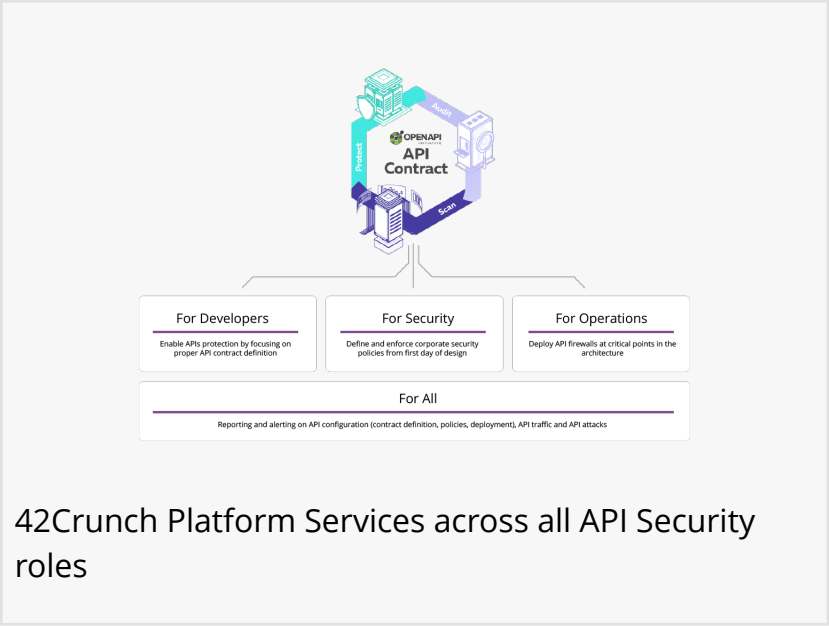
42Crunch announces the launch of the first API Security platform

42Crunch announced today the release of 42Crunch Platform, the first API security cloud platform to discover API vulnerabilities and protect API from attacks.



42Crunch Platform Services across all API Security roles

IRVINE, CA, USA, March 6, 2019 /EINPresswire.com/ -- 42Crunch, the leading API security company, announced today the release of the 42Crunch API Platform, the world's first API security cloud platform to discover vulnerabilities in APIs and protect them from attack. The 42Crunch Platform can protect SaaS, Web, or IoT APIs, as well as microservices.

This follows the launch of the free API Contract Security Audit tool at APISecurity.io earlier this month. The tool helps API developers improve their API definitions that follow the OpenAPI Specification into proper API contracts. Now, with this latest release, customers have access to the full 42Crunch Platform.

> The world of applications exchanging data over HTTP is changing at an incredible pace, and we foresee the market of web application security quickly becoming the market of API security"
>
> *Jacques Declas, CEO, 42Crunch*

As APIs have proliferated across application environments, and the quantity and sensitivity of the data they transmit have increased, API attacks have become more frequent and more complex, making them the number one threat for any company. Moreover, APIs allow direct, often public, access to critical data that has traditionally been hidden in data centers.

The market has already seen a huge increase in API attacks over the past few years. API breaches include such big names as Facebook, T-Mobile, Panera Bread, Verizon, and the latest vulnerability disclosures by the United States Postal Service (USPS) and Google+. Gartner

predicts that “by 2022, API abuse will be the most frequent attack vector resulting in data breaches for enterprise web applications”.

42Crunch Platform offers a set of integrated services that can be leveraged as part of the APIs’ DevSecOps cycle:
• API Contract Security Audit: An exhaustive security audit of the OpenAPI definition, with detailed security scoring that helps developers define and strengthen their API contracts.
• API Contract Conformance Scan: A scan of live API endpoints that discovers potential vulnerabilities and discrepancies in your API implementation against the API contract.
• API Protection: A straightforward and easy way to protect APIs and apply policies that can be deployed in our lightweight, low-latency, API-native micro firewall. API Firewall automatically enforces traffic based on your API contract and applies security policies to protect API endpoints wherever they are.

The traditional approach in web application security requires customers to use a combination of products — such as SAST, DAST, WAF, RASP, and API management — to address different security concerns, in different network zones, and at different stages of the application life cycle. This approach is difficult to operate, consolidate, maintain, and deploy.

42Crunch Platform aims to overcome these difficulties. With our platform, enterprises can centrally enforce and monitor corporate security policies, using tools that have been designed both to be API-centric and to work together. Thanks to the combination of the integrated services, security teams get a 360° view of the entire API portfolio, including audit grades, usage, prevented attacks, and potential vulnerabilities.

“Our experience at 42Crunch both in the web application security and API integration space made it very clear that API security is the biggest challenge for security teams today, and that we had to change the way companies can protect their applications and data in a much more holistic, integrated, and simple way than they do today in web application security”, Jacques Declas adds.

APIs are not web applications. APIs have unique logic, unique authentication and authorization mechanisms, and unique vulnerabilities. They can be consumed by humans, machines, or other APIs. Traditional security solutions only focus on known attack types and lack granular understanding of these aforementioned aspects of APIs. This makes the traditional solutions incapable of detecting or preventing attacks that exploit the vulnerabilities unique to APIs. 42Crunch’s approach is to start with the API contract and to offer developers tools to help them define that contract to be very strict. The API contract becomes the core of the positive security model of our API Firewall, and policies are tailored automatically to each and every API. This virtually eliminates false positives and false negatives, and does not require training any AI for weeks on end to learn the model. API Contract Conformance Scan completes the loop by automating tests based on the API contract, allowing to refine both the API contract itself and the policies attached to the API.

API development is agile and fast-paced. Manual approaches to API security are doomed to fail, because you cannot just apply security once and forget about it. Instead, enterprises need to inject security checks as early as possible in the API lifecycle and continuously test and apply proper policies as existing API evolves and new APIs are built. We have designed our platform in such a way that the entire flow through the platform (Audit, Scan, Protect) can be automated and attached to the CI/CD pipeline, efficiently enabling a DevSecOps approach.

The distributed nature of API deployments means that you need to enforce security right in front of the API, in any network zone, in any combination of endpoint locations, whether on-premises or in a public or private cloud. It also means that you must handle the east-west traffic as well as the north-south traffic.
The API Firewall of 42Crunch Platform can be deployed in Kubernetes and Docker, on public clouds (Amazon, Azure, Google), or on the customer's private cloud in a matter of minutes.

Isabelle Mauny
42Crunch
...
email us here
Visit us on social media:
Twitter
LinkedIn
