END-TO-END API SECURITY
Throughout the API Lifecycle

42Crunch and Microsoft deliver a seamless DevSecOps environment for API security from design, through to production and runtime

INCREASED API ADOPTION, PRESENTS NEW SECURITY CHALLENGES

In an increasingly automated world, we've seen explosive growth in the development and usage of APIs with more than 80% of total web traffic now generated by API calls[1]. And this trend is not slowing down with API traffic growing twice as fast as human-based web traffic[2]. The global increase in API traffic has been mirrored by an increase in the volume and variety of API attacks. Legacy application security tools like static code analysis and web application firewalls are poorly suited to defend against many of these attacks and this has necessitated the publication of a dedicated OWASP API security Top 10 listing.

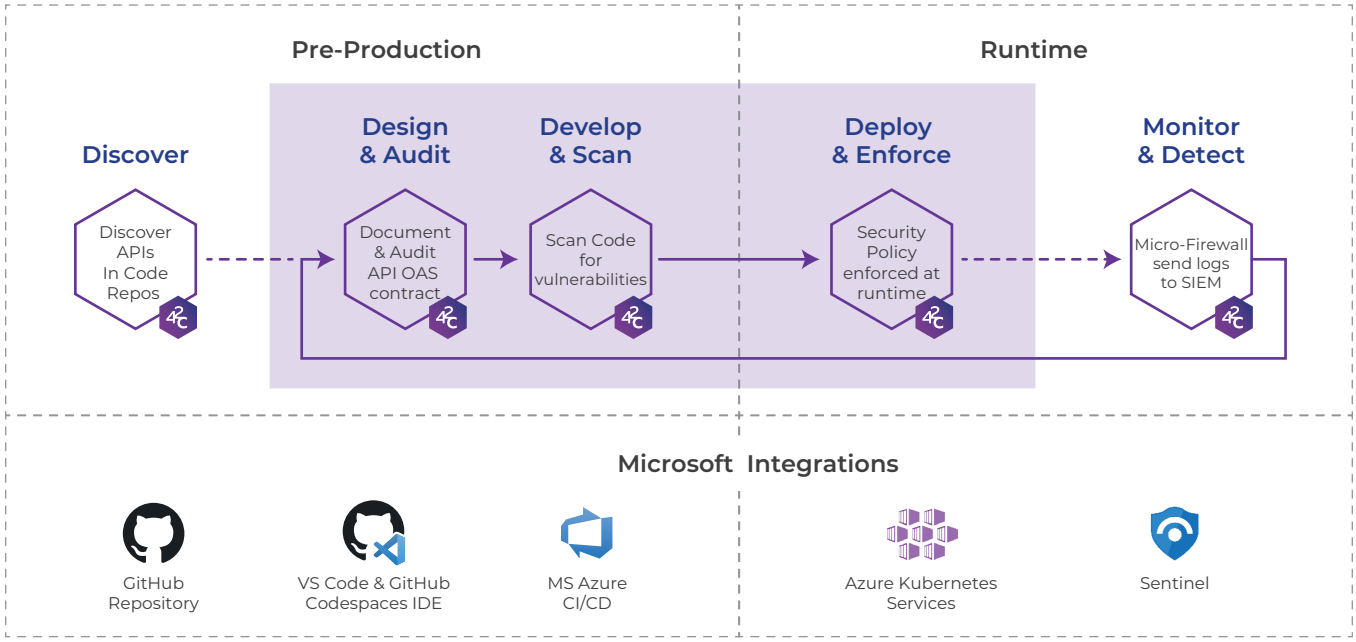
API SECURITY FIRST FOR EFFICIENCY & INNOVATION

An effective API security strategy starts early in the software development lifecycle. 42Crunch and Microsoft are collaborating to enable a DevSecOps approach that helps developers build more secure and resilient APIs without compromising on productivity or innovation. The 42Crunch Developer-First API Security platform is purpose-built to enable a combined shift-left and shield-right approach to securing APIs. The out-of the-box Integrations with many of Microsoft's key enterprise platforms enable a seamless DevSecOps experience for API security throughout the API lifecycle.

> While Azure Pipelines already had security testing extensions ... there had been a glaring gap of the one specifically designed for REST APIs. We are happy to see 42Crunch bridge that gap with their solution.
>
> STEVEN MURAWSKI
>
> *Cloud Advocate, Microsoft*

[1] Akamai 2019 State of the Internet / Security: Retail Attacks and API Traffic

[2] Cloudflare Blogpost 2021 https://blog.cloudflare.com/landscape-of-api-traffic/



API **INVENTORY**

WIth 42Crunch we meet developers where they are by integrating with leading IDEs like **VSCode** and **GitHub Codespaces** which allows them to get instant feedback on security issues without having to change environments. Through a GitHub action, during a pull request, 42Crunch automatically scans enterprise GitHub repositories for all OAS files and imports them to the API security platform.

API **DESIGN**

42Crunch API Audit (downloaded by over half a million developers) runs as a plug-in in **VSCode** and **GitHub Codespaces** to automate testing as part of the CI/CD pipeline. Vulnerabilities found during the audit are presented to the developers directly in the IDE as well as the GitHub repository along with detailed remediation steps.

API **TESTING**

42Crunch API Scan runs as an automated task within the CI/CD pipeline through **GitHub** or **Azure DevOps**. Alternatively, scans can be run incrementally by developers directly from **VSCode** or **Codespaces** to ensure that issues are caught earlier in the development process and don't result in a failed test.

API **PROTECTION**

42Crunch API firewall runs in front of your API and uses a positive security model to ensure that API requests and responses conform to the audited OAS contract. The firewall runs as a VM or in **Azure Container** or **Azure Kubernetes Services** as a sidecar container alongside your API or **Azure API Management** gateway.

API **MONITORING**

The 42Crunch API firewall sends logs to **Azure Sentinel** for analysis of real time attack data. Sentinel provides actionable insights and visualizations that highlight anomalous activity and attack patterns including account takeovers and malicious bots.

42Crunch is now available for purchase on the Azure Marketplace

Get it from Microsoft Azure Marketplace