Automate End-to-End API Security with 42Crunch and Microsoft

The ubiquity of APIs in our world today is such that APIs now represent more than 80% of total web traffic generated and API traffic is growing twice as fast as human-based web traffic. Unfortunately, the global increase in API traffic has been mirrored by an increase in the volume and variety of API attacks. More than 30% of all automated traffic comes from bots and much of that traffic is now being used to attack APIs. Traditional application security tools like static code analysis and web application firewalls are poorly suited to defend against many of these attacks and security teams are buckling under the pressure of keeping pace with API output

42Crunch and Microsoft have partnered to deliver a new approach that helps enterprise customers address API threats across the entire cloud application lifecycle. The 42Crunch API Security Platform is integrated with the Microsoft Defender for APIs to enable a seamless DevSecOps experience for API security throughout the API lifecycle. This integration empowers developers to test their APIs for security during development and empowers security admins to gain full lifecycle visibility into the security posture of their APIs within Defender for Cloud.

Efficient Security

Make security testing easy for developers as they design and build APIs and ensure that security does not become a bottleneck.

Automate for Scale

Automate manual tasks to achieve the scale necessary to address the growing volume of APIs.

Achieve Cost Savings

At least ten times cheaper to remediate an API vulnerability during development compared to at runtime.

End-to-End API Protection

Improve overall API security posture with security policies implemented throughout the API lifecycle from design to runtime

Security Governance

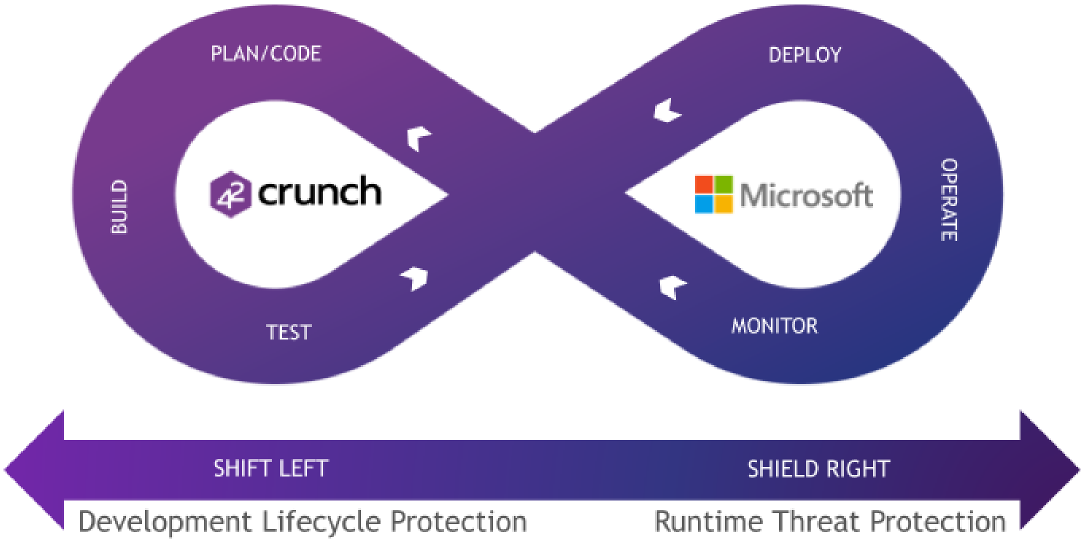
Ensure adherence to corporate policies with clear auditing of APIs at all stages of the API lifecycle.

Regulatory Compliance

Adhere to API security mandates in legislation across many different sectors, including GDPR, HIPAA, PCI-DSS & SEC.

> Together with 42Crunch, we bridge the gap of API security from development to runtime and empower security teams to exercise governance over their API ecosystem throughout the development lifecycle.
>
> VLAD KORSUNSKY
>
> *VP Cloud and Enterprise Security, Microsoft*

DevSecOps for End-to-End API Security



Loved by Developers, Trusted by Security

The combination of 42Crunch and Microsoft enables enterprises to improve their overall API security posture across the entire API lifecycle

Development Lifecycle Protection

- Proactively assess API vulnerabilities with API security testing & scanning
- API Code analysis for refinement
- API Management configuration hardening in Infrastructure-as-Code templates

API Runtime Threat Protection

- API gateway configuration hardening
- API risk prioritization
- Data classification
- OWASP API Top 10 coverage
- Behavioral anomaly discovery
- Remediation guidance and workflows

ABOUT 42CRUNCH

42Crunch enables a standardized approach to securing APIs that automates the enforcement of API security compliance across distributed development and security ecosystems. Our API security testing and protection services are used by Fortune 500 enterprises and over 1 million developers worldwide. The 42Crunch API security platform empowers developers to build security from the IDE into the API pipeline and gives application security teams control of security policy enforcement from the CI/CD across the entire API lifecycle. This seamless DevSecOps approach to API security reduces governance costs and accelerates the delivery of secure APIs.

OPENAPI INITIATIVE ISO 27001 OWASP

Member of
Microsoft Intelligent Security Association
Microsoft

42Crunch is now available for purchase on the Azure Marketplace

Get it from
Microsoft Azure Marketplace