Cloud and Tech Trends to Follow in 2017

European Cloud Alliance

@CloudAllianceEu

Content

Context

The European Cloud is Rising

What's happening in 2017

This year will see European organizations – large and small, public and private – shift a larger share than ever of their IT applications to the cloud. The exact size of the cloud computing market in Europe is difficult to measure, because ideas about what should be included in this term vary. The most basic definition includes two broad families of cloud services:

- IT infrastructure offered as a service: here the cloud provider stocks a data center with servers and basic software such as operating systems and databases, adds a layer of virtualization and management automation, and then rents out customizable slices of this infrastructure by the hour or even minute so that customers can deploy and manage their own IT applications;
- Full scale IT applications offered as a service: here the cloud provider builds a complete application such as CRM (Customer Relationship Management) or Messaging and Communication, then makes it available to customers over the Internet for a monthly or annual fee per user.

There are countless variations on these two themes that we need not summarize here. Suffice it to say that the market for cloud services is big and its impact on European economic growth is even bigger. According the European Commission, the cloud is expected to add €103 billion of net new GDP to the European economy in the year 2020.

The common belief that cloud computing in Europe is dominated exclusively by American providers is not supported by the facts. According to IDC, the top four big name American cloud firms – Amazon, Microsoft, Google and IBM – account for considerably less than half of total cloud revenue in Europe. The reality is that the European cloud market is extremely diverse, because European customers are themselves diverse. To meet this burgeoning demand, a whole host of specialized native European cloud providers have grown up alongside the U.S. firms. The European contenders include the French Cloudwatt, the Italo-Czech Aruba Cloud, the German ProfitBricks, the Swiss CloudSigma, the Swedish CityCloud, the Finnish UpCloud, and the British DataCentred, among many others.

The dynamic and competitive European market for cloud services will be a key driver of the continent's economic growth in the years ahead.

Privacy

1. Your Data Protection Commissioner is calling – do you have a plan to comply with GDPR?

What's happening in 2017?

The European Union's General Data Protection Regulation was passed in April 2016. It won't take full effect until May 2018, but its complex array of legal mandates will impact nearly every business and government organization in Europe. Accordingly, the time to begin preparing for GDPR is now.

The most important consequence of the new regulation will be to raise the stakes for all organizations, large or small, that process personally identifiable information (PII). The cost of mistakes or gaps in the way organizations handle such information will become higher. The amount of specialist knowledge and technical skill required to manage PII correctly will increase. Many organizations, especially smaller ones, will find it difficult and expensive to build this expertise internally. As a result, they may find it easier and less expensive to entrust applications that handle PII to cloud providers who have the necessary scale and technical resources to cope with the GDPR's challenges.

The GDPR's main requirements include stronger consent for the processing of personal information, 72 hour notification of breaches, careful assessment of the privacy impact of new technologies, appointment of Data Protection Officers in organizations engaged in the large-scale monitoring of individuals or processing of sensitive information, enhanced rights of individuals to access and control the information that is gathered about them, and – last but not least – a new and rigorous accountability which will oblige organizations to demonstrate that the processing they perform is done in accordance with the Regulation.

To comply with the GDPR you will need to make a careful inventory of any and all personally identifiable information that you collect and assess whether the uses you make of it are allowable. For every type of PII an organization handles, it will be essential to ask "do we really need this information?" The easiest way to make PII compliant with the GDPR is not to collect it in the first place. Organizations may also find that sophisticated new techniques such as machine learning enable them to glean insights about customer behavior that do not require detailed PII, but rely instead on anonymized aggregates.

For PII that cannot be dispensed with, detailed assessment will be necessary. Since the information may reside in many different IT applications, databases and files containing information about individuals – be they customers, employees, citizens, patients, students, etc. – this data inventory task will be demanding and error-prone. Fortunately, some specialized software tools to help with this task are becoming available. Firms such as AvePoint and OneTrust offer cloud-based privacy management solutions that can at least partially automate the process of examining your data and identifying GDPR and related compliance issues.

Action Items for Business

Don't wait until 2018 to start planning for GDPR compliance. Plan now for a thorough audit of your business processes and inventory of personally identifiable data. In particular, consider for each type of PII whether you really need it, and – if you do need it – whether you can delegate some of the burden of GDPR compliance to cloud providers by entrusting the data to them.

Action Items for Government

Years of negotiations among the European Commission, the European Parliament and the European Council have resulted in a massive and complex piece of legislation. Many organizations subject to the GDPR – both private enterprises and government agencies, and especially the smaller ones – may not fully understand the steps they must take to achieve compliance. Some national Data Protection Authorities have issued helpful guidance materials, but this is not enough. A more concerted effort to help organizations along the path to compliance is needed, including special measures to educate the thousands of non-EU firms that will be subject to the GDPR.

But perhaps the most important role of public authorities – both the EC itself and the national Data Protection Authorities – is to ensure that the GDPR serves its stated purpose of promoting the free exchange of data within Europe and with the rest of the world. The GDPR must not be allowed to become a barrier to innovation and new business models such as those based on machine learning.

a. You may need to hire your own Data Protection Officer

What's happening in 2017?

A key requirement of the GDPR is that every company processing personal information on a large scale – which includes information regarding employees as well as customers – must hire a qualified Data Protection Officer (DPO). While earlier drafts of the GDPR required all firms with 250 or more employees to have a DPO, in the final version the mandate no longer depends on the size of the firm, but on the amount and intensity of PII processing. A DPO is required if an organization acting as a data controller or data processor has "core activities" that require "regular and systematic monitoring of data subjects on a large scale" or consist of "processing on a large scale of special categories of data." In the absence of any explicit quantitative threshold, these rather vague legal terms will require careful study by your legal staff and your board to determine whether the mandate applies to your organization. And don't forget, we're not just talking about companies: the GDPR requires all "public authorities or bodies" except courts to have DPOs. Most important of all, don't conclude that simply because your organization is not required to have a DPO it is therefore exempt from the GDPR. This is not so – the GDPR applies to every organization handling PII.

But what exactly is a Data Protection Officer? What are the qualifications? The regulation does not define specific credentials that DPO's must possess, but states that they must have "expert knowledge of data protection law and practices". DPOs are further granted a significant degree of independence from their employer and are protected from arbitrary dismissal. The International Association of Privacy Professionals (IAPP) has a good overview of DPO requirements here.

A large number of organizations will be affected by the DPO requirement. The IAPP has conservatively estimated that 28,000 DPOs will be needed in the EU alone. Many non-EU firms that provide online services to EU citizens may not realize that they too are subject to the GDPR and may have to hire their own DPOs. In fact, IAPP estimates that some 47,000 DPOs will be needed outside the EU.

It is important to understand that you cannot hire just anyone to be your DPO – the person must be qualified, and must be authorized to act in an independent manner to instruct your employees of their rights and obligations under the GDPR.

Not all firms that need a DPO will need one full-time. You may choose to make the DPO position an internal staff position, or hire an outsider. A number of specialist firms and consultancies are already offering rent-a-DPO services.

Action items for business

As part of your broader GDPR audit you'll need to decide whether you need to hire a DPO. Don't put this decision off for 2018.

Action items for government

Government agencies need to plan and budget for the DPO function now. Many smaller agencies will find it convenient to hire outside firms to provide the DPO service.

2. You will soon be able to use a single electronic ID anywhere in the EU

What's happening in 2017?

As an ever greater share of economic activity shifts to the cloud, the need for secure and easy-to-use electronic identities increases. Until now Europe has suffered from a patchwork of national regulations governing such identities. Fortunately, a new EU standard for cross-border electronic IDs and signatures that can serve in business and consumer transactions as well as in interactions with government administrations is coming. The eIDAS regulation for electronic identification and trust services was passed in July 2016 and will become mandatory in 2018. The Commission's purpose in drafting eIDAS was to make it easy to conduct cross-border electronic transactions using standard credentials issued by any EU member state. Electronic identity services as envisaged by eIDAS will by definition reside in the cloud and will ease the flow of electronic transactions of all kinds.

Since it is a regulation rather than a mere directive, eIDAS will automatically have the force of law in all member states and will thus create uniform rules for electronic signatures. eIDAS replaces the 1999 Electronic Signatures Directive, which largely failed to achieve its goal of making electronic signatures widely used throughout the EU. In the words of the European Commission:

- *"With eIDAS, the EU has managed to lay down the right foundations and a predictable legal framework for people, companies (in particular SMEs) and public administrations to safely access to services and do transactions online and across border in just 'one click'. Indeed, rolling out eIDAS means higher security and more convenience for any online activity such submitting tax declarations, enrolling in a foreign university, remotely opening a bank account, setting up a business in another Member State, authenticating for internet payments, bidding to on line call for tender, etc."*

Action items for business

eIDAS offers immediate and clear benefits for any firm doing cross-border business in Europe. It will make life easier for consumers who want to buy goods or services from providers outside their home countries. It will also make it easier for EU citizens to deal with government administrations when they reside in other EU countries than their own. However, eIDAS is complex and some of its wording is vague. Firms should begin planning for eIDAS implementation as soon as possible.

Action items for government

eIDAS will be crucial for the development of the Digital Single Market. For government agencies and administrations, acceptance of eIDAS Qualified Electronic Signatures (QES) issued by other EU member states will become mandatory in 2018. It is therefore essential to begin implementation planning without delay.

3. European electronic payments will be disrupted by new cloud services

What's happening in 2017

Electronic payments have been routine in Europe for many years. But fast-evolving technology and a new EU directive on payment services are driving big changes in the payments landscape that will impact every business and consumer in Europe. The directive is the Revised Payment Services Directive (also known as PSD2). Adopted by the EU at the end of 2015, it requires all EU member states to incorporate its provisions into their national laws by January 2018.

The fundamental purpose of PSD2 is to take Europe's vast bank-controlled payments industry – including credit and debit cards, retail point-of-sale networks, online consumer payments for e-commerce, and online business-to-business payments – and nudge it into the cloud era. While establishing strong security requirements for electronic payments, the directive also introduces a bold dose of competition into what has traditionally been one of Europe's most regulated industries, by requiring banks to make all customer accounts accessible to third-party electronic service providers under certain conditions. When duly authorized by customers, these third parties will be able to execute payments on the customers' behalf, analyze their financial data and provide other innovative services.

The intent of the directive is to create a vast competitive European market for cloud-based payment services. For example, one day soon, a restaurant might present you with its bill by sending a simple email or text message to your phone, and you might settle the bill by replying with a message authorizing payment of the agreed amount. Behind the scenes, your email or messaging service provider will access your bank account and transfer the money to the restaurant's bank account. No need to take out your credit card or checkbook or chase down that pesky waiter who seems to have disappeared.

Action items for business

PSD2 opens up entirely new and even quite radical possibilities for cloud-based payment services, but its details and even its existence are little known to many in the business community outside the banking and payments industry. Consumer-facing businesses of all kinds should begin educating themselves about the evolution of online payments and PSD2 sooner rather than later. Two in-depth reports from industry leaders are a good place to begin: Interconnected Commerce: a Revolution in Value Creation from global data center provider Equinix, and PSD2: A Catalyst for New Growth Strategies in Payments and Digital Banking from consulting firm Accenture.

4. The death of the password is near

What's happening in 2017?

Computing devices can now recognize fingerprints and faces. While not new, this capability is going to become more widespread and routine as standards such as FIDO (Fast IDentity Online) are adopted by software and hardware suppliers.

The real revolution is not simply unlocking your phone with your fingertip or logging on to your PC with a glance, but being able to use these gestures to log onto any web site or online service in a cryptographically secure way. This is what the FIDO standard –

embraced by most of the world's leading technology providers as well as by many large banks and governments – promises to deliver.

A key idea of FIDO is to divide the authentication process into two steps: first users authenticate themselves to their local device, using a biometric such as a fingerprint or iris scan or perhaps only a PIN; then the device uses public key cryptography to authenticate itself and the user to a remote web service or application. Every service that a user registers for from a specific device will use a different public-private key pair. Thus passwords or other secrets that must be shared over a network and stored on servers disappear completely, making their theft or inadvertent disclosure impossible. To achieve a fraudulent logon, a hacker would need to possess both the user's local access method (biometric or PIN) for a specific device and the device itself.

Action items for business

Unlike eIDAS, adoption of FIDO by businesses is entirely optional. While the initial technical work developing FIDO has been done by tech firms such as Nok Nok Labs, Google and Microsoft, a number of large banks and credit card brands now endorse it. European web-based and app-based businesses looking to accelerate their growth should consider FIDO as a way of smoothing transactions for consumers and customers.

Action items for government

Several European government agencies such as the UK Cabinet Office and the German Federal Office for Information Security have joined the FIDO Alliance. But European authorities, including the Commission, could and should do more to promote the adoption of FIDO in order to accelerate the growth of European digital businesses.

5. Security begins on your desktop (or laptop)

What's happening in 2017?

Recent years have witnessed a seemingly endless stream of severe security breaches of networks and computers at major corporations and government agencies, particularly in the United States. In nearly all of these cases the hackers succeeded because the targeted organizations failed to implement fundamental precautions such as two factor authentication or continuous security monitoring. A striking fact about these massive systemic breaches is that all of them affected networks or data centers operated by the target organizations themselves - none of them to date has occurred at a major cloud provider. There is a reason for this disparity: cloud providers are specialist organizations who can afford to invest more in the technical resources and human expertise needed to protect sensitive data.

While many organizations are devoting greater resources to hardening the defenses of their data centers or shifting key applications to outside cloud providers, paradoxically, the greatest remaining security threat to most organizations today may lie in the devices sitting on users' desks: the humble PC. While mobile has overtaken the PC as the world's most commonly used computing platform, the PC nevertheless remains the backbone of daily work in most business and government establishments. Technology pundits may consider the PC a "legacy platform", but hundreds of millions of these platforms will remain in use for years to come in EU workplaces.

Because they are so widely used, the PC and in particular its most commonly used operating system, Microsoft Windows, have historically been subject to large numbers of

attacks by hackers. The sheer amount of data stored on PCs or accessible from them makes it imperative for organizations to upgrade the security of these devices. The good news is that modern hardware and operating systems can now harden PCs from many of the attacks that have made headlines in recent years.

A long list of new security features have been built into the versions of Windows 10 intended for enterprise use, including the following:

- Virtualization-based security isolates critical operating system services into a segregated, virtualized environment similar to a virtual machine;
- Secure booting uses a specialized hardware feature in modern PCs (the TPM or Trusted Platform Module) to ensure that the hardware and the OS haven't been tampered with;
- Device Guard uses hardware features in Intel and AMD chips and the Unified Extensible Firmware Interface (UEFI) to prevent unauthorized code from running – instead of "blacklisting" undesirable applications, enterprises can now create "white lists" of approved applications, which will be the only ones that can execute;
- Credential Guard uses low-level virtualization to isolate sensitive information such as account and network login credentials;
- Hello and Passport implement the FIDO standard for biometric user authentication and secure cryptographic logon to web services and network applications;

Linux and Apple PCs have historically not faced the same intensity of hostile hacker attacks as Windows, and consequently the developers of these operating systems have not yet deployed an array of security features equivalent to those now available in Windows 10. Nevertheless, versions of Linux commonly used on desktop PCs such as Ubuntu have added many security features that exploit modern software methods and the hardware features such as TPM found on modern PCs. As for Apple, although it has for years declined to use standard TPM chips in its laptops, its most recent enterprise-grade laptops such as the MacBook Pro include a fingerprint sensor and a security chip supplying functionality similar to a TPM.

Action items for business and government

Whether they use Windows, Linux or Apple's macOS (aka OS X), organizations that rely on PCs should upgrade both their hardware and operating systems to modern security-hardened versions.

6. You can't buy the world's best machine learning software (because it's free)

What's happening in 2017?

AI – also known as machine learning or just "ML" – is accelerating rapidly. In just the past few months both Google and Microsoft have introduced dramatically improved services for online translation based on a new technique known as "deep learning". But what's more remarkable is that the same software used to build these new services is now available to the rest of us at no cost.

The world's titans of artificial intelligence – Google, Microsoft, Facebook, Amazon – are now competing to offer as free open source software the same powerful machine learning frameworks they use for their own internal product development. The first of these tools to be open-sourced and perhaps the best known is Google's TensorFlow, which – like rival offerings from Microsoft, Amazon and Facebook – draws its inspiration and techniques from the extraordinary worldwide flowering in recent years of university machine learning research.

The spread of commercial applications of machine learning is only just beginning, and there can be little doubt that 2017 will bring remarkable new examples of its use. The crucial raw material for machine learning applications is data. A striking example can be seen in machine translation. A little known fact about the deep learning algorithms behind the recent extraordinary progress in this area is that they are trained on a unique multi-lingual corpus of more than a billion words in over 20 languages – the corpus is built from the transcribed debates in the European Parliament.

Action items for business

Most machine learning software tools are still not quite ready for novice developers. However, small and medium businesses should begin to think carefully about how they might apply ML in their own markets. The key question you should ask is: do I have large amounts of data that could be fed into ML tools to yield new insights into my business or new services for my customers? Keep in mind that the cloud providers as well as a host of startups are packaging such tasks as image recognition and text analysis behind easier-to-use APIs (application programming interfaces) that require less expertise than the underlying tools themselves.

Action items for government

EU policy makers should recognize that the availability of extraordinarily powerful machine learning frameworks as free and open source software opens up vast new opportunities both for European research and commercial applications. The EU should educate and incent European firms large and small to engage fully with the machine learning revolution.

7. Now you can rent the world's most powerful supercomputer by the hour

What's happening in 2017?

If the world's AI titans are offering their machine learning software for free, they of course have an ulterior motive: they want you to rent time on their cloud services to use that software. But the price of cloud computing is coming down and the amount of compute power available on a pay-as-you-go basis is staggering. Microsoft's CEO has recently promised to "make the world's most powerful supercomputer available to everyone". By that he means that Microsoft's cloud service Azure is installing thousands of servers with customized chips especially designed for AI applications. Google and Amazon are installing similar chips in their cloud data centers, as are certain European cloud providers such as OVH.

This means that small and medium businesses – or single departments in large enterprises – can begin to build their own AI business applications and run them in an affordable way on "supercomputer" platforms that until recently were the exclusive preserve of the technology giants. The key to building effective business applications of machine learning is being able to run multiple experiments quickly and cheaply to find what works. The ability to "fail fast" is essential to moving up the learning curve. This is what the new cloud "supercomputer" offerings provide.

However, you don't have to tie yourself to any specific cloud provider to get the benefits of AI. It is always possible to shift machine learning frameworks from one cloud to another, run them on multiple clouds at the same time, or even test them out on your own laptop. Because the leading software tools of machine learning are open source, they can be installed anywhere. And because they are largely based on published academic research, the commercial cloud providers that originally developed them will not enjoy lock-in power over users.

Action items for business

You will only need a "supercomputer in the cloud" if you build the kinds of applications that require such power. These applications might include machine learning as discussed above, or they might be more conventional big data analytics – both kinds can benefit from the new hardware now available from cloud providers for cost effective pay-as-you-go use.

Action items for government

The pace of change in machine learning is rapid and accelerating. It is essential that policy makers encourage European entrepreneurs and established businesses to take advantage of the new capabilities now arriving on the market.

8. Building a mobile app for your customers may be cheaper than you think

What's happening in 2017?

The world is going mobile, but can your enterprise afford to build the kind of mobile app that your customers will be happy to use? Until recently the conventional wisdom was that mobile apps of acceptable quality had to be so-called "native" apps – that is, apps built with the low-level developer tools provided by Apple for iOS or Google for Android. However, building

such native apps can be very expensive – often costing tens of thousands to hundreds of thousands of euros.

Now new options are emerging that make it possible to build mobile apps offering native-like functionality with more accessible tools such as the JavaScript language used to build interactive web sites. Once such option is Facebook's React Native, which the social media giant uses to build some of its own mobile apps such as Instagram and which it offers as free and open source software. Apps built with React Native in JavaScript can run (with some modest tweaking) on iPhones and iPads, Android devices and even on Microsoft's Universal Windows Platform. A rival option is NativeScript, developed by the Bulgarian firm Telerik to work with Google's open source Angular 2 web framework (which in turn relies on Microsoft's open source TypeScript enhancement to JavaScript).

Action items for business

If you have a sensible business case for a mobile app but were put off by the costs, you should investigate the possibility of building (or hiring outside developers to build) an app using one of the new JavaScript-based native frameworks.

Action items for government

Developer education is a key to driving the growth of the European app economy. University training in computer science is often out of touch with the most current methods used in building commercial mobile and web applications. Policy makers should promote alternative forms of training for European developers at all stages of their careers.

9. Internet of Things

What's happening in 2017?

The Internet of Things (IoT) promises to turn the countless mundane artifacts that surround us in our daily lives into always-on Internet-connected data processing devices.

Gartner predicts that by 2020 the typical home in mature markets such as the US and northern Europe will have hundreds of "smart" objects. 50% of everyday consumable household items will be replenished automatically by such devices. Your refrigerator will know when you need more milk and – if you give it permission – will take the liberty of ordering more from your chosen e-commerce supplier.

The economic opportunities offered by the IoT will not be small. The European Commission estimates that the total market value of the IoT in the EU will exceed one trillion euros in 2020.

In many ways the IoT represents the culmination of all the major technology trends of the past decade: it takes mobility to the extreme by putting compute power into the smallest and most mundane of devices; it makes the Internet universal by connecting almost everything; it generalizes cloud computing by bringing it into every facet of our daily lives; and – last but not least – it will open the way to untold new applications of machine learning and big data analytics by providing an immense and unending stream of new data for the algorithms living in giant cloud data centers to interpret.

Because the applications of the IoT are so numerous and so universal, it is impossible to make a simple list of them. Most IoT applications will begin with manufactured items that consumers use in daily life or are part of industrial infrastructure of some kind. But the IoT must not be reduced to the "things" that it connects. The IoT should be seen as a whole, as

an integrated ecosystem through which data in vast quantities circulates and is transformed. The IoT does not consist simply of putting a microprocessor in your refrigerator and giving it an IP address. It also encompasses the data that your refrigerator collects and sends to the cloud, and the applications that analyze the data and make inferences about it: does this refrigerator require maintenance? does this consumer need more milk delivered? is this family eating a healthy diet?

The Internet of Things will touch nearly every area of the economy. But it presents a truly strategic opportunity for Europe's vast ecosystem of small and medium manufacturers of equipment – ranging from the most humble household appliances to the most sophisticated machine tools and components of larger assemblies such as aircraft and cars. Additionally, the IoT will provide significant growth opportunities for the many service providers, both small and large, whose work involves maintaining or operating these devices. For example, the IoT will transform the work of artisans such as plumbers and electricians maintain and repair the infrastructure of European dwellings and offices.

Action items for business

Manufacturers of consumer appliances and industrial equipment should already be actively investigating Internet of Things scenarios and applications. But they should take a long-term and ecosystem perspective – they should not let themselves be prematurely locked into isolated IoT tools or platforms acquired for point applications. Above all, they should not neglect the security and privacy implications of the IoT. For context, businesses should review IoT forecasts from experts such as Gartner, Forrester, and the Internet of Things Institute.

Action items for government

The IoT will be a boon for the European economy. However, it brings with it serious security and privacy risks that must be addressed aggressively from the start. The recent hijacking of thousands of inexpensive Chinese-made digital cameras to orchestrate a denial-of-service attack on Internet infrastructure provider Dyn is an example of what can go wrong when IoT security is neglected.

10. The world's computing power is becoming more concentrated and more dispersed

What's happening in 2017?

The computing power housed in the world's data centers is becoming more and more concentrated. The latest version of Cisco's annual study of global Internet traffic forecasts that by 2020 some 92% of the server-based business applications in the world will be concentrated in just a few hundred "hyper-scale" cloud data centers. Organizations will increasingly find that it is difficult or impossible for their own on-premises facilities to match the low costs, superior availability and vastly greater flexibility of the cloud. Hyper-scale cloud data centers are also likely to be far more secure than the smaller facilities that user organizations operate themselves. The cloud providers have the scale and the opportunity to hire the world's best security experts and deploy the most up-to-date defenses.

Many of these hyper-scale data centers will be located in Europe, operated by a mix of European and international providers. Ultimately the role of these infrastructure providers will recede into the background, while the business applications that leverage this infrastructure and create value for European consumers and entrepreneurs alike will come to the fore.

Europe has diverse strengths in manufacturing, services and innovative social policies that will allow it to capture the lion's share of value creation in the cloud.

Yet while cloud growth continues to surge, some analysts and venture capitalists and Cisco itself are beginning to argue that the pure cloud era is coming to an end. What explains this seeming paradox? The answer is that while enterprise data centers are consolidating into hyper-scale cloud facilities that leverage economies of scale and concentrated expertise, a parallel explosion of computing power is occurring at the edges of the global Internet. We have already discussed the Internet of Things, which places inexpensive, low-powered microprocessors and network radios in everyday devices such as refrigerators, thermostats and lamps. This is one form of edge computing. But there is another, more advanced kind, which involves clusters of powerful processors operating and exchanging data among themselves in a local context. The self-driving cars of the near-future, for example, may have a hundred or more processors working cooperatively to control the vehicle locally while simultaneous exchanging data with a remote cloud data center.

This new combination of edge computing and the cloud is coming to be known as "fog computing". While still in its early stages, it is a key trend to watch.

Action items for business

As the next "fog" stage of cloud computing looms on the horizon, it is time for European enterprises to consider whether it is still economically and strategically justified to operate large data centers on their own, given the efficiencies and flexibility of cloud computing. At the same time, equipment manufacturers must begin to think about the transformation of their products from mere hardware into sophisticated computing platforms that gather and process vast amounts of data locally as well as sending it to the cloud.

Action items for government

While the immediate concern for European policy makers must be to ensure that Europe captures the full benefits of the cloud revolution, they should not take their eyes off the emerging fog computing trend. The rapid development of self-driving vehicles is one key application of fog computing, and it is an example of great consequence for European industry.