SALT

How Protecting Your APIs Protects Your Bottom Line

Get Smarter

Table of Contents

Introduction

API attacks have dominated the cybersecurity news cycle lately. In early 2022, T-Mobile made news for an API-based breach of 37 million PII records of its past and present customers. And later that year, Optus, a major telecommunications company in Australia, experienced an API security incident that exposed around 10 million customer records. And API attacks that aren't quite as ”newsworthy” happen every single day. In fact, the Salt Q3 2022 State of API Security Report showed that 94% of survey respondents had experienced API security problems in production, with 19% admitting to an API-related breach.

The Gartner prediction that “by 2022, API abuses will move from an infrequent to the most-frequent attack vector, resulting in data breaches for enterprise web applications” has certainly come true.

Securing APIs is no longer a luxury, but it also shouldn’t be seen just as a burden. The reality is, protecting your APIs offers real business benefits - in risk reduction, expense mitigation, and revenue growth opportunities. Here we explore some of these bottom-line gains that security and development leaders can point to as the benefits of investing in API security.

Reduce risk and introduce controls

Today's security leaders are constantly seeking to close security control gaps and ultimately reduce their risk. APIs have emerged as a predominant business enabler, and they increasingly provide unprecedented access throughout business systems, so it's become crucial to protect them.

But how do you put a financial metric around risk reduction? One calculation we often utilize to consider the cost of API risk is:

Breach Likelihood (%) X Breach Impact ($) = Breach Risk ($)

Each customer's scenario is unique, but if we factor in industry-standard statistics, the "industry" API risk calculation is:

19% X $9.4M = $1.786M

(Salt Security Q3 2022 State of API Security survey respondents who have experienced an API related security breach over the past year)

(Average Cost of a Data Breach report by IBM, 2022)

If you need to compare risk vs. investment value, you would simply divide your breach risk by the cost of your solution. An organization spending $300K on API security would enjoy a 6x ROI, for example. The cost/benefit math is almost always eye-opening and supports the business case for API security.

SALT

Eliminate API blind spots and control gaps

What you don't know can hurt you. An accurate view of your attack surface is essential to informing your security strategy, but understanding your attack surface is especially challenging with APIs, in part because they're constantly changing. In fact, a recent Salt Security survey found that 11% of respondents update their APIs daily, and 31% update them weekly.

Before keeping up with the changes, you first need to know about all of the APIs in your environment, including unknown (shadow) and outdated (zombie) APIs that should have long since been deprecated. Because APIs are being continually released and updated - and developers aren't always great about informing security teams - you need automatic discovery of new and changed APIs, including customer-facing, partner-facing (provided and consumed), third-party, and internal APIs.

But knowing an API exists is not enough. You need to know about each API at a granular level – understanding its intended functionality, assessing its risk, and determining if it exposes sensitive data such as personally identifiable information (PII). Automatic and continuous discovery helps ensure that your view of the attack surface and sensitive data exposure is comprehensive and remains up to date.

Only by knowing all of the APIs in your environment and what information they expose can you understand your true risk and begin to close control gaps.

40%-800%

The percentage of previously unknown, undocumented APIs that Salt typically uncovers in a new customer environment.

Ensure you are aware of all the APIs in your environment

Understand any personally identifiable (PII) or otherwise sensitive information that is transferred during these API calls

Make sure these insights stay accurate automatically and continuously, even as APIs get added or changed

SALT

Eliminate API blind spots and control gaps

Questions to ask yourself

- **Are you confident you know all of the APIs in your environment?** (hint: according to the Salt Security Q3 2022 State of API Security, only 14% said were very confident that their API inventory was complete)
- **What would it cost your organization if your customers' PII data were stolen?** (hint: according to the 2021 IBM Cost of a Data Breach report, organizations lose $180 per lost or stolen PII record)
- **How would your C-suite and board of directors react if your organization suffered a breach because of an unknown or unprotected API?**
- **How much peace of mind would having a complete and accurate API inventory give you?**
- **Do you know how many APIs you have?**
- **Do you know which APIs handle sensitive data?**
- **If someone were tampering or trying to abuse your APIs, would you be able to detect this behavior and block it?**

Stories from Salt Customers

Insurance Industry Review on Gartner Peer Insights

5.0

Sep. 8, 2022

"Like a lot of companies, our company has increased its usage of APIs. Our CISO understood that we needed to get ahead of potential risk by adopting an API security solution that could protect our assets."

– Application Security Analyst in the Insurance Industry

XOLV Technology Solutions

"One of the solutions we considered needed our documentation of our APIs and endpoints, but that's part of the problem. We're sure we don't know about all our APIs... Now that we have Salt, we've got a solid idea of what's out there, and we're protected in runtime."

– Jason Weitzman, Senior Security Engineer

DEIN DEAL

"Once we deployed the Salt platform, we were surprised to discover a lot of old APIs still running. We also discovered some routes for calling those APIs that were not alive anymore."

– Alexandre Branquart, Chief Technology Officer

SALT

Uncover malicious API activity to decrease the potential of a major security breach

There is no way around it – study after study shows that security breaches cost millions. And with APIs being the most frequent attack vector for application attacks according to Gartner, it simply makes financial sense to do everything you can to protect your production APIs during runtime.

Unlike when they launch more traditional attacks, bad actors targeting APIs use far more subtle methods to uncover and exploit vulnerabilities. They're looking for business logic flaws they can exploit to access data they should not be able to get. For example, attackers often obtain access to an API – in many cases using valid credentials they've established – and then manipulate elements of an API request to find a logic gap and exploit it to abuse an API or gain unauthorized access to systems or data.

Hackers have to do a lot of experimentation to find these business logic flaws, so this reconnaissance activity can take days and weeks. And the API manipulations used during recon are often subtle, so you need sophisticated – and accurate – anomaly detection to spot them. Combining big data with AI and ML will enable you to capture and baseline all API traffic and spot these deviations. Given the duration of API attacks, you need to apply cloud-scale big data to this problem, so that you have enough context over time to find these attackers.

$9.44 in the US
$4.35M globally

The average cost of a data breach

2022 Cost of a Data Breach, IBM

Protect the most frequently attacked element in your environment – your APIs

Recognize and thwart API business logic attacks, attack types your traditional tools like WAFs and API gateways are not built to identify

Tap cloud-scale big data and advanced ML/AI to provide the context needed to uncover "low and slow" attacks over time

SALT

Uncover malicious API activity to decrease the potential of a major security breach

Questions to ask yourself

- **Are attackers actively probing your APIs for weaknesses?**
  (hint: according to the Salt Security Q3 2022 State of API Security report, malicious traffic currently accounts for 2.1% of all API traffic)
- **Have your applications been breached via an API attack? How would you know?**
- **What would you estimate the cost of a breach to be at your organization?**
- **What would happen to you and your team if an API attack led to a major breach?**
- **Can you automatically and confidently block malicious API traffic?**
- **Can you distinguish between good and bad API activity? Would you recognize malicious behavior if it were to slowly and methodically take place over weeks and months?**

Stories from Salt Customers

BerkshireBank

"Salt Security makes it easy for us to mitigate the risk of API-based exposure when storing and sharing information online about our customers' financial data."

– Ryan Melle, CISO

navan
Formerly TripActions

"We're moving fast and our APIs are changing all the time, so we count on Salt to understand our users' baseline activity and adjust the baseline as we evolve."

– Tarik Ghbeish, Product Security Engineer

FINASTRA

"After evaluating multiple API security platforms, we found that only Salt Security had an architecture that could deploy in any of our environments, identify all our APIs, and recognize and block attackers before they could do any damage."

– Nir Valtman, Head of Product and Data Security

SALT

Reduce the potential of future API attacks and the resulting application downtime

Security leaders fear many things, but top on the list are security breaches and resulting downtime (and the certain fallout resulting from both of these). Attacks cost millions, but downtime costs also add up quickly.

Organizations are in a constant battle to stay ahead of the bad guys. API security solutions must analyze APIs to identify gaps before an attacker finds them and enable developers to proactively eliminate potential vulnerabilities while simultaneously sharpening their API security best practices.

After you've stopped the "bleeding" by delivering runtime protection of APIs already in production, it's time to eliminate future gaps. DevOps teams play an essential role in security. Despite everyone's best efforts, no one can write perfect code, so software releases have security gaps. APIs are no different. Agile development practices and tight release cycles mean that stretched-thin development teams are constantly under pressure to meet tight schedules. APIs have the added challenge that most of the exploits against them cannot be identified in pre-prod testing.

So runtime security provides your most critical protection, but you always want to improve the security posture of your code, so you want your dev teams to identify and eliminate gaps. Today's leading API security solutions can block fraudsters and learn from their reconnaissance activities to provide insights into the vulnerabilities unique to a given API and remediation details to eliminate those gaps quickly.

$300,000/hour

The average cost of downtime of hardware and critical applications

2022 Hourly Cost of Downtime Survey, ITIC

Take preventative measures to prevent API attacks that can lead to costly downtime of apps and services

Find and fix business logic vulnerabilities as early in the API development lifecycle as possible

Learn from security insights gained during runtime to harden your existing APIs and build more secure APIs in the future

SALT

Reduce the potential of future API attacks and the resulting application downtime

Questions to ask yourself

- **What would you estimate the cost of downtime to be at your organization?**
- **What application outages would be disastrous to your organization? Which would be ok?**
- **What would you do if an API attack caused one of those applications to go down? How long would it take before your business was irreparably harmed?**
- **What would happen if your board realized you could have implemented a solution to prevent this issue but prioritized something else instead?**
- **How can you help your developers build better code based on the insights your security team uncovers?**

Stories from Salt Customers

Insurance Industry Review on Gartner Peer Insights

★★★★★ 5.0

Sep. 8, 2022

"Salt makes it easy for us to see vulnerabilities or potential problems in the APIs we're running. We stay ahead of the risk that way."

– Application Security Analyst in the Insurance Industry

Banking Industry Review on Gartner Peer Insights

★★★★★ 5.0

Dec. 27, 2022

"The Salt platform has also allowed us to spot vulnerabilities in pre-production and running APIs. We can then review the details and send them to the developers for remediation."

– Security Specialist in the Banking Industry

XOLV Technology Solutions

"[Salt Security] started identifying errors and delivering insights on how to craft better APIs within minutes."

– Jason Weitzman, Application Security Engineer

Minimize expense

While new technology is often required to address new attack vectors like API security, security budgets aren’t unlimited. Security leaders know that it’s important to minimize expenses and leverage existing team structures and processes whenever possible. API security solutions are a new element in the security stack, so you can’t eliminate another tool to pay for them. However, you can leverage an investment in API security to reduce other costs such as vulnerability remediation and compliance, and you can leverage existing team members and processes to implement API security.

SALT

Decrease costs by fixing vulnerable APIs quicker and with less friction

API vulnerabilities are different from traditional software vulnerabilities, which is why traditional vulnerability management tools cannot spot them. API vulnerabilities are almost always business logic-based, and because each API is unique, they are all in essence zero-day vulnerabilities.

But how do you spot these logic-based vulnerabilities? Unfortunately, you can't simply "test" or "scan" APIs – security teams must see APIs in action and understand their functional purpose. They also need to understand the behavioral characteristics of each API parameter and element. A single API endpoint can have thousands of possible permutations of business and underlying application logic that need to be vetted and exercised to understand if the endpoint is capable of performing any negative behaviors.

Security leaders need a solution that can do "double duty" to discover API vulnerabilities as early and quickly as possible in the development process and also reduce the effort required to fix vulnerabilities once discovered. Development teams need to work more efficiently and focus limited remediation efforts on high-priority vulnerabilities that are being actively exploited in production. Together, security and development teams can collaborate to have the most impact and ultimately reduce time and cost.

47%

of organizations have identified vulnerabilities in production APIs during the past year

Q3 2022 State of API Security, Salt Security

Shift left and shield right with pre-production API testing tuned to your APIs and remediation insights learned in runtime

Turns attackers into penetration testers. See how they probe your APIs and identify high- priority business logic vulnerabilities

Provide developers with detailed information to fix vulnerabilities found in production

SALT

Decrease costs by fixing vulnerable APIs quicker and with less friction

Questions to ask yourself

- **How quickly are API vulnerabilities being discovered today?**
- **Can you identify business logic-based API vulnerabilities?**
- **What is your mean time to resolution (MTTR) for API vulnerabilities? What could go wrong during that period of time?**
- **How does your MTTR differ between API-related vulnerabilities and other applications?**
- **How much time does it take your developers to research how to fix an API-related vulnerability? What else could they be doing with that valuable time?**
- **How frequently do you update your APIs? Does that process potentially add new unknown vulnerabilities to your environment?** (hint: according to the Salt Security Q3 2022 State of API Security report, 42% are making updates to their APIs at least weekly)

Stories from Salt Customers

Banking Industry Review on Gartner Peer Insights

★★★★★ 5.0

Dec. 27, 2022

"The Salt platform has also allowed us to spot vulnerabilities in pre-production and running APIs. We can then review the details and send them to the developers for remediation."

– Security Specialist at a Banking Institution

ARMIS®

"DevOps teams don't want reactive protection – they're all about proactive detection. Salt provides actionable info our dev teams can use to make the security of our APIs inherently better."

– Curtis Simpson, CISO

SALT

Eliminate potential costly regulatory fines

Organizations spend a lot to build and maintain compliance practices, and those costs go up if they have to pay regulatory fines. A study by Globalscape showed that organizations spend $5.47 million on compliance compared to an average of $14.82 million for non-compliance.

It's no surprise that in the API security realm regulators are starting to realize the implications of insecure and unknown APIs. PCI DSS and NIST have begun implementing API-related mandates, as have the New York Department of Financial Services and the Australian Government. Even regulatory bodies that don't yet definitively identify the need for API security can still institute fines tied to poor API visibility or threat detection, particularly if a PII loss occurs.

Organizations must pay attention to API-related and adjacent regulations. Regulators often need a complete list of all APIs in an environment as well as classification of data types within them. Without comprehensive API discovery, it's difficult to pull together such an inventory. And it's nearly impossible when zombie APIs (outdated but not deprecated APIs) and shadow APIs are involved. You need an API security solution that automatically and continuous inventories APIs and can help you respond to requests from auditors and regulators, without scrambling and extensive manual efforts.

$5,000-$100,000 per month

is the range of PCI compliance fines, which will continue until an organization can demonstrate the issue is appropriately resolved.

PCI Compliance Guide

Prevent sensitive data exposure and the resulting fines

Address API-related regulator questions with ease

Quickly get a complete and accurate inventory of APIs to provide to auditors and regulators

Achieve new compliance certifications

SALT

Eliminate potential costly regulatory fines

Questions to ask yourself

- **What compliance mandates is your company subject to?**
- **What compliance frameworks would you like to achieve to open new markets?**
- **Have you ever been fined by a regulator? If so, how much was the fine?**
- **How much would your business suffer should you find yourself out of compliance with an industry compliance mandate?** (hint: according to a true cost of compliance study by Ponemon Institute and Globalscape, the average loss of revenue due to a single non-compliance event is $4 million)
- **Do you know which APIs transmit personally identifiable information?** (hint: according to the Salt Security Q3 2022 State of API Security report, 91% of all APIs protected by the Salt contain sensitive PII data)

Stories from Salt Customers

BerkshireBank

"We're seeing an increase in the number of API transactions, but we're also seeing an increase in API attacks. We have to keep our data secure and our regulators happy, and we can't get in the way of digital transformation – Salt fits right into that."

– Ryan Melle, CISO

ARMIS®

"We've also been able to use Salt for compliance and FedRAMP. We were able to submit the full catalog of all our APIs and where sensitive data was involved to FedRAMP right out of the Salt platform."

– Curtis Simpson, CISO

SALT

Protect APIs without additional headcount

Security leaders face the trifecta of tight budgets, already over-tasked teams, and an industry security skills shortage, so adding headcount to accommodate new security use cases is rarely an option.

But even though you can't add more bodies, that doesn't mean you can avoid the work of implementing new security measures to protect the business. API security is one of the arenas where organizations simply cannot afford to take a "wait and see" approach. Security leaders need to ensure that they can address API security concerns without needing to bring in an army of new team members to support it. They need to look for solutions that take no more than a few hours a week to manage, fit within existing workflows, and make the most of the investments in people and technology you've already made. Leveraging advanced artificial intelligence and machine learning models to automate manual workloads at scale can make security teams exponentially more efficient.

$134,800/year

is the average cybersecurity salary in North America, not including benefits, which equates to $64.81 per hour.

(ISC)2 Cybersecurity Workforce Study, 2022

Adding an API security discipline should not require adding team members

Ensure that your API security tools fits within existing workflows to maximize team efficiency

Consider leveraging existing tools to mirror traffic to your API security solution to maximize efficiency

SALT

Protect APIs without additional headcount

Questions to ask yourself

- **Does your security team have excess bandwidth?**
- **How much time could your team spend per week to undertake a new security discipline like API security?** (hint: Salt customers spend on average 4 staff hours per week working in the Salt platform)
- **What is the average salary for a security team members at your organization? Does your budget allow you to add 1 more this fiscal year? 2 more? 0?**
- **What operations and management tools and processes do you already have in place that an API security solution could integrate with to help your team be more efficient?**
- **What infrastructure do you already have in place that could help you "jump start" your API security program by mirroring traffic? API gateway? WAF? Load balancers? Microservices? Cloud traffic?**

Stories from Salt Customers

FINASTRA

"Salt Security has automatically blocked tens of 1000s of credential stuffing attacks. Without Salt, we'd be out of business."

– Nir Valtman, Head of Product and Data Security

XOLV Technology Solutions

"Deploying the Salt platform took almost no effort – it integrated quickly with our existing Cloudflare, AWS, Jira, and other systems. It also started identifying errors and delivering insights on how to craft better APIs within minutes."

– Jason Weitzman, Application Security Engineer

"We were pleased about full-time employees that we don't have to hire since Salt's AI/ML is automating manual work."

– Banking Customer

Retail Industry Review on G2 Peer Review Site

★★★★☆

Feb. 1, 2022

"A very lightweight solution that builds upon existing integrations, a responsive and open-minded support team, and an easy-to-navigate product."

– Retail Customer

Increase revenue opportunities

Hundreds of millions of application programming interfaces (APIs) power today's digital economy, and that figure continues to expand at a relentless pace. APIs are at the heart of digital innovation, and with that comes revenue opportunities. API security done right can help open these doors and provide faster development and smoother deployments as well as free up team members from tedious manual processes to work on value-added projects.

SALT

Unlock existing security team members to do more interesting, value-added projects

It's no secret that security teams are burned out and being asked to do more with less. Frequent, boring manual tasks only make matters worse. Every day, these teams have to hunt down information from multiple sources, across many alerts, and then attempt to stitch them together to see the bigger picture.

Fortunately, advanced ML/AI-based threat detection tools have changed the industry in recent years, reducing that monotony and freeing up security teams (and developers) to do more interesting work. This evolution has happened across all attack vectors, and API security is no different.

What could your team accomplish if they could continuously and automatically know all of the APIs in your environment, what typical usage patterns look like, and what sensitive data is exchanged? What if they could automatically baseline API and user behavior and recognize unusual and malicious activity, whether it spans hours, days, weeks, or months – all without manual work? And finally, what if they could get meaningful alerts that provide all of the information they need to understand what attackers are doing, how they're doing it, and optionally automatically block their activities, even while they're still doing reconnaissance on your APIs?

This kind of true insight allows security teams to be more efficient and effective, pinpointing true threats and acting accordingly. And it eliminates the manual effort required to spot API attacks, freeing security teams and developers to do more meaningful work. It also allows security to be the team of "yes let's do it" versus "no, it won't be safe."

There is a

700,000 US

– and –

3.4M global

shortage of cybersecurity professionals.

(ISC)2 Cybersecurity Workforce Study, 2022

Clearly see all of the steps an attacker has taken over weeks and months in one place versus hunting through dozens of alerts

Leverage advanced ML/AI to gain context and reduce alerts and false positives

Automatically block malicious activity through your existing WAF without having to write a single rule

SALT

Unlock existing security team members to do more interesting, value-added projects

Questions to ask yourself

- **What could your team be doing if they weren't manually reviewing logs and writing WAF rules that will still detect only the most basic of API attacks?**
- **Does your team spend too much time chasing down false positives?** (hint: Salt customers experience a 94% reduction in alerts than they would with other tools)
- **Would your team be more engaged if they could eliminate boring, manual tasks?**
- **What if your API security solution could recognize true anomalies, determine probable malicious intent, and block users through your WAF or API gateway? What kind of time would that save (not to mention, how much better protected would your organization be)?**

Stories from Salt Customers

ARMIS®

"Without Salt, they would have had to build all that monitoring capability themselves for all these new APIs, but with Salt doing that work, they can instead build new integrations."

– Curtis Simpson, CISO

Healthcare & Biotech Industry Review on Gartner Peer Insights

4.0

Aug. 26, 2022

"The Salt platform gives us immediate alerts about potential threats so we can respond fast. We especially like the intelligence of the system. It learns the patterns of our APIs, and it flags anomalies, and by our actions, after it learns which anomalies are non-issues, so we don't waste time chasing phantom threats."

– Security Director, Healthcare and Biotechnology Industry

SALT

Accelerate innovation by building and delivering new applications more quickly

APIs drive today's economy, helping organizations bring data together in new ways to provide the applications and services that consumers expect. Therefore, it's no surprise that a recent study featured in Forbes found that businesses that utilize APIs were more profitable over the past decade, experiencing 12.7% higher growth in market capitalization growth than those that did not use APIs. APIs allow access to a company's most valuable data, helping them efficiently reuse internal capabilities, share assets, and co-innovate with partners.

Because APIs are so lucrative and essential, delaying API deployment over security concerns can hurt a company's bottom line. Top-notch API security practices, on the other hand, can have the opposite affect and speed up innovation. Today's sophisticated API security tools can prevent exploits of vulnerable APIs, acting as a safety net and enabling organizations to roll out new software with greater speed and confidence. These advanced API security platforms can also gain insights from running traffic to provide remediation advice to harden APIs, so developers can make current and future APIs more secure.

54%

of organizations have slowed the rollout of a new application due to an API security concern.

Q3 2022 State of API Security, Salt Security

Deploy new APIs quickly to open new revenue opportunities, without worrying about security gaps

Gain knowledge from unsuccessful attack attempts that will harden future APIs

Give useful, clear security guidance to developers based upon what is happening with their APIs "in the wild"

Accelerate innovation by building and delivering new applications more quickly

Questions to ask yourself

- **Have you ever slowed the deployment of an application due to API security concerns?**
- **Have you ever had to roll back an application or temporarily take it offline over API security concerns?**
- **How quickly do you build and deploy new APIs today? How quickly could you be launching them if you could easily demonstrate security readiness?**
- **How much quicker could you be deploying APIs if you were confident that any vulnerabilities missed during development would be countered with comprehensive runtime protection coverage?**
- **What if your security team could say “yes” and keep up with the API development demands of the business rather than being the “no” police?**

Stories from Salt Customers

Banking Industry Review on Gartner Peer Insights

5.0

Sep. 16, 2022

“We are rapidly moving to APIs for everything, everywhere. Salt gives us the confidence that we're covered and have visibility. It speeds up our development velocity and assures us that attacks and vulnerabilities are seen, counted, and mitigated.”

– Cybersecurity Manager in the Banking Industry

A transportation customer was forced to delay the release of new payment application that would have provided a markedly better customer experience due to a lack of API security controls. They are now eagerly awaiting deploying of this application now that they have brought in Salt to provide the necessary API security controls.

– Transportation Company (now a Salt customer)

A digital banking leader was increasingly relying on APIs to deliver innovative products and services, but the security team couldn’t provide the proper vetting without slowing down the business. After implementing Salt, the bank continuously discovers APIs as the business rolls them out, enabling continuous innovation.

– Digital Banking Company (now a Salt customer)

SALT

Monetize your data with secure APIs

APIs are essential for companies to support their innovative and revenue-generating digital transformation initiatives. Open banking services, mobile and online services, digital information sharing apps, DoorDash, Uber, PayPal, Spotify, Netflix, Tesla – you name it – they all require APIs to function.

Companies are developing and pushing out APIs faster, and in larger quantities, than ever before. APIs allow companies to build and bring advanced services to market, opening up new avenues of business and revenue streams. Digitalization hastened this trend, and Covid accelerated its implementation. Companies had to quickly deploy remote services for workers and customers and build product integrations to support a myriad of devices – all of which increased the use of APIs.

One of the most exciting revenue opportunities for organizations is to monetize their APIs. Automotive manufacturers have begun embracing this approach and are selling customer data from their APIs to insurance companies. Insurers are happy to pay for this service, because it helps them set more appropriate rates for their users. Social media companies are monetizing this data better than anyone! Consumers gain a more frictionless user experience when they can log in to a new application using their Facebook or Google credentials, giving these tech giants the opportunity to sell more tailored advertising to marketers.

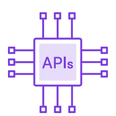
The monetary opportunities of APIs are immense, but to harness them, security leaders must ensure the protection of those APIs. APIs support the interconnectivity of a company's crown jewels – the essential and sensitive data that businesses require to deliver their digital goods and services.

13%

of organizations say that monetizing data is the main driver behind the use of APIs.

Q3 2022 State of API Security, Salt Security

Embrace the monetary opportunities promised by APIs, but first ensure they are protected or risk greater financial loss



Ensure you have a complete inventory of all of your APIs and what traffic is flowing through them to avoid missing out on additional opportunities

Build secure APIs and improve them over time with insights learned during runtime to avoid downtime and lost revenue

SALT

Monetize your data with secure APIs

Questions to ask yourself

- **What revenue streams could your organization benefit from if you could prove your APIs were protected?**
- **Which APIs in your organization are already being monetized? How many more could be?**
- **What would happen if the APIs you already use to drive revenue were breached? What would such an incident do to the confidence of your business partners?**
- **What would happen if an API attack led to a major breach and outage? How long would it take to recover that lost revenue and lost trust?**

Stories from Salt Customers

BerkshireBank

"We want to be a business enabler. We want to enhance digital transformation for ourselves and our customers, and the best way for us to allow business to move forward quickly is to stay out of the way, but our top priority is keeping everything secure. Salt lets us do both."

– Ryan Melle, CISO

One prospective customer was not able to introduce a new application to provide critical medical treatment because there was concern about the security of the payment APIs. After deploying Salt, the company was able to solve its API security challenges and launch the application, increasing revenue and improving patient outcomes.

– Pharmaceutical Company (now a Salt customer)

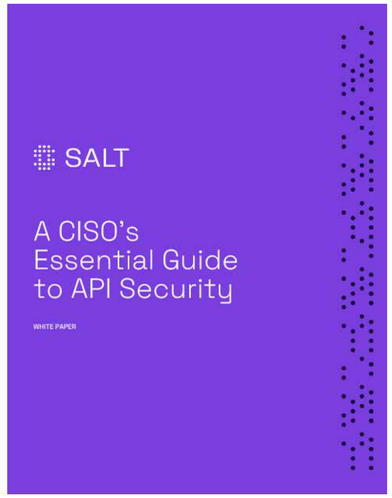
Final thoughts

It’s a constant race! API security solutions must help organizations stay one step ahead of the bad guys. Companies need the ability to automatically and continuously identify and catalog their APIs, protect them in runtime, and protect their future selves with shift-left practices. Deploying API security helps companies stay out of the wrong news headlines and protect their own and their customers’ data from attack.

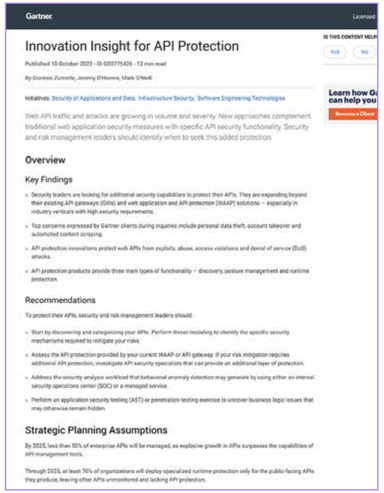
Security leaders who embrace the challenge of API security don’t just avoid problems – they also realize the many business benefits of doing so, namely reduced risk, minimized expenses, and new revenue opportunities. The time is now to start experiencing the full benefits of a comprehensive API security strategy.

Additional resources

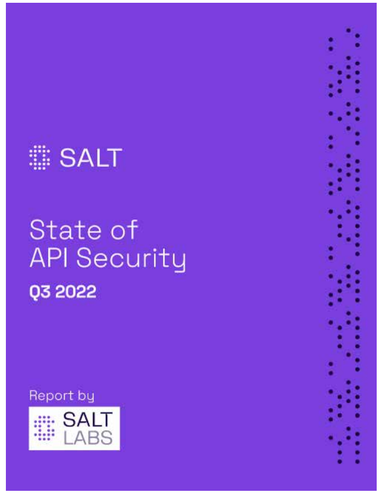
Salt loves to help you Get Smart(er) about API security – check out these additional resources.



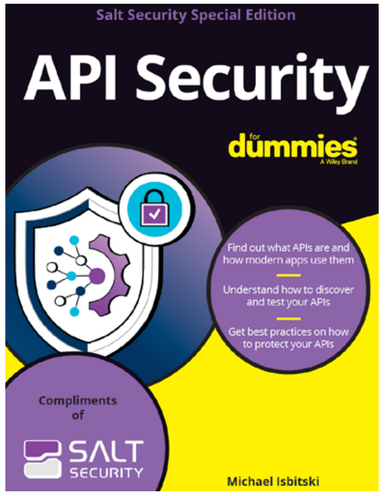
[A CISO's Essential Guide to API Security]



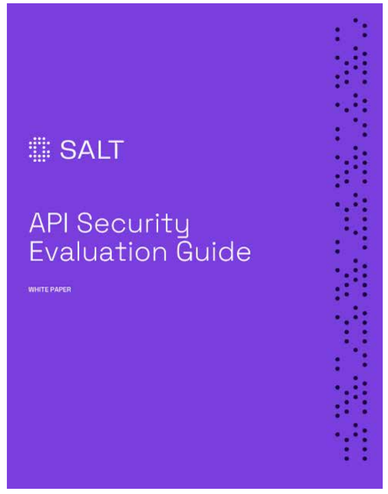
[Gartner® Innovation Insight for API Protection]



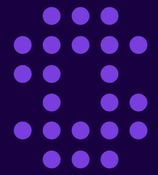
[Q3 2022 State of API Security Report]



[API Security for Dummies]



[API Security Evaluation Guide]



SALT

Securing Your Innovation

EB303-03012023