451 Research
Now a Part of
S&P Global Market Intelligence

PATHFINDER REPORT

Security Benefits of Open Virtualized RAN

COMMISSIONED BY

ALTIOSTAR
Leading Network Transformation

intel

CISCO

Red Hat

MAY 2020

About this paper

A Pathfinder paper navigates decision-makers through the issues surrounding a specific technology or business case, explores the business value of adoption, and recommends the range of considerations and concrete next steps in the decision-making process.

ABOUT THE AUTHOR

ERIC HANSELMAN

CHIEF ANALYST

Eric Hanselman is the Chief Analyst at 451 Research. He has an extensive, hands-on understanding of a broad range of IT subject areas, having direct experience in the areas of networks, virtualization, security and semiconductors. He coordinates industry analysis across the broad portfolio of 451 Research disciplines. The convergence of forces across the technology landscape is creating tectonic shifts in the industry, including SDN/NFV, hyperconvergence and the Internet of Things (IoT). Eric helps 451 Research's clients navigate these turbulent waters and determine their impacts and how they can best capitalize on them. Eric is also a member of 451 Research's Center of Excellence for Quantum Technologies.

Executive Summary

As operators expand radio networks with upgrades and new buildouts, open architectures offer clear benefits regarding flexibility and agility. Avoiding vendor lock-in and the ability to build best-of-breed capabilities are very valuable, but many overlook a key benefit that comes along with standardized interfaces and greater visibility – improved security. Two important factors can drive improved security: improved modularity and reduced interdependencies. With open interfaces available deeper within radio access network (RAN) infrastructure, there are options for isolating controls, greater observability and independently generated operational telemetry. Those interfaces provide modularity, which can allow more granular security attestation. It can reduce dependencies on unique software capabilities, making it less risky to update software to apply fixes. Avoiding single vendor lock-in allows operators to put best-of-breed security capabilities to work more easily. These can strengthen operators' control over their security posture at a time when threats on the network are expanding rapidly. Open architectures offer manifold benefits that are just starting to be realized.

Key Findings

- Open approaches to building RAN infrastructure can increase security and lower risk.
- The threat landscape for operators is expanding dramatically, and stronger mitigations and controls need to be in place to address these risks.
- Supply chain flexibility can increase reliability by expanding options.
- Operators can better control their own security posture through direct ownership of security processes.
- Creating modularity within the RAN enables CI/CD processes, speeding software updates.
- 5G offers some security enhancements, but 4G security improvements are needed today, and open deployments can speed their introduction.
- Virtualization offers additional security telemetry and control for RAN functions.

Introduction

The mobile network is one of the most challenging operational environments for technology. The blend of technical capabilities, regulatory constraints, logistical difficulty, ecosystem complexity and cost concerns create a stew that network operators are constantly working to perfect. At the same time, consolidation across the telecom industry and regulatory and political pressures have narrowed the choices in traditional equipment vendors.

MOBILE NETWORK CHALLENGES	
CONSTRAINED VENDOR ECOSYSTEMS	Traditional procurement relationships have limited many operator choices and hindered innovation.
INCREASING DEMANDS	IoT device volumes, 4G densification, increasing data volumes.
LIMITED FUNCTIONAL CONTROL	Operators rely on vendors for trust, update schedules and security controls.
LIMITED EQUIPMENT INTEROPERABILITY	Mixing vendor systems is limited to higher-level interconnection, requiring single-vendor islands of deployment.

Traditional operational models for network operators place a strong dependence on a small number of vendors. This constrains the options that are available for operators to address the many demands on their networks. The problem can be particularly acute in the radio access network because there is limited interoperability between the components that traditional, proprietary vendors offer. Interconnection between vendors can only happen at higher levels, closer to the network core, requiring single-vendor islands of RAN functionality, if operators want the flexibility of multivendor ecosystems.

Taking an open approach to network infrastructure can allow operators to more easily expand their supplier ecosystem and match the capabilities they deploy to the operational and security models that best suit their goals. Open approaches can allow RAN environments to leverage the right capabilities for the right situation.

Opportunities in New RAN

One of the most important aspects of RAN technology today is that the vendor landscape outside of the traditional vendors is rapidly expanding. New entrants with approaches that step beyond the traditional limitations offer new operational models. This is a trend that operators have been pushing to enable and from which they expect to benefit. While the telecom industry has faced consolidation over the previous decade, within the last few years, this new class of vendor has arrived, offering open and virtualized capabilities. Driven by new models and expectations of operational agility, these newer vendors have grown to provide mature, robust offerings that have been proved in real-world deployments.

One of the primary goals of operator efforts to encourage innovation in vendors is to increase openness. Historically, RAN implementation required the use of single-vendor equipment deployments for most of the functionality from the network core out to the antenna. Performance trumped interoperability in a world where cost was the primary driver. With the inevitable decrease in cost for higher-performance components, performance margins have increased to a point where they can more easily support open interfaces, and vendors have responded with a raft of products that feature open interfaces and greater deployment flexibility.

OPPORTUNITIES IN NEW RAN	
EXPANDED VENDOR ECOSYSTEM	Open approaches increase options for operators to tailor capabilities more closely with their requirements.
PLATFORM FLEXIBILITY	Virtualization and commercial-off-the-shelf hardware expand supply chain and deployment choices.
GREATER OPERATOR CONTROL	Expanded vendor choice and greater control over security operations and posture.
IMPROVED OPERATIONAL EFFICIENCY	Leveraging the benefits of virtualization and cloud-native design principles can increase agility.

The expectation is that these new offerings will deliver benefits through greater operational efficiency in much the same way that virtualization achieved efficiency in mainstream technology applications. It has taken time to adapt these techniques to telecom requirements, but they are now ready to be deployed alongside legacy systems. The benefits of open interfaces are being proved out in the network core, where software-defined networking and network function virtualization have delivered impressive gains in agility and cost management. They are now bringing those same gains to the RAN. They also bring with them improvements in security that are urgently needed as the threat model for mobile networks undergoes major changes.

Challenges of Traditional Architectures

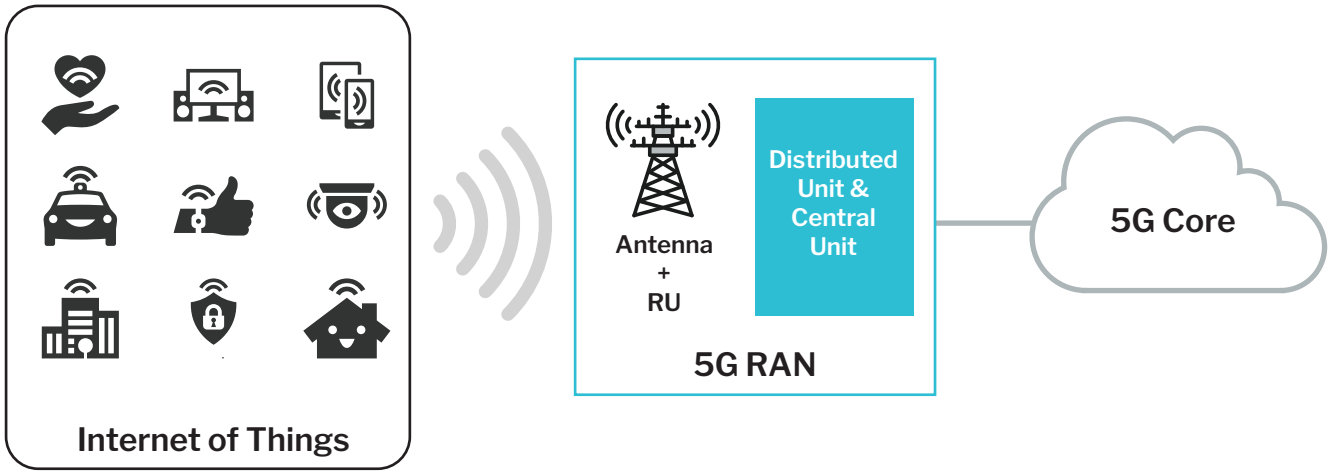
As operators begin deploying new network services and architectures, they face an expanding set of threats.

RAN CHALLENGES	
INCREASING DENSITY AND SCALE	Scaling is complex, and greater network access is increasing the attack surface.
NEW CLASSES OF DEVICES	IoT, vehicle communications and smart cities applications are bringing devices that are more complex to secure.
INCREASING ATTACK SOPHISTICATION	Attackers have better tools and more targets.

The sophistication of attacks and attackers continues to advance while the difficulty of securing network infrastructure increases. Where equipment vendors have played a strong role in providing protection capabilities, the opening of services located deeper within provider networks and more rapid exploitation of devices connecting to them are putting additional pressure on operators to shoulder more of the protection burden.

Figure 1: The integrity of network elements that support 5G's security enhancements is critical

Source: Cisco



With fewer equipment providers in a typical network, any weakness in their equipment poses a greater risk. There are simply more places where any vulnerability would appear in a network when networks approach a monoculture with a single vendor. Added to this is the lack of transparency that operators have into proprietary interfaces. They're forced to rely on the telemetry provided by the vendor at a high level, and they have to trust that it will be sufficient to detect and defend against attacks.

The challenges that vendor monocultures create are amplified in next-generation 5G networks where the dangers present in 5G systems are different from those present in 4G. In 5G, the 'edge' will be a mix of core and radio functions with no clear demarcation between the two domains. All parts of the 5G network will handle sensitive data, so closed proprietary systems and a lack of transparency become a problem that operators could find very expensive to fix retroactively.

Networks built with traditional hardware-based systems are also missing out on the additional protection that virtualization can provide. The isolation and introspection capabilities of virtualization can add greater operational awareness to any environment. Virtualization also has the potential to speed remediation efforts and reduce risk in patching and updating.

Significant security enhancements will arrive with 5G technologies, but the integrity of the network elements that support them are still critical. Operators still need to protect existing infrastructure elements in their current networks to reduce the risks of compromise. That means that better security needs to be a priority in all networks, independent of where operators are in their journey to 5G.

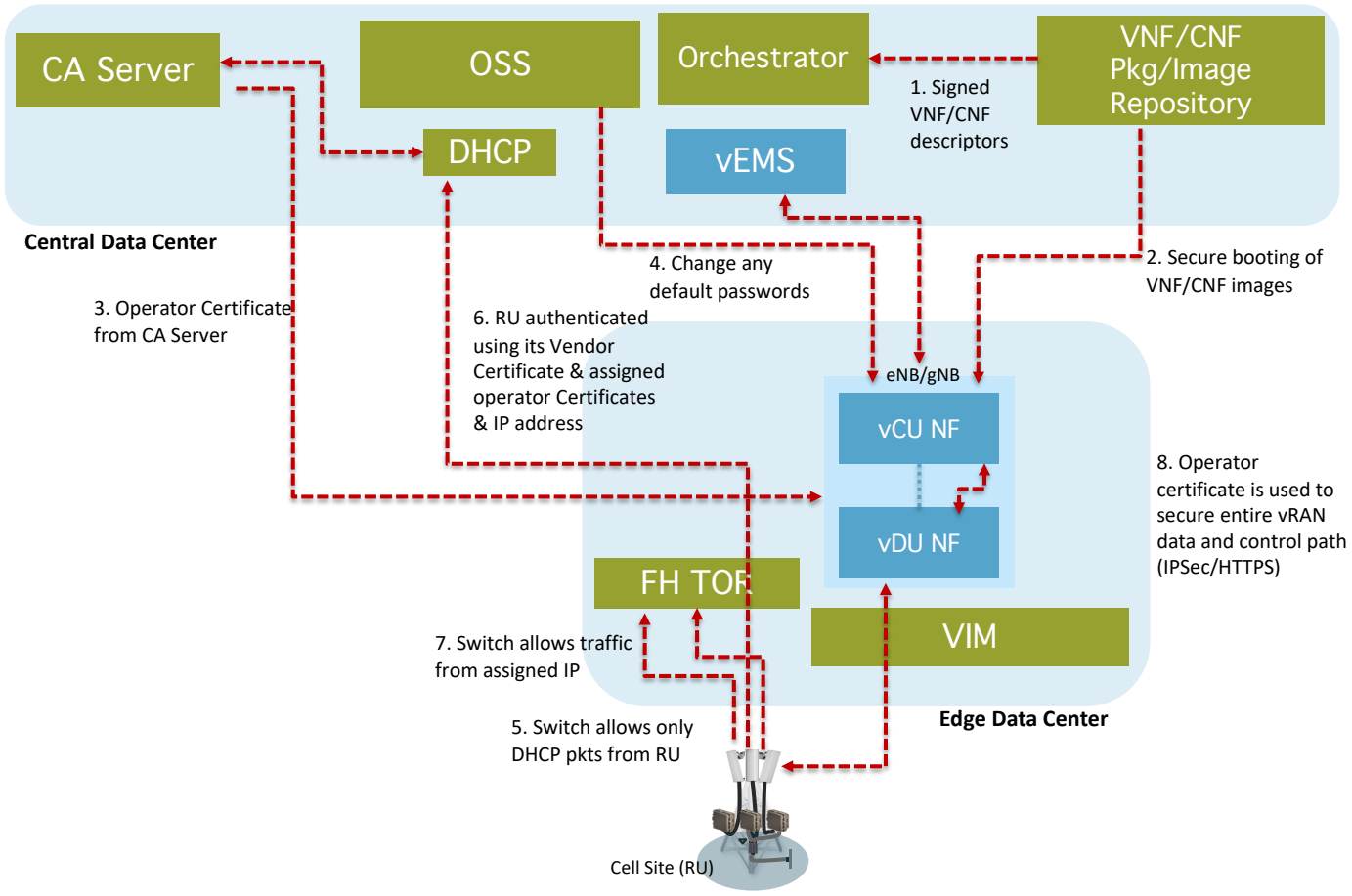
Security Advantages of Open Environments

Networks that are designed and built with open concepts can benefit from significant security advantages. Using open interfaces creates a level of modularity that allows operators to mix and match the elements they use to build networks. That flexibility lets operators target the right elements to build out capabilities, and it lets them interchange those elements to address security concerns. Operators can directly manage their security posture with open networks in ways that were more difficult with proprietary approaches. Historically, vendors have shouldered the task of building trust in infrastructure components, but as a 2018 outage demonstrated, that's not always without risk. The networks of O2 in the UK and SoftBank in Japan were apparently taken down when they deployed software from a single vendor that had been built with an expired certificate, preventing it from running. If the operators had owned the trust environment for their software, they could have identified the problem before it was put into production.

Vendor diversity is one of several security benefits that open environments offer. Modularity is the means through which operators can expand their vendor ecosystems and achieve vendor diversity. Having access to a greater variety of vendors gives operators new options for existing capabilities and provides alternatives for service implementations. Diversity helps operators mitigate security vulnerabilities by allowing them to replace individual elements of their RAN rather than complete sections. It also increases the likelihood that even if an attack affects one part of the network, other parts will be resistant and not be affected. Bringing independent software development domains into deployed systems reduces the risk that common coding errors or build practices could affect the entire network.

Figure 2: Open vRANs offer increased transparency

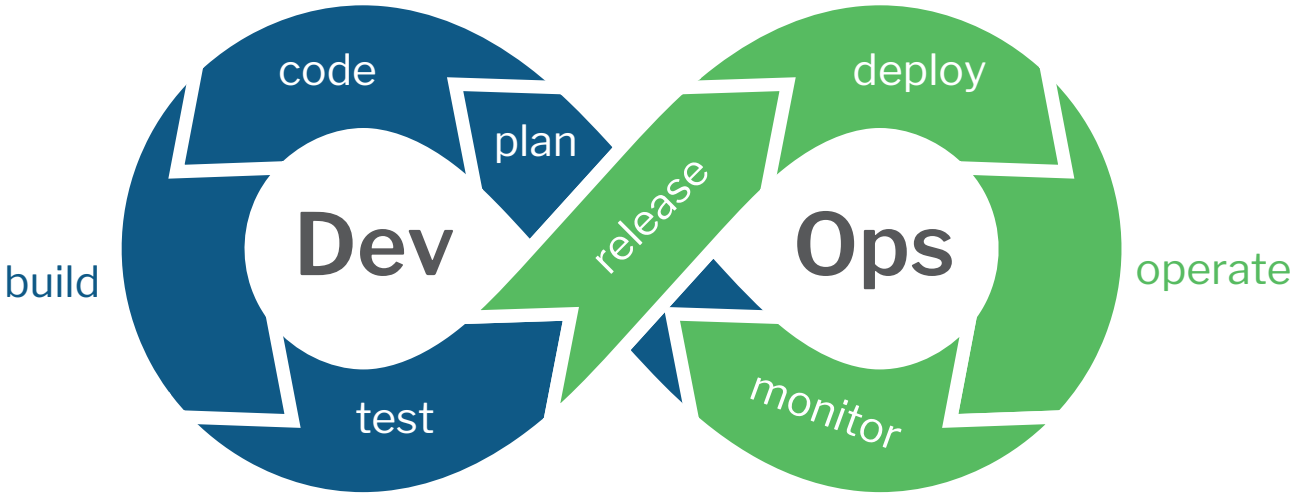
Source: Altiostar



An increase in visibility is another benefit that open virtualized radio access networks (vRANs) can provide. The improvement comes through two aspects of this approach. The first is the additional telemetry that the virtualization platform provides. The virtual hosts provide significant additional data about the operation of the virtualized functions running on them. This data can offer greater fidelity because its creation is isolated from the function's execution environment, decreasing the risk that it could be tampered with by an attacker. The second improvement comes from the ability to track activity at open interfaces. This is an additional monitoring capability that's difficult to derive in proprietary systems. As the diagram above shows, having access to low-level interfaces in a software system improves security inspection and control possibilities. It illustrates the rich set of exchanges that can be monitored to track the behavior of granular functional elements.

Virtualization platforms and open interfaces both provide telemetry for security monitoring and open the door to the use of more effective analytics as a security and operations tool. Behavioral analytics can augment security capabilities and allow operators to identify attack behaviors and compromised elements in their networks faster.

Figure 3: CI/CD increases security by speeding the time to resolve software defects
Source: 451 Research



Isolation can receive a boost with modularity as well. The defined interfaces that exist between functional elements in an open vRAN provide isolation and the opportunity to insert controls, as well as monitoring. That isolation allows software updates and patches to be installed with less risk that version dependencies will create issues. That modularity can create operational agility with the ability to swap functional elements with new versions or capabilities. This makes it possible to move toward a continuous integration/continuous delivery (CI/CD) operating model, where more frequent – but smaller – changes are rolled out to the network. By reducing the scope of required testing, updates to fix software defects that create vulnerabilities can be put into production faster, reducing the window of vulnerability. An implicit benefit of a CI/CD operating model is that any change that is pushed out can just as easily be pulled back. This rollback capability offers a level of resilience to operators that can result in improved uptime. A CI/CD footing not only helps security by reducing the time needed to resolve software defects but also speeds new service deployment.

Integrating CI/CD or DevOps methodologies can bring the benefits that hyperscale cloud providers have been enjoying to RAN infrastructure. Operators can regain control of the infrastructure deployment process and leverage the robust security capabilities that are available in cloud-native designs.

Open RAN Architectures

The architectures of open vRAN environments aren't radically different than those of proprietary offerings, but they do offer the ability to have far more granular disaggregation of the component parts. An open virtualized RAN decomposes hardware and software so that each is separately assessable and uses fungible modular elements interconnected via open interfaces. That creates flexibility, and it also can increase availability. Virtualized implementations can more easily add redundant instances on their supporting platforms. This increases availability by reducing downtime required for upgrades and equipment restarts. Redundant instances can be swapped in more rapidly than a physical system can restart. This is an area where operators can adopt the operational models that hyperscalers have leveraged with rolling upgrades to reduce risk in the upgrade process. Reducing the downtime for upgrades allows them to be performed more rapidly, ensuring that better code is deployed faster.

The more granular instances also allow for more efficient scaling, letting operators tailor their deployments to meet performance, application and security requirements. In the same way that functional splits between real-time and non-real-time can be shifted in a vRAN, security functions for monitoring and control can be more easily placed where they're needed, and vRAN functional elements can also be shifted to provide better isolation. This is particularly important as operators look to provide improved isolation for applications like network slicing. Replicated radio and signaling functions can be created for each zone of isolation. Virtualization makes this shift possible, and openness makes it accessible to the operator.

One of the more impactful aspects of open vRAN on security is the ability for operators to manage trust in their networks. When operators control the platforms on which virtualized functions run, they also control the trust infrastructure. Through the cryptographic signing of functional elements, the identity and provenance of each is known and managed. Operators validate each new version and can have confidence that they know what's running in which locations on their networks.

Transitions to Open

The reality for most operators is that the adoption of open vRAN practices and capabilities will happen as a transition from their existing, proprietary deployments. While greenfield deployments have received recent publicity, it's important to understand the situation in which most open networks will operate. Many operators already have experience with the first steps in disaggregating their RANs. Increasing density requirements have led to remote radio units being physically separated from baseband units, linked via common public radio interface (CPRI) connections. Decomposing RANs with open interfaces is the next logical step in this process. Efforts around open interfaces leveraging enhanced CPRI (eCPRI), such as those in the O-RAN Alliance, are addressing this transition, but there are more significant things that must be done. Next steps for operators involve the expansion of their vendor ecosystems to extend their options.

A key part of this transitional process is changing expectations in equipment procurement and vendor relationships. Operators must place expectations on vendors to provide systems that offer open and interoperable products. That starts with the RFP/RFQ and tender processes. Open attributes must be included as requirements for RAN procurement. The depth and capabilities will vary by operator, but this is the first step in bringing open options into discussions with vendors.

Historically, operators have often deployed RAN infrastructure by allocating different geographic regions to different equipment vendors. In a world where interoperability was challenging, this made sense. In an open approach, that's no longer required. Operators can start by deploying a new frequency band or region using open systems and transition open equipment as capacity or service needs demand. It's a change in mindset that can increase the flexibility with which operators respond to changing market requirements.

Operators need to take a more active role in expanding their ecosystems. Open approaches offer more control for operators, and that comes with more ownership of operational processes. They'll need to take more of the vendor coordination and qualification tasks.

Operational Benefits

Open vRAN benefits deliver a set of operational advantages for operator security teams. The increased visibility can enhance their situational awareness and strengthen their security posture. The ability for operators to see deeper into their RAN interfaces lets them directly audit messaging at low levels and use analytics to detect anomalous behavior caused by attackers.

Security teams have more leverage with vendors in an open environment. Because it's easier to switch providers of functional components, vendors have a greater incentive to be responsive to operator concerns. Open vRANs can also enhance supply chain security. Recent regulatory intervention in mobile network supply chains has required operators to reassess their vendor partnerships and consider alternatives. Operator responses to regulatory inquiries about the security of mobile networks have often cited concerns about costs and lack of availability of a diverse RAN ecosystem.

Openness increases security innovation for operators as well. New approaches to security management have access to a richer set of information and more control points to operate through. The ability to experiment with new functions and new vendors is enhanced, creating the possibility to explore new ways to secure the network and its operation.

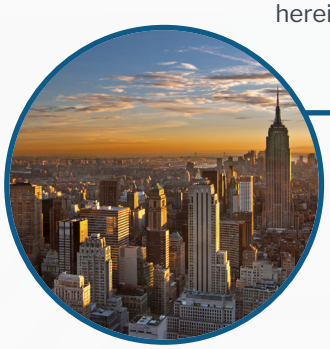
Conclusions

With all the complexities facing operators in working to build more secure networks, it can be a great benefit to understand the ways in which open approaches simplify operations. Open vRAN can give operators the granular isolation to flexibly build the networks that they need, where they need them, with the security protections that meet their requirements. Open architectures bring interoperable components from a much wider variety of suppliers, enabling greater functionality and enhanced security. They give operators more granular control over security decisions and their operations. Open environments give operators more direct control of their ecosystem and the ability to build vendor diversity. Together, these benefits are a strong incentive for operators to embrace open virtualized RAN approaches.

451 Research®
Now a Part of
S&P Global Market Intelligence

About 451 Research

451 Research is a leading information technology research and advisory company focusing on technology innovation and market disruption. More than 100 analysts and consultants provide essential insight to more than 1,000 client organizations globally through a combination of syndicated research and data, advisory and go-to-market services, and live events. Founded in 2000, 451 Research is a part of S&P Global Market Intelligence.



NEW YORK
55 Water Street
New York, NY 10041
+1 212 505 3030

SAN FRANCISCO
One California Street,
31st Floor
San Francisco, CA 94111
+1 212 505 3030

LONDON
20 Canada Square
Canary Wharf
London E14 5LH, UK
+44 (0) 203 929 5700

BOSTON
75-101 Federal Street
Boston, MA 02110
+1 617 598 7200

451 Research®
Now a Part of
S&P Global Market Intelligence