MuleSoft

EBOOK

5 ways AI, IoT, and security are shaping the API economy

Edited by MuleSoft founder **Ross Mason**

Table of contents

Foreword

Ross Mason

Technology moves fast. What's shiny and new one day is quickly tossed aside when the next thing surfaces. As such, it's a bizarre concept to think about connecting technology built decades ago with modern day gadgets. Imagine trying to connect a Sony Walkman from the '70s with your Google Home to enjoy music.

However, if you're an IT expert, you're probably accustomed to connecting technologies together from different decades. When gathering business data, you're likely to reach into your decades-old mainframe with custom code and connect it to a new SaaS application.

Connecting technology built in different decades is no easy feat. According to MuleSoft's 2019 Connectivity Benchmark Report, legacy infrastructure and systems are the most frequently reported challenge to digital transformation, and 59% of IT leaders say their legacy infrastructure makes it hard to introduce new technologies like artificial intelligence (AI), bots, and the internet of things (IoT). Yet, these emerging technologies are set to disrupt every industry in the sam way mobile, SaaS, and the cloud did over the past 10 years. Organizations cannot afford to be left behind.

For organizations to effectively compete in ever-evolving business landscapes, they need to build adaptable digital platforms via APIs. With these building blocks in place, disparate legacy systems and new-age technologies can easily plug in and out of application networks as fads come and go. With a thoughtful API strategy in place, organizations can unlock value from existing systems and leverage emerging technology—all while remaining secure. With more than 20,000

public APIs on the web underpinning the apps we use every day, the new economy these APIs are driving is changing the way companies are built and operated. According to the Connectivity Benchmark Report, 36% of today's technology leaders generated more than a quarter of their organizations' revenue as a direct result of APIs. Think of McDonald's delivering food directly to doorsteps via Uber Eats, or HSBC providing a single financial dashboard for customers regardless of where they bank—all possible because of APIs.

In this ebook, we will share several points of view on how a thoughtful API strategy can help organizations take full advantage of emerging technology like AI and IoT without compromising on security. Let's dive in.

01 To deliver on AI's promise: Take the brain from the jar

By Ross Mason

Everyone is talking about artificial intelligence (AI). The technology might still be in its nascent stages, but we're already getting a glimpse of its promise. The opportunity to automate manual tasks and gain new insights to support business decision-making could have a huge impact on organizations; so much so that IDC forecasts businesses will be spending $77.6 billion on cognitive and AI systems by 2022.

However, as with any technological innovation, there are challenges to overcome before we will start to see AI's full potential. While most talk about the desired benefits of deriving insights from massive data sets or automating business processes, many overlook how difficult it is to make the connections needed in the enterprise to achieve those outcomes. Siloed data and a lack of connectivity between enterprise applications severely restrict AI's current ability to influence the digital ecosystem around it, rendering it little more than a rather expensive brain in a jar.

The trouble with AI

The C-suite might generally be on board with the need for AI, but in most cases they're still trying to learn how it can be leveraged strategically. Where it's being used perhaps most often, and where we'll likely see most early use cases, is in analyzing large sets of data and identifying patterns to generate new business insight. It's all about predicting behavior, based on the outcomes of thousands of other similar situations that have occurred in the past—a task virtually impossible for a human to do manually given the quantity of data involved.

In addition to the volume of data, another challenge lies in the structure and quality of the data. Organizations are often restricted by the fact that data is locked up in siloed systems and applications. As a result, getting that data into an AI engine to start revealing insight can be a major problem and limit AI's potential to offer competitive insight. To get the most value out of AI, it's not a case of knowing the right questions to ask but having the ability to connect AI engines to the right sources of data.

Automating the future

Business automation is one of the major areas that AI is set to disrupt. For example, JPMorgan has created its own AI engine, LOXM, which uses the lessons learned during billions of past trades to quickly execute deals that secure the best price. This type of automation can translate to other industries too; retailers will often spend hours trawling through sales and footfall records to identify staffing requirements and allocate resources to their store network. It's currently a laborious and inefficient task. However, if the retailer set AI to work on that same data, the manual process could be replaced by an automated system. The AI engine crunches the data, spots where staff is needed most, and then updates the HR systems to schedule shifts. Additionally, automating these cumbersome processes will free up staff to work on higher-value activities that drive greater benefit for the business and improve employee satisfaction.

However, the AI brain needs to be able to connect with enterprise systems if it wants to automate tasks. To illustrate this with an example, one company I've encountered has been working to create an AI-powered chatbot to help with customer support. However, they hit a brick wall because even a task as simple as updating a customer's details required AI to be

integrated with seven or eight different systems. The truth is, if you don't have this connectivity fabric in place, your AI systems will be capable of thinking, but not doing.

Making the brain in a jar intelligent

These challenges largely stem from a misunderstanding that AI will just plug into an enterprise like a new brain. Unfortunately, some AI vendors have further fuelled unrealistic expectations by trumpeting various big-name projects, without clarifying that these capabilities can't be reused to achieve different outcomes. This will only add to buyer dissatisfaction and technical debt for those that leap straight in without first laying the foundations for AI.

To do so, organizations first need to become more composable, building a connected nervous system called an application network, which enables AI to plug in and out of any data source or capability that can provide or consume the intelligence it creates. The custom code integrations of the past won't be practicable in the AI-world, where things can change in an instant. Instead, organizations need a much more fluid approach that allows them to decouple very complex systems and turn their technology components into flexible pieces.

This can best be achieved with an API strategy, which enables organizations to easily connect together any application, data source or device into a central nervous system of sorts, where data can freely flow. The central nervous system, or application network, is how the 'brain' of AI can plug into a business' digital ecosystem to consume its data and then provide valuable insights and actions. In the case of the customer service chatbot I mentioned earlier, with an application network, the business could enable AI to access any system where customer information is stored and then instantly update it with their new address.

The future's bright

While we're still some way off mainstream adoption of AI, we're already seeing impressive results. For example, one insurance company I spoke with is using AI to discern which of its customers are most likely to renew their premiums, and then automatically contact them via SMS. The firm saw a 60% engagement rate and 30% renewal rate from that text message bot campaign alone.

If connectivity challenges are overcome, the potential for AI to uncover valuable new insights will change the speed of business, while automating repetitive tasks will free up organizations to focus on more value-add activities.[1]

1 This article first appeared on Computer Business Review.

02 Powering customer journeys in the age of AI

By Ani Pandit

Technology has been the cornerstone of economic growth around the world for hundreds of years. It has underpinned the last three industrial revolutions and is now the driving factor in today's Fourth Industrial Revolution—marked by emerging technologies in a variety of fields. Unsurprisingly, artificial intelligence (AI) is one of the key technologies driving this new revolution. As described in the 1950s by the father of modern computer science, Alan Turing, "What we want is a machine that can learn from experience." His paper "Computing Machinery and Intelligence" is the earliest description of neural networks and how computer intelligence should be measured. While the concept of AI isn't new, we're only on the cusp of seeing AI drive real business value in the enterprise.

Businesses today are trying to augment and improve their customer, partner, and employee experiences by leveraging AI. However, what many have yet to realize is that AI is only as good as the APIs that support it.

For example, we're seeing the rise of conversational commerce, where consumers can interact with businesses and their services via digital voice assistants such as Alexa and Siri. Two very important things occur here. First, the voice assistant uses AI and machine learning technology—or algorithms that are trained using massive amounts of existing data—to understand voice commands. Second, the voice assistant acts on those commands by calling backend services with APIs that do the actionable work. This can include getting product information from a database or placing an order with the order

management system. APIs truly bring AI to life and, without them, the value of AI models cannot be unlocked for the enterprise.

The AI problem

Many businesses are beginning to deploy AI-based systems. According to Gartner's survey of over 3,000+ CIOs, 21% said they are already piloting AI initiatives or have short-term plans for them. Another 25% said they have medium- or long-term plans.

However, many businesses are adopting AI as a point solution to help customers with queries via a chatbot or with making recommendations via an AI and machine learning-based platform. These point solutions don't have the ability to influence the entire customer journey. The customer journey in today's digital world is complex, with interactions spanning many different applications, data sources, and devices. It is very hard for businesses to unlock and integrate data across all the application silos in their enterprise (e.g., ERP, CRM, mainframes, databases) to create a 360-degree view of the customer.

So, how do businesses go about unlocking these information systems to make AI a reality? The answer is an API strategy. With the ability to securely share data across systems regardless of format or source, APIs become the nervous system of the enterprise. As a result of making appropriate API calls, applications that interact with AI models can now take actionable steps, based on the insights provided by the AI system—or the brain.

How APIs can bring AI to life

The key to building a successful AI-based platform is to invest in delivering consistent APIs that are easily discoverable and consumable by developers across the organization. Fortunately,

with the emergence of API marketplaces, software developers don't have to break a sweat to create everything from scratch. Instead, they can discover and reuse the work done by others internally and externally to accelerate development work.

Additionally, APIs help train the AI system by enabling access to the right information. APIs also provide the ability for AI systems to act across the entire customer journey by enabling a communication channel—the nervous system—with the broader application landscape. By calling appropriate APIs, developers can act on insights provided by the AI system. For example, Alexa or Siri cannot place an order for a customer directly in the backend ERP system without a bridge. An API can serve as that bridge as well as be reused for other application interactions to that ERP system down the road.

At their core, APIs are developed to play a specific role—unlocking data from legacy systems, composing data into processes, or delivering an experience. By unlocking data that exists in siloed systems, businesses end up democratizing the availability of data across the enterprise. Developers can then choose information sources to train the AI models and connect the AI systems into the enterprise's broader application network to take action.

Using AI to enhance the customer journey

As AI systems and APIs get leveraged together to build adaptive and actionable platforms, the customer journey changes dramatically. Consider this scenario: A bank offers a mobile app that targets customers looking to buy or sell a home. In the app, customers can simply point at the property they are interested in and immediately rich data comes together via APIs to provide historical information on property sales, nearby listings and market trends. Customers can then interact with an AI-powered digital assistant on the app to start the loan

application process, including getting lender approval and mortgage rates. All the data captured from the mobile app can then feed the mortgage origination process to reduce errors and provide a fast and superior experience to the customer.

Businesses haven't truly realized the full potential of AI systems at a strategic level, where they are building adaptive platforms that truly create differentiated value for their customers. Most organizations are leveraging AI to analyze large volumes of data and generate insights on customer engagement, though it's not strategic enough. Strategic value can be realized when these AI systems are plugged into the enterprise's wider application network to drive personalized, 1:1 customer journeys. With an API strategy in place, businesses can start to realize the full potential AI has to offer.[2]

2 This article first appeared on TechCrunch.

03 Making APIs the bedrock of IoT development

By Ian Fairclough

The Internet of Things (IoT) is set to explode in the months and years ahead. Analyst IHS predicts by 2025 there will be 75.4 billion connected devices in use, while MuleSoft's Connectivity Benchmark Report found nearly half of IT leaders are investing or planning to invest in the IoT. This rapid growth is partly driven by an endless number of potential IoT use cases, from smart parking sensors that help drivers find space in crowded cities to predictive maintenance that can keep manufacturing production lines from unplanned downtime.

With IoT's incredible diversity, it's hard to envision exactly where it will end up. We're only at the beginning of what the technology is going to do for us and how it will impact our lives. For businesses in particular, the development of the IoT opens up a whole new world of opportunity for transmitting useful data that makes businesses more efficient and helps them to understand their customers better. However, despite the endless possibilities, there are several challenges standing in the way, especially when it comes to making IoT data accessible and actionable.

Identifying the obstacles

Before the IoT can reach its potential, businesses must identify a way to connect a range of devices and sensors with enterprises' backend systems. With Gartner estimating that half the cost of implementing IoT will be driven by integration, there's a real need for organizations to plan for how they will overcome this challenge.

For starters, organizations need to ensure IoT data can be transmitted and read in a way that doesn't disrupt the devices themselves, such as through open interfaces. Organizations also need to connect a range of monolithic legacy systems to the new-age IoT devices. At present, legacy systems communicate in a myriad of ways, making it difficult for organizations to consume the data they create in a standardized fashion. This will lead to limited adoption of the IoT and consumption of its data if it isn't addressed.

In addition to addressing these integration challenges, organizations must also ensure their deployment model is scalable. The more devices businesses can connect to the IoT, the greater its potential to transmit useful and actionable information. Without effective scaling, the potential of the IoT will go largely unfulfilled, as the costs and practicalities of connecting so many devices in a meaningful way will simply become insurmountable. As more of their physical assets are connected to the internet, businesses must also consider how they will manage access to prevent security breaches or devices being overwhelmed by legitimate users.

Building a bright future for IoT, one API at a time

The most effective way to overcome these challenges is to deploy IoT in a modular fashion, with a flexible integration layer between devices, data, and the overall IT ecosystem. This can best be achieved using APIs to build an application network. Underpinned by APIs, application networks enable applications, data, and devices to be plugged in and out seamlessly, without negative knock-on effects on other devices or data transmissions.

Therefore, when a change is made – something that is inevitable given the speed at which IoT will need to evolve – there aren't any rigid dependencies that would constrict those changes, or create integration challenges. In much the same

way that HTML provided the standardization that led to the explosion of the internet, APIs are becoming the standard interface enabling organizations to build application networks and paving the way for the rise of the IoT.

It's all about standardization

In addition to the efficiency benefits, organizations can also create new revenue streams by monetizing the devices they've connected to the IoT. For example, they could allow other organizations and third parties to build their own services and capabilities on top of IoT devices and the data being generated, in a similar way to how open banking is revolutionizing financial services. By using APIs to expose IoT devices and data in a standardized way, the opportunities for enterprises to benefit commercially will increase exponentially. APIs also offer a solution to the security dilemma, enabling organizations to build in security by design by embedding standardized access and authentication controls into the APIs to regulate access to IoT devices and data.

The key point to remember is that standardization is the crucial ingredient for making the IoT a success. When the devices connected to the internet can easily communicate, the capabilities they enable will become more useful and accessible. This in turn encourages consumption and adoption, driving innovation. APIs are therefore set to become the bedrock of IoT's future, connecting its various layers and helping to democratize the data being collected from billions of devices and sensors. Ultimately, APIs enable the IoT to become far more consumable, unlocking a whole new future full of untold opportunities that are impossible to envision today.[3]

3 This article first appeared on Diginomica.

04 How IoT can enhance customer experience

By Jonathan Stern

To attract and retain customers in today's competitive landscape, businesses need to provide an exceptional customer experience that stands out in the marketplace. Rather than following a one-size-fits-all approach, the most successful businesses are rapidly tailoring offerings for customers in real time.

The internet of things (IoT) has emerged as an effective method for providing real-time value. Across the globe, IoT deployments are rapidly gaining steam. According to analyst firm Gartner, there will be 20.4 billion connected things in use by 2020. Of these, 7.6 billion will be used by businesses. It's clear that IoT will soon touch consumers' lives in myriad ways – whether realized or not.

With IoT growing rapidly due to the cost of hardware dropping and connectivity between IoT devices, cloud, and on-premises systems becoming easier, many businesses are beginning to explore its benefits. As shown in MuleSoft's Connectivity Benchmark Report: the top three technology trends that IT leaders are currently investing in or are planning to invest in are security (57%), big data and analytics (55%) and the internet of things (49%). These trends fit hand-in-glove. Especially when you consider that to enhance customer experiences, businesses need to not only collect data securely, but also analyze and put the data into context to make it actionable.

Connecting the layers of IoT

Successful IoT deployments consist of layers, including the devices that collect the data, the networks that deliver the data, and the applications that analyze and make sense of that data. While they need to work together as an integrated whole, it's important that organizations future-proof their businesses by making the components modular. Essentially, the components need to be managed independently, given the rapid pace of technological change. This will allow components in place now to be altered or swapped out in relatively short order in the future, to take advantage of enhancements.

For example, IoT sensors may need to be replaced every few months, networks may need to be changed every few years, and legacy systems may need to be tapped into in various ways over time. Whether changing an IoT sensor or tapping into a new data source, it's imperative that changes of any kind do not impact the different layers and cause everything to break versus bend. For example, an organization should be able to quickly plug in a new IoT device or easily swap out its network without having any adverse effects on the applications themselves. Additionally, it's important that the data itself is held independently from any particular system, so multiple parties can use it in different ways. For example, data gathered from a motorway could be used to monitor congestion, provide real-time guidance for drivers, and also allow for more informed planning of new roads.

To design IoT infrastructure in a modular and agile fashion while democratizing the data collected, organizations are starting to build application networks. Underpinned by APIs, application networks enable applications, data, and devices to be plugged in and out seamlessly without negative knock-on effects. Therefore, when a change is made—something that is inevitable—there aren't dependencies that would constrict advancement and evolution.

Another benefit with taking an API-led approach is that security is built in by design, as IT teams can regulate and enforce who has access to what data. Given security is a critical factor when designing and deploying IoT projects, there needs to be a way to not only identify the devices on the network to confirm they should be accessing stored data but also authorize that devices only have access to the data they require to complete their particular task.

Putting IoT into action

When it comes to IoT deployments, the retail sector is currently leading the charge. Using data generated by everything from intelligent vending machines and shop shelves to point-of-sale systems, retailers are able to gain insights into shopper tastes and habits previously not possible. With this new data, retailers can adjust everything from store layouts and stock mixes to match the requirements of particular customer groups. Where previously data would have been gathered for later analysis, IoT deployments allow this analysis and insight to happen in real time.

IoT-powered innovation is also being seen in a range of other areas. At Sydney's iconic Bondi Beach, the local council has installed an IoT project comprising of network-connected rubbish bins. The bins monitor how full they are and communicate with rubbish collectors when they need to be emptied. Meanwhile, safety on Australian docks is being improved as a result of the rollout of an IoT project that tracks the position of staff and heavy machinery in real time. By using a combination of RFID tags, radar, and wireless networking, staff movements can be monitored to ensure their safety is not compromised when heavy machinery is working.

Additionally, one of America's fastest-growing restaurant chains is analyzing beer consumption with IoT sensors. By connecting its IoT flow sensors with its point of sales system via APIs and

an application network, the restaurant chain is able to measure pour volume against sales transaction data to predict preferences and optimize inventory planning. As a result, the restaurant chain can improve the customer experience while operating more efficiently.

Looking forward, the role and value of IoT will continue to grow and deliver customer experiences not yet anticipated. With a thoughtful approach to designing and deploying IoT projects correctly now, organizations will enjoy significant added benefits in the future.[4]

4 This article first appeared on iStart.

05 Zero trust: The key to securing the API economy

By Ross Mason

There's no doubt that today's businesses are under increasing pressure to innovate faster. Looking to deliver innovative offerings at an accelerated pace to meet ever-evolving customer expectations, many are turning to modern development models underpinned by the cloud, microservices architectures, and containerization technologies. The result is a large-scale mashup of hundreds—sometimes even thousands—of APIs, responsible for connecting and sharing data between disparate systems, applications, and devices located both inside and outside of an organization's four walls.

As a result, APIs are everywhere. ProgrammableWeb currently provides the largest API directory on the web, with access to over 21,700 public APIs worldwide; a catalog that is constantly expanding as developers add new ways to connect IT capabilities. And according to Gartner, "By 2022, API abuses will be the most-frequent attack vector resulting in data breaches for enterprise web applications."

With APIs now behind most mission-critical business capabilities, securing them has become paramount. In today's API economy, organizations don't have defined perimeters anymore. They live everywhere their employees, customers and partners do, making perimeter-based security models ineffective and even "negligent," according to Forrester. Instead, organizations need to adopt a zero trust security model, where security can lie within the APIs themselves. As a result, organizations will be able to move faster without compromising security.

Understanding the security challenge

The difficulty faced by many organizations is that moving fast and staying secure are often at odds with one another. Digital transformation has made applications, networks and devices the powerhouse of the modern business, but it also exposes organizations to unprecedented levels of risk from security breaches.

Malicious outsiders are primed and ready to exploit vulnerabilities in web-facing applications with a growing array of tactics, while employee use of "shadow IT" and increasing adoption of cloud, mobile, artificial intelligence (AI) and the internet of things (IoT), further increase the number of attack vectors that security teams must guard against. It's no surprise then that Gartner forecasted worldwide information security spending will exceed $124 billion in 2019.

Improving security with modern APIs

In increasingly dispersed and dynamic IT environments, traditional perimeter-based security approaches can't meet the scalability, adaptability or reliability needed to manage risk. The answer lies in modern APIs, which enable the business to create standardized, accessible and well-defined entry points that are easy to visualize and therefore secure. Switching from a traditional perimeter-based model to an API-centric model allows IT to secure every access point according to a standardized framework. It also allows IT to control who has access to IT capabilities and set read/write capabilities to define what level of access they have, simplifying the process and enabling more robust security.

Additionally, modern APIs enable organizations to build secure application networks, where IT and business capabilities are made discoverable and reusable through managed APIs. The APIs, in a sense, become productized and can be plugged in

and out of the network as market conditions or requirements shift. Security best practices are, therefore, built into every access point from the very beginning, making them secure by design.

The need for zero trust security

Traditional approaches to security will no longer work in today's API economy. Transport Layer Security (TLS), credentials, firewalls, reverse proxies and demilitarized zones (DMZs) were designed for a web environment, where users interact with apps via a browser. In the new world, users, APIs, and devices interact without this intermediary, so network perimeter approaches are no longer effective or scalable and could even introduce new security risks.

Organizations, therefore, need to embrace a model where perimeters are redefined around APIs. Instead of networks or applications having a fixed perimeter, the APIs that connect them should be given verifiable identities so they can interact with each other securely and without friction. The result is a zero trust model, where APIs are responsible for authentication, authorization and access control in a distributed fashion using identities. This approach is highly scalable, works across any application network and relies on the well-understood models of multi-factor authentication and digital signature to authenticate log-ins and authorize actions.

A decentralized chain of trust also allows IT teams to trace back actions, further improving security and transparency. Not only will this help provide the foundation on which organizations can drive digital transformation and growth, it offers a best practice way to satisfy regulators, as we enter a new era of security and privacy compliance.

Ultimately, the pressure that organizations are under to innovate faster while remaining secure will only continue to increase as the API economy gathers momentum. Rising

demand for digital services and IT capabilities, alongside the growing threat from cybercriminals, is making it more challenging than ever for IT to satisfy the needs of the business while keeping it secure. In such a fast-paced environment, rigid perimeter-based security measures are simply inadequate. In today's world, organizations need a no perimeter, zero trust, API centric security model that not only brings unprecedented levels of security but also increases agility for organizations looking to digitally transform.[5]

5 This article first appeared on SC Magazine.

Conclusion: Building a thoughtful API strategy

At its core, digital transformation enables companies to reframe their relationships with customers, suppliers, and employees by leveraging new technology to engage in ways that were not possible before. These new technologies — artificial intelligence (AI), Internet of Things (IoT), bots, and more — demand a new level of connectivity that cannot be achieved with yesterday's integration approaches.

Businesses and IT leaders must act now to ensure their organizations stay relevant and competitive. It's not enough to implement a new application or technology. Success hinges on the ability to bring many different technologies, sometimes from different decades, together to create experiences and offerings that stand out to customers. Connectivity is the biggest differentiator for success today.

Fortunately, modern-day APIs are the instruments that provide both a consumable and controlled means of accessing data. APIs make it possible to unlock valuable data trapped within legacy systems and power new mobile apps with data orchestrated from a variety of systems. They can be productized and reused to drive rapid innovation. What's more, IT teams can build, package, house, and deliver these APIs to be externalized so others can join their digital ecosystem to co-create value. By securely opening up APIs and data sources, IT teams can democratize innovation and enable new villages in and around their organizations to innovate freely. The key here is that IT shifts focus from just delivering projects to driving reuse of their digital assets.

With APIs getting credit for the ecosystem successes of digitally-native companies like Amazon, Netflix, and Uber, it's not surprising that CEOs and boards are driving their teams to follow suit.

Visit MuleSoft's API strategy hub to chart your organization's API strategy journey, align stakeholders on your digital strategy, and get insights from leading organizations on how to measure the success of your API ecosystem.

About MuleSoft

MuleSoft, a Salesforce company

MuleSoft's mission is to help organizations change and innovate faster by making it easy to connect the world's applications, data, and devices. With its API-led approach to connectivity, MuleSoft's market-leading Anypoint Platform™ empowers over 1,600 organizations in approximately 60 countries to build application networks. By unlocking data across the enterprise with application networks, organizations can easily deliver new revenue channels, increase operational efficiency, and create differentiated customer experiences.

For more information, visit **mulesoft.com**