The API-First Transformation

V12.2021 (DRAFT)

(Sample Chapter)

The digital world is always changing

In this book, we'd like to invite you on a one-of-a-kind tour of the API-first world. This tour will include a deep dive into what "API-first" means, along with discussions of how microservices, the API lifecycle, and governance all play a role in shaping not just an API-first world, but potentially the culture, health, and strength of your business for years to come.

But before we take you on this tour of the API-first world, we need to share a little bit about how the digital world has been seismically shifting for the last fifty years. This includes, in particular, how the last twenty years of the web has increased the pace and volatility of doing business in a global marketplace. To be able to fully appreciate this moment in time, it helps to learn a little bit more about all the momentum that has been accumulating over these decades, and how we find ourselves at a convergence of global networking, the cloud (where we can find all the digital resources we need to scale infrastructure like we've never experienced before), and with mobile devices bringing the internet into our pockets, our cars, our homes, and businesses.

As a result of these massive shifts, today's leading technology companies like Amazon, eBay, Salesforce, Twitter, Twilio, and Stripe are successfully demonstrating why being API-first matters, providing just a glimpse at the opportunity that exists to build entirely new products and industries within an API-first world.

So let's start our tour of the API-first world with a look back at the digital past, which has set the context for the API-first future.

The web, mobile, devices, and the journey to the cloud

The seeds of the modern API movement were planted in 1958 with the formation of the United States government's Advanced Research Projects Agency (ARPA), which was part of the era's frenetic Cold War race for technological innovation. These API seeds were further cultivated with the Semi-Automatic Ground Environment (SAGE) built by the US military around this time as the nation's first air defense system; then came object-oriented programming in 1960, computer time-sharing in 1961, and commercial networks like the IBM SABRE reservation system by 1964.

However, it wasn't until the introduction of ARPA's new kind of network, ARPANet, in 1969 that we'd see the real potential of APIs begin spreading across the United States, laying the foundation for the web and the cloud that we know today. It would take fifty years for these seeds to grow, with the introduction and evolution of several other essential technologies before we'd reach the tipping point we are experiencing today—with APIs now emerging as the building blocks for the modern enterprise architecture that powers the web, mobile, and device applications we all depend on every day.

API seeds planted with ARPANet

By the 1970s, we had the essential ingredients needed for modern APIs, but it would take another five decades and significant amounts of investment and adoption of key computer technologies before we'd realize the API potential that exists today. While universities and the

military were busy evolving networks, commercial implementations under the umbrella of electronic data interchange (EDI) were taking root, leveraging FTP and machine-readable files as the foundation for a more digitally enabled economy, which is something that continues to evolve until this day. While EDI was building momentum, we were also going through the personal computer revolution, seeing massive business adoption of local area networks, the continued expansion of ARPANet, and ultimately the birth of the World Wide Web in the 1990s. All of this set in motion a flurry of API advancements, beginning with Common Object Request Broker Architecture (CORBA) in the 1990s and then service-oriented architecture (SOA) in the early 2000s. But it would still take another twenty years of alignment in how we deliver infrastructure via the World Wide Web before we would get where we find ourselves today.

Web APIs changing the game

As SOA was being recognized by organizations as the foundation of enterprise interoperability in the early 2000s, a simple, web-based style of APIs jumped out of the enterprise toolbox and began being used to power a new breed of technology companies like Salesforce, eBay, and Amazon. As these companies grew these simpler web APIs were also being applied to make things much more social by Flickr, Delicious, Facebook, and Twitter. However, it was Amazon's continued investment in APIs that would shift things into overdrive with the introduction of API-defined Amazon Web Services in 2006, which would provide us the unlimited resources we would really need to make all of this work at the scale we would need. As this momentum was picking up speed, we also began to see the online world move into the palms of our hands with the iPhone and Android mobile phones in 2007 and 2008; the momentum then spread to our cars, homes, and devices with the Internet of Things (IoT) by 2010. All of this digital progress would set in motion a decade of API growth and expansion that would be needed to deliver digital resources and capabilities we depend on not only across our growing web applications, but also our mobile phones and the increasing number of other connected devices we have begun plugging into the web.

All of this brings us to the 2020s, where we have the global network, digital resources, applications, and end-user adoption we need to take us into the future, allowing us to invent entirely new industries while also increasing the velocity at which business gets done across almost every business sector today.

APIs going mainstream

APIs are not new. You can see their reflection across the early computer industry that emerged out of World War II and well into the space race. However, the current breed of web APIs is unique to the last two decades and related to every major technology innovation in the last twenty years—the cloud, mobile applications, IoT, and the continued evolution of the web. Where we stand in the 2020s is 50 years in the making, resulting in the intersection of computing, networking, and desktop, web, mobile, and device access to the digital resources and capabilities across our enterprise organizations. APIs are how you provide access to these digital resources and opportunities across multiple channels; in other words, extracting maximum value from the capabilities of APIs is what will determine the velocity at which you can evolve, iterate, and innovate across this increasingly distributed digital landscape.

In the last decade, it has become clear to every enterprise organization that you have to be properly utilizing APIs to effectively and efficiently operate across multiple application channels to satisfy the ever-increasing need for integration, but it is putting an emphasis on just the API where the leaders in this digital economy are finding their competitive edge.

In short, these leaders are putting the API-first philosophy at the forefront of every step of their digital journey.

APIs are defining the future

As soon as the World Wide Web captured the attention of the business world, top enterprise organizations began utilizing APIs, and then taking what they learned from this API journey and applying it as part of a microservices evolution of internal operations. These are the enterprises that have taken the lead in the last five years, because they understand the importance of putting APIs first when it comes to the delivery of any application or integration, as well as the internal, partner, and public implications of being API-first and how it all comes together to move an organization forward at scale.

These leading organizations understand not only that APIs are essential for digital transformation, but also that digital transformation is an ongoing journey and not just a destination. Digital transformation is drawing a line between the enterprise organizations that are API-first and those who are API-last, defining the line for who will grow and thrive in coming years and who will fall behind or go away completely. This reality is shining the light on how APIs have delivered for Salesforce, Amazon, Google, Facebook, and the other technology giants of the last two decades, and how APIs are what will define the next generation enterprise organizations who will lead in every other business sector—because, in an API-first world, we are all technology companies.

The growing complexity of API systems

By numerous measures, the API growth rate is exploding. There is a good reason for this: APIs are at the heart of digital transformation across every industry because they enable adaptability, rapid experimentation, and new category creation, activities that McKinsey estimates to be worth *$60 trillion US dollars by 2025*. We live in an increasingly connected world. APIs provide that connection. Top businesses recognize the opportunity and are moving to meet it.

API stands for “application programming interface.” Like the dashboard for an automobile, an API allows anyone to access and benefit from powerful functionality without having to understand how the underlying subsystems (e.g., the car’s engine, brakes, or transmission) work. Using APIs frees developers to focus more energy on the unique business problem they are trying to solve.

Many API tutorials, books, and conferences emphasize making the individual units go faster, do more, or be more intuitive. However, as companies continue to pave the way for API production and consumption within their organizations, they discover that the continued optimizations to individual pieces no longer generate the expected performance.

As the number of automobiles on the road increases, the automobiles collectively exhibit properties unique to a *system*. On the positive side, having many cars (and the infrastructure to support them like drivers, mobile computing, and road networks) makes modern conveniences like curb-side checkout and ride-sharing possible. On the other hand, a complex system will also exhibit negative emergent behaviors that could not have been predicted while only focused on the individual car, things like traffic congestion and road rage.

As organizations continue growing their API usage, these ecosystem effects occur—whether organizational leaders are aware of them or not. Companies that manage more than a handful of APIs experience a non-linear increase in configuration and communication management challenges. This results in complexity, and complexity leads to emergent behaviors. *This is an API ecosystem.*

Overcoming the complexity in an API ecosystem requires different approaches. Just as a mechanic has a very different job than a traffic engineer, the requirements for maintaining a single API deployment are different from the requirements for sustaining an organization's complex API ecosystem. Success requires not only perspective and know-how but also specialized tooling capable of larger, more holistic sets of business objectives.

Companies can ignore the management of this valuable business asset at their peril. Or they can recognize the unique challenges presented by their burgeoning API ecosystem and act accordingly.

Why ad hoc API approaches don't scale

An API journey doesn't start with a cast of thousands. For most companies, their first API began as a targeted means to a specific business end. Scaling architectures, processes, training, and tooling was far from the minds of all involved at the onset. From design to documentation, development to deployment, these select few applied whatever experience, frameworks, and gut instinct were available. This scrappy approach to APIs is *ad hoc* (which is defined by Merriam-Webster as "fashioned from whatever is immediately available"). It is also completely normal to those just starting.

API sprawl left unchecked

Scaling, however, creates new challenges. As the number of teams, expectations, and APIs grows, this ad hoc environment where anything goes can cause problems. If left unchecked, these problems can begin to affect company performance negatively. An organization has outgrown its ad hoc API approach if leaders notice:

- It isn't easy to pinpoint who has access to what, or what data is coming into and going out of the organization
- An inability to meet operational SLAs, either in delivery, uptime, or new feature additions
- When things do break, the recovery time is long (and often keeps getting longer)
- A lost customer due to fragmented or incompatible pieces that the customer was unwilling to cobble together
- Out-of-date or incomplete documentation undermines platform goals

- A security breach due to lack of security standards (or unenforced standards)
- Repeated rollbacks or patching of APIs deployed to production
- Incomplete or missing metrics make API evolution a trial-and-error process
- Increasing time for developer onboarding
- Teams seem to be spending more time in meetings figuring out how something works

Why does this happen? When a small handful of individuals are responsible for API development, the number of architectural styles, tooling, and supported outcomes can be easily comprehended. Creating alignment is as easy as gathering everyone in a conference room (or on video chat).

But if more than a handful of people are creating APIs, then suddenly more experiences, architectural styles, and bespoke tooling is introduced into the company's growing API ecosystem. In the absence of repeatable processes, documented techniques, or dedicated tooling, the results from API production will become unpredictable—coordination costs across unaligned pockets of practice increase along with inefficiency. Higher-order alignment suffers. As described in the book *Accelerate: Building and Scaling High Performing Technology Organizations*, "teams become adrift, concentrated on micro-optimizations disconnected from aligned business delivery."

The need to get more strategic

In extraordinary cases, it is possible for small, ad hoc teams to meet significant, holistic concerns of an API ecosystem. What is far more likely, however, is the day-to-day delivery pressure of the expanding API ecosystem overwhelms the small teams' attention. When this happens, broader architectural concerns like API consistency and quality are deemed "nice to have" rather than being considered absolutely essential.

That is unfortunate, because architectural decisions like the form and function of an API are precisely those that are incredibly difficult to change once released. APIs are, by nature, cross-cutting, have a profound impact and high cost of change, and are make-or-break strategically.

To successfully scale beyond ad hoc API development, companies need more than traditional software management. They need an API platform that supports each API, and the entire API ecosystem, throughout the entire lifecycle. Having an API platform that understands the interconnectedness of API issues can hold teams to account, managing their attention and responsibility and attending to the system as a system, balancing their respective forces and demands better than fragmented, haphazardly implemented tools. Finally, an API platform supports various complementary API styles from REST to GraphQL to WebSockets and beyond, for a growing API ecosystem.

Managing an API ecosystem as a shared resource across an enterprise is a significant challenge. The issues with a growing API ecosystem require a robust and differently leveled approach. However, with the right API platform, moving beyond ad hoc API development for scaled success is possible.

Leveling the competitive landscape using APIs

In business, we are all looking for the competitive edge that will allow us to lead the pack. Companies of all shapes and sizes are painfully aware they are going through a chaotic digital transformation. It isn't enough anymore to just keep up, we need innovation to become part of our operational DNA, and it is increasingly important that we are able to keep up with the speed of business in a digital era. Companies seek exceptional software development teams that are able to deliver access to multiple online channels, going beyond just doing business at acceptable levels, and making sure they lead the pack in every way. Whether a company is API-first or API-last has become the measure of who leads and who is behind in the landscape across every industry today.

Multiple digital channels

APIs emerged in the early 2000s as a response to how to deliver more distributed resources via increasingly popular, large, and collaborative websites like Salesforce, eBay, and Amazon. Once mobile phones and their mobile applications emerged on the scene by 2008, innovative developers realized that they could more efficiently deliver digital resources not only to their web properties but also to the rapidly growing number of mobile applications. Simple web APIs excelled at making sure the digital bits were always where they needed to be. As soon as web APIs were applied to mobile solutions, innovative developers noticed how efficient web APIs were over always-constrained mobile networks, and began innovating using APIs to connect common everyday objects like thermostats, lights, cameras, cars, signs, and more to the web, creating the Internet of Things (IoT). This, in turn, set in motion a wave of innovation that would change how business was done over the next decade.

Enabling digital innovation

Seeing the potential in delivering digital resources across multiple channels, a handful of innovative technology companies began to see the benefits of getting more organized and disciplined when it came to using APIs to provide real-world solutions to common business problems. Realizing that if you were API-first, and you were focusing on the API before you focused on any of these growing numbers of channels, that APIs could be designed and delivered as standalone products that possessed clear business value. This allowed innovative technology companies to redefine how they do business inside and outside the firewall, and iterate upon a legacy infrastructure with an emphasis on well-planned and more precisely designed web APIs that leveraged a feedback loop with consumers, which then facilitated rapid iterations of these APIs-as-products to meet business needs.

This new cycle enabled entirely new types of applications by turning commodity infrastructure like telephony, payments, storage, and other essential business resources into digital products, that in turn would power entirely new ways of doing business like ridesharing and the "gig economy" to flourish.

Changing how we move

APIs enabled Amazon to dominate the publishing industry and then spread across every other retail sector. APIs gave Twilio and Stripe the agility, flexibility, and velocity they needed to redefine telecommunications and the payment industry.

APIs address the need to be available across multiple web, mobile, and device channels, but there's more: once your teams have been effectively using APIs to deliver your core business capabilities, they also begin to see increased velocity in how new resources and digital capabilities can be delivered, leading to the digital innovation we spoke of earlier. This agility, flexibility, and velocity help make teams, and their organizations, more responsive to change. Helping equip your development teams with API-first superpowers can change the gravity of the industry you operate in and even allow you to move in entirely new directions.

Organizational muscle memory

Salesforce, eBay, and Amazon have a 20-year head start over their competitors. Facebook, Google, and Twitter have a 15-year head start over their competitors. Twilio and Stripe, have a 10-year head start over their competitors. Their teams have gained the knowledge and achieved the consistency they need to not just prioritize working with APIs, but to do it well. This allows the teams at these top companies to achieve a level of consistency and reliability that their competitors only dream of, giving them a significant advantage that will be hard to change.

Being API-first means you are building strength and capacity for doing APIs well, creating a team-wide and an organization-wide muscle memory for what is needed to respond to the demands of consumers in a digital world while also embracing change (or even better, *being* the change). These organizations are able to establish effective API operations that employ a well-known API lifecycle to rapidly iterate upon legacy infrastructure—while also delivering the next generation of digital resources and capabilities needed across desktop, web, mobile, and device applications.

Staying ahead of the game

Being API-first has enabled the leading companies named above—and many others—to:

- Move faster
- More effectively change direction within their core business
- Rapidly innovate around new digital capabilities
- Respond more efficiently to market shifts
- Maximize their global reach into entirely new markets

APIs are how technology companies redefined the global business landscape over the last two decades. In the last five years of this evolution, APIs have also gone mainstream, pushing financial, healthcare, and even government to better adapt, be more competitive, and find their API-first way. This demonstrates how APIs are not only leveling and redefining the competitive landscape for a new breed of technology companies, but also becoming a lifeline for companies who have been in business for decades, or even centuries. Being API-first provides a much-needed path forward for enterprise organizations to redefine themselves in a digital world, stay ahead of the game, and remain competitive in an increasingly volatile business landscape.

Increased regulatory compliance through APIs

APIs are more than just the backbone supporting digital products, services, and experiences. They are also a critical, standardized way for organizations to demonstrate data efficacy and responsibility. When done correctly, APIs can drive regulatory compliance and provide a safe, secure channel for consumers to access, interact, and extract an enterprise's functionalities. Done poorly, APIs can result in serious problems—including massive financial penalties like the European Union's recent US$267 million ruling against WhatsApp.

Most common regulatory standards of concern for APIs

Companies utilizing APIs in every industry need to be aware of the regulatory environment where they operate. Regulations and policies have been instituted throughout the world that stipulate how businesses acquire, manage, and utilize users' data. Some of the most common compliance standards include:

- General Data Protection Regulation (GDPR)
- California Consumer Privacy Act (CCPA)
- Revised Payment Services Directive (PSD2) and open banking
- 21st Century Cures Act/Fast Healthcare Interoperability Resources (FHIR)

Let's do a deeper dive on these particular standards, because each one brings a unique set of considerations into the picture.

GDPR

GDPR is a European privacy and security data standard implemented in 2018. It outlines expectations for how companies may handle users' data. It applies to European firms and firms that may be based outside of the EU but collect and process the personal information of EU residents. It requires European individuals' data rights and security best practices to be applied before data is collected.

Perhaps the most notable impact of GDPR is the requirement that companies need to be able to provide information on who they have shared personal information with if requested by users. This can be difficult to obtain for those that provide APIs open to any third party without registration or account management.

CCPA

Among states in the United States, California is outsized. It has 17 million more people than America's second most populous state, Florida. Further, if California were a sovereign nation, it would rank the world's fifth largest, ahead of India but behind Germany. It is because of that influence that when California's privacy law went into effect on January 1, 2020, it effectively became mandatory for any company doing even modest business in the United States.

Like the GDPR, the CCPA grants rights to California residents on how their data is collected and used. Unlike the GDPR, it widens the definition of personal information to include an expansive list of items, including inferences ("preferences, characteristics,

psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes").
Upon a request for information, companies need to be able to:

- Disclose what personal information they have on the requestor, where it was sourced, how it is used, whether it is being disclosed or sold, and (if so) to whom
- Delete any personal information
- Provide the ability to opt-out of allowing personal information to be sold to third parties
- Continue equal service and pricing, even if the requestor exercises their privacy rights

PSD2 and open banking

While GDPR and the CCPA impact any company handling personal data, Europe's PSD2 is specific to the financial sector. PSD2 is a European regulation for electronic payment services. Progressively rolled out in stages starting in 2018, it requires banks to provide common API access to secure payments, boost innovation, and help banking services adapt to new technologies. The standardized access to traditional banking products, like clients' accounts, is often referred to as "open banking."

Additional standards—including NextGenPSD2, OpenBankingUK, and the French STET standards—define how financial API offerings are designed. In addition, Australia and Brazil are working on their own versions of PSD2 (CDR and Open Banking Brazil, respectively).

21st Century Cures Act/FHIR

The 21st Century Cures Act is a United States law intended to "accelerate the discovery, development, and delivery of 21st-century cures." As part of this act, in May of 2020 the Centers for Medicare and Medicaid Services (CMS) decreed that most health care provider organizations must implement APIs. Further, they adopted Health Level 7 (HL7) Fast Healthcare Interoperability Resources (FHIR) Release 4.0.1 as the data exchange standard.

That 2020 CMS ruling stipulated that any hospital that uses an electronic health record (EHR) must demonstrate its system can comply with federal data exchange standards. Given that Medicare and Medicaid represented nearly $1.5 trillion in 2019 spending, the network of impacted health companies is vast.

Other impacting regulations and standards

In addition to the items mentioned above, numerous other regulations may impact an API's design and usage across many industries. In US healthcare, that includes HIPAA (the Health Insurance Portability and Accountability Act of 1996). The finance industry adheres to the PCI DSS (Payment Card Industry Data Security Standard). SOC (Service Organization Controls) reports are commonplace in the accounting industry. Finally, ISO 27001, which details general information security practices, impacts API design and usage in all industries.

Meeting regulatory requirements

As the regulations and standards above demonstrate, it is not enough for a company to know where its data lies. Companies must understand how data is utilized throughout the organization and to whom it flows.

Basic data handling best practices are good for all APIs, not just when required for compliance reasons. These practices include:

- Using SSL and data encryption both in transit and at rest
- Password hashing
- Avoiding exposing information in URLs
- Pseudonymization of any real user data to be used for testing on dev or staging machines
- Considering the inclusion of timestamps in requests
- Avoiding exposing API keys

Going further, companies should have a structured, thoughtful approach to the data provided or ingested via APIs. This is essential to ensure that everyone in the company takes the same approach to common goals in a coordinated, timely way. This may mean a more significant role for enterprise risk management in API design, deployment, and integration conversations.

Any company with APIs should maintain a canonical inventory of services within the organization. They must not allow anonymous API access. Each consumer of the API should have a known primary contact person that is regularly audited to ensure it is current. There needs to be detailed log records of every read and write to identify who accessed what and when. Thankfully, an interface like an API is ideal to centralize and mandate these operations for complete and compliant records when called upon.

Regardless of where the responsibility for compliance falls, however, companies should provide mechanisms to constantly audit API access, address problems, and provide remediation proof in the presence of external oversight. If they can do that, they are well on their way to meeting their API regulatory compliance obligations.

Every company is now an API company

As multiple recent and worldwide disruptions have shown, modern businesses must emphasize adaptability and agility. The flexibility provided by modular API architectures is the difference between capturing emergent opportunities and reacting to seemingly random fate.

Here's one example: a large US-based retailer, Target Corporation, experimented with curbside pickup on and off for years. However, COVID-19 changed consumer behavior nearly overnight. In the three-month quarter ending on May 2, 2020, the Minneapolis-based big-box retailer reported a 278% increase in curbside pickup, in-store pickup, and Shipt delivery. Meanwhile, in the same quarter, Walmart reported online record sales.

Companies who invest early

In the cases above, earlier investments in digital infrastructure, linked by APIs, allowed traditionally physical retailers Target and Walmart to successfully pivot when the marketplace changed. Rather than treat their IT departments as cost centers, Target and Walmart—and other forward-thinking retailers—use APIs to create new, digital customer services and experiences. This repositioning turns their IT into not only a differentiator but a competitive advantage; while other bricks-and-mortar are still struggling to recover, API-powered companies thrive.

Changes in consumer sentiment aren't the only reason entire industries seek to grow their API usage. Regulation is inducing some industries, like healthcare and banking, to offer standardized APIs. APIs are used within the automotive sector to embed efficiency data, driving statistics, route information, and real-time alerts into dashboards. Other sectors, like telecommunications, are prompted by industry interoperability needs.

APIs allow developers to utilize a broader array of datasets and off-the-shelf functionality. Even when used internally, APIs connect otherwise disconnected and siloed apps like CRM, ERP, finance, communication, and marketing platforms—which collectively are the lifeblood of many businesses—into a coherent whole. These activities can be orchestrated and optimized with APIs.

A massive API opportunity

Despite these advantages, the number of companies with mature API programs remains small. Many organizations have fewer than a dozen APIs, instead of the hundreds that are often needed to properly capture, leverage, and evolve existing value propositions. Even among those companies that do have a large number of APIs, many lack an articulated API strategy, are unclear about the potential of APIs, and remain uncertain about how to implement an API program that maximizes consumer and business impact.

The good news is that the tooling for designing great API experiences, instituting the necessary governance, and driving discovery is far more advanced today than it was a decade ago. Instead of writing APIs from scratch, companies can leverage API networks that provide discoverability for existing APIs and an API platform that supports and automates critical points of the API lifecycle. With this modern tooling as the foundation, companies can create resilient, adaptable architectures for revenue growth and value through APIs.