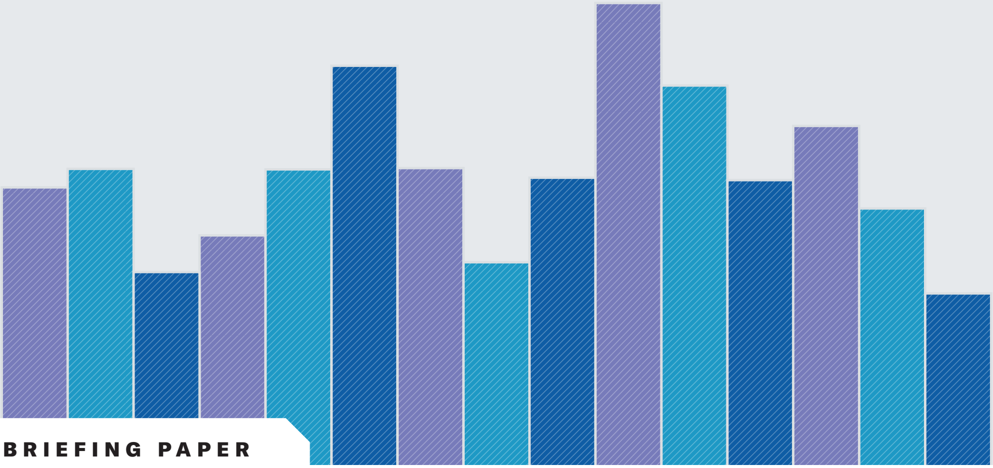
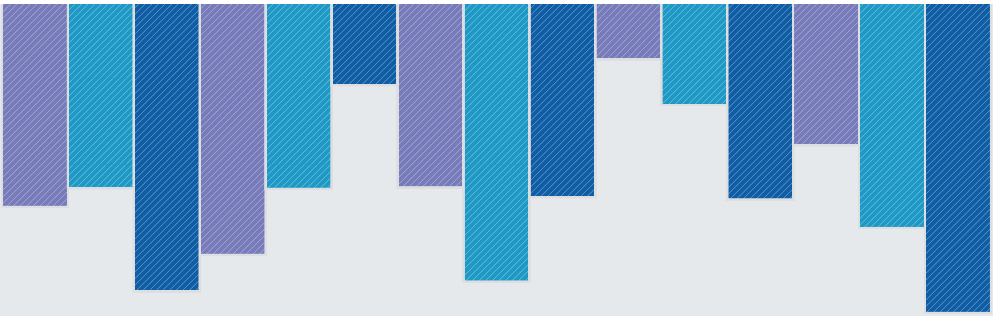
Harvard Business Review
ANALYTIC SERVICES



BRIEFING PAPER

Preventing Data Breaches in 2020

Secure APIs to Protect Data, Bolster Trust, and Gain a Competitive Edge



Sponsored by

datatheorem

In March 2020, one company experienced a significant data security and privacy breach. In a two-week span, this particular company lost more than $12 billion in market capitalization, was served with over a dozen class action lawsuits, and suffered brand damage worldwide that likely will have ramifications in their future. This company simultaneously was experiencing unprecedented growth due to the need for more collaboration and videoconferencing software during the Covid-19 pandemic response. This company is called Zoom.

One of several important lessons we can learn from Zoom is that there are high costs and penalties when an organization underestimates the need for a comprehensive application security (AppSec) and data privacy program. Another lesson is that it is possible to reverse the security misfortunes of a business just as Zoom has by investing in a more comprehensive way to protect the data and privacy of their users as they move forward.

Building and securing applications is a challenging task, especially when the goal of most development teams is to create new features, improve performance, and ensure availability. Security is often an afterthought. Security can be a competitive advantage but historically has been treated as a necessary cost center by many business leaders. Companies rarely can attract and retain enough cybersecurity talent to create a sustainable advantage in this ever-changing area of technology. However, that should not be the main goal for most companies. Instead, companies should invest in an AppSec security program that can keep pace with the speed of their application development teams using agile methodologies. The need to automate security at the pace of DevOps is one of the important lessons we are learning from these recent data breaches. Security has to keep up with the apps. In general, security has fallen short in this area, and our industry has the data breach headlines to prove it.

Further, hackers are always finding new ways to steal valuable data. Leveraging automated hacking tools to continuously find and exploit vulnerabilities is another practical technique that the best teams employ to discover AppSec weaknesses, strengthen application resiliency, and harden data protection efforts.

Organizations of all sizes are utilizing technology to stay connected and informed like never before. Businesses are building and utilizing applications more than ever to remotely work and collaborate to overcome the physical separation required during these unique times. The massive amounts of data that are being collected and transported by these applications are as essential as ever. Yet, the vast majority of companies do not have enough security skills and software tools to oversee all of their liabilities for application security and data privacy.
We hope this Harvard Business Review Analytic Services report, “Preventing Data Breaches,” will both inform and encourage more leaders to invest in sustainable security programs that proactively protect their data, applications, and underlying application programming interfaces (APIs) and cloud services in order to protect themselves and their customers.

Doug Dooley
Chief Operating Officer
Data Theorem

Preventing Data Breaches in 2020

Secure APIs to Protect Data, Bolster Trust, and Gain a Competitive Edge

The enormous rise in the collection and sharing of data has enabled a number of modern capabilities. From surfacing real-time, customized product recommendations to anticipating needs and requests with personalized virtualized assistants, data insights continue to drive business and spur innovation. While technologies like machine learning and the internet of things all produce massive tides of data, application programming interfaces (APIs) act as the connective tissue that allows the extraction of that value. Subsequently, enterprise growth demands the use of APIs as the development vehicle for cloud technologies.

"The business at the heart of the enterprise is data, and APIs are how you access that data," says Kathleen Moriarty, security innovations principal in the office of the chief technology officer at Dell EMC and former two-term security area director for the Internet Engineering Task Force.

Despite the innovations and insights APIs can provide, a simple oversight in security means that data once thought private can be accessed by bad actors or even curious members of the public. When pathways to private data are breached, not only do companies lose the trust of their customers, which can result in stock losses and decreased revenue, but also a company's API security oversight could result in hundreds of thousands of dollars in fines and even a court summons.

No organization is immune from data breaches, but increasingly, businesses face growing risks while failing to secure what will become one of the most frequent attack vectors in coming years—the API. The very principle that makes data sharing so powerful carries serious risks, and the same convenience

HIGHLIGHTS

Application programming interfaces (APIs) are quickly **becoming one of the most frequent attack vectors**, leading to data breaches across geography and industries that cost companies time, money, reputation, and customers.

When seeking to secure APIs, chief information security officers should **implement continuous monitoring and automated security solutions,** avoiding outdated tools like web application firewalls (WAFs) and point-of-attack remedies that can leave unknown critical vulnerabilities open to attack.

By adopting continuous-monitoring API security tools, companies can **gain the 24/7 insight into API behavior that is required to maintain modern API security** in an automated, repeatable, and scalable way.

The surface attack area for an API can include web applications, mobile applications, and cloud applications like cloud storage.

that allows companies to gain competitive advantages with their unique data insights can create massive security gaps, as APIs are quickly becoming targets for exposing and exploiting sensitive security vulnerabilities. Waiting until after a breach to implement a modern API security strategy can allow valuable data to leak for weeks or even months after a breach occurs. Similarly, resting on the false security of application firewalls or the work of temporary teams hired to fix security issues manually can be just as detrimental.

To mitigate API risks, security and business leaders must establish a dynamic security cycle of discovery, threat analysis, and prevention before a breach has occurred. Businesses that are proactive in securing mobile, web, and cloud services will have a stronger security posture than those that react with temporary security solutions after an API breach.

This Harvard Business Review Analytic Services paper will examine the evolution of security risks and challenges associated with APIs, explore recent API data breaches and how organizations respond, and provide best practices for safeguarding data through modern API security. Organizations should integrate automated security into their software development lifecycle and adopt continuous and automated monitoring before a breach occurs in order to ensure that their data remains private and controlled.

The Value and Risks of APIs

Across industries, data is a competitive differentiator. APIs allow companies to leverage both internal and external data to enhance products, services, and ultimately the customer experience. It is, therefore, unsurprising that their use has grown tremendously over the past decade and that the rate of adoption continues to accelerate. "APIs are quickly becoming the way that applications are being built," says Chris Porter, vice president and chief information security officer (CISO) at Fannie Mae. "It's so much faster for developers to build, to create business value, when there are APIs and microservices to build on top of."

APIs have created more opportunities and opened new doors for developers, and their growth is reflected in modern app infrastructure. "Architectures themselves are very different in how they're being built today versus how they were built in the past," adds Porter. "In the past, they were built more on OS-layer [operating system] access or client agents, whereas today it's more about API access. There are different levels of authentication or encryption, and you may or may not have API gateways."

But while modern APIs help enable DevOps teams to move and create with increasing speed, security teams sometimes struggle to keep up. Security strategies like the use of WAFs have been traditionally popular within the enterprise, but these security measures increasingly fall short as APIs dynamically evolve. By 2021, Gartner predicts that 90% of web-enabled applications will have more surface area for attack in the form of exposed APIs, an increase from 40% in 2019. By 2022, APIs will be the most frequent attack vector, resulting in data breaches that have the potential to expose billions of records.[1]

"One of the reasons why API security is so complex is that we're building modern experiences and applications that call data from lots of different sources," says Maribel Lopez, technology industry analyst and strategic advisor at Lopez Research. Dynamically securing these interfaces for all data sources is critical to securing the API.

"It's different than the dynamic content you've had in the past," says Porter. "Now you're clicking on a link and it's reaching out via API to grab data and show it on a screen in a certain way. As legacy applications are moving to a newer space, we have to protect all of that surface attack area." These evolving content mechanisms come with a price, however; there are more attack surfaces for CISOs to protect than ever before.

API Weaknesses and Data Breach Ramifications

For businesses from McDonald's to T-Mobile, leaky APIs are already a common cause of security breaches, and they are occurring regardless of business vertical, size, or location, says Porter. Accepting—and then securing—the vulnerabilities in APIs is a necessary task for CISOs. "From the CISO's perspective, using an API is a necessary risk if the company is going to do business online or electronically," says Dell EMC's Moriarty.

The surface attack area for an API can include web applications, mobile applications, and cloud applications like cloud storage. According to the 2019 Verizon Data Breach Investigations Report, the retail sector, for instance, experienced the majority of its data breaches via web apps.

API breaches are detrimental to both the business and the customer, as they expose personal information like

“We’re living in a data-driven world, and the ability to access and manipulate data is extremely powerful right now,” says Kathleen Moriarty at Dell EMC.

date of birth, credit card numbers, Social Security numbers, bank accounts, names, emails, photos, and even biometric identifiers like heart rates. In November 2018, for instance, an authentication weakness in a U.S. Postal Service (USPS) API leaked over 60 million user records, including street addresses, phone numbers, and mailing campaign data.[2] The unsecured API allowed virtually anyone to access and even modify records in the USPS’s extensive database.[3]

What’s worse, oftentimes CISOs don’t discover a hack until data has already been stolen. For example, in early 2020, Twitter discovered that accounts had been mined for information for months after a feature that allowed people to find friends by their phone numbers was hacked via a weak API endpoint.[4] Similarly, in 2019, 30 million authentication tokens as well as personally identifiable information (PII) were stolen from Facebook through an unsecured API that had been open for more than 20 months.[5] A whopping 200 million-plus Venmo transactions were compromised that same year via an API that allowed the mass scraping of data, which included full names and the memos attached to transactions.[6] This API was made available to the public, meaning anyone with a bit of coding knowledge could tap into a trove of private data.

In so many of these cases, the failure to secure API endpoints caused significant data breaches that affected millions of users. “We’re living in a data-driven world, and the ability to access and manipulate data is extremely powerful right now,” says Moriarty.

Data breaches can have long-lasting effects on both the company that experienced the breach and the customers whose data and privacy were exposed. “For consumers, [a breach] could result in identity theft that involves long and costly efforts to resolve with financial and other impacts,” says Moriarty. Financial loss is among the most common consequences for companies and is often accompanied by a loss of trust, damage to reputation, operational disruption, and potentially legal summonses and class action lawsuits, as failing to secure customer PII can be in violation of state, federal, and international laws.

For some companies, location-specific data regulations like the California Consumer Privacy Act and Europe’s General Data Protection Regulation (GDPR) can exacerbate the damage of a data leak by enforcing strong accountability measures with often significant financial ramifications. For example, under the GDPR, businesses face fines up to 20 million euros, or up to 4% of the annual worldwide turnover of the preceding financial year, if a data breach is not found and disclosed within 72 hours.[7]

API Security Strategies

Gartner reports a 30% year-over-year increase in client inquiries regarding API security, and in a recent survey conducted by ESG Global, 92% of respondents said their enterprises are concerned about losing data through insecure

“Even if you don’t know where everything is today, what you need to do is define what acceptable behavior looks like and make sure that only acceptable behavior is happening.”

Maribel Lopez, technology industry analyst and strategic advisor at Lopez Research

APIs.[8] But for many organizations, enterprise API security remains largely underserved and under-resourced.

A data breach can be a tipping point for businesses to reexamine their strategies and rebuild a robust framework for modern security. However, when faced with a data breach, many companies are so focused on securing the leak and responding to consumers and shareholders that longer-term vulnerabilities are neglected.

Hiring a third-party consulting firm to manually fix the leaky API is a frequently used strategy, though it tends to be more of a “security Band-Aid” than a holistic solution to an enduring threat. While the current breach may be resolved by hiring a cleanup crew, the broader issue of API security must be addressed, as point-in-time fixes do not prepare against other unattended risks, nor do they provide solutions that improve API security on an ongoing basis.

“In the original set of application development, we were a little more sensitive to security risks,” says Lopez. Now, she adds, “there are so many types of security attacks that API attacks can be pretty low on the list, but the things that you least expect are the things that trip you up.”

Similarly, relying on outdated security methods like WAFs can produce a false sense of security. WAFs work by detecting and filtering out threats that have the potential to compromise or expose data by examining HTTP, or hypertext transfer protocol, traffic before it reaches the application server. While WAFs are a staple security measure for compliance, the reality is that they struggle to cope with today’s highly distributed computing environments.

According to the Ponemon Institute, a research organization that conducts independent research on privacy, data protection, and information security policy, 65% of respondents say attacks are bypassing the WAF. Further, only 9% of the survey respondents indicate that their WAFs have never been breached. Because the architectural design of the WAFs is a perimeter-centric defense and because they are focused on exploit-based attacks, the WAF actually provides very low effective coverage of common modern risks such as API-centric vulnerabilities.

Traditional API security tools like the WAF are quickly becoming outdated, and businesses should instead look to modern systems of continuous monitoring and security to protect today’s 24/7 data flows. Modern tools employ analyzers and scanners that use machine learning techniques to create dynamic security frameworks and monitoring solutions that match the speed of contemporary sharing rather than relying on a standard set of provisional rules. These analyzers will often provide remediation guidelines or even auto-remediation techniques to immediately fix problems found in the configuration and software stack that support the API service.

“A continuous-monitoring framework enables the quick detection of any variation from expected security controls,” says Moriarty. “If you’re continuously monitoring any set of controls, you have expected policies those controls would meet. If they fall out of compliance, you would know quickly and be able to implement risk-based decision making according to business requirements.”

Defining responsibility for the API landscape and auto-inventory is important to enforcing policies across company divisions.

Continuous API Security: The Path Forward

To mitigate API security risks and develop a continuous monitoring security strategy, companies should start by auto-discovery and mapping of APIs at their organization. APIs cross many divisions within a company—not all of which are security-focused—and this can create security gaps and blind spots for CISOs. Defining responsibility for the API landscape and auto-inventory is important to enforcing policies across company divisions.

“Even if you don’t know where everything is today, what you need to do is define what acceptable behavior looks like and make sure that only acceptable behavior is happening,” says Lopez. Developing a full API visibility strategy must include the surfacing of “shadow APIs,” or APIs that have not been sanctioned by IT or security teams.

Subsequently, business leaders can initiate an API security compliance framework and feedback loop between DevOps and security teams and implement an ongoing system of continuous API monitoring to prevent future attacks.

“Security teams may help to provide the resources and knowledge across development teams,” says Moriarty. “This could include setting policies and guidelines on transport encryption, authentication, authorization, and access controls to secure coding practices to integrate into DevOps processes.”

Continuous security testing throughout development can help businesses avoid API breaches and subsequent data leaks as well as save much-needed development time. Implementing continuous monitoring methods can help businesses maintain API security in an automated, repeatable, and scalable way.

It is imperative that CISOs be aware of all API endpoints and gateways and remain vigilant about securing them, particularly via mobile, web, and cloud applications.

Other steps organizations can take include finding a security vendor to help with the ever-evolving process of API security. "Having a good partner who can make sure you get it right for your environment is super important," says Fannie Mae CISO Porter. Baking security into the heart of an organization's culture can help strengthen security measures, too. "Define what security is, and have everyone be responsible for it," says Lopez.

As CISOs and business leaders work toward developing a robust and secure API strategy at their organizations, they should consider the following:

API security risks are constantly evolving.

Data is passing through more doors than ever before. It is imperative that CISOs be aware of all API endpoints and gateways and remain vigilant about securing them, particularly via mobile, web, and cloud applications. Traditional security strategies like WAFs can lull enterprises into a dangerous false sense of security.

Short-term solutions are long-term problems.

Hiring in-house help or consultants to "fix" a problem after a data breach occurs does not mean the organization is secure. On the contrary, security Band-Aids may cause loss of time, revenue, and customers down the line. Strong organizational security is a complex and continually evolving strategy that is crucial to customer trust and business survival—not a temporary reaction to a data breach.

Security is a 24/7 job.

Fixing one leak doesn't mean data is secure. Implement an ongoing system of continuous API monitoring for 24/7 coverage, fastest time to operations, and minimal complexity. Building a continuous API security program that remains effective and resilient even after people move on to other priorities and projects should be the primary focus for enterprise-grade API security.

Conclusion

APIs will continue to be instrumental in spurring local and global business growth in the coming years, and businesses must take steps to fiercely protect them as they transmit sensitive and often private data.

Businesses can manage the risk of data leaks through continuous monitoring and an automated security solution and by eschewing temporary solutions after a breach. Organizations must recognize the limitations of traditional security tools like WAFs while embracing more contemporary solutions that take advantage of analyzers and scanners, which employ auto-remediation techniques to combat dynamic threats. "Companies can establish security guidelines for API use that include protection of the endpoints, transport of data, access controls, relying on strong authentication and authorization, as well as data input validation," says Moriarty. "But if you miss any one of those," she cautions, "attackers will seek out the weak point."

Embarking on the creation of a continuous API security framework is only the beginning, and maintaining API security must remain a prioritized and ongoing task. "Though API security risks are clearly an area of concern, we know how to mitigate those risks," Moriarty says. "It's just a matter of creating practices and setting policies—and educating on those policies—to improve our collective security standards."

API security ultimately starts with making sure the endpoints and gateways are always guarded. "An API is a doorway to your data," says Lopez. "The very nature of that is that it's slightly open. It's designed to be open enough that you can send things through it and get something out of it. Whenever you open up a doorway, it's a vulnerability."

Endnotes

[1] Mark O’Neill, Dionisio Zumerle, and Jeremy D’Hoinne, “API Security: What You Need to Do to Protect Your APIs,” Gartner, August 28, 2019, https://www.gartner.com/doc/reprints?id=1-1OH7K9NT&ct=190910&st=sb.

[2] Liao, Shannon, “USPS took a year to fix a vulnerability that exposed all 60 million users’ data,” November 22, 2018, The Verge, https://www.theverge.com/2018/11/22/18107945/usps-postal-service-data-vulnerability-security-patch-60-million-users.

[3] Muncaster, Phil, “US Postal Service Exposes 60 Million Users in API Snafu,” November 22, 2018, Infosecurity Magazine, https://www.infosecurity-magazine.com/news/us-postal-service-exposes-60m/.

[4] Twitter Privacy Center, “An Incident Impacting your Account Identity,” February 3, 2020, https://privacy.twitter.com/en/blog/2020/an-incident-impacting-your-account-identity.

[5] Cheng, Lebin, “Three API security risks in the wake of the Facebook breach,” February 17, 2020, Help Net Security, https://www.helpnetsecurity.com/2020/02/17/api-security-facebook-breach/.

[6] Robles, Patricio, “The Venmo API is Still Making Millions of User Transactions Available to the Public,” June 20, 2019, ProgrammableWeb, https://www.programmableweb.com/news/venmo-api-still-making-millions-user-transactions-available-to-public/brief/2019/06/20.

[7] GDPR.eu, “What are the GDPR fines?” https://gdpr.eu/fines/.

[8] Cahill, Doug, “Cybersecurity Predictions for 2020,” ESG, December 1, 2019, https://www.esg-global.com/research/esg-brief-cybersecurity-predictions-for-2020.

Harvard Business Review
ANALYTIC SERVICES

ABOUT US

Harvard Business Review Analytic Services is an independent commercial research unit within Harvard Business Review Group, conducting research on and comparative analysis of important management challenges and emerging business opportunities. Seeking to provide business intelligence and peer-group insight, each report is published based on the findings of original quantitative and/or qualitative research and analysis. Quantitative surveys are conducted with the HBR Advisory Council, HBR's global research panel, and qualitative research is conducted with senior business executives and subject-matter experts from within and beyond the Harvard Business Review author community. Email us at hbranalyticservices@hbr.org.

hbr.org/hbr-analytic-services