in connectivity enablement by integrating SIM functionalities into their chipsets.

Similarly, SIM manufacturers such as Thales have expanded their offerings beyond designing and manufacturing SIM cards. They now provide combo eSIMs with embedded security elements, as well as enhanced connectivity-enablement solutions like remote-service provisioning platforms and automated connectivity-enablement platforms that leverage the RSM capabilities of eSIMs and iSIMs.

Figure 2. Industrial IoT ecosystem (simplified)



Source: Arthur D. Little

Module manufacturers such as Quectel have also seen their roles evolve. They previously focused on assembling connectivity modules, but the shift to eSIMs requires them to be more involved in SIM sourcing (the eSIM is soldered onto the module they manufacture). Module manufacturers are also beginning to resell connectivity and connectivity management services, moving further up the value chain.

OEMs such as Sagemcom traditionally focused on designing and manufacturing IoT devices in collaboration with chipset and module manufacturers. As the market develops, specialized OEMs are increasingly providing comprehensive IoT solutions that include devices, platforms, and connectivity services, de facto acting as solution providers to end customers. These OEMs are increasingly partnering with players across the ecosystem to offer an end-to-end managed solution to the client.

System integrators such as Accenture continue to help businesses implement end-to-end IoT solutions by integrating and configuring various IT systems and platforms and leveraging partnerships with multiple players.

The MNO role is being challenged

Connectivity sourcing strategies are changing as eSIM/iSIM adoption increases. Traditionally, solution providers or system integrators liaised with MNOs for all their IoT connectivity requirements (SIM + IoT subscription), but next-gen SIM products are disrupting that model.

Figure 3. OEM connectivity sourcing models

Source: Arthur D. Little

Solution providers are increasingly sourcing e/iSIM from other players across the value chain, including chipset and module makers for SIM products and SIM manufacturers for SIM products and connectivity-enablement platforms.

As for the connectivity itself, although MNOs are expected to continue to dominate that market, alternative players such as mobile virtual network operators (MVNOs) are playing an increasingly important role. These include module makers like Telit and SIM manufacturers like Giesecke+Devrient, which acquired IoT MVNO POD a few years ago. e/iSIM adoption is challenging the historical hegemony of MNOs over IoT connectivity and connectivity management solutions.

IoT SOLUTION PROVIDERS SHOULD ACT NOW

IoT connectivity services, once monopolized by MNOs, are increasingly being democratized. This creates opportunities for solution providers, which now have multiple connectivity sourcing strategies to consider (see Figure 3).

Strategy 1: Fully outsourced connectivity & services

Until recently, most OEMs opted for this strategy, which involves completely outsourcing their cellular connectivity needs to partner MNOs or MVNOs. In this approach, services like connectivity bootstrapping, connectivity management, and service provisioning are outsourced to external partners. This approach requires the least technical expertise and demands the least transformation to existing processes, but it offers less control over service quality. For instance, ABB forged a partnership with China Telecom in 2023. It intends to leverage China Telecom's 5G network and cloud computing expertise for its industrial IoT solutions targeted at Chinese clients. Similarly, Caterpillar entered a global IoT partnership with AT&T, relying on AT&T's global SIM, control center, and subscription management.

Strategy 2: Outsourced connectivity, insourced services

In this approach, OEMs take a more hands-on approach by managing their connectivity platform internally and partnering with MNOs or MVNOs for connectivity service provision. This hybrid model gives OEMs greater control over their operations and the quality of service their IoT solution delivers. By managing their connectivity management platform and integrating it into their IoT platform solutions, OEMs are better able to develop custom, end-to-end client solutions. Maersk, a logistics fleet operator, exemplifies this strategy by integrating its IoT platform with its self-managed connectivity management platform while partnering with Onomondo, an IoT MVNO, to deliver global IoT connectivity to clients. Similarly, Sagemcom, a prominent utility OEM, operates its own connectivity platform and collaborates with connectivity providers to deliver end-to-end solutions tailored for clients.

Strategy 3: Insourced connectivity & services

The most ambitious OEMs venture into this strategy, becoming IoT MVNOs and providing fully insourced IoT connectivity solutions. This approach demands significant investment and technological prowess. Landis+Gyr, the largest global utility OEM, exemplifies this strategy, having developed a comprehensive IoT platform solution. It can offer end-to-end services to customers, leveraging its global agreement with Vodafone Business to offer a turnkey IoT solution that includes connectivity services, becoming de facto IoT MVNO. Orbcomm, a leading logistics OEM, operates both satellite and cellular connectivity, leveraging wholesale contracts with tier 1 MNOs to offer global turnkey IoT solutions. OEMs that embrace this strategy position themselves as one-stop providers, facilitating the procurement process for clients.

To choose the right strategy, solution providers need to assess the maturity of their IoT markets and anticipate the evolution of their clients' needs. Once OEMs decide on a sourcing strategy, they must define and implement transformation initiatives (e.g., changes in internal processes, new go-to-market, recruiting of relevant expertise, development of in-house intellectual property) that will allow them to successfully implement their chosen strategy.

Until recently, managing an IoT connectivity platform was technically complex because the underlying connectivity enablement/management standards for IoT had not been updated to meet the new use-case requirements. Until this year, the standards relied on SM-DP (server management data preparation) and SM-SR (sever management secure routing), which are legacy standards designed for machine-to-machine use cases rather than massive IoT. These legacy standards required complex integration and significant technical expertise.

This year, GSMA is updating the IoT connectivity standards to SM-DP+, which should facilitate the technical integrations required to join platforms with mobile operators' servers. In addition to the complexity of managing connectivity-enablement platforms, non-MNOs solution providers faced the issue of securing the bootstrapping of their IoT devices across all their desired geographies. This was a major barrier for managing IoT connectivity platforms, but SIM manufacturers Thales Group and Move recently started offering alternatives to bootstrapping that significantly reduce the complexity of provisioning the first connectivity service to headless IoT devices. These technical developments are reducing the barriers to entry for OEMs to manage their own IoT platforms and should encourage more OEMs to transition from strategy 1 to strategies 2 or 3.

IT'S CRUCIAL FOR OEMs TO TAKE A PROACTIVE, AGILE APPROACH TO ADAPTING THEIR VALUE PROPOSITION

Based on expert interviews and internal analyses, Arthur D. Little believes that OEMs managing a fleet of 1 million or more IoT endpoints should move from strategy 1 to strategy 2 and operate their own connectivity-enablement platform. If an OEM's IoT fleet reaches 3 million to 5 million endpoints, they should consider becoming an IoT provider, leveraging connectivity wholesale agreements with one or more MNOs. This is only a rough guide: a detailed strategic/business planning/technical assessment should be conducted before making a final decision.

OEMs must understand the impact of new SIM products on manufacturing

As the industrial IoT landscape evolves, it's crucial for OEMs to take a proactive, agile approach to adapting their value proposition. This will help them develop robust IoT solutions that are continuously enriched with state-of-the-art products and services. For example, OEMs should consider including in their offers:

- The latest automated connectivity management features to offer their clients better network quality with lower TCO
- The latest device-security products and services (e.g., eSIM combo and IoT SAFE) to reduce device manufacturing costs and improve TCO and profit margins

Adding the products and services above will impact design and manufacturing; OEMs will need to anticipate and adapt their processes:

- Increase eSIM adoption to simplify the manufacturing process and reduce the number of SKUs per endpoint
- Consider aligning eSIM sourcing processes with device-design security processes to leverage products such as combo eSIMs and services such as IoT SAFE

CONCLUSION

NEW OPPORTUNITIES, NEW STRATEGIES

OEMs AND SOLUTION PROVIDERS SHOULD RETHINK THEIR STRATEGIES

There is a growing cellular IoT opportunity being triggered by the arrival of e/iSIMs and associated services. We believe OEMs and solution providers should rethink their strategies:

1. Develop a one-stop shop for connectivity enablement and services and capture additional value by leveraging proximity to their client base. In-house connectivity/connectivity-enablement expertise should be developed gradually to move away from a fully outsourced model as they scale their managed fleet.
2. Enrich value propositions with the latest connectivity-enablement and security services while anticipating the impact on complex design and manufacturing processes.

NOTES

Arthur D. Little has been at the forefront of innovation since 1886. We are an acknowledged thought leader in linking strategy, innovation and transformation in technology-intensive and converging industries. We navigate our clients through changing business ecosystems to uncover new growth opportunities. We enable our clients to build innovation capabilities and transform their organizations.

Our consultants have strong practical industry experience combined with excellent knowledge of key trends and dynamics. ADL is present in the most important business centers around the world. We are proud to serve most of the Fortune 1000 companies, in addition to other leading firms and public sector organizations.

For further information, please visit www.adlittle.com.

Copyright © Arthur D. Little – 2024. All rights reserved.