Checkmarx
The world runs on code. We secure it.

Solution Brief

CHECKMARX API SECURITY

You Can't Secure What You Can't See

Challenges of API Security in a Modern, Cloud-Native World

The Decades-Long History of APIs.

When observing common, monolithic applications that are still in use today, APIs were considered a niche technology used only in specific circumstances and to perform certain functions in those environments. However, in the early 2000s, companies like Salesforce, eBay, and Amazon built their business on the usage of APIs and forever changed how business is done online.

Soon to follow, social media companies like Facebook, Twitter, Flickr, etc., began building their platforms on APIs, which became the backbone of social media companies today.

And now, APIs are everywhere modern applications can be found. APIs have grown from a few dozen in the early 2000, and now, estimates demonstrate that by 2030, nearly 2 billion APIs will be in operation.

APIs Powering Cloud Transformation

As organizations embrace the benefits of the cloud transformation and begin moving their monolithic applications to modern, cloud-native architectures (often assembled using loosely couple microservices), APIs are the foundation of this transformation and enable:

- **Integrations** – APIs make it easy to share data between applications and services.
- **Distributed environments** - APIs allow developers to take advantage of modern, distributed infrastructures.
- **Lower development effort** - APIs allow developers to incorporate functionality by borrowing it from third-party services instead of writing it themselves.
- **Simplified user experience** - APIs drive better user experiences by allowing users to share data with multiple applications seamlessly.

API Sprawl in a MAD World

Modern, cloud-native applications also increasingly consist of microservices, containers, open source libraries, infrastructure as code, and an abundance of APIs. In fact, so many APIs has caused a phenomenon called API sprawl.

API sprawl challenges affect both internal APIs that a company develops in-house to connect its own microservices or applications, and external APIs which are APIs created by third parties to support integrations with outside resources.

API sprawl can become so great, and the API documentation so haphazard, that security teams have trouble keeping up. And in some cases, developers aren't telling security teams about new or updates to existing APIs. As a result, security teams don't know about them, and can't configure other security controls to help protect them.

Common API Security Approaches are Inadequate

Most organizations already have WAFs and API gateways today to protect their applications – including APIs. However, these solutions can't protect what they can't see. They don't always sit in front of the entire application and – in the case of WAFs – often don't have API-level context to protect individual APIs. Other solutions attempt to discover APIs by integrating with and analyzing the traffic flowing through these and other network solutions, such as load balancers. These solutions can discover APIs, but only for the APIs that are behind these devices, so they don't fully address the problem of shadow and zombie APIs.

API Security During Software Development

Although run-time security controls do help to secure APIs, here at Checkmarx, we believe there is a better way of addressing API security much sooner, within the software development life cycle itself.

Not only can APIs be better secured with superior secure coding practices, but they can also be discovered in source code using advanced static application security testing solutions like Checkmarx SAST, that discovers APIs during various phases of the SDLC.

Even better, shadow APIs that are undocumented and zombie APIs that should be decommissioned can also be discovered and inventoried, and then compared against what is defined in API documentation.

Being a leader in the application security testing (AST) domain, Checkmarx has developed a completely new and innovative way of securing APIs that complements WAFs and API gateways, so organizations can improve their API security posture overall.

Checkmarx API Security – A New Approach That's Badly Needed

Checkmarx API Security, which is part of the **Checkmarx One™ Application Security Platform,** provides a differentiated approach that becomes embedded into the modern API lifecycle to help organizations understand their API footprint and overall security risk.

Checkmarx API Security Benefits:

- **Complete API visibility:** Provides AppSec teams with the most accurate and up-to-date view into their entire API attack surface, eliminating the problem of shadow and zombie APIs.
- **True shift-left approach:** Discovers APIs in application source code to identify and fix problems earlier in the SDLC—faster, with less cost, and lower risk.
- **Prioritized remediation:** Focuses developers and AppSec teams on solving the most critical issues by prioritizing API vulnerabilities based on their real impact and risk.
- **Holistic view into application risk:** Scans the entire application with a single solution, eliminating the need for additional API-specific tools to reduce the overhead on over-burdened AppSec teams

Checkmarx API Security Integrates With the Way You Build Software

Modern API lifecycle

Train – Begins with our AppSec learning platform.
Helps your developers learn about potential security vulnerabilities and improves secure coding practices when starting to build APIs, with content structured the way developers want to learn, and making learning fun to help drive adoption and consumption.

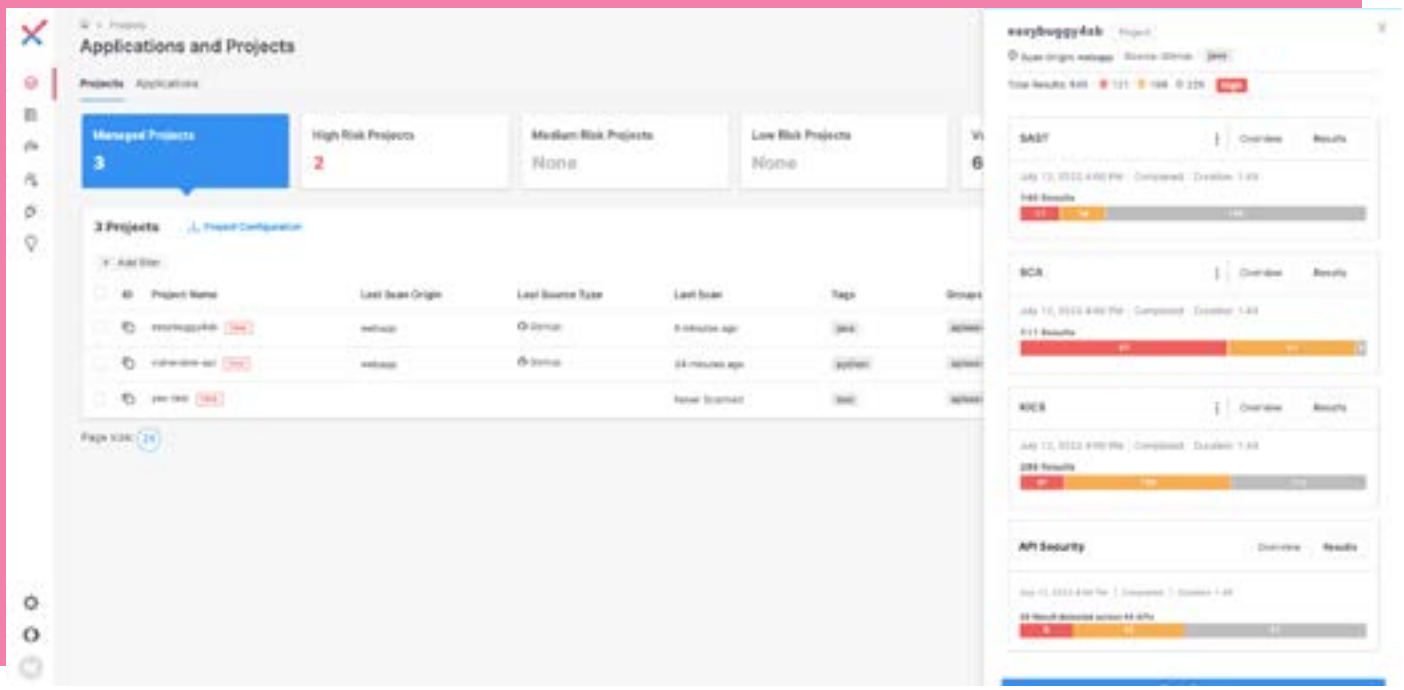
Design – Takes an API-first security approach.
Scans API documentation (i.e., Swagger, RAML) files before your developers start coding to ensure that security is added into the design phase. Enforces API design best practices and assesses your overall API design for misconfigurations, identifying risks in path definitions, authentication schema, and transport encryption.

Code – Integrates and automates scans in the tools you use.
Enables developers to remediate vulnerabilities in their favorite tools where they can kick off an application scan at any time using the CLI, and not wait until after code check-in to focus on security. It also provides guided remediation to help resolve vulnerabilities faster by prioritizing, recommending mitigation points, and surfacing just-in-time learning for discovered vulnerabilities.

Check-in – Identifies vulnerabilities with API discovery and builds API inventory.
Automatically scans source code at check-in or code merge to identify vulnerabilities in your APIs. Discovers every API in the application at scan time, and aggregates findings for a full API inventory. Then compares the inventory to your API documentation to find discrepancies and pinpoint your shadow APIs.

Build – Integrates into your pipeline with real-time feedback and automatic bug tracking.
Automatically scans source code in your pipeline through CI/CD integrations, and immediately sends developers or AppSec teams updates about vulnerabilities discovered during Check-in or Build, then automatically opens tickets for newly discovered vulnerabilities and closes them when resolved.

Deploy – Secures application deployments using infrastructure as code.
Using KICS by Checkmarx, this open source solution parses common IaC files to detect insecure configurations that could expose your APIs to attack. It also integrates with CI/CD tools and supports all mainstream IaC platforms, including Terraform, Kubernetes, Docker, AWS CloudFormation, Ansible, and Helm.



Checkmarx One: API Security Results Overview