



Internet of Things

MVNO proliferation puts spotlight on competitive differentiation, ancillary capabilities

FIRST ANALYSIS WHITE PAPER

Integrative insights on emerging opportunities

October 23, 2024



David Gearhart, CFA

Direct: 312-258-7128
dgearhart@firstanalysis.com

Main: 312-258-1400
www.firstanalysis.com

Howard Smith

Direct: 312-258-7117
hsmith@firstanalysis.com

Charles Morgan

Direct: 312-258-7147
cmorgan@firstanalysis.com

First Analysis Internet of Things Team

Howard Smith

Managing Director
hsmith@firstanalysis.com
312-258-7117

David Gearhart

Senior Vice President
dgearhart@firstanalysis.com
312-258-7128

Matthew Nicklin

Managing Director
mnicklin@firstanalysis.com
312-258-7181

Charles Morgan

Analyst
cmorgan@firstanalysis.com
312-258-7147

First Analysis

1 S. Wacker Dr., Suite 3900
Chicago, IL 60606
312-258-1400
www.firstanalysis.com

About the Authors



David Gearhart, CFA

David Gearhart has worked in finance and investment for two decades and joined First Analysis in 2011. He works with entrepreneurs as an investor and as an advisor on growth transactions to help build leading Internet of Things and e-commerce software businesses. He has played a key role in building First Analysis' Internet of Things and e-commerce franchises and is a thought leader in his sectors, having authored several widely read white papers. He supports First Analysis' investments in CoolR Group, EdgeIQ, Freeosk and Smart-Commerce. Prior to joining First Analysis, he was an accountant with The Northern Trust Co. and an options broker with American Option Services. He earned a bachelor's degree from Purdue University with a concentration in economics and finance and his MBA at DePaul University with a focus on finance and entrepreneurship. He is a CFA charterholder.



Howard Smith

Howard Smith has over three decades of experience at First Analysis, working with entrepreneurs as an investor and as an advisor on growth transactions to help build leading technology businesses. He leads the firm's work in the Internet of Things, cybersecurity and internet infrastructure sectors. He also built the firm's historical franchises in call centers and computer telephony. His thought-leading research in these areas has been cited for excellence by the Wall Street Journal and other publications. He supports First Analysis' investments in EdgeIQ, Fortress Information Security, ObservIQ, Stamus Networks and Tracer. Prior to joining First Analysis in 1994, he was a senior tax consultant with Arthur Andersen & Co. He earned an MBA with honors from the University of Chicago and a bachelor's degree in accounting with highest honors from the University of Illinois at Urbana-Champaign. He is a certified public accountant.



Charles Morgan

Charles Morgan is an analyst with First Analysis. He joined the firm in 2022 after completing two internships. Charles graduated from Denison University in 2022 with a bachelor's degree in economics.

About First Analysis

First Analysis has a four-decade record of serving emerging growth companies, established industry leaders and institutional investors in emerging high-growth tech-driven sectors, both through its venture capital investments and through First Analysis Securities Corp. (FASC), which provides investment banking and related services. FASC is a FINRA-registered broker-dealer and member SIPC. First Analysis' integrative research process underpins all its efforts, combining 1) dynamic investment research on thousands of companies with 2) thousands of relationships among executives, investors and other key participants in our focus areas, yielding a deep, comprehensive understanding of each sector's near-term and long-term potential.

INTERNET OF THINGS

October 23, 2024

FIRST ANALYSIS WHITE PAPER

Integrative insights on emerging opportunities

Table of Contents

IoT MVNO count has increased.....	1
What is an MVNO?.....	1
Why do they exist?.....	3
Many players already in the MVNO market	5
Why has the number of MVNOs increased?	6
MVNOs that move beyond basic connectivity will be most successful.....	9
Software.....	10
Physical infrastructure.....	24
Professional services	30
Strategic approach and focus	31
What to watch as MVNO market evolves	36
Increasing M&A.....	36
Limited access to capital.....	38
Impact of eSIMs.....	38
OEMs as MVNOs.....	38
A complex and dynamic sector.....	39

INTERNET OF THINGS

MVNO proliferation puts spotlight on competitive differentiation, ancillary capabilities

- The number of mobile virtual network operators (MVNOs) serving the IoT market appears to have increased dramatically over the past few years.
- We attribute the perceived increase primarily to four factors: The compelling opportunity for MVNOs in the IoT market, loss of interest in the IoT market among the large mobile network operators, the appearance of mobile virtual network enablers (MVNEs), and reduced barriers to entry.
- We think the most successful MVNOs will be those that move beyond simply reselling connectivity to provide unique added value to their IoT customers. We detail several such strategies being pursued by MVNOs and companies in adjacent segments. These strategies often blur the boundaries of traditional value chains.
- We highlight companies pioneering these promising strategies. We also highlight key trends and factors to watch.

IoT MVNO COUNT HAS INCREASED

The number of mobile virtual network operators (MVNOs) serving the IoT market appears to have increased dramatically over the past few years. At conferences we

attended over the last 12 months, for example, we observed more MVNOs at each event, counting those exhibiting and not, than we did at any single IoT conference we attended in North America over the prior decade. In addition, a market survey using online searches for IoT data connectivity providers yielded dozens of companies, many relatively young and new to our tracking list. Because of this, we think it is timely to review the MVNO space, including possible drivers of the increase as well as differentiation that increases the probability of creating long-term value.

WHAT IS AN MVNO?

All IoT solutions require access to a communication network to transmit data captured by physical devices to the cloud. Applications requiring wider transmission range and greater throughput often use cellular. These IoT providers make arrangements with third parties for cellular access and compensate them for the quantity of data passing over their networks. Arrangements can be made directly with mobile network operators (MNOs), also known as cellular service providers (CSPs) or carriers, who own radio spectrum and physical infrastructure essential to enable long-range communications, such as towers, base stations and core networks. These large, household-name

TABLE 1: Major MNOs by continent



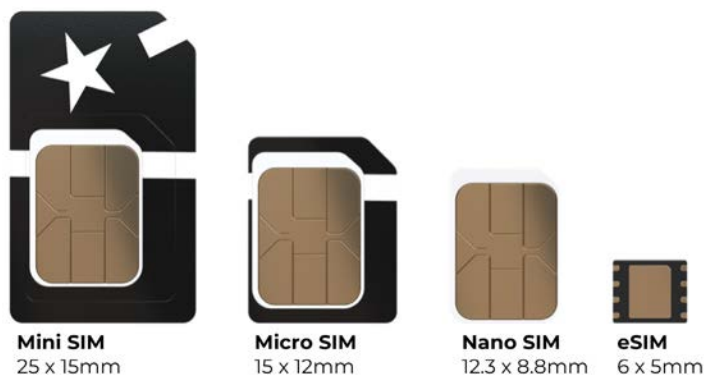
Source: Integra, Mobile Magazine, GlobalData, Statista, econnex, Simetric.

carriers, which include AT&T, T-Mobile, and Verizon, among many others (see Table 1), made significant investments in wireless infrastructure to support voice and consumer mobility (smartphone) services, and they continue to spend material sums for upgrades and maintenance. Alternatively, IoT solution providers can source connectivity indirectly through MVNOs. MVNOs

don't own spectrum and rarely own infrastructure. Instead, they negotiate agreements with several different MNOs, which give them access to each MNO's network and those of their partners, leasing data capacity and establishing wholesale rates at which they can purchase data that is subsequently resold to solution providers.

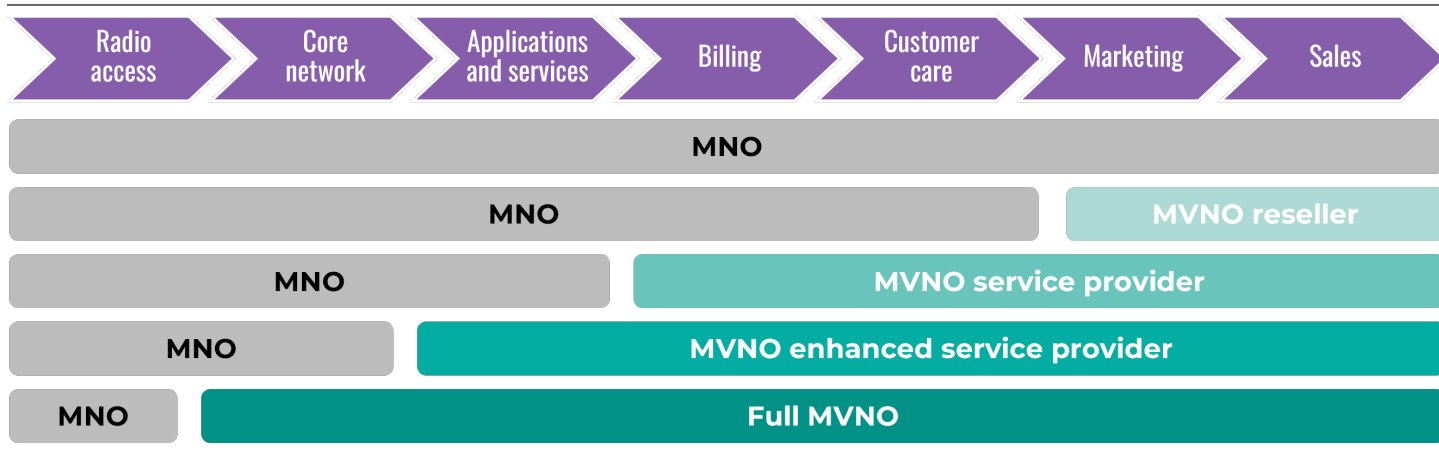
MVNOs can be categorized by whether they own physical infrastructure, the software capabilities provided (whether proprietary or third-party) and customer support offered. The most basic MVNO type is a branded reseller that doesn't own infrastructure, offers no value-added capabilities or support, and just focuses on marketing and selling connectivity; carriers and other partners provide the things these MVNOs lack. The other MVNO types (see Table 2) are more interesting and add more value, as they made the strategic decision to invest in hardware infrastructure and/or software to enable some proprietary capabilities, provide dedicated customer service and support, or integrate with third parties for needed capabilities. The most advanced

Types of SIM cards



Source: Soracom.

TABLE 2: Types of MVNOs by capabilities and services provided



Source: Onomondo.

of these is a full MVNO, which owns infrastructure elements, offers the complete range of software needed to manage IoT connectivity, and provides service and support. Between these extremes are “service provider” MVNOs and “light” or “enhanced service provider” MVNOs. Other slightly different types include “efficiency” MVNOs, which focus on specific and niche markets and strip out material cost that gets passed on to customers (often under a bundled offering), and MVNOs that procure connectivity from other MVNOs instead of MNOs. Across these variations, many MVNOs establish their own brands, investing materially in marketing to increase visibility

and in field sales and support teams to find opportunities and facilitate IoT solution deployment.

WHY DO THEY EXIST?

It seems like the answer to this question should be straightforward and definitive. However, our conversations with MVNOs and industry participants yielded more reasons for the existence of MVNOs than we had contemplated – all of them credible. While we didn’t expect a single reason, we found it interesting and surprising that there was no consensus around one or two primary reasons. Each MVNO seemingly had a different opinion, underscoring that the space is more complex and nuanced than it appears on the surface. Below, we highlight a few of the answers provided, which in aggregate help explain the existence of MVNOs.

To meet the IoT market’s need for more competitive data pricing and flexible plans. Connectivity cost is an acute consideration for IoT companies, particularly end-to-end solution providers, due to its offsetting impact on higher-gross-margin products, like application software. But most providers don’t have the scale (measured by number of connections and per-connection bandwidth needs) to garner the attention of carriers, let alone successfully negotiate directly with them to achieve

MVNO value proposition



Leverage Zipit Buying Power

Thanks to our strategic relationships with leading carriers around the world, it’s often more economical to buy through us.

Source: Zipit Wireless.

materially lower or optimal pricing. Pennies per connection per month matter, especially for applications with low average revenue per user, or if the solution provider must adjust list prices to remain competitive against larger peers. MVNOs play a significant role in this pricing dynamic and provide a valuable service by aggregating the data needs of their existing and prospective customer bases. MVNOs purchase cellular connectivity to meet this need from MNOs, leveraging this greater combined scale to procure volume-based discounts. MVNOs earn a markup but pass most of the savings on to IoT companies, giving them access to much lower pricing than they could secure on their own. In addition, by buying in bulk and pooling data, MVNOs can create highly tailored and flexible pricing plans that are well aligned with IoT companies' specific use cases, lower data needs, and underlying business models that support solution providers' viability.

To address IoT's greater support needs and fill gaps created by carrier disinterest.

Developing and maintaining an IoT solution is challenging, requiring expertise across multiple disciplines. Companies embarking on this journey invariably run into trouble, even if using off-the-shelf hardware and software components and modules. For support, such as consulting on solution design or troubleshooting issues, most turn

to their vendors, typically connectivity providers (at least initially). This is unsurprising considering connectivity is core to every solution and given connectivity providers' visibility, professional networks, and perceived IoT expertise. However, MNOs generally have little interest in being the destination for IoT support. The IoT market is more variable and less straightforward than the consumer handset market, so IoT support requires more time, effort and money. MNOs find it difficult to justify allocating finite resources to accounts that generate little revenue per connection and have relatively few connections.

For this reason, MNOs do not prioritize IoT support tickets and requests unless they are from large accounts or prospects. This has led to a persistent gap in the market for support, which created the opportunity for MVNO founders to inhabit the same position as MNOs: By reselling connectivity, they would become the default destination for support requests. Since their focus is solely IoT (no need to prioritize consumer data), MVNOs have been able to offer superior support and further attract prospects. They employ IoT knowledge experts and specialists to help companies launch and maintain solutions. MNOs can monetize their networks through MVNOs while offloading IoT support needs, so MNOs view dedicated IoT MVNOs positively and even send opportunities their way.

To provide global coverage at lower cost with greater performance.

Many IoT solution providers and original equipment manufacturers (OEMs) operate internationally or aspire to deploy devices in multiple countries. But procuring reliable, secure and continuous connectivity at competitive rates wherever devices are to be permanently located is challenging without MVNOs. Despite MNOs' negotiated roaming agreements and relationships with carriers in most countries, turning to domestic MNOs is not a viable option. Roaming (when a device with a domestic MNO SIM is in a foreign country running on a local carrier network) is very expensive, as it is only meant to be temporary. Even for companies willing to bear this cost, permanent roaming is not allowed in many countries. Devices can be kicked off

MVNO value proposition

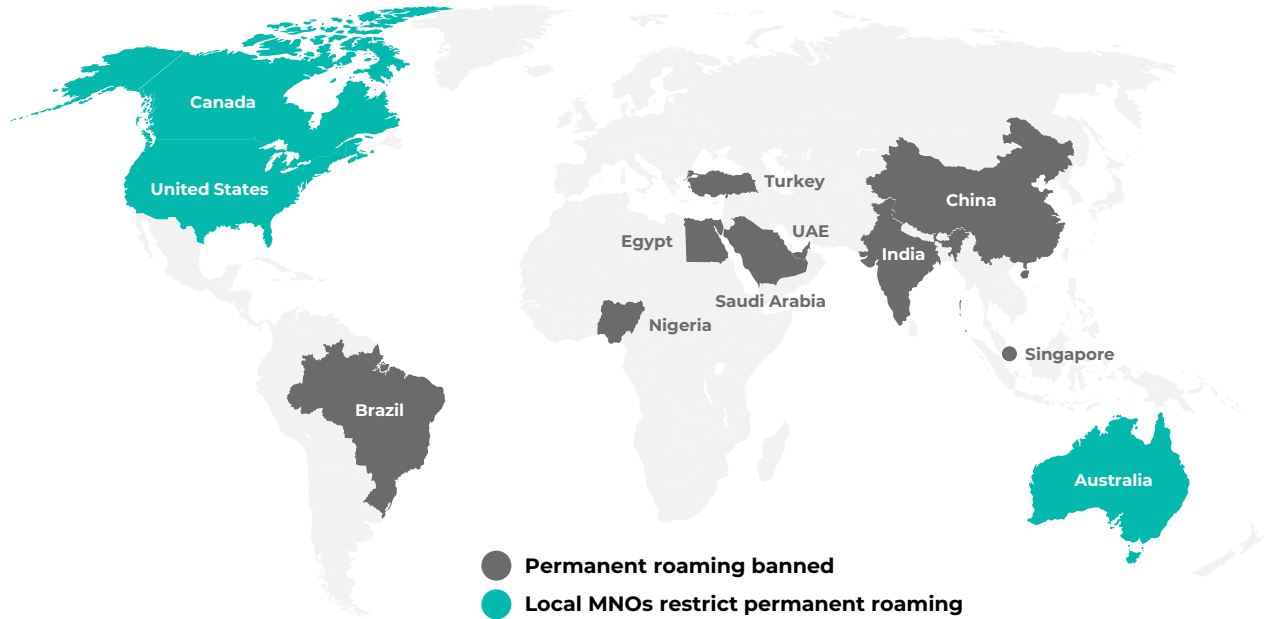


Unlock Multiple Options for Global Coverage

With localized connectivity, global SIM and multi-carrier SIM offerings, we'll help you find the best coverage for your devices and use case, at a price that's fair and helps you scale.

Source: Zipit Wireless.

TABLE 3: Major countries where permanent roaming is restricted



Source: Counterpoint Research Analysis.

the network after a short period of time, and some countries, such as Brazil, Turkey, China and Saudi Arabia, do not even allow roaming (see Table 3). In addition, roaming suffers performance issues (affecting latency and throughput) due to the longer paths data must traverse by default (involving the domestic country/network, not just the foreign country/network).

While IoT solution providers and OEMs could negotiate agreements directly with carriers in desired countries, integrate with their networks and thereby avoiding roaming challenges, it would be time consuming and expensive. In contrast, by leveraging MVNOs, IoT solution providers and OEMs can avoid the bulk of these challenges. MVNOs essentially establish global networks, patching together countries and their MNOs by negotiating with and integrating their networks so MVNOs' customers don't have to. As a result, MVNO customers see competitive local rates delivered under a single bill and better performance than they could get otherwise, as data traffic remains in-country.

Other reasons. Some of the other reasons for the existence of MVNOs mentioned in our conversations included:

- To help customers avoid getting locked into multi-year contracts with specific MNOs,
- to target market segments and niches not coveted or monetized by carriers,
- to provide specialized tools for IoT solution development and deployment not offered by MNOs, and
- to offer systems and platforms built and optimized for IoT that are separate and distinct from those used by MNOs to support consumer handsets.

MANY PLAYERS ALREADY IN THE MVNO MARKET

By our count, there are 150 to 200 IoT-centric MVNOs active worldwide selling cellular connectivity to companies leveraging connected devices, including solution providers and OEMs. This count is consistent with the comments from several leading MVNOs we surveyed and estimates we have seen from other researchers. For many of the players we identified, connectivity resale is their primary business.

TABLE 4: The more visible MVNOs

MAIN PLAYERS

OTHER PLAYERS

Source: Industry and company reports, First Analysis.

We also counted companies that primarily focus on a different part of the IoT solution stack (such as hardware) but also resell connectivity. Some of these companies have built sizeable businesses in resale connectivity despite its secondary status in their business models. We highlight the MVNOs we identified in Table 4.

Despite the large number of MVNOs, only a fraction of them truly matter in terms of scale and influence. The bulk of IoT MVNO subscribers and connectivity revenue is at roughly 20-25 MVNOs, many of which are long established and well known. These MVNOs typically have some combination of physical infrastructure, proprietary capabilities, technical expertise, go-to-market savvy, and resources that enabled their success. This group has remained consistent over the last several years. Outside of

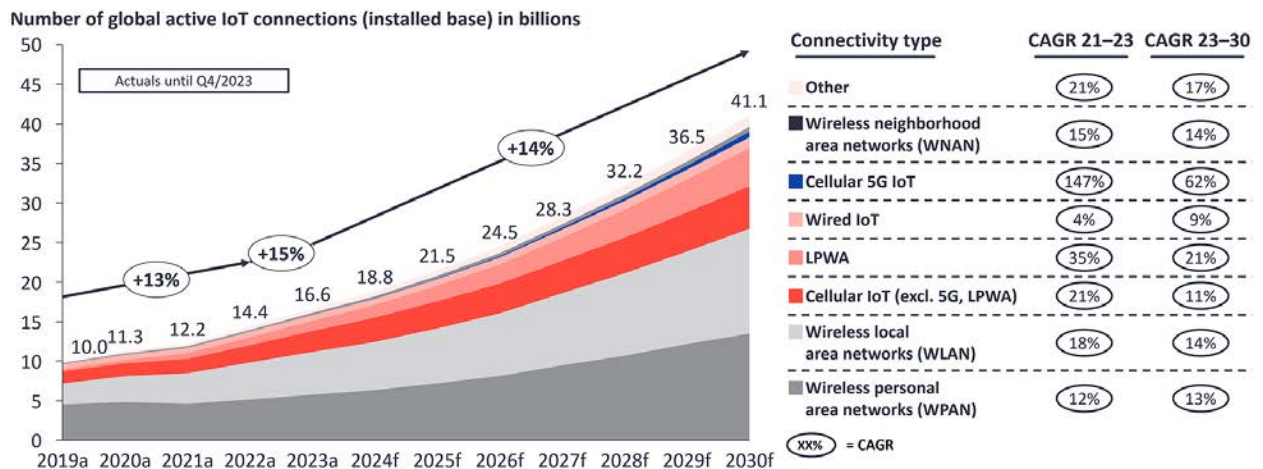
these 20-25 companies, MVNOs tend to be small: either branded reseller MVNOs or MVNOs with modest capabilities. Much of the growth of MVNOs appears to be in the branded reseller category.

WHY HAS THE NUMBER OF MVNOs INCREASED?

We heard several plausible explanations from existing MVNOs and other industry participants for the apparent increase in the number of MVNOs active in the market. We attribute the perceived increase primarily to four of these explanations, and we expect these four factors to continue to attract new MVNO entrants:

IoT opportunity remains compelling. Data service providers have long been drawn to the IoT market by the sheer number of

TABLE 5: Global IoT market forecast by connectivity type (2019-2030)



Source: IoT Analytics Research 2023.

CAGR: Compound annual growth rate. LPWA: Low power wide area. A: Actual. F: Forecast.

assets worldwide that can be connected to a wireless network using dedicated devices and sensors and monetized on an ongoing basis. It has been suggested that the devices required to address the entire market represent between 50 billion and 250 billion individual data connections. This includes various connectivity types, including those that have a recurring cost (such as cellular and satellite) and those that do not (such as Wi-Fi, Bluetooth, and Zigbee). The market is currently at about 20 billion connections, with cellular accounting for about 20% (see Table 5). We think the newer MVNOs recognized that the number of potential connections still far exceeds actual connections and were attracted to the market by the high probability of pure connection growth remaining strong for many years to come. We also think newer vendors have chosen to resell cellular because cellular networks are ubiquitous, validated and likely to be maintained given the significant investment in building them and their large consumer customer bases.

MNO pullback: After living through the hype, many are losing interest in typical opportunities. We have been hearing more regularly from our contacts that several MNOs are less bullish on IoT relative to years past and have been losing interest in the market. Besides reducing efforts and resources allocated to IoT initiatives, some

are passing IoT opportunities to MVNO partners to handle, while a few are also considering ceding some IoT customers and subscribers to MVNOs. This is largely happening around small opportunities, as measured by connected and connectable assets and devices. The shift can be attributed to the modest revenue small deals bring carriers relative to sales and ongoing support costs,

“IoT is becoming a purely wholesale opportunity for MNOs”

given small deals have low average revenue per device and low device counts.

By sharing these deals with MVNOs, MNOs not only avoid associated operating costs, but they are still able to monetize the connections by selling connectivity to MNVOs on a wholesale basis. Further, MNOs’ sales and technology skill sets for their core consumer handset and data business are not well aligned with the skill sets required to target IoT. We think prospective MVNOs are becoming increasingly aware of this dynamic and are attracted to the opportunity to capture these smaller opportunities, which represent a substantial portion of the market in aggregate and are less likely to be contested by MNOs going forward. Only 10-20% of IoT subscribers are held by

MVNO value proposition: Abstracting telecom complexities for global enterprises



Source: FloLIVE.

MVNOs, but this percentage should gradually increase over time, especially if opportunities are passed to them.

Appearance and visibility of mobile virtual network enablers. Several companies in IoT cellular connectivity enable others to launch and operate MVNO businesses easily and cost effectively. These companies, aptly named mobile virtual network enablers (MVNEs), typically own some physical network infrastructure, such as a core network, and proprietary software systems, including business and operations support systems for billing, administration, connectivity management and other functions. Often, they have direct integrations into MNOs. MVNEs expose these assets and make them available on an outsourced-service or white-label basis to companies seeking to be MVNOs. With MVNEs, new MVNOs avoid the upfront costs and time required to integrate with carrier networks, develop proprietary software systems, and integrate with third-party point solutions. They rely on MVNEs' internally built or integrated systems so the MVNO can simply focus on marketing and support. MVNOs also benefit from MVNEs' scale and proven reliability compared to what MVNOs can achieve on their own.

Some MVNEs are also mobile virtual network aggregators (MVNAs), which purchase cellular connectivity on a wholesale basis from multiple MNOs and resell it to branded reseller MVNOs. While MVNAs

add a layer to the value chain, MVNOs can still benefit from the lower pricing MVNAs secure with their greater scale.

Despite the number of MVNEs being small due to the high cost to build and maintain such platforms and services, MVNEs have become increasingly more visible in IoT and more widely used as they are powering more branded MVNOs than one would expect. MVNEs should continue to foster new MVNO entrants due to the cost, time and functionality advantages they provide.

Lower entry barriers. In addition to MVNEs, which provide the bulk of what companies need to launch and run an MVNO, several point-solution companies have appeared to support prospective and existing MVNOs. Companies not wanting to leverage an MVNE's full suite of capabilities can adopt needed components, including connectivity and device management and billing, on an ad hoc basis from dedicated third parties. While not as aggressive as MVNEs in lowering entry barriers, point solutions still materially reduce the cost and time required relative to internal development and maintenance, helping to foster market entry. The benefit of a point solution is often best-of-breed functionality, typically with more frequent updates than in comprehensive suites. We expect more point solutions to emerge, giving MVNOs more options and access to the capabilities they need, and we expect increasing com-

petition among point solutions to reduce pricing and further reduce MVNO entry barriers.

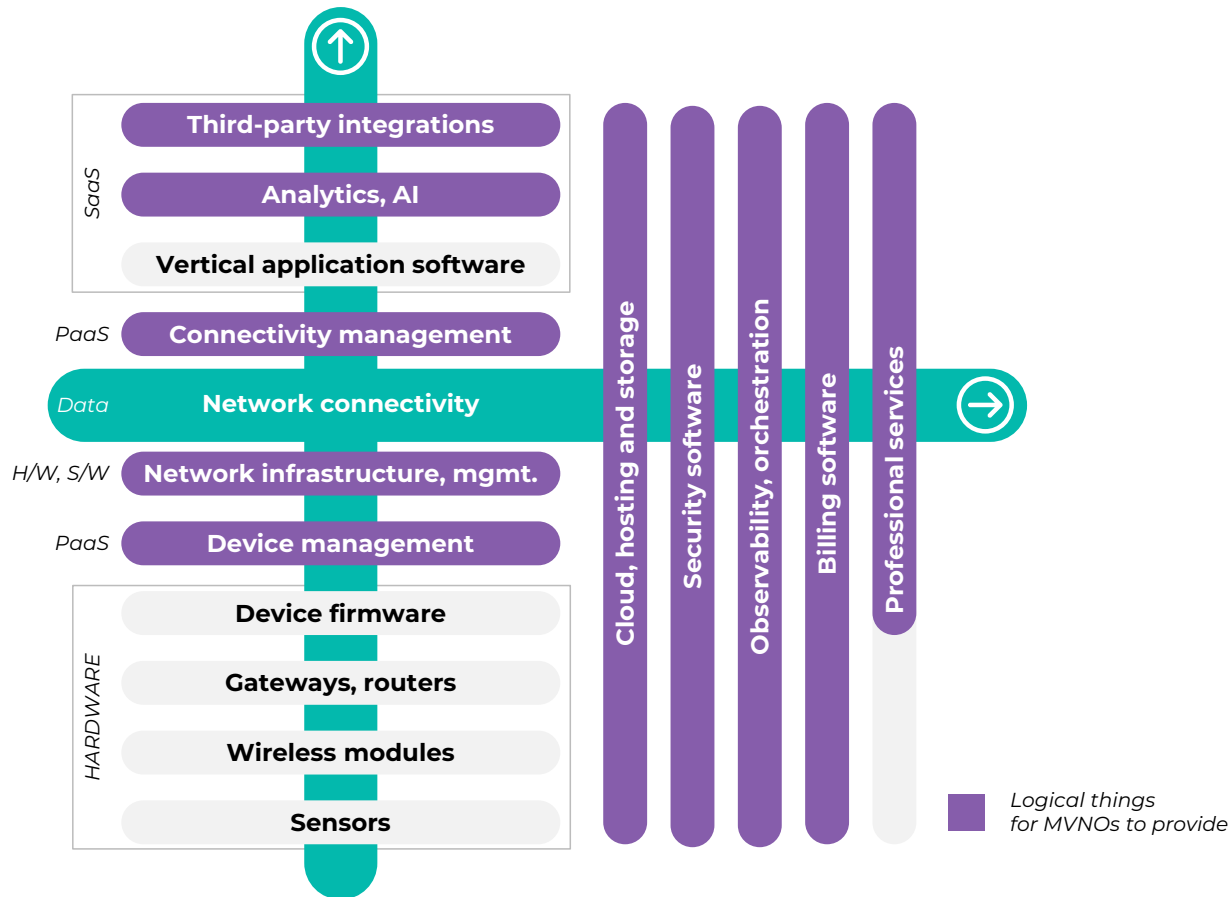
Another factor lowering entry barriers is today's greater ease of building platforms and integrations. Some companies approach connectivity with a desire to be more than a branded reseller and set out to develop core capabilities, such as core networks and connectivity management platforms, and integrate with carriers, thereby offering more value to users. Traditionally, building platforms and integrations has been time consuming and expensive, representing a barrier for prospective entrants. However, we have been hearing that the software stack for doing both has gotten simpler, lowering the entry barrier relative to the recent past. We expect to see a steady

stream of more advanced MVNO entrants that take advantage of evolving toolsets to enter the market with owned and proprietary capabilities (albeit fewer than branded reseller MVNO entrants).

MVNOs THAT MOVE BEYOND BASIC CONNECTIVITY WILL BE MOST SUCCESSFUL

While MVNOs provide valuable services for the IoT industry, it is important to remember their main product – cellular network connectivity – is largely undifferentiated between sellers, making it essentially a commodity. As MVNOs have competed against each other to win business, trading margin and profitability for market share gains, pricing per byte has trended down-

TABLE 6: Components of the IoT value chain it makes sense for MVNOs to offer



Source: First Analysis.

Notes: AI: Artificial intelligence. SaaS: Software as a service. PaaS: Platform as a service. H/W: Hardware. S/W: Software.

ward for years, manifesting in lower pricing (or bigger byte buckets for the same cost). Given the apparent increase in the number of MVNOs, particularly branded resellers, we think pricing pressure will continue, as most newcomers do not have other ways to attract business. Most MVNOs already highlight number of carrier networks, number of countries supported, and network performance. Given the lack of differentiation, we think most MVNOs will not fare well over time, as the ever-lower pricing will affect revenue growth and gross margin, ultimately pressuring many to exit the business. We think the most successful MVNOs, in contrast, will be those that adjust their approach and purposely become more than data resellers.

Many established MVNOs have already taken steps to move beyond connectivity, investing in various parts of the value chain (see Table 6), such as software that augments and complements their core businesses, and building more knowledgeable professional service and support teams. In areas where they lack expertise or the efforts are too great to undertake, MVNOs increasingly look to partner with point solution providers. We expect these activities to continue, as MVNOs have realized that building IoT solutions from scratch and managing and maintaining them is complex and challenging for most companies. It requires expertise in multiple distinct disciplines and is expensive. By offering one or more pieces of the value chain, wrapped around connectivity, MVNOs can reduce the burden on solution providers. This makes a lot of sense, particularly since connectivity is the point of commonality in all IoT solutions, one that MVNOs are wise to exploit as the center of gravity to attract customers. We think customers will be steadily drawn to MVNOs and willing to pay for the clear value of their added capabilities and services. Some of the newer MVNOs will likely follow this approach, as they see peers having success applying it.

That said, not all offerings that can be wrapped around connectivity are equal. Some are more difficult than others for MVNOs to deliver to solution providers and OEMs, and some provide more value to customers. Below, we briefly look at some software, service and other offerings provided by MVNOs and point solution providers in the market. We describe each of these, characterize their rarity and difficulty, discuss how sustainable their differentiation is, and assess the likelihood for them to become widespread. Obviously, the benefits of offering multiple capabilities and services together, whether proprietary or in partnership, are additive in value – increasing MVNOs' probability of success. We also review other paths to differentiation. We think these offerings, when used by MVNOs in the right combinations, will resonate with customers and provide growth tailwinds, which should benefit point solution providers as well.

Software

Connectivity management software is a collection of centralized functions used by service providers, including MVNOs and their reseller partners, to manage operations and support customers remotely. It is typically architected and delivered as a platform. Through the platform, MVNOs can establish customer accounts, create pricing plans and products, assign customers to them, and use integrations with MNOs or partners to activate, deactivate and suspend SIMs as needed. Activation is critical and involves provisioning SIM cards – assigning designated wireless carriers' profiles to subscriber identity modules (SIMs) and confirming SIMs are registered in appropriate databases so devices attach to the right networks and carriers.

The platform also enables MVNOs to track SIMs by location (making all connections visible across networks and deployments), monitor usage (looking for excess or irreg-

ular usage), create and manage automation rules for alerts and notifications and workflows for suspending and deactivating SIMs under specific scenarios and for changing plans, detecting and troubleshooting problems, and viewing performance metrics and reports.

Most MVNOs have exposed connectivity management functions to their customers – IoT solution providers and OEMs. This is aimed at fostering self-service, where customers can order SIMs, change plans, and create and set their own automation rules.

Connectivity management capabilities can be quite sophisticated in terms of visibility and control, extending well beyond the basic functions mentioned above. For example, we have encountered platforms that can leverage core network functions to automatically switch devices/SIMs from one supported network or carrier to another in case of network failure or disruption and if switching would improve performance (provide greater availability or better throughput). Related to this example, we see MVNO platforms now also supporting embedded SIMs (eSIMs). An eSIM is






a single SKU permanently mounted to a device's circuitry. It is pre-integrated with the networks and carriers and contains the profiles supported by the MVNO. MVNO platforms supporting eSIMs can provision them, change network profiles remotely, and set rules that cause them to change carriers automatically in case of service disruption and depending on performance levels and rates.

In another example, connectivity management platforms can enable observability and orchestration through integrations with multiple MNO and MVNO platforms. With this more unified view of customers' subscribers across disparate platforms, platform providers can continually analyze usage, pricing plans, and performance holistically, making adjustments as needed using automation rules to reduce or optimize costs.

Not long ago, basic connectivity management software capabilities were scant or rudimentary across the industry, but they've since become table stakes and widespread – most established MVNOs have some proprietary capabilities. Even

Wireless Logic SIMPro connectivity management platform

Our connectivity management platform provides a single window to securely manage IoT assets across any network and any number of deployments.

-  **Deploy and manage assets** quickly and easily
-  **Optimise costs** and **pre-empt issues** through powerful insights
-  **Real-time** help and support
-  **Automate** connectivity using our powerful APIs
-  **Unified** and **flexible billing** for all business structures



Source: Wireless Logic.

Notable connectivity management platforms



Source: First Analysis.

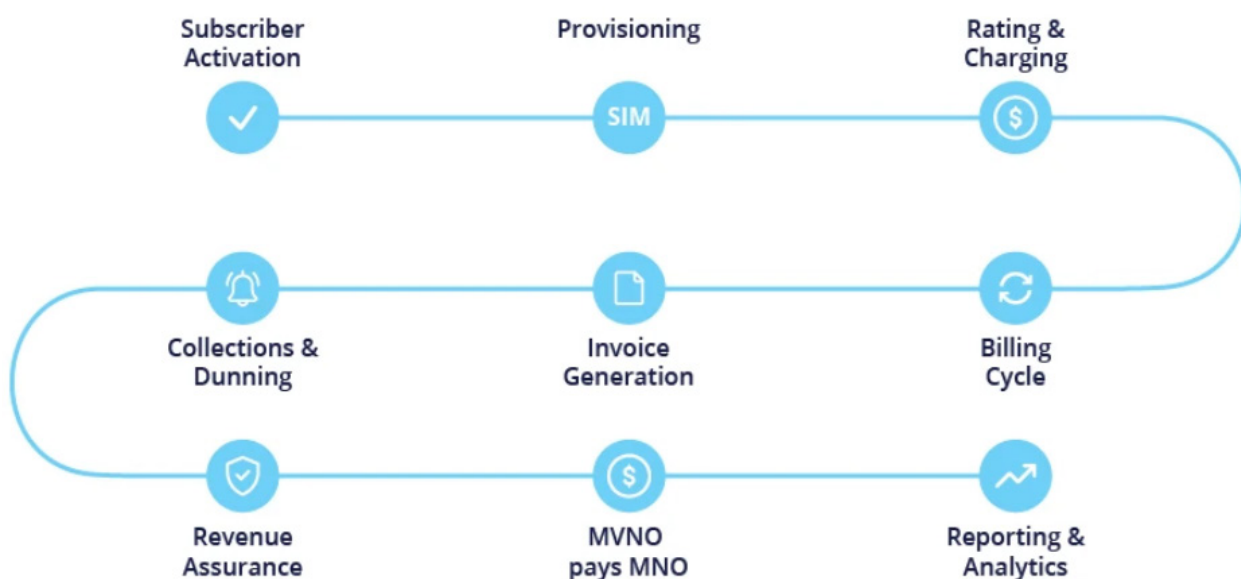
branded resellers have platforms, often leveraging MVNE platforms. More advanced capabilities are less common, suggesting an opportunity for MVNOs to differentiate themselves from peers by investing in this area. However, we think sustainable differentiation around most advanced functionality will be limited, as the capabilities providing significant utility are likely to become industry standards. For example, we fully expect network switching capabilities to become widespread, especially around eSIMs as they become the main vehicle for

connectivity delivery in the next few years and given these capabilities will become critical for MVNOs to remain competitive.

But, more importantly, a handful of third-party platform providers are positioned to offer an expanding roster of advanced capabilities broadly to the MVNO space. It is cheaper for MVNOs to use third parties than to invest to build and maintain such capabilities while gaining best-of-breed functionality. For this reason, we think third parties will be successful in enabling more advanced connectivity management, particularly since we don't believe the industry needs many of them to support it.

Billing is a key component of business support systems (BSS), a broad category of software-defined processes telecommunication service providers use to automate customer-facing operations. The software generates monthly invoices for each account, applying contracted rate plans to the data used per connection. It is a tremendously complex process, especially at scale and particularly since accounts often mix rate plans and add-on services that must be correctly applied to each active connection and then aggregated into a single bill.

MVNO billing step by step



Source: Tridens Technology.

A sampling of billing platforms enabling MVNOs



Source: First Analysis.

This complexity is magnified for telecommunication companies, including MVNOs, providing data connections across multiple carriers and geographies, as their billing systems need to correctly apply appropriate taxes, tariffs and other items. To provide billing, companies need to be integrated with MNOs' networks and software infrastructure to access information on active connections, data usage and customer-specific information.

It's rare for MVNOs to use proprietary billing software and likely to remain so; most use third-party billing software. This is unsurprising, considering the vast majority of MNOs themselves, which typically have far more resources than MVNOs, have outsourced their billing needs to dedicated providers because billing is complex and the systems are expensive. We have only

run across a handful of MVNOs with proprietary billing software. A few, while using this software for their own customers, have differentiated themselves by making it available as a service to other MVNOs. In any case, they software can provide visibility into bills on various parameters, enable end-user accounts to track subscription services beyond connectivity on the same invoice, and can support new pricing or business models as they emerge.

While we think creating proprietary billing software offers the potential for MVNOs to differentiate their offerings, we don't expect many more existing or new MVNOs to develop proprietary billing software due to its cost and complexity. We believe the industry only needs a small number of billing software providers to adequately support it.



Greenville, South Carolina-based **Zipit Wireless** differentiates itself from other cellular resellers with its proprietary platform software, which features robust SIM management, billing and reporting capabilities. In terms of connectivity, it offers global coverage enabled by direct relationships and integrations with large carriers. This gives Zipit access to hundreds of regional operators. IoT solution providers and OEMs can leverage a single global (multicarrier) SIM in their devices to connect to networks and roam across carriers or use a dedicated SIM in each region or geography, choosing the best carrier. To meet the needs of different IoT applications, Zipit supports multiple network types (including 4G LTE, LTE-M, NB-IoT, 5G) and optimizes rate plans for IoT business models. Through Zipit's platform, customers can select and manage their connections, including provisioning and activating SIMs, and change data plans and carriers to optimize performance and business profitability.

By pulling data directly from carriers via application programming interfaces (APIs), the platform provides visibility into the vari-

Active Lines and Data Usage per Device Type per Carrier:			
	Lines	Data (MBs)	Avg (MBs)
AT&T - GPS Tracker	459	1,634.0	3.6
AT&T - Fleet GPS	4,521	3,567,069.0	789.0
Verizon - Fleet GPS	1,247	1,051,221.0	843.0
T-Mobile - Fleet GPS	269	195,294.0	726.0
Sub-Total Active Lines and Data Usage	6,496	4,815,218.04	741.3

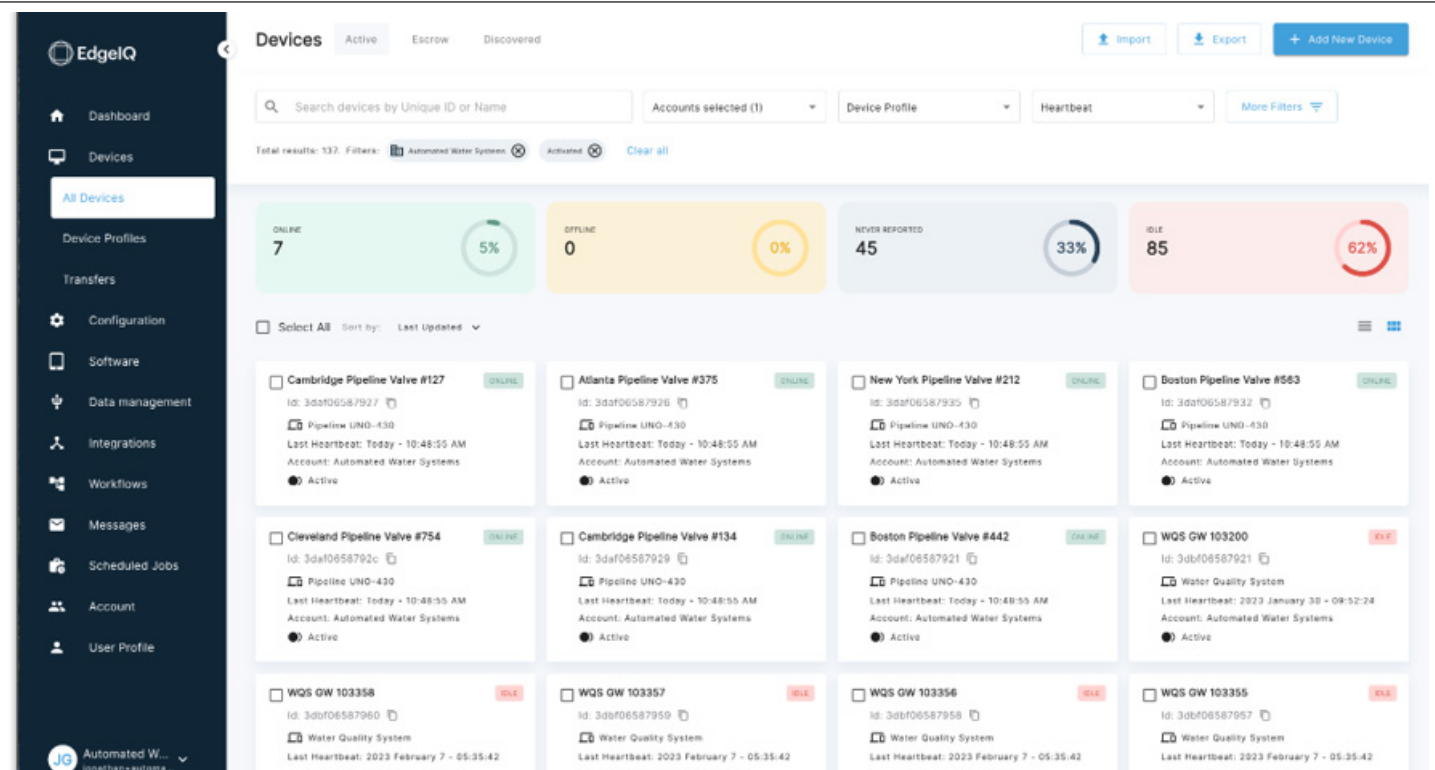
Source: Zipit Wireless.

ous attributes and metrics needed to guide these changes, such as number of devices active and idle by network type and carrier and data consumed per device and across deployments. Zipit's subscription billing solution processes this information, enabling solution providers and OEMs to automatically invoice their end customers for recurring data service, whether under fixed-fee, flat-fee or usage-based plans and taking into account any promotions, discounts and refunds. The configurable invoicing process can generate monthly, annual, seasonal or custom invoices. Notably, the platform allows customers to invoice their end users for connectivity and application and other subscription services, including add-on modules, in a single bill. Zipit calculates, collects and files taxes according to applicable laws and regulations. By enabling customers to associate their offerings with connections' activation status and usage, Zipit makes invoicing more reliable and makes it easier for its customers to manage their businesses.

Zipit made its billing software available as a standalone service to address the unmet need it saw for billing software in the market. It has already garnered traction with several enterprises and even rival MVNOs, evidencing the strength of its solution. In addition, Zipit enables IoT solution providers and OEMs to expose the platform's capabilities to end users, giving end users access to self-service tools for selecting and managing subscription services. Notable customers include Bushnell, Hunter Industries, Multi-Tech, Samsung, BrightSign, Thermo-Fisher and Cubic.

Device management software enables companies offering hardware standalone or as part of a complete solution to access and manage their connected devices over a network. It provides tools to identify, catalog, provision, configure, troubleshoot and update devices remotely over the air (OTA). Device management software is table stakes, because manually touching, configuring and updating devices in the field becomes impractical and prohibitively ex-

A device management dashboard



Source: EdgelQ.

pensive as device counts and geographic dispersion increases. Historically, this software was developed internally by hardware companies as an extension of firmware and also hardcoded into a cloud back-end or even the application layer. About four years ago, third-party device management software providers began to emerge as discussed in our June 2022 IoT Quarterly Insights report, [Rapid growth ahead for dedicated third-party device management providers](#).

Using third-party device management software works because base device management functionality required across hardware vendors is standard, and hardware providers are increasingly receptive to outsourcing because it costs less than building and maintaining internal device management platforms. In addition, it allows organizations to shift resources to more strategic and differentiating capabilities. Further, third-party software can provide best-of-breed functionality from more frequent updates. Some dedicated device management platforms go further than base configuration and OTA functionality by offering advanced features such as wellness monitoring (assessing unit health and identifying units needing service before material issues arise), access control and hierarchies (defining employee roles and

permissions), security scanning (for malicious firmware and vulnerabilities), analytics, auditing and reporting, and mixed-fleet management.

It's uncommon for MVNOs to internally develop and own basic device management software and even less common for them to develop more advanced software. Several MVNOs indicate on their websites they offer device management software, but often the functionality they describe – specifically, activating and deactivating devices, diagnosing network issues, and viewing signal strength – is more related to connectivity or SIMs than device management. Given the apparent scarcity of device management offerings from MVNOs, device management software's clear value, and the fact it complements connectivity management, we think there is a material opportunity for MVNOs to differentiate by adding device management capabilities.

That said, developing and maintaining software that is device agnostic (able to accommodate various hardware types and nuances and running on either the edge or cloud) is complex and not well aligned with most MVNOs' skillsets. Mixed device bases are an acute challenge for MVNOs, which enable many different solution providers using distinct hardware with different

Device wellness monitoring: Alerts categorized by importance

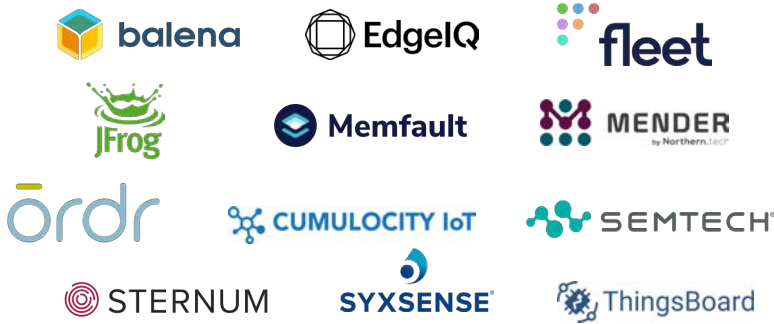
The screenshot displays the Cumulocity IoT Alarms interface. On the left is a navigation sidebar with options: Home, Devices, Overviews, Alarms (selected), Device control, Events, Groups, Device types, and Management. The main panel is titled 'Alarms' and features a filter bar with 'Critical', 'Major', 'Minor', and 'Warning' categories. Below the filter bar, there are four sections corresponding to these categories:

- CRITICAL:** Contains two alerts. The first alert (ID 1322) states: 'Real-time event processing is currently overloaded and may stop processing your events. Please contact support.' It is dated 10 Sep 2021, 12:36:47 and associated with CEP Engine t1692. The second alert (ID 35) states: 'Streaming analytics using CEL (Esper) is deprecated and no longer supported. Please refer to our documentation to migrate your real-time rules to Apama (https://cumulocity.com/guides/apama/overview-analytics/#migrate-from-esper)'. It is dated 6 Sep 2021, 05:00:16 and associated with CEP Engine t1692.
- MAJOR:** Contains three alerts. The first two are 'No data received from device within required interval.' with timestamps 21 Sep 2021, 14:25:29 and 14 Sep 2021, 15:26:05, both associated with Catarino64 (measurements). The third alert (ID 2) is an 'Exception on tenant t1692 in statement "smartRule7401737: GetRuleConfiguration": Invocation exception when invoking method "findManagedObjectById" of class "com.cumulocity.cep.server.core.function.DataAccessSingleRowFunctionPlugin" passing parameters [7401737, com.espertech.esper.client.hook.EPLMethodInvocationContext@28f947f6] for statement "durable:smartRule7401737: GetRuleConfiguration": MongoException : java.lang.SecurityException: deny Connect mongodb: 1.' dated 27 Jul 2021, 09:05:39 and associated with CEP Engine t1692.
- MINOR:** Displays 'No alarms to display.'
- WARNING:** Displays 'No alarms to display.'

At the top right of the main panel, there are controls for 'Show cleared alarms', 'Clear all', 'Realtime', and 'Reload'. The user 'admin' is logged in.

Source: Cumulocity IoT by Software AG.

Device management software via point solution providers



Device management software via MVNOs



Source: First Analysis.

software stacks. Without a device-agnostic solution, each would require integration and likely some custom development. Some MVNOs will be able to build their own device management layers, thereby achieving sustainable differentiation with unique-to-advanced device visibility and feature sets. Most, however, will need to partner with point solutions providers, providing point solution providers' offerings on a branded or white-label basis. Both proprietary and third-party models can be successful, although the economics and value obviously differ. Only a handful of MVNOs appear to be using third-party device management capabilities today, but this number is likely to rise.



EdgelQ, a First Analysis venture capital portfolio company based in Boston and formerly known as MachineShop, is a soft-

ware company that evolved from broader IoT application enablement to a hyperfocus on workflows associated with device life cycle management. EdgelQ was among the first to coin the term "DeviceOps," a nod to the broader automation, integration and orchestration needs of businesses that make, deploy and support connected products and networking equipment. Its platform, called Symphony, includes workflows and life cycle (state) and fleet management functions, such as provisioning, command and configuration, monitoring, alerting, diagnostics, remediation, and software updates. It also provides a rich, flexible multi-tier user and account hierarchy capability.

Relative to peers, EdgelQ Symphony differentiates itself by being workflow-centric, API-first and cloud agnostic. The platform is also operating system and network agnostic and offers both agentless and agent-based approaches for different deployment models. This flexibility allows EdgelQ to connect with and manage devices that may have their own cloud-native platforms and APIs. This approach has key advantages, particularly in terms of deployment velocity, administration and security, that have helped EdgelQ capture marquee enterprise accounts. EdgelQ recently began integrating its DeviceOps capabilities into MVNO and MNO connectivity management platforms. These relationships will expand the value of offerings from both segments by further simplifying device and connectivity management workflows into single, orchestrated workstreams in conjunction with customer relationship management, enterprise resource planning, customer success management, and customer-specific operational platforms.

EdgelQ addresses the market horizontally with traction in building automation systems, physical security, supply chain, networking, retail, and industrial automation applications. Notable customers include Johnson Controls, Carrier, and Digi International. The EdgelQ offering is a SaaS business model. There is a base annual subscription that scales based on device volume. EdgelQ Symphony now also includes premium modules for advanced orchestration and observability features.

Vendors with observability and orchestration capabilities



Source: First Analysis.

Observability systems bring siloed data into a single, unified view to enable greater operational visibility and efficiency and unlock unique insights to better manage and optimize businesses and offer service innovation. They involve software – a platform or middleware – that can be integrated with various data sources, using either pre-built connectors or custom development. This software automates collecting structured and unstructured data from disparate sources and normalizes it before combining it, analyzing it, and presenting output in a user interface. Technology vendors can use observability systems to improve internal operations or expose them to their end customers as an outsourced service, driving incremental value and stickiness.

In IoT, these systems can integrate many different sources and categories of data, including horizontal platforms, vertical applications and tools, and enterprise systems, whether they are in the same category (similar offerings from different vendors) or from different categories. For example, solution providers often have subscribers spread across several competitive networks. By bringing connection data from multiple cellular MVNO and MNO vendor platforms together in a single view, solution providers can improve decision making and management with centralized visibility. For the same reason, it also makes sense to tie cellular and satellite connectivity management platforms together. In another example, integrating across categories –

horizontal connectivity and device management platforms, where data is complementary – helps in understanding performance and troubleshooting issues.

Orchestration software is closely linked to observability. It initiates actions such as basic alerts and notifications and more advanced workflows and processes in response to data or events. The data used to trigger these actions comes from across interconnected systems and solutions, brought together for greater observability as discussed above, and can be either raw or processed data. The triggers, or automation rules, are created and managed within the orchestration software layer.

Notably, the orchestration software leverages the same integrations that facilitate observability when initiating workflows. These integrations give orchestration software access to and use of existing workflows and the ability to coordinate or stitch together processes across multiple systems to create altogether new workflows and more complete, end-to-end processes that were not possible when systems were separated.

Orchestration is used to react to events, remediating problems and issues, but it is also being used to prevent problems using data insights to enable predictive and proactive responses. The goal of orchestration is to automate manual processes, saving time and costs, while generating other business efficiencies.

Observability and orchestration, used either separately or in combination, have the potential to be transformative. For this reason, we believe companies that enable and use these capabilities have a higher probability of long-term success than peers who don't. Several MVNOs and supporting software vendors have platforms already being used in some capacity for observability and orchestration. Others have platforms that are strong enough to enable these capabilities in the future.

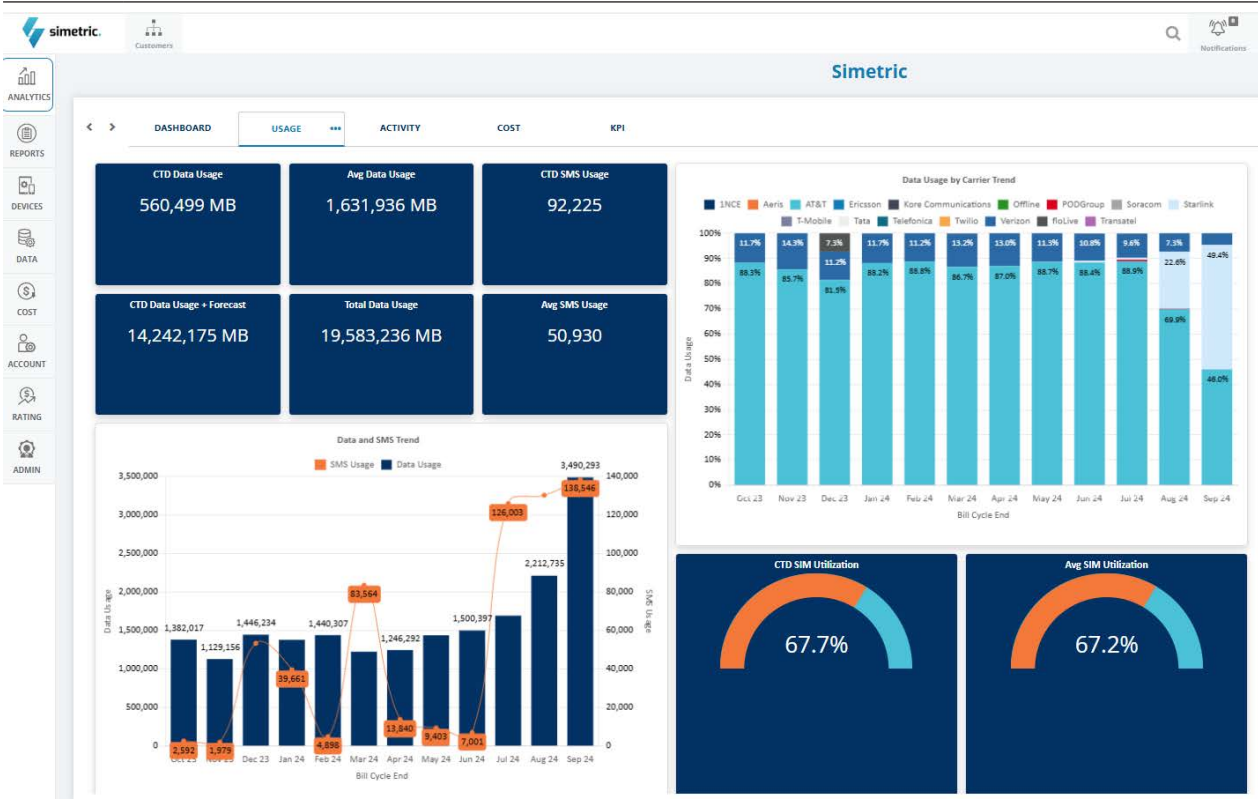
The value and sustainability of this approach is largely a function of integrations between platforms and third-party systems,

solutions, applications and data sources – the number, combinations, and especially the attributes of integrations that provide unique visibility and/or control. Some integrations are obviously more valuable than others, and multiple integrations can provide greater value to customers and end users alike than the sum of the individual benefits derived from each system or data set integrated.

The number of integrations used by most players tends to be small, suggesting observability and orchestration in IoT connectivity is an early or emerging development. We believe most existing platforms are just scratching the surface relative to specific integrations needed. This underscores the challenge of this approach, despite its material potential: Each integration takes significant time and effort.

From our conversations with several vendors, it was apparent that prospective integration partners are hesitant to share their systems data and access to control workflows and processes due to security risks. In addition, ambiguity regarding how these integrations will be monetized and how and whether the associated economics will be shared can impede discussions and agreements. Prospective partners also have competing priorities, which further causes delays. Sometimes, large MVNO customers and prospective partners have been able to move things forward based on their ownership of the data in question and their leverage. But large customers also often have competing priorities that hinder progress. Despite the challenges, we think companies that persevere and steadily build their integrations with relevant partners to support new data insights and process controls will foster sustainable differentiation and stand out among peers.

A connectivity management platform



Source: Simetric.



Simetric, based in Alpharetta, Georgia, offers a hybrid connectivity management platform that aggregates customers' IoT connections across cellular networks into a single interface for better visibility and more efficient control. It is primarily meant for enterprise solution providers with multiple acquired or independently run offerings supported by a variety of network operators or connectivity resellers. The core platform is enabled through integrations with several large operators, including AT&T, T-Mobile, Verizon and Vodafone, and client systems, which give Simetric access to granular data on each device connected and the functions needed to execute changes. Importantly, Simetric's software normalizes many of the variations that exist between carrier platforms, resolving the inherent lack of standardization, so visualized data is uniform and functions are cohesive to users.

The platform's capabilities are comprehensive and robust. Customers can use its reporting tools to review historical information across carriers on data usage, SIM status, connection cost, and other metrics. Its proprietary analytics and customizable query tools can reveal trends and

anomalies in real time. This visibility enables customers to identify opportunities for immediate attention and optimization. The platform can make adjustments, such as deactivating and suspending SIMs or changing (cycling) rate plans, manually using Simetric's intuitive workflows or automatically based on business rules that trigger specific processes for individual and bulk SIMs at one or more carriers – all without customers or departments having to know the identities of the underlying carriers. Simetric also has interesting hierarchy capabilities that enable customers to provide partners access to Simetric, further improving service and operational efficiency. Simetric's visibility into connectivity data is so strong that Simetric data is being used by third parties for billing end customers and by MNOs themselves to manage internal processes.

The monthly fee Simetric charges is based on number of SIMs customers have active within their network operator's platform combined with selected feature plans and add-ons. Over 2,500 companies worldwide use Simetric, including MNOs such as AT&T and Tata and some notable MVNOs, for internal or white-label use, to create new revenue streams, to better service customers and meet their evolving needs, to differentiate from peers, and to navigate a market landscape that is becoming more dynamic.

**Sampling of security software:
Via point solutions providers**



**Sampling of security software:
Via MVNOs**



Source: First Analysis.

Security software is used to protect networks, devices, systems and applications from digital attacks, such as stealing, exposing, altering, or destroying data, diminishing functionality or performance, and allowing unauthorized user access or control. It is a necessity for any software-defined solution that connects to the internet, making it applicable to all industries, especially IoT, where every solution has vulnerabilities and attack vectors, including multiple value-chain components and remote accessibility.

Most IoT vendors have deployed some form of security software as a result, whether proprietary, third-party or some combination of the two. It is particularly important for MVNOs to focus on security – and the vast majority do – because of connectivity's central role. One MVNO with a strong focus on security is **Aeris Communications**.

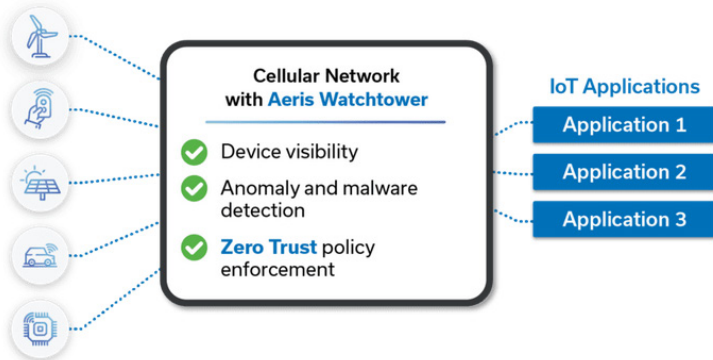
As one might expect, the depth and breadth of security software varies among MVNOs due to differences in resources, expertise and priorities. We have encountered MVNOs with rudimentary capabilities

and others with highly robust offerings that connect multiple disciplines. Some of the security software capabilities we've observed are device-centric, such as identifying unauthorized devices and activity and enforcing policies that stipulate where devices can operate and data limits. Other capabilities are more network-centric, such as monitoring network traffic, inspecting packets, and controlling traffic. Software that controls traffic can block data transmission to and from certain destinations when irregularities are detected, as well as block, suspend, and quarantine specific devices. We have also seen sophisticated approaches involving multifactor authentication, identifiers and keys for governing user and device network access inside and outside organizations. We summarize these and other capabilities we've encountered with example threats in Table 7.

While security software is seemingly widespread, we still think it's worthwhile for MVNOs, especially those with limited capabilities, to have a dedicated focus on security and invest in this area. There will always be a need to counter and protect against growing ranks of bad actors continually looking for vulnerabilities to exploit and evolving their methods. MVNOs should be able to attract and satisfy customers while extracting value for themselves simply by delivering a competent security offering that is regularly updated and maintained. There is also the potential for these same MVNOs to differentiate by looking for security software gaps in the market among peers and bulking up capabilities in those areas as well as developing sophisticated capabilities in specific areas and the reputation that goes along with it. Relative to the other offerings highlighted in this section, we see security as the most consistent way to add value and differentiate. That said, security is a challenging area that requires resources and expertise to truly unlock value.












IoT Devices



Source: Aeris Communications.

TABLE 7: Sampling of security threats and potential remedies

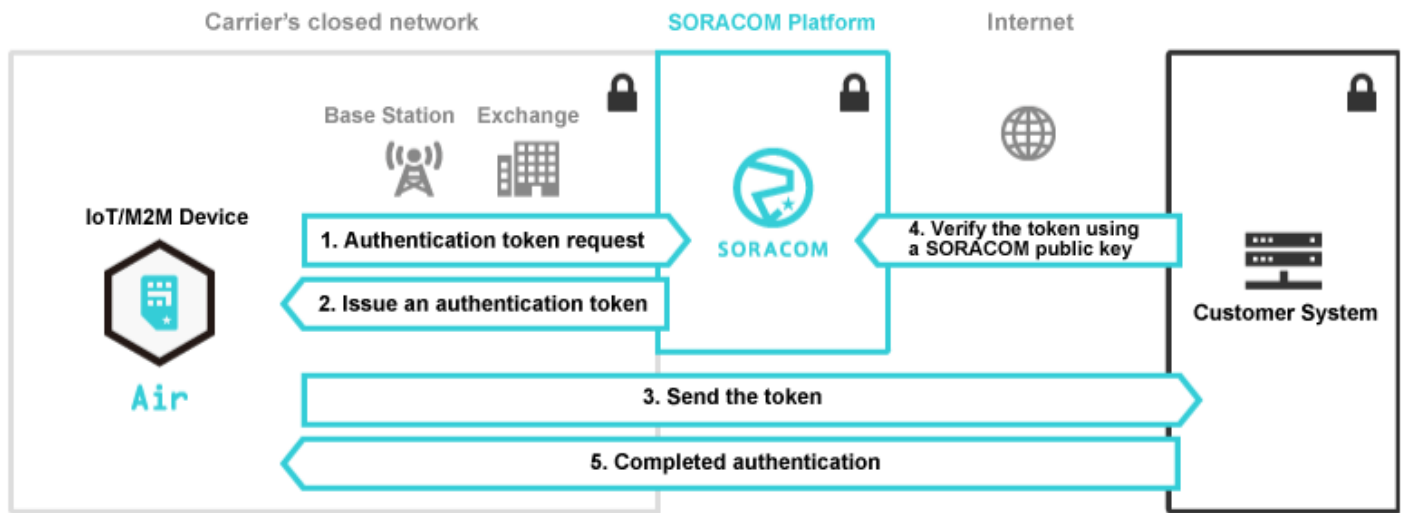
Security threat	Description	Protective capabilities/systems
 Distributed Denial of Service attacks (DDoS)	Overloading IoT devices with excessive requests, causing service disruption.	Rate limiting: Controls the rate of traffic to prevent overwhelming the device Traffic filtering: Identifies and blocks abnormal traffic patterns Edge computing: Offloads traffic processing to edge devices to mitigate impact
 Botnets	IoT devices are compromised and controlled by attackers to form a network that executes malicious tasks, like DDoS attacks or spam distribution.	Device authentication: Ensures only authorized users and devices can access the network Firmware updates: Regular updates to patch vulnerabilities that botnets exploit Intrusion detection systems (IDS): Detect unusual activity that may indicate a botnet infection
 Malware	Malicious software installed on IoT devices to perform unauthorized actions, such as data theft or further spreading the malware.	Endpoint protection: Anti-malware software or services installed on IoT devices Secure boot: Ensures that the device only runs trusted and verified firmware/software Sandboxing: Isolates applications to prevent malware from spreading to other parts of the system
 Phishing	Attackers trick users into revealing sensitive information or installing malware onto devices communicating with IoT devices, often via fake communications or websites.	User education and awareness: Training users to recognize phishing attempts Two-factor authentication (2FA): Adds an additional layer of security to verify user identity
 Malicious traffic	Traffic containing malicious payloads intended to compromise IoT devices, such as SQL injection or cross-site scripting (XSS).	Web application firewalls (WAF): Filters out malicious traffic based on predefined rules Deep packet inspection (DPI): Examines data packets for malicious content Encryption: Ensures data integrity by encrypting traffic between IoT devices and the network
 Man-in-the-middle attacks (MitM)	Interception of communication between IoT devices to eavesdrop, alter, or inject malicious content.	Secure communication protocols: Use of transport layer security/secure sockets layer to encrypt communications Mutual authentication: Both the device and server authenticate each other to prevent unauthorized access
 Ransomware	Malware that locks or encrypts IoT devices or their data, demanding payment for restoration.	Regular backups: Ensures data can be restored without paying ransom Access control: Limits access to critical system functions, reducing ransomware impact
 Brute force attacks	Attackers systematically try different passwords until they find the correct one, gaining unauthorized access to IoT devices.	Account lockout policies: Locks the account after a certain number of failed login attempts Complex password enforcement: Requires strong, unique passwords that are difficult to guess
 Physical attacks	Direct physical access to IoT devices, enabling tampering, data theft, or unauthorized control.	Tamper detection: Sensors or mechanisms that detect and respond to physical tampering Physical security measures: Securing devices in locked or restricted areas

Source: National Institute of Standards and Technology, European Union Agency for Cybersecurity, IoT Security Foundation, IEEE.

Hybrid connectivity refers to bringing different types of communication networks together in a system or solution. This is often done to extend primary coverage or enable backup and failover (secondary) coverage, but in some configurations, it is used to preserve battery power by offloading data to another network. Typically, only one network is active at any given time. While there are multiple wireless networks

that can be combined, the combination of cellular (terrestrial) and satellite networks is particularly important in IoT. Cellular networks are ubiquitous, offering robust coverage and throughput in urban areas; however, mobile and fixed devices can struggle to access cellular networks or maintain reliable connections in rural areas, and cellular connectivity is nearly worthless on the ocean. Verticals where this is a problem

Hardware authentication for IoT



Source: Soracom.

include oil and gas, agriculture, construction, fleet and maritime. By including satellite components – historically, as part of a dual-mode device that features separate cellular and satellite modules and antennas – device makers can greatly extend their devices' coverage range. They can automatically switch devices to satellite radio when cellular connectivity is inadequate or is failing, thereby ensuring real-time, two-way communication and preserving application return on investment.

Supporting satellite connectivity makes sense for MVNOs as satellite connectivity perfectly complements cellular, and the systems and support required for satellite

connectivity align well with those MVNOs already use for cellular. Supporting satellite connectivity also provides additional value, as most solution providers have at least some connections beyond cellular coverage or that sometimes experience issues that could be mitigated with satellite connectivity. The declining cost of satellite connectivity makes it even more compelling.

Nonetheless, MVNO support for hybrid connectivity is not yet common. Only a handful of the several hundred MVNOs have relationships with satellite companies where they either purchase satellite data capacity to resell or refer customers as part

Satellite network operators

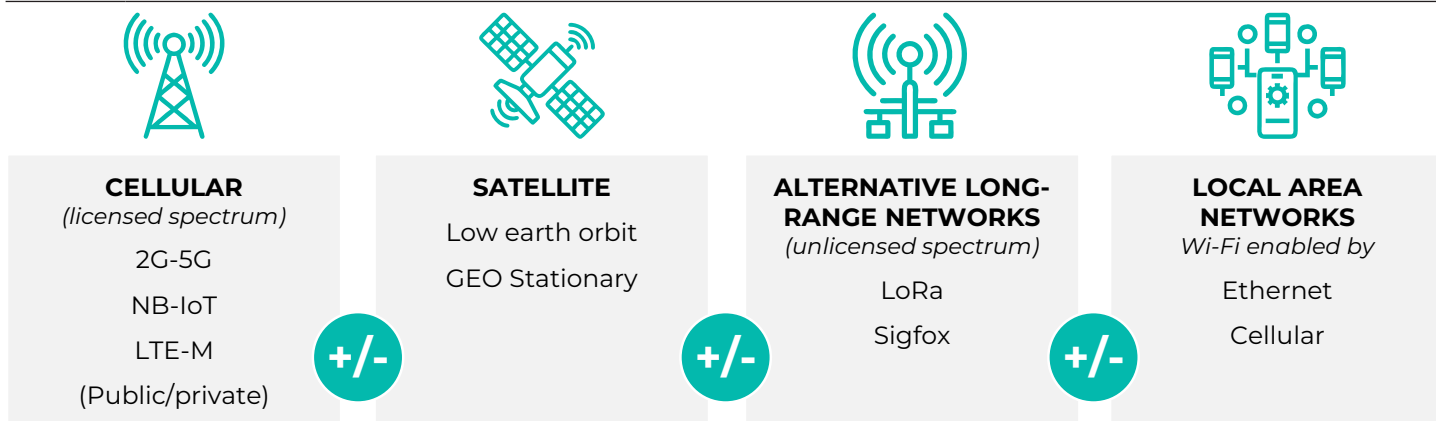


Sampling of satellite connectivity resellers



Source: First Analysis.

Network technologies that can be combined to form hybrid models



Source: Industry reports, First Analysis.

of channel arrangements. Examples include **Wireless Logic** and **KORE Wireless**. These MVNOs often leverage the same software systems used to manage their cellular businesses for the satellite offering or have access to partner capabilities through integrations. While cellular-satellite offerings and other hybrid connectivity options represent an opportunity to differentiate, we think the opportunity will be limited. In our conversations with leading MVNOs, several indicated plans to support hybrid models in the near term, particularly satellite, which will make it much more common in the industry. Others noted plans to evaluate alternative networks. We think hybrid connectivity will become a customer requirement at some point, pushing more MVNOs to support it to stay competitive.



We also expect support for hybrid configurations to accelerate due to the presence of several innovative vendors that are pushing certain technology advances and standards. These advances and standards make it possible to enable satellite and other long-range network connectivity in existing hardware devices and designs without having to make physical changes to the device. One such vendor is Skylo Technologies. Skylo uses firmware and SIM card profile updates to enable existing cellular NB-IoT devices to transmit and receive data using satellite networks without needing to add costly satellite components or re-design the hardware. Another is **Fossa Systems**, which uses a firmware update to enable cellular-LoRa hybrid devices to access its proprietary satellite constellation via the devices' existing LoRa chipset and antennas.

Other companies have similar approaches, and we expect new entrants with intriguing hybrid connectivity approaches that are simple to implement and cost effective. Many will partner with MVNOs and benefit by leveraging the resale channel to scale. Their MVNO partners should also benefit, for a time, from the differentiation of offering these hybrid connectivity capabilities.



Enabling satellite connectivity via
existing NB-IoT devices



Enabling satellite connectivity via
existing LoRa devices and antennas



Source: First Analysis.



Skylo is based in Mountain View, California. Its partnerships and software enable cellular MNOs and MVNOs to offer complementary satellite connectivity, expanding their coverage footprint. With Skylo, MVNOs and MNOs can better support existing customers and capture prospects by unlocking additional IoT and consumer use cases. Like an MVNO, Skylo negotiated agreements with owners of physical communication infrastructure – in this case, geostationary satellite companies including Viasat/Inmarsat, Ligado Networks and Strigo – to gain network access and permission to resell mobile satellite service spectrum and power. It also built its own network core and established its own ground stations in North America and Europe to more cost effectively move information between devices and partner satellite constellations.

The company's software stack is a true differentiator, as it allows existing cellular devices such as trackers and sensors to connect to satellite networks without requiring physical changes to devices, such as adding satellite radios, which can be expensive. For narrowband devices, MNOs and MVNOs can make satellite connectivity available to existing and new subscribers by simply updating software clients or profiles on eSIMs. The software is also being incorporated at the chipset (via partners Qualcomm, Altair and Samsung) and module levels (via Quectel, Flex and

muRata), providing other paths. Once enabled with the software, devices can roam seamlessly over satellite networks as easily and frictionlessly as they do over cellular networks.

Skylo is ideal for MNOs and MVNOs supporting customers in fleet, agriculture, energy, maritime, and emergency response sectors, where terrestrial connectivity is limited, unreliable or non-existent and that require long-range primary or backup connections. Skylo enables MNOs and MVNOs to offer a holistic solution across customers' entire footprints – all from a single SKU. We note Skylo doesn't provide connectivity and device management capabilities or professional services; its partners do. Skylo does, however, have some billing capabilities and a dashboard that can be integrated to provide visibility into various metrics.

Skylo is a player to watch given its ability to help partners differentiate themselves and generate incremental revenue by easily adding satellite connectivity to address the growing demand for ubiquitous connectivity. Skylo's MVNO partners, such as Soracom, FloLIVE, Emnify and Transatel, and its major carrier relationship with Deutsche Telekom validate the value of its offering and model.

Physical infrastructure

Core networks

Core networks are critical components of telecommunications systems. They consist of networking hardware such as switches, routers and gateways (in centralized or distributed locations) as well as

Some of the MVNOs with a proprietary core network



Source: First Analysis.

sophisticated software. Core networks are separate and distinct from radio access networks (RANs), or the towers controlled by carriers. Core networks sit between the scattered elements of the network infrastructure – communication nodes, subnetworks and platforms – linking them through fiber optic cables. By linking these elements, core networks are essentially large gateways to other networks and destinations, including the internet, that provide multiple paths to exchange information. Redundancy is built in. This structure enables core networks to fulfill their primary function of routing data traffic reliably

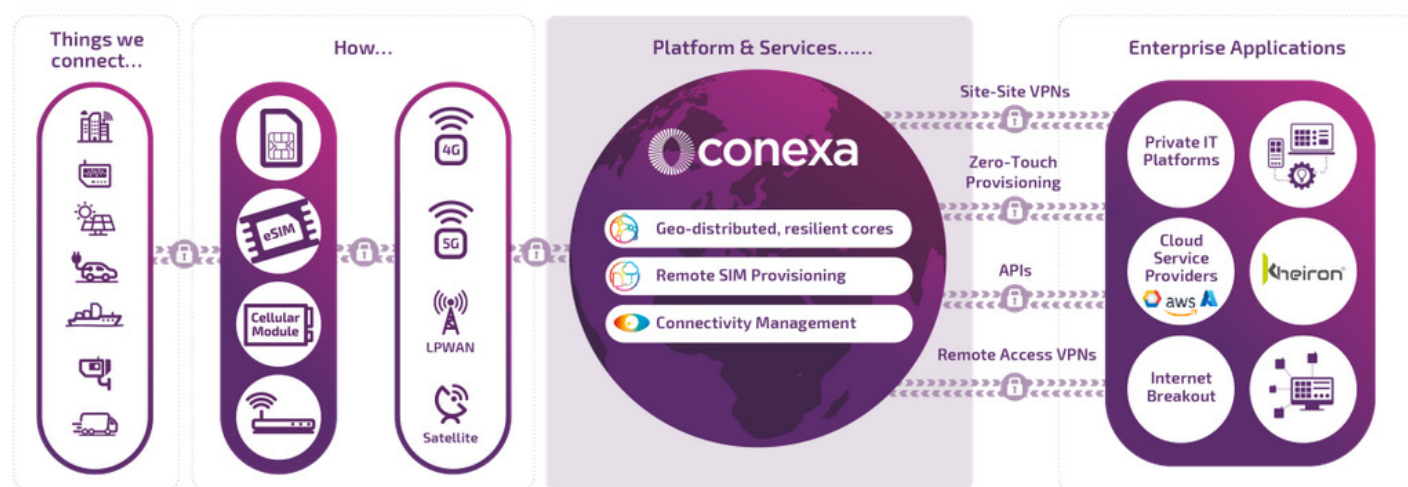
at high speed. Core networks also work closely with other network elements. They help make it possible to identify devices trying to connect to the network and their locations, authenticate them, verify authorizations for specific services, and track service usage for billing purposes. In general, core networks are owned, operated and maintained by MNOs alongside their other assets.

MVNOs do not need to own a core network to provide connectivity services, as they can leverage MNOs' core networks. In fact, most MVNOs do not have their own core network, because core networks are extremely challenging to build, requiring deep expertise and significant time and capital investments. Operating and maintaining core networks is similarly challenging. However, a handful of MVNOs that recognized having a core network unlocks competitive advantages elected to do so to differentiate their services despite the challenges and costs.

Advantages of proprietary core networks

Greater reliability. Owning a core network provides direct access to network elements that in turn provides visibility into real-time event data (such as issues and faults) and more robust performance metrics. With this

Wireless Logic platform and service around distributed core



Source: Wireless Logic.

MVNO as a service: White label, light or full

White Label MVNO	Light MVNO	Full MVNO
Designed for providers that want to focus on marketing and sales under their own brand, with the option to grow into a light or full model.	For Mobile providers that would like to have more control and tailor their own offerings without having to worry about the technology behind it.	For MVNOs that want to offer a real time self-service platform or are interested in better global wholesale rates on multiple radio networks
iBASIS PROVIDES <ul style="list-style-type: none">✓ Branded Platform / APIs✓ Global Access LTE-M/3G/4G/5G✓ Branded SIM✓ Core Network✓ Rating & Billing YOU PROVIDE <ul style="list-style-type: none">✓ 1st Line Support✓ Sales & Marketing	iBASIS PROVIDES <ul style="list-style-type: none">✓ Branded Platform / APIs✓ Global Access LTE-M/3G/4G/5G✓ Branded SIM✓ Core Network YOU PROVIDE <ul style="list-style-type: none">✓ Rating & Billing✓ 1st Line Support✓ Sales & Marketing	iBASIS PROVIDES <ul style="list-style-type: none">✓ Branded Platform / APIs✓ Global Access LTE-M/3G/4G/5G YOU PROVIDE <ul style="list-style-type: none">✓ Branded SIM✓ Core Network Elements✓ Rating & Billing✓ 1st Line Support✓ Sales & Marketing

Source: iBASIS.

direct access and data, MVNOs can react faster to resolve issues, make adjustments and improve reliability, all without the delays and lesser control inherent in working through a partner, such as an MNO.

Reduced latency. Latency refers to the time it takes data to travel from its origin to a destination. In global deployments, when a device is roaming in another country, data is routed to the connectivity provider's core network and data center in the device's home country before being sent to its final destination, even if that destination is local to the device. This leads to material latency. By having a core network in the roaming country, an MVNO can enable data from such a device to travel directly from the device to the local core network and then to the local destination, noticeably reducing latency.

Compliance. Several countries have laws regarding data localization and sovereignty that prohibit data generated and gathered inside these countries from leaving them. The visibility and control enabled by having core networks or distributed core elements in such countries allows MVNOs to better satisfy associated compliance

requirements, in real time, by monitoring traffic origination and routing or restricting it accordingly.

Billing accuracy. Core networks provide their operators significant visibility into data traffic, including the ability to track data used by device at the individual connection level. By combining this granular usage data with information from subscriber databases regarding the services devices can consume, MVNOs can enable internal billing software or third-party billing with highly accurate data. MVNOs need accurate, granular data to bill correctly, especially for difficult plans such as pay-as-you-go.

Flexibility. MVNOs that own core networks gain significant flexibility, such as the ability to tailor and customize network attributes to meet the needs of IoT users, which are an amalgamation of diverse use cases and requirements.

Simplified logistics. MVNOs with core networks can offer largely uniform coverage and experiences globally, enabling devices to connect in the same manner anywhere in the world. They can offer a single SIM for global coverage, eliminating

the need to manufacture and distribute different SIM cards for each region, simplifying logistics, and lowering costs.

Each of these advantages is material, and in aggregate they provide material utility and value to MVNOs, their IoT solution provider customers, OEMs, and end users. In the future, more MVNOs may build or acquire their own core networks to differentiate their offerings, as the market now has only a small number of MVNOs with proprietary cores, and we believe there is room for more. However, the significant investment required to build, operate and maintain core networks, not to mention the expertise required (which most MVNOs don't have), means the number of MVNOs with core networks will likely remain low. Some MVNOs have recognized this and exposed their core networks to other MVNOs as an outsourced service, putting them in a good competitive position and reducing the incentive for other MVNOs to build their own cores.



Soracom, an MVNO headquartered in Tokyo and enabled by its relationships with over 350 carriers that give it near-global coverage, resells cellular connectivity to IoT solution providers operating in a range of industries. It supports all cellular network types and speeds (2G, 3G, 4G LTE, 5G CAT-M1, NB-IoT). It offers removable and embedded SIMs to fit any device and form factor and automatically connect to carrier networks. It also supports single-pane-of-glass management for both satellite and LoRa connectivity providers (Astrocast, Skylo and Sigfox) to extend the reach of truly remote IoT applications.

In contrast to most MVNOs, Soracom built its own core network, represented by its virtualized packet gateway, which has distinct benefits and enables more sophisticated capabilities relative to standard offerings. The core network also enables

Soracom user console

A screenshot of the Soracom user console interface. The interface features a top navigation bar with a menu icon, the Soracom logo, and links for 'Product Updates', 'Global', 'Support', and a user profile. The main content area displays a table of SIM cards with columns for Name, Group, ICCID, Status, Plan, Subscription, Speed class, Expiry Date / Time, and IMEI Lock. Annotations with arrows point to various features: 'Assign SIM names and create groups' points to the 'Name' column; 'Automate actions with Event Handler' points to a 'New Automation' modal window; 'Restrict SIMs to devices with IMEI lock' points to the 'IMEI Lock' column; 'Order new SIMs on demand' points to a 'New Order' modal window; and 'Store data and visualise usage consumption' points to a 'Data Usage' graph. The 'New Automation' modal shows a target SIM ID, a trigger condition (Exceeds 10MB per day), and an action (Deactivate SIM). The 'New Order' modal shows a list of SIM packs and a 'Place order' button. The 'Data Usage' graph shows a line chart of data consumption over time.

Source: Soracom.

Notable MVNEs



Source: First Analysis.

Soracom to provide improved data routing, latency and security and to deliver a much more reliable service. The core network provides Soracom greater visibility into network performance and changing conditions. It uses this information to direct SIMs to automatically select the best network (tower) available and switch to others if coverage deteriorates. It also provides deep visibility into data packets, yielding information that supports the company's pay-as-you-go pricing model and helping solution providers avoid paying for unused data capacity. This focus on minimizing the cost to solution providers extends to its User Console. Customers use this portal to provision, activate, name and group SIMs en masse and manage plan changes. More importantly, the console enables customers to set data limits by SIM and device groups, issue alerts when limits are exceeded, create automated rules for when to start and stop or pause SIMs (such as for seasonality), and downgrade service speed to control costs.

More advanced functions can be accessed in areas such as protocol conversion, authentication, data funneling (to public or private clouds), device management, and data visualization. Soracom's platform can be used directly, or customers can build and consume Soracom features inside their own applications. Soracom is a strong player with good momentum, evidenced

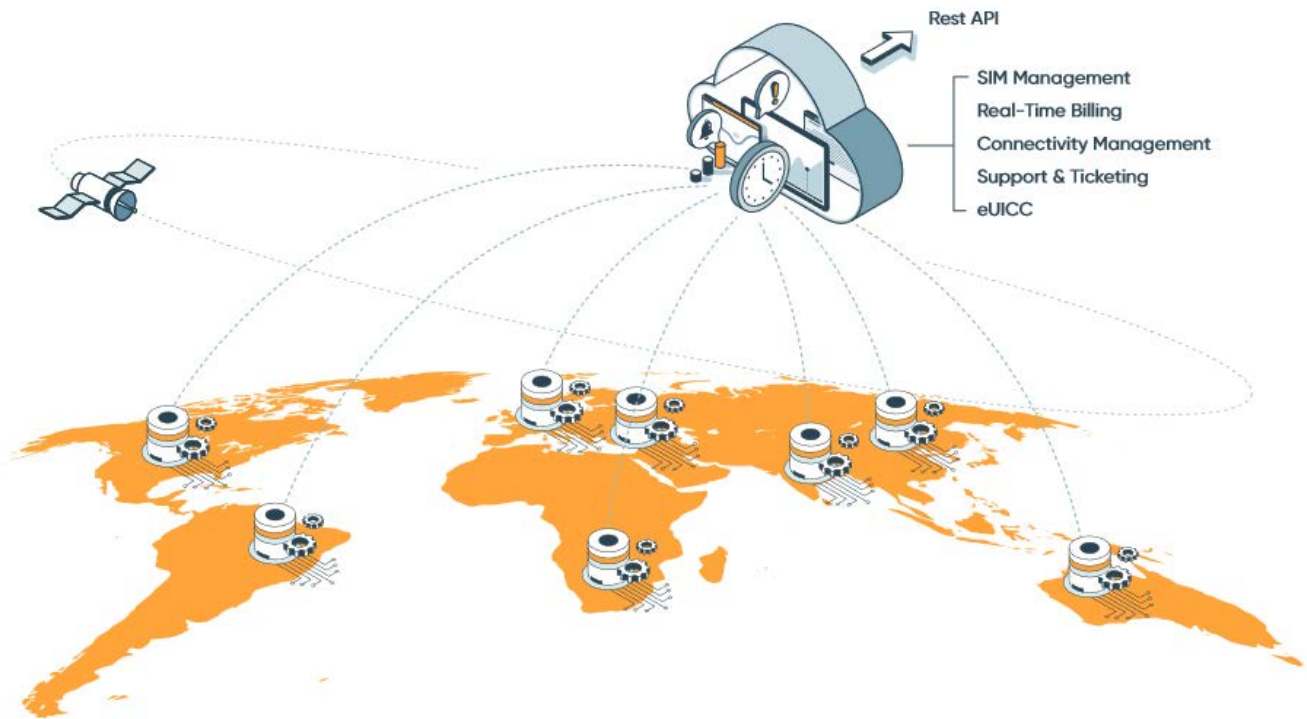
by its over 20,000 customers, from start-ups to enterprises, including Komatsu, OpConnect, Pebblebee and Panasonic.

The MVNE model

Mobile virtual network enablers, through their own physical network infrastructure, proprietary systems, and integrations, enable companies to quickly launch MVNO businesses and cost-effectively operate them. They also provide significant utility and value to existing MVNOs and MNOs that wish to upgrade their capabilities, increase reliability or extend coverage in specific areas while reducing ongoing internal support costs.

Unsurprisingly, MVNEs are doing quite well in the market, as evidenced by the strong growth in number of branded reseller MVNOs and MVNEs' increasing use by legacy MVNOs, which recognize the superior visibility, reach and control afforded by MVNEs' core networks and software.

Many companies, including MVNOs, theoretically could adopt the MVNE approach to differentiate and add value and be similarly successful, given the market's receptivity and given MVNEs are uncommon (only five to 10 are active today). That said, given most companies lack the resources – time, cost and expertise – to build and maintain the required platforms, systems and core networks in multiple regions, we don't expect many new MVNEs to appear over time. Further, capital availability for launching new MVNEs will likely be constrained due to prospective investors' uncertainty about the number of MVNEs the industry can support. We think there is little room for new MVNEs, given the clear inefficiency of building highly redundant infrastructure and systems. The few MVNEs that do manage to enter the market will likely come from the ranks of existing MVNOs that already own infrastructure and systems that can be relatively easily delivered as an outsourced service. For these reasons, we think existing and prospective MVNOs looking to differentiate should direct their efforts elsewhere.



Source: FloLIVE.



FloLIVE, headquartered in London, provides cellular data services worldwide to device manufacturers and solution vendors through its cloud-native, software-defined suite and infrastructure that was purposefully designed and built for IoT applications. Among MVNOs, it is one of the few that own the entirety of the technology stack, including the core network, basic support systems, and the connectivity management layer. Having this stack enables FloLIVE to provide robust service, support and other capabilities in a combined suite. It has deployed full-fledged core networks (2G to 5G) in many parts of the world, integrating them with local MNOs. By leveraging its own core, FloLIVE bypasses significant MNO infrastructure, enabling faster data speeds and reducing latency issues.

Having core networks in certain geographies also allows it and, by extension, its customers to avoid roaming, which is banned in an increasing number of countries, and helps ensure compliance with data regulations such as Europe's General Data Protection Regulation. FloLIVE customer devices can access cellular networks anywhere in the world once the SIMs and eSIMs provided by FloLIVE are installed and active.

FloLIVE's sophisticated FloSIM software handles provisioning, registering devices with the cloud, determining appropriate international mobile subscriber identities and carriers based on location, and loading pre-defined rules. Customers can use FloCloud for connectivity management. FloCloud is a platform used to activate, de-activate and suspend SIMs, to automatically or manually direct SIMs to different networks based on performance, to failover to other networks to maintain connections, and to deploy configuration updates

MVNOs with strong focus on professional services



Source: First Analysis.

over the air. FloBSS, the company's flexible and out-of-the-box billing system, is tightly integrated with these other components, providing visibility needed for rating, tariffs, taxing, and invoicing and managing customers. It features templates but can be customized to handle all types of plans (such as pre- and post-paid and hybrid plans), structures and models (such as pooled and pay-for-use), currencies and carriers. It can also accommodate bring-your-own-connectivity (BYOC) and layering and billing for non-connectivity services. Notably, FloLIVE has exposed its technology stack, making its components or the total offering available to both existing MVNOs that want to bulk up their capabilities and companies that want to

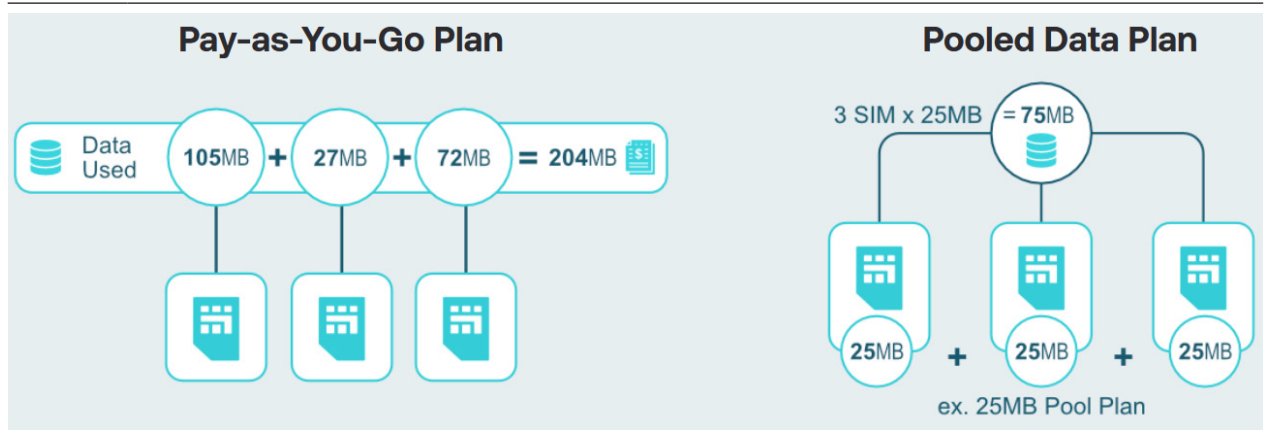
enter the market to become MVNOs themselves. It is one of the first true MVNEs, and its strong capabilities make it a player to watch.

Professional services

Professional services are any form of assistance provided by vendors' staffs dedicated to supporting customers in designing, building, launching and managing IoT solutions. These services generally fall within one of a few high-level categories, including consulting, creating products, testing and support/troubleshooting. For example, consultants or solution architects may offer recommendations on hardware and user-interface design, solution architecture, battery optimization, implementation, and third-party vendor selection for hardware, security services and database software. Engineers may design hardware and manage assembly. Developers may code vertical-specific applications and configure infrastructure software. These same knowledge workers are often used for testing, identifying root causes of issues, and remediation. The specific services offered and their depth as well as the quality vary by firm, as they are determined by company strategy and employee knowledge.

It is common for MVNOs to offer some level of professional services. We have encountered some that provide basic services and others that offer extensive "white-glove"

A few pricing models illustrated



Source: Soracom.

services, where MVNO professionals do much, if not all, of the work to build, launch and maintain IoT solutions to fit customer specifications. Notably, not all MVNOs charge for this, especially for large accounts or prospects that have potential to scale. While offering professional services is common in the industry and not always monetized directly, we think it is a viable way for MVNOs to create value beyond connectivity and differentiate, given the needs we see among IoT solution providers and the limited resources available to them. As previously mentioned, it is difficult to create an IoT solution, and it is likely to remain challenging.

As new IoT technologies, capabilities, and approaches emerge, demand for support among IoT solution providers is likely to remain robust, and we think providers will find MVNOs offering dedicated support an attractive option. MVNOs with strong expertise in selected parts of the value

chain or in specific vertical markets should fare best, as their help can lead to unique solutions, greater reliability, and performance advantages relative to solutions created with more generic services offered by horizontal MVNOs. That said, it can be hard to find, attract and retain high-quality talent in specific value chain areas or verticals, given talent shortages and competing opportunities.

Strategic approach and focus

Creative pricing models. Some MVNOs offer pricing models aligned to IoT solution providers’ data needs and business models (see Table 8). The fixed price model, where customers pay a set price per connection for a specific amount of data each month, either pre- or post-paid, with excess data use resulting in an overage charge, has long been common. But due to IoT solutions’ typically low data consumption, this model often results in unused data, meaning customers pay for capacity they didn’t

Table 8: Observed pricing models

FIXED (CAPPED) A specific amount of data is provided monthly per connection at a set price; reaching the data limit can lead to disrupted service or extra charges for excess use	UNLIMITED No limitation on the quantity of data that can be consumed monthly per connection; the price is fixed, no overages	PAY-AS-YOU-GO <i>(usage or event-based)</i> Customers pay for only the actual data consumed in a period; no overage charges
POOLED A set amount of data shared among a group of devices; any excess consumption by devices is meant to be offset by those consuming less than expected	ONE-TIME (CAPEX) Multi-year plan paid in full upfront, granting a set amount of data services that a connection draws from over time; consuming the full allotment requires a new plan purchase	HYBRID The combination of two or more pricing models within a single plan
BUNDLED A collection of different data-related services or products that are packaged and priced together	DEVELOPER An amount of mobile data, covering a set number of devices, is provided free to developers and solution providers every month for testing and pilots, in exchange for the potential to scale on that network’s platform	FREE TRIAL The use of wireless data for free for a stipulated (limited) time for a specified number of devices

Source: First Analysis.

need. A handful of MVNOs recognized this inefficiency and created pay-per-use or pay-as-you-go plans, where there is no penalty for underutilization and customers pay only for what they use. A variation is a pooled plan, where unconsumed data aggregated across connections can be used to offset excess use or carried forward. Another approach is the fixed rate, long-term plan, which is payable entirely in advance (full-capex model) and provides a specific amount of data per connection for use within a multiple-year period. Customers can consume the data however they wish, but should it be exhausted before the term ends, overages are charged or another bundle purchase is required. Solution providers and OEMs have responded well to both options. The pooled plan leads to cost savings, and the fixed, long-term plan helps them establish sustainable business models. The pay-as-you-go model is starting to become common among MVNOs, and we have heard from several MVNOs that they are launching full capex models in the near term. Both may become ubiquitous and even a prerequisite for remaining competitive. That said, we have heard questions about the sustainability of the full capex model, given MVNOs adopting it face the challenge of cost inflation and continually investing more in capabilities to remain competitive with a largely fixed-fee base, only a portion of which renews each year with higher pricing.



1NCE, based in Cologne, Germany, is a cellular connectivity and software service provider focused on enabling IoT applications. It is a strategic partner of Deutsche Telekom that was created through a joint venture, which gives 1NCE direct access to Deutsche Telekom's wireless infrastructure and roaming partner network. This equates to global coverage, enabling 1NCE to reach 165 countries and support any radio standards active in these regions (2G, 3G, 4G/LTE-M, NB-IoT). 1NCE's differentiation, as

hinted at by its name, is in its pricing model: It sells multiple years of global connectivity and software service at a flat rate per device with a one-time payment.



























This offering, called the IoT Lifetime Flat plan, includes a SIM card and 500 megabytes of data and 250 short-messaging-service messages that a device can consume over a 10-year period (the assumed maximum lifetime of an IoT device). The Lifetime Flat is \$10 to \$12.50 per data plan, depending on whether it is for a removable or embedded SIM.



The plan includes complimentary access to 1NCE's connectivity management platform, which enables customers to activate, suspend and deactivate SIM cards and, for eSIMs, transition to other networks. Its 1NCE OS is a suite of software tools for monitoring and locating devices, authenticating devices, managing energy usage, and integrating device data exchange to any cloud, including AWS. The approach was formulated to help solution providers building low-bandwidth applications, such as applications for smart utilities, asset tracking and supply chains. It helps them more quickly connect their hardware to networks and get data to the cloud while making connectivity more affordable, predictable and manageable.

Notably, the plan is truly a flat-rate plan, as 1NCE doesn't charge for set-up, roaming in supported countries, secure data channels via virtual private networks, or network changes. For devices exceeding data and message limits, plans can be renewed or

TABLE 9: Many distinct market verticals

 Agriculture	 Asset tracking	 Automotive	 Autonomous & robotics	 Building/property mgmt	 Construction	 Digital signage & media
 Energy & utilities	 Envir, natural resources	 Food & beverage	 Healthcare	 Hospitality	 Industrial	 Lone worker
 Manufacturing, fabrication	 Mobility/micro-mobility	 Oil & gas	 Payment systems	 Public sector, government	 Retail & vending	 Security & surveillance
 Smart city	 Smart home	 Transportation & logistics	 Waste management	 Wearables		

Source: First Analysis.

topped off at the same price point automatically through the customer portal, ensuring service continuity. 1NCE's model has been disruptive, as evidenced by its more than 20 million connections across more than 15,000 customers worldwide since the company's late-2017 launch.

Vertical focus and expertise. MVNOs typically approach the market horizontally, serving most, if not all, vertical segments and industries (see Table 9) with the same underlying infrastructure, software and systems. This is unsurprising as connectivity is applicable to all markets and a horizontal approach equates to the largest number of customer opportunities. But a handful of MVNOs – many of them new to

the market – have eschewed the traditional broad approach and opted to focus on one or a few vertical markets to achieve growth and scale. These MVNOs have recognized that each vertical application has unique technical challenges and requirements and that a one-size-fits-all platform and professional services team does not always lead to the best results in terms of cost-effectiveness, communication reliability, latency and impact on battery life. In response, some MVNOs have put together teams that combine professionals with deep wireless technical knowledge and subject matter experts to tailor optimized connectivity services and dedicated support for targeted markets. Often, this has required adjusting existing software and systems, creating unique and custom features and functionality, and releasing new solutions and applications.

MVNOs with a more concentrated vertical focus

**Source:** First Analysis.

We think a vertical-centric approach is a viable strategy to pursue. It is uncommon among MVNOs, and we think providing deep sector knowledge will always be a reliable way to deliver value. This value can come from enhanced offerings or providing turnkey hardware and templated vertical-specific applications that meet the unique needs of a targeted vertical out of the box. An example of an enhanced offering is releasing intelligent tower and network routing as part of connectivity man-

agement to improve connection throughput and reduce latency while reducing impact on battery life to connect to a network. But the value is more likely to come from professional services. IoT solutions within the same vertical often share requirements in areas such as data package size, communication frequency, and battery life. These solutions also often share constraints related to environmental conditions such as temperature, light, humidity, moisture, obstructions, and the existence of network infrastructure. Their enabling hardware is often comprised of similar components from a handful of vendors. Each of these constitutes a variable that can affect communication reliability and battery (or device) longevity.

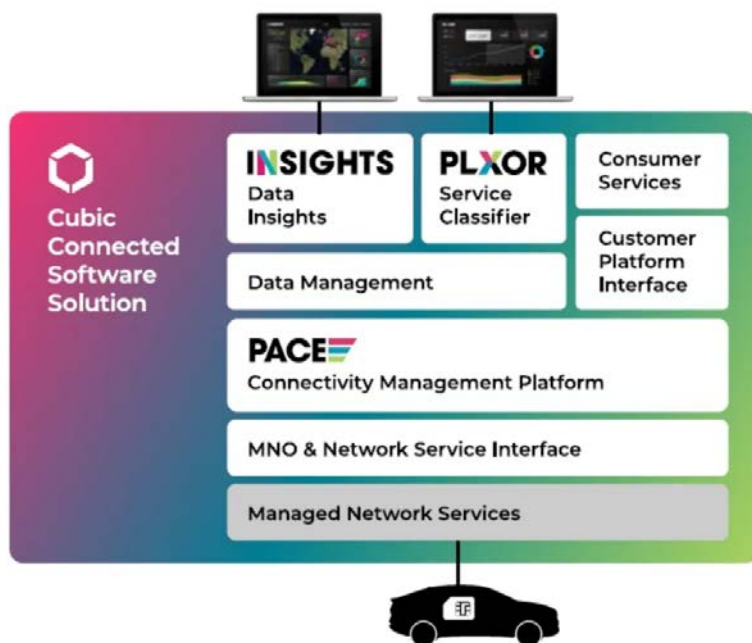
A dedicated vertical expert brings not only understanding of the vertical's application requirements, but also knowledge of and experience with how those variables relate to common issues and hardware failure points. This understanding and knowledge can be used by MVNO customers to more expeditiously and successfully design and architect solutions, select hardware vendors and components, configure hardware and solutions, and adapt and troubleshoot

networks. Importantly, this knowledge compounds within vertical-focused MVNOs over time. That said, it can be a challenge for MVNOs to master specific verticals internally: It can take time for staff to mature, and these professionals are always susceptible to poaching by peers. Further, building an immediately experienced team through hiring alone can be expensive. But once accomplished, the vertical approach can be a sustainable differentiator augmented by advertising and product support efficiency gains and quicker product evolution associated with focusing on a few specific verticals.



Cubic Telecom, headquartered in Dublin, focuses on IoT connectivity in the automotive OEM market. It also supports vehicles in tangential markets like transportation and agriculture. Strengths of the automotive OEM market include its large number of vehicles that can be connected and the trend for OEMs increasingly to embed sophisticated software that requires real-time connectivity for capabilities and services buyers increasingly want (referred to as software-defined connected vehicles, or SDCVs). These capabilities and services include autonomous driving, vehicle-to-vehicle (V2V) communication, infotainment, navigation, and traffic monitoring. In addition, OEMs want to be able to capture and analyze data to monitor vehicles in real time.

To provide connectivity for its offerings, Cubic entered into agreements with over 90 MNOs, giving it coverage in more than 190 countries, and it built its own core network. It also created the PACE platform, which is used to remotely provision SIMs, localize eSIMs, manage devices, networks and data plans, and handle billing. PACE is integrated into OEM systems and can be used to update vehicle software to resolve issues and deliver new features and services. On top of PACE, Cubic created PLXOR, a traffic classification solution that provides visibility into which applications drivers use (such as infotainment, navigation, and telemetry) and how much data ve-



Source: Cubic Telecom.

Vendors that bundle connectivity with other IoT value chain components



Source: First Analysis.

hicles consume by vehicle, fleet or region. It also offers Insights, a vehicle data analytics solution for understanding vehicle and technology service performance. OEMs use the visibility and analytics provided by these solutions to bill for services separately, personalize content, tailor pricing packages, and inform decisions regarding third-party service provider partnerships. Cubic is looking to extend its value proposition by adding support for non-terrestrial networks. Cubic has a strong offering with momentum, evidenced by its over 20 million vehicle connections that send over 1 billion data transmissions per day and its strong pace of adding 450,000 vehicles per month. Cubic's traction underscores the viability of well-executed MVNO vertical market strategies. Cubic's customers include Volkswagen, Porsche, Harley-Davidson, Audi and CNH Industrial.

Bundling. Prospective IoT solution companies (often startups) and OEMs early in their IoT journeys increasingly look for pre-built, end-to-end solutions that can be configured for specific use cases. This demand is being driven by several factors. First, these customers often want to get to market quickly and at lower cost relative to internal development, typically by starting with a proof of concept to gauge market interest. Second, they often want to deal with a single vendor. Third, they may lack IoT expertise and want to avoid common challenges while deploying a more reliable and functional solution than they could initially deliver on their own. Some vendors have responded to this demand with bundled approaches that combine two or more proprietary or third-party components to

form generic offerings constituting material portions of end-to-end IoT solutions out of the box. In some cases, the bundles include connectivity purchased from MNOs for resale, irrespective of whether connectivity is the vendor's primary business. For example, IoT platform providers **Blues Wireless** and **Particle** provide cellular modules and development kits combined with connectivity and management software to expedite their customers' IoT solution development and deployment. We have also come across companies pairing connectivity and enabling hardware with templated end-user application software.

Bundled offerings are relatively uncommon among MVNOs, but given how compelling they can be, we think the strategy is viable and will likely become more common over time. Some bundles will be easier to configure and deploy and feature stronger functionality due to tighter integrations than others, offering a path to sustainable differentiation. But there are risks: As some bundle customers grow and contribute to these bundled MVNOs' success, there will be a tendency for successful customers to churn as their solutions reach scales that warrant switching to proprietary hardware designs and dedicated MVNOs. Also, MVNOs adopting a bundled strategy while still having customers for traditional MVNO services risk having those customers view these MVNOs as competitors and churn as a result.



Boise, Idaho-based **Blues Wireless**, with its suite of solution components, reduces the effort required for customers to wirelessly connect their physical products to the cloud and create digital IoT solutions. Developers incorporate its optimized components into IoT solutions, eliminating many steps involved in building a complete offering while circumventing the technical challenges typically encountered. The foundational component is the Notecard – a



The Notecard



Source: Blues Wireless.

communication module developers embed in their devices. Different Notecards are available depending on use case and application requirements. Blues offers cellular (LTE CAT-1, CAT-M, NB-IoT), Wi-Fi, cellular plus Wi-Fi, and LoRa versions. The cellular Notecards, which feature a pre-provisioned SIM and work with Blues production boards (NoteCarrier), include a 500-mega-byte data plan that a device has 10 years to consume.

To provide connectivity, it negotiated a deal with a major carrier, which gave it access to that carrier's network and roaming partner network and coverage in over 135 countries. While Blues resells connectivity bundled with its hardware to support applications, it does not consider itself an MVNO in the traditional sense. It provides connectivity so its customers do not have to concern themselves with contracts, fees or monthly subscriptions.

The Notecard transmits data captured by a device to Notehub, a Blues cloud-based offering. Notehub is used to securely route data to cloud applications chosen by customers and to organize and manage Notecard fleets and update firmware. Customers compensate Blues for Notehub services like event routing, API retrievals, web requests, and device management

with consumption credits. Each Notecard comes with 5,000 consumption credits, which are replenished to that level every month for free. Customers can purchase additional data and consumption credits as needed.

Besides the enabling hardware, connectivity, and platform, Blues also provides full coding, available in Github, for 50 pre-built applications for tracking, monitoring, and managing items in various verticals. The code is meant to be reference designs for OEMs, product managers, and engineers to accelerate development with Notecard and Notehub. Blues has over 800 customers, ranging from startup to enterprise level, with some doing multi-millions in Notecard volumes.

Other offerings or enhanced functionality MVNOs can add to differentiate include data visualization, data storage and management, network management and control, and private networking.

WHAT TO WATCH AS MVNO MARKET EVOLVES

Increasing M&A

Merger and acquisition activity will likely increase as MVNOs look to consolidate and differentiate. Transaction activity in the MVNO space has been healthy and increasing over the last decade, evidenced by the many connectivity and ancillary capability providers that have been acquired, some by sector leaders (see Table 10). We think activity will remain robust and likely accelerate, given the sheer number of players in the space, which is growing and arguably already above the number needed to support the IoT industry, and given challenges in the form of pricing pressure and other dynamics. Most industry participants are undifferentiated (simply resellers) and have only invested in sales and marketing to drive awareness instead of building material proprietary capabilities.

As pricing compresses and the expense required to acquire and support customers increases, we expect several MVNOs will opt to exit the industry. To manage margin pressure and survive, some remaining

Table 10: Select M&A activity, 2011-present

(\$ in millions)					
Date	Target	Buyer	Enterprise value (EV)	EV/ revenue	EV/ EBITDA
Jun 2011	GlobalConnect	Telit	\$2.4	-	-
Jan 2013	Crossbridge Solutions	Telit	\$9.0	-	-
Mar 2014	Jazz Wireless Data	KORE Wireless	-	-	-
Nov 2014	RacoWireless	KORE Wireless	-	-	-
Dec 2014	Wireless Maingate	Sierra Wireless	\$90.0	4.7x	11.7x
Jun 2015	MobiquiThings	Sierra Wireless	\$15.7	4.7x	-
Mar 2016	Wyless	KORE Wireless	-	-	-
Aug 2017	Numerex	Sierra Wireless	\$107.0	1.4x	12.3x
Aug 2017	Wireless Innovation	Lyceum Capital	-	-	-
Mar 2018	Ibasis	Tofane (KPN)	-	-	-
Jun 2018	Stream Technologies	ARM	-	-	-
Dec 2018	Transatel	NTT Communications	-	-	-
Dec 2018	LJC Telecom SAS	Globalgig	-	-	-
Dec 2018	Aspider NGI	KORE Wireless	-	-	-
Feb 2019	M2MBlue	Wireless Logic	-	-	-
Jul 2019	Matooma	Wireless Logic	-	-	-
Jul 2019	SIMPoint	Wireless Logic	-	-	-
Nov 2019	M2M Group (M2M One)	Sierra Wireless	\$19.8	1.1x	7.4x
Apr 2020	Thingstream AG	U-blox	\$10.0	-	-
Dec 2020	Arkessa	Wireless Logic	-	-	-
Dec 2020	New Line Mobile	Wireless Logic	-	-	-
Dec 2020	Datamobile AG	Wireless Logic	-	-	-
Jan 2021	Com4	Wireless Logic	-	-	-
Jul 2021	Podsystem Limited	Giesecke+Devrient	-	-	-
Jul 2021	Things Mobile Srl	Wireless Logic	-	-	-
Sep 2021	Orbcomm	GI Partners	\$1,148.7	4.7x	23.2x
Feb 2022	Simon IoT	KORE Wireless	-	-	-
Mar 2022	Evacomm (VIAA)	Globalgig	-	-	-
Apr 2022	NextM2M	JT IoT	-	-	-
Jul 2022	Jola	Wireless Logic	\$84.4	-	-
Jul 2022	Mobius Networks	Wireless Logic	-	-	-
Jul 2022	Top Connect	JT IoT	-	-	-
Aug 2022	Sierra Wireless	Semtech	\$1,230.2	2.1x	67.6x
Dec 2022	Ericsson IoT assets	Aeris Communications	-	-	-
Dec 2022	Digital Republic AG	Mobilezone	-	-	-
Jan 2023	Truphone assets	1Global	-	-	-
Mar 2023	Blue Wireless	Wireless Logic	-	-	-
Mar 2023	Twilio's IoT Business Unit	KORE Wireless	\$12.4	-	-
Aug 2023	Webbing	Wireless Logic	\$200.0	-	-
Aug 2023	Cinco Telecom	Emnify	-	-	-
Dec 2023	Cubic Telecom	Softbank	\$1,001.0	-	-
Feb 2024	M2M DataGlobal	OPTConnect	-	-	-
Jul 2024	M2M France	M2M Data Connect	-	-	-
Maximum			\$1,230.2	4.7x	67.6x
Minimum			\$2.4	1.1x	7.4x
Average			\$302.4	3.1x	24.4x
Median			\$84.4	3.4x	12.3x

Source: Company and industry reports, Capital IQ, First Analysis.

MVNOs will likely take advantage of this and pursue a consolidation strategy, purchasing other MVNOs for their customer and subscriber bases to increase overall scale and improve negotiating leverage with MNOs. These transactions' valuation multiples will likely be low, reflecting the target MVNOs' commodity-like nature or lack of proprietary capabilities in the case of those that have built their business on third-party offerings such as MVNEs. Other MVNOs will likely seek to acquire features and functionality to differentiate their offerings and create stickiness, most likely acquiring point solutions but also other MVNOs with proprietary capabilities. These transactions' valuations will likely be higher given they offer better growth and margin expansion potential.

Limited access to capital

The typical MVNO looking for capital in the near term is likely to struggle garnering interest from investors, let alone realizing targeted valuations. Investors today are spoiled with numerous opportunities across sectors and technologies. Many of these opportunities feature proprietary technology, stronger margin profiles, and valuations that are down from peak levels. Against this backdrop, we believe only tightly run MVNOs with above-industry-average margins and readily apparent proprietary technology or capabilities will realistically be considered for funding. Those that pass muster on these criteria will likely face more intense scrutiny to validate claims relative to previous years, when several providers purporting to have proprietary

technology received significant funding at lofty valuations despite being little more than branded resellers.

Impact of eSIMs

Embedded SIMs could shift power away from MVNOs. Today, connectivity providers, including MVNOs, have a significant amount of power due to their control over physical SIMs, which unlike eSIMs can be removed from their devices. Most MVNOs have their own branded physical SIMs. These SIMs contain profiles and authentication keys devices need to access the mobile networks of carriers that MVNOs have established relationships with. MVNOs contract third parties to make and configure these SIMs with the appropriate profiles and keys. By contrast, eSIM manufacturers, which include some of the largest semiconductor and chipset companies, control the profiles and other information loaded onto eSIMs. While many profiles can be stored on an eSIM and eSIMs can be updated remotely, some MVNOs have suggested eSIM manufacturers will leverage their greater control over eSIMs to only support their preferred data providers and limit MVNO access unless they pay a per-unit fee.

As eSIMs become more widespread, it's worth monitoring this risk given the outsized negative impact it could have on branded reseller MVNOs by limiting customer access or increasing MVNOs' costs.

OEMs as MVNOs

More OEMs are offering connectivity and are arguably MVNOs themselves. We have noticed an increase in the number of OEMs offering connectivity alongside their products, whether they are finished goods or components for other products. Many OEMs have entered relationships with MNOs, leveraging their scale to procure connectivity at competitive rates. They typically either bundle this connectivity with their physical products under a one-time charge, sell it as part of a monthly recurring service with an end-user application, or sell it as a standalone option. Since these

SIM card types



Source: CSL Group.

OEMs purchase connectivity from multiple MNOs and resell it, they are functionally de facto MVNOs.

Adding connectivity makes sense for OEMs, as it enables them to deliver more value to customers more quickly by reducing the number of vendors customers need to deal with to assemble an end-to-end solution. Further, we believe large OEMs will have a measure of control over eSIMs (alongside semiconductor and chipset companies), which should enable them to provide their customers increasingly demanded network switching flexibility. We believe the number of OEMs offering connectivity will continue to rise for a couple reasons. First, offering connectivity is a way for OEMs to differentiate, create stickiness, and remain competitive. Second, improvements in technology and the advent of MVNEs have made it easier for virtually

any company to launch and support connectivity services. While we think OEMs with connectivity will take some market share from pure IoT connectivity providers, we don't expect the impact to be dire, as OEMs are generally not well equipped to sell services and support given most lack relevant systems and expertise.

A COMPLEX AND DYNAMIC SECTOR

Creativity and competition have conspired to create a complex, dynamic and rapidly evolving market in the MVNO sector. Careful study aimed at understanding which models create the most value for IoT solution providers will be key to sorting out winners and losers. We hope readers find this analysis a useful framework for making this assessment.

USE OF THIS DOCUMENT:

This communication is provided by First Analysis for informational purposes only. This communication is not intended to provide investment recommendations or investment analysis on any specific industry or company. Neither the information nor any opinion expressed herein constitutes a solicitation by us of the purchase or sale of any securities. This is not a complete analysis of every material fact regarding any company or industry. The content of this communication is solely our judgment as of this date and is subject to change. The information has been obtained from sources we consider to be reliable, but we cannot guarantee its accuracy. Past performance and any projections herein should not be taken as indications or guarantees of future events or performance. All investing involves risks, including loss of principal. Transaction advisory services and securities offered through First Analysis Securities Corp. (FASC), a registered broker dealer with FINRA and member SIPC. FASC may act as financial advisor and/or underwriter for companies mentioned in this communication. Venture capital investment advisory services offered through First Analysis Capital Management LLC, a registered investment adviser with the SEC. FASC and First Analysis Capital Management LLC, are subsidiaries of First Analysis Corp. Venture capital funds associated with First Analysis Corp., other First Analysis affiliates, and their employees may have interests in companies mentioned in this communication. More information is available on request by calling (312) 258-1400 or by writing to: First Analysis, One South Wacker Drive, Suite 3900, Chicago, IL 60606. Copyright 2024 First Analysis Securities Corp.



First Analysis has a four-decade record of serving emerging growth companies, established industry leaders, and institutional investors in emerging high-growth tech-driven sectors, both through its venture capital investments and through First Analysis Securities Corp. (FASC), which provides investment banking and related services. FASC is a FINRA-registered broker-dealer and member SIPC. First Analysis's integrative research process underpins all its efforts, combining 1) dynamic investment research on thousands of companies with 2) thousands of relationships among executives, investors, and other key participants in our focus areas, yielding a deep, comprehensive understanding of each sector's near-term and long-term potential.

One South Wacker Drive, Suite 3900 • Chicago, IL 60606 • 312-258-1400 • www.firstanalysis.com