THREATX

API [In] Security: The Consumer Perspective

Survey Report

Background

APIs are the foundation of the Internet. Nearly every modern software application, including the inner workings of that mobile device that never leaves your side, uses—or is—an API. As companies expand digital transformation initiatives, APIs enable development teams to integrate data from external sources and deliver new services and capabilities rapidly, requiring little to no downtime for consumers.

Whether consumers realize it or not, APIs power their connectivity on a daily—if not hourly—basis. Using the Dunkin Donuts app to mobile order your coffee so you don't have to wait in line? Using the PayPal app to make a purchase on Nike's website? APIs enable these transactions. Searching for the best deals on a flight via a central travel booking site? APIs connect Kayak with American Airlines, Delta, United Airlines, and others. Using a Facebook, Twitter, LinkedIn, or Google username and password to log in to a new app or website? Once again, you can thank APIs.

APIs connect consumers to businesses and businesses to one another while also acting as an enabler that allows brands to deploy cross-service capabilities.
In short, APIs power the digital experiences of consumers today.

As API use increases, so do security risks. APIs are easy to deploy, but hard to control. Application developers may—with best intentions—provide new APIs without going through the expected security review. The rapid proliferation of APIs has far surpassed security's ability to protect these assets and they have quickly become the attack vector of choice for threat actors who exploit insecure APIs for malicious purposes. This trend is sure to continue with Gartner predicting that APIs will be the primary attack vector in 2022.

Executive Summary

With API use—and its associated risk—increasing, the result is a steady stream of "data breach" headlines. Lack of API security is often the culprit. In 2021, APIs were exploited in breaches that impacted Amazon's Twitch, Facebook, Instagram, LinkedIn, Peloton, and T-Mobile, among others.

ThreatX conducted the API [In] Security: The Consumer Perspective survey to understand the potential impact of API security, or lack thereof, on the consumer experience.

The results of this survey indicate:

1. Businesses are increasing the use of APIs as they accelerate digital transformation and enable new services, as well as forge paths for innovation and growth, including partnerships.

2. Consumers appreciate the ease and convenience afforded by APIs, and do not heavily scrutinize requests to share data between apps. However, these same consumers report understanding the potential impact of insecure APIs and that sharing data between applications can put personal data at risk.

3. Despite the growing number of data breaches, consumers remain hesitant to ditch their brands, especially those that play a prominent role in their day-to-day lives. That being said, consumers do not feel brands do enough to protect their personal information and would pay more for a product that is marketed as "secure."

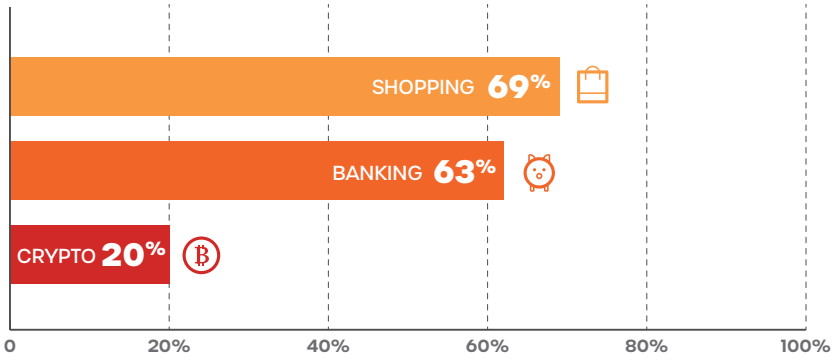
4. Brands would be wise to build security into their applications.

APIs, Security, and Consumers

How do consumers interact with APIs via their web and mobile applications?

Consumers use mobile or web applications for financial transactions and online shopping — experiences that often engage APIs, particularly in the context of mobile transactions:

In the last 30 days, which of the following services have you used a mobile application or website for? *(select all that apply)*



Additionally, consumers engage with businesses and transact information through many other mobile and web applications:

- **70%** use messaging apps
- **66%** use social media apps
- **54%** use gaming apps
- **41%** use health services apps
- **34%** use fitness apps

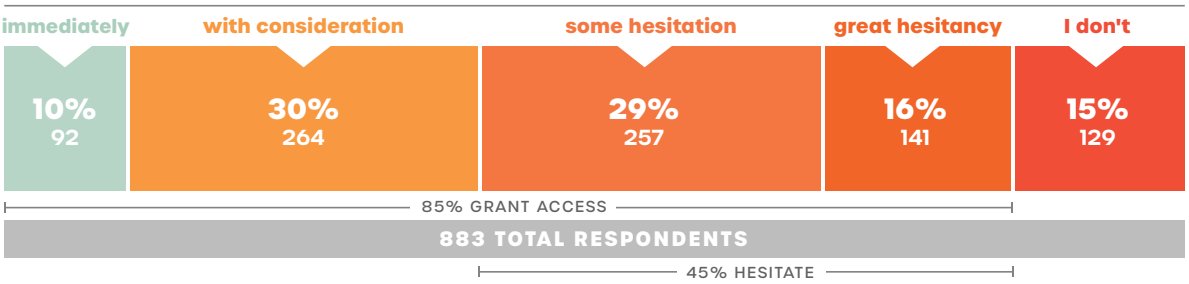
Many of these mobile apps and IoT services are enabled through APIs and the increased connectivity they provide between services. Every transaction (financial or other) routes through APIs, the security of which must be maintained by the brand, and if it is not, increases the probability of an attack resulting in a data breach.

Consumers Rely on APIs for Integration

Consumers take full advantage of the ease of use and convenience afforded by APIs that help them utilize cross-service capabilities. Take, for example, integrating OpenTable with iCalendar, Google Drive with Slack, or Ally Bank with Vanguard.

85% of respondents grant access *for applications to connect with one another and share data.*

How readily do you grant access for applications to connect with one another?
For example: Zoom requesting access to Google Calendar, or Spotify requesting access to Facebook.



Yet, consumers clearly understand that doing so opens their personal identifiable information (PII) at risk.

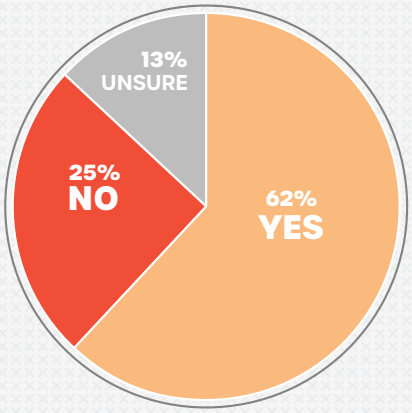
- **91% of respondents** understand that by connecting applications, it means that data is shared between them; this is often enabled through APIs. The result of this API connectivity means a consumer's data proliferates across a broader number of applications, effectively increasing an individual's attack surface.

It is with this in mind that ***45% of respondents hesitate*** *before granting access between applications.*

Business Engagement Is on the Rise

Businesses take advantage of the consumer's desire for convenience too, and leverage APIs to connect to other value-added services.

- **62% of respondents** experienced an increase in business engagement via website or mobile app. *In this instance, consider telehealth visits connected to medical payment systems, or incentivization and rewards programs associated with e-commerce retailers.*



In the last 24 months, have you experienced an increase in businesses engaging with you via websites or mobile applications? (ex: doctors offices, school, vendors)?

However, such an increase in engagement requires that consumers transmit more PII. And, every time a business engages with consumers via a web or mobile application, APIs are likely right there—making it possible—and sending data back for billing, or record keeping purposes.

- **86% transmit PII** through a website or mobile application at least once a month
- **58% transmit personal data daily or weekly**

The Dark Side of APIs

While convenience and ease of use are huge benefits of APIs, consumers, as well as businesses, should consider the associated risk.

> *Despite high-profile API breaches that occurred in 2021, **41% of respondents were unsure of the brands** involved in these events. This tells us that, as an industry, our education efforts on the dangers posed by vulnerable APIs needs to increase.*

Even if consumers are unsure of the brands that have undergone recent breaches, and let's face it, there are so many it's hard to keep track, the way consumers respond to a breach changes based on what personal data is affected.

- When asked how they would respond after their brand of choice experiences a data breach, **only 13% of respondents reported that they would stop using the brand.**
- In contrast, **56% of consumers report that they change their login credentials** for accounts associated with the brand following a breach.

Most consumers would choose to keep the convenience of APIs and take only a small step to improve security by changing their credentials.

However, consumers broadly reported that if the following PII was stolen from a brand in a breach, they would stop working with that brand altogether:

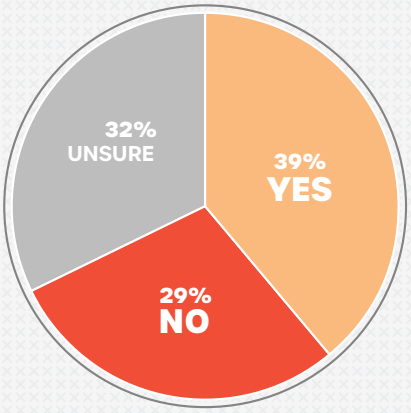
- Banking information *(72% reported that loss of this would cause them to leave a brand)*
- Social Security number *(68%)*
- Credit card number *(64%)*

In contrast, respondents seemed unconcerned with the loss of:

- Fitness data *(only 7% reported that stealing this would cause them to leave the brand)*
- Photos *(27%)*
- Personal communications *(33%)*
- Home address *(36%)*

Do consumers trust that brands have their best interest at heart?

- **61% of respondents** do not feel confident that brands prioritize building security into their APIs and associated applications. When asked if brands prioritize the security of their PII, 64% of respondents reported "no" or "not sure."



Do you believe brands prioritize building security into their applications?

Additionally, after hearing about a data breach, **26% of respondents** assume that a brand did everything in their power to protect against an attack. And, **74% of respondents** reported that they either have "minimal" or "no" influence to encourage brands to take their security more seriously, which may signal a resignation among consumers that data breaches are inevitable.

This should be a disheartening wake-up call for brands. As more and more technological advancements rely on the APIs that support web and mobile applications, the lack of protection felt by consumers, and the predicted increase of data breaches, will likely sow more discontent.

Will security efforts pay off for brands?

YES. Brands would be wise to build security into their applications, which requires both secure development processes and protection solutions in place.

- **65% of respondents** would consider paying more for an application or tech that was marketed as "secure."
- **Only 30% of respondents** reported that if a mobile, web application, or piece of technology they purchased was down once per week for updates they would leave the brand.

So, go ahead! Take your best first step towards building API security in depth today.

Organizations are often focused primarily on building the next great piece of code—to remain competitive in challenging markets—and building in security can seem like a hindrance, or a "nice to have" rather than a necessity. In addition, many lose focus when it comes to sunsetting and deprecating API endpoints. These unused and vulnerable APIs—some are spun up without authorization ("rogue"), others sit in production long after their useful life expires ("zombie")—can leave organizations with exposed endpoints that attackers can exploit to wreak havoc on consumers and their personal data.

The data shows that security may actually be a differentiator for brands rather than a hindrance. Investing more time and money into developing a robust security program could be the difference between a confident and brand-loyal consumer, and one that will move on to the next application or piece of software after one too many breaches.

DEMOGRAPHICS

This survey was conducted in December 2021 and included 883 respondents from the United States. The participants were representative of the general population, diverse in their household incomes, and what they use web and mobile applications for. Responses were narrowed down to participants between the ages of 18-70.