



Saving Millions of Dollars by Streamlining your Application Security

By Anshu Bansal
CEO & CO-FOUNDER
CloudDefense.ai

Contents

1.	The Changing Security Landscape.....	2
2.	Cost Of Fixing The Security Defects.....	3
3.	How Clouddefense Helps.....	6
4.	Existing Security Tools And Processes Are Costing You A Fortune.....	8
5.	Problems Identified By Surveying Large Corporations.....	10
6.	Clouddefense's Integrated Approach: Simplicity With Actionable Insight.....	12
7.	Legal Compliance Issues In Open-source Libraries.....	14
8.	Prevent Accidentally Slipping Security Issues Into Production.....	18
9.	Ensuring Security Health Of Your Entire Organization.....	20
10.	Prevent Accidental Slippage Of Secrets, Passwords In Production.....	24
11.	Container Security And Container Registry Scanning.....	27
12.	API Scanning.....	29
13.	Auto-remediation For SCA.....	31
14.	Seamless Integration And Support.....	33
15.	Vfeed's Advance Vulnerability Database And Reporting.....	37

The Changing Security Landscape

DevSecOps represents a transformation in security practice, culture and tools. DevSecOps is a shared responsibility to put security into the center of the product development lifecycle.

DevSecOps combines the best practices of DevOps with modern security practices. A streamlined approach to automation and security testing allows better and safer product development without additional risks and costs for organizations.

IT companies around the world are now embedding security practices and culture into CI/CD pipelines allowing for better security and compliance and faster cheap productive costs.

In this technical paper we explore the unique challenges of the changing security landscape and explore how CloudDefense can help your team save money, avoid risk and build a better and safer product.

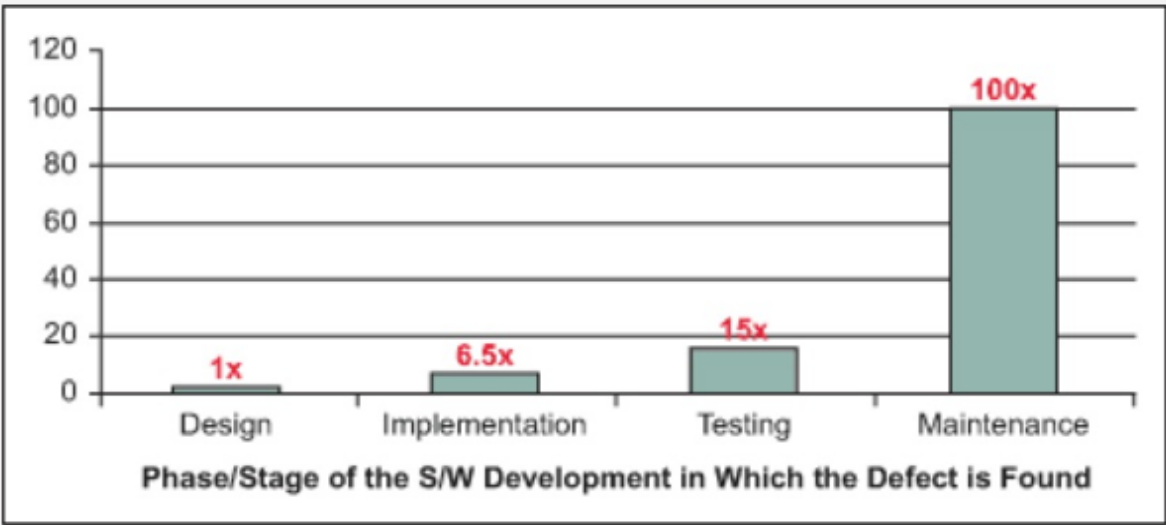
“Relative Cost associated to fix security vulnerabilities”. CloudDefense analyzes current security practices and security tools in large organizations.

Cost of Fixing The Security Defects

“It Costs Millions of Dollars to Fix Defects Late in The Cycle”

A report from IBM System Institute revealed that defects identified after the release of the product are 100 times more expensive to fix than those discovered during the design phase.

Figure 1: Relative Costs to Fix Software Defects (Source: IBM Systems Sciences Institute)



Average Bug Cost at various stage of the SDLC

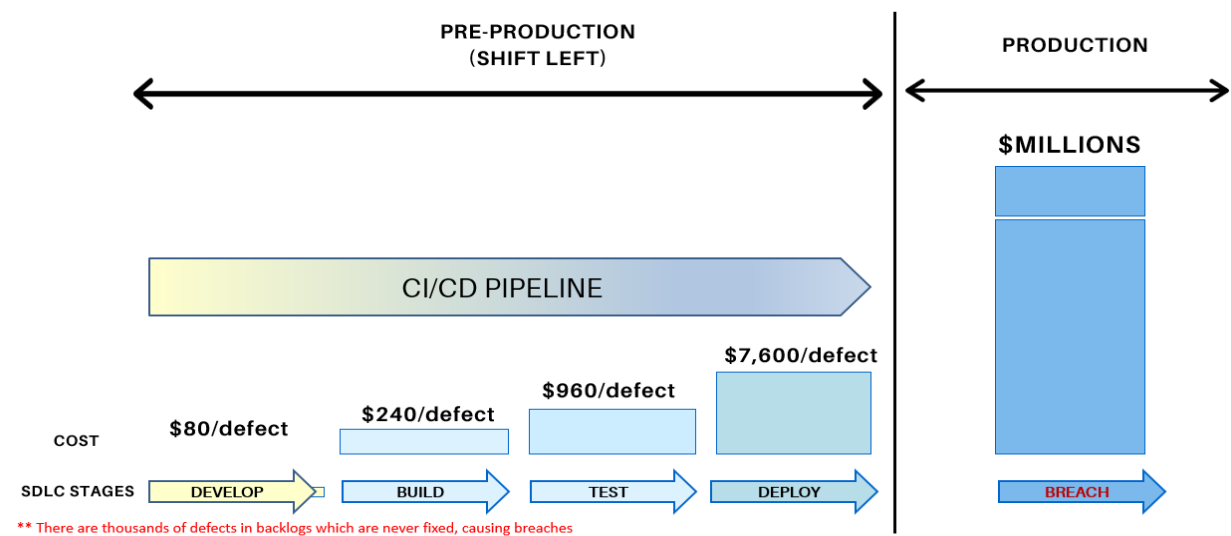
Source: IBM

https://www.ibm.com/devops/method/experience/deliver/dibbe_edwards_devops_shift_left/

Per [IBM Security](#) & the **Ponemon Institute**, if vulnerabilities are detected early in the development process, it costs around \$80 to fix a defect, in comparison to the fix if detected during the production phase, which costs \$7600 per defect on average.



Vulnerability Cost at various stage of the SDLC



Security Breach Cost in Production

Source: IBM
<http://www-01.ibm.com/support/docview.wss?uid=swg27048410&aid=1>

Understanding The Risks

Here are few financial impacts in case of security breaches:

- **GDPR Penalties:** Penalties in the new GDPR, which start at 2% of global revenue and go up to 4% of global revenue. - [Source](#)
- Among companies with full security integration, 45 percent can remediate critical vulnerabilities within a day. Just 25 percent of those with low security integration can remediate within a day. [Source](#)
- In 2018, poor quality software cost organizations \$2.8 trillion in the US alone . [Source](#)
- On average, software developers make [100 to 150 errors for every thousand lines of code](#)
- The cost to address bugs post-release costs \$16,000 to address, but a bug found at the design phase costs \$25. [Source](#)
- **SecDevOps** — will be embedded into 80 percent of rapid development teams by 2021. - [Source](#)
- Data breaches in the U.S. have compromised at least 900 million people's records in the last decade (this constitutes the reported/tracked numbers according to the records kept by the Privacy Rights Clearinghouse, so actual numbers are presumably much higher). - [Source](#)

How CloudDefense Helps

CloudDefense's agent integrates into the continuous integration or build system of your choice and actively analyzes the security health of the application through various security analysis.

We use a proprietary vulnerability dataset powered by [vFeed, Inc.](#), which is richer than NVD (national vulnerability database). Our vulnerability dataset refreshes every 12 hours. New vulnerabilities get discovered everyday and it takes approximately 2-4 weeks to reach the NVD database.

1) Software Composition Analysis for Open-Source Libraries (SCA):

- A typical application consists of 60%-70% of open-source libraries
- Not all opensource libraries can be used due to complex open-source licensing requirements, it takes months of manual effort to resolve open -source licenses
- Unapproved licenses cause legal issues.

2) Static Code Analysis Security Testing (SAST):

- The code that your developer writes. Typically, Business logic code only consists of 30% of your application

3) Dynamic Code Analysis Security Testing (DAST/Pen Testing):

- Only performed for Web Applications

4) API Scanning :

- Swagger/open APIs

5) Container (Docker Repository/Kubernetes) Security:

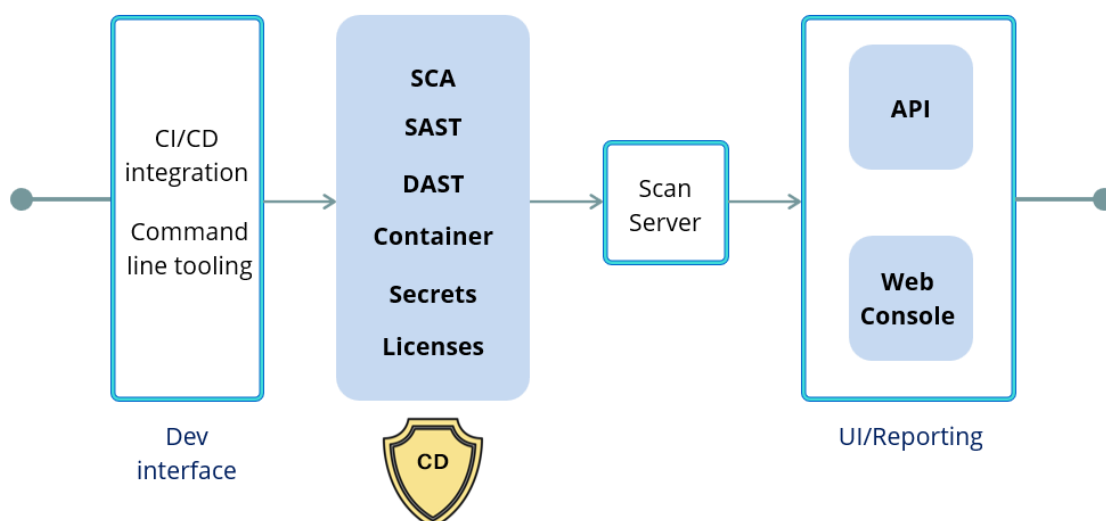
- All layers of the containers

6) Secret/hidden password Scanning:

- Hidden passwords, S3 keys, AWS secrets, GCP and Azure Secrets

Complexity behind simple interfaces

Loved by Developers and Security teams



CloudDefense Agent's Seamless Integration

This new approach is called “**Shift-Left**”. In this approach, security testing is performed during the early stages of development, allowing developers to focus on security during the development phase instead of waiting for security bugs later in the cycle. Shifting left enables project teams to test, provide feedback, and review changes & progress frequently.

Existing Security Tools & Processes Are Costing You A Fortune

At present, when CISOs and their Security teams look to secure their applications, they need to consider many questions before deciding which tool to use:

- *Will the tool support the technology stack that my applications are built in?*
- *Will the tool integrate with my CI/CD Pipeline?*
- *Will the tool support my application's Monolith or Microservices based architecture?*
- *Need for an On-Premise or a Cloud Based solution?*
- *Do I need to buy separate Containers Scanning*
- *Will the tool cover the total footprint of my applications*

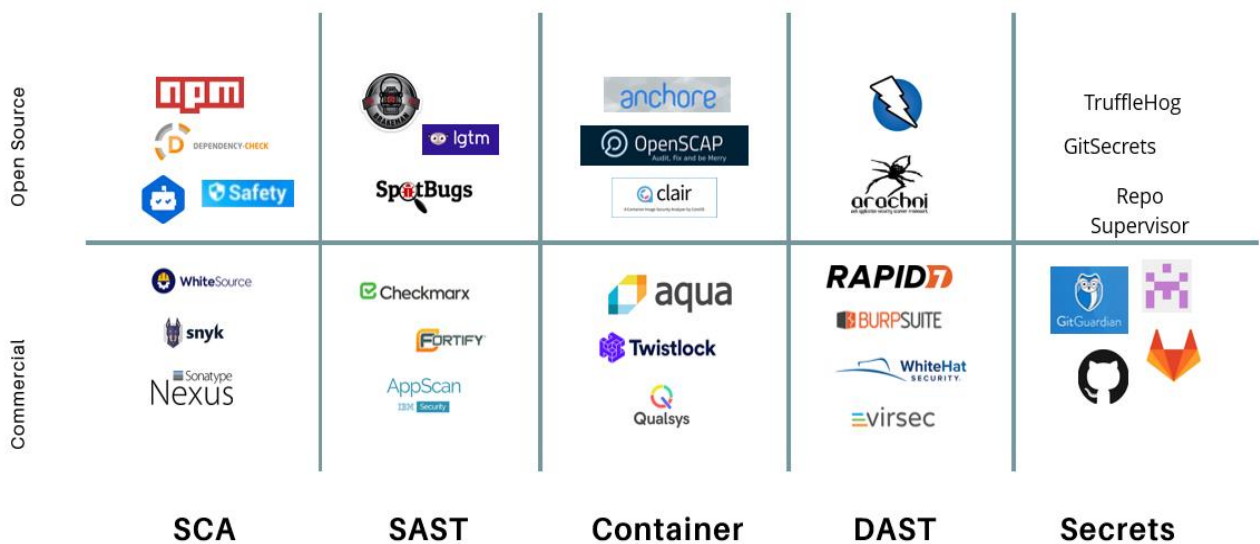
We have listed out some of the verticalized solutions for security testing available in the market today. You may need a combination of tools to do a full set of security analysis. Some of our customers are using 8 tools to cover various programming languages used in their organization.

In our experience, this causes the following problems:

- Enormous cost of managing and running multiple security tools
- Dependency on the Information Security team in terms of waiting on security testing. Usually, the InfoSec team is fairly small in comparison to the number of developers in an organization, this causes a huge bottleneck.
- Having to manage security test results from various tools for compliance
- Manually filtering through the false positives and finding the actionable vulnerabilities.
- Lack of centralized policy-based controls and reporting across the organization

Current landscape at enterprises: managing MANY scanning tools

100s of engineering hours wasted. Multiple Product delays. e.g. our customer Columbia Univ uses 8 tools.



Various Tools Available Covering Only Specific Area of Security

Problems Identified By Surveying Large Corporations

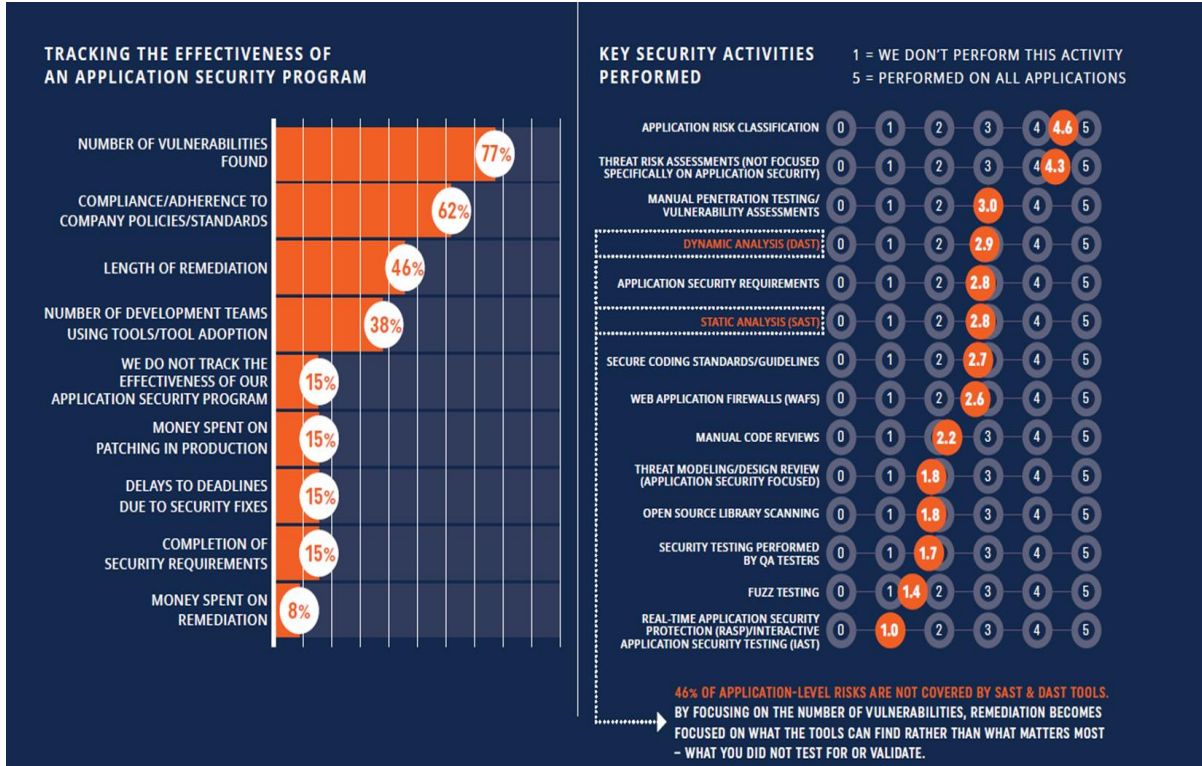
Based on the survey done across many corporations such as *Facebook, Microsoft, Google, Oracle* as well as notable companies in the banking and healthcare industries, some of the findings were astonishing.

We have captured some of the high-level problem statements here:

- The information security team was managing multiple tools to do application security. Some financial customers such as UBS Bank were using 5+ tools to manage their security.
- So much data was being generated from the tools that we would need dedicated experts to identify the actionable data.
- With the process having to be repeated with every release, managers and developers were overwhelmed with the constant requests from the InfoSec team.
- Security issues were getting added to backlog which was never ending and hard to prioritize
- Lack of conformity as security processes varied across teams.
- CISO were reviewing security from multiple sources.
- Existing tools were hard to integrate into their CI/CD pipeline.

A report by Forrester shows that the number of vulnerabilities are getting added at a pace where application owners are having trouble with fixing the vulnerabilities due to budget and deadline constraints. Additionally, the report shows that DAST and SAST testing might not be enough.

Here is the snapshot from the report:



Typical Security Activities Performed In an Organization

CloudDefense's Integrated Approach: Simplicity With Actionable Insight

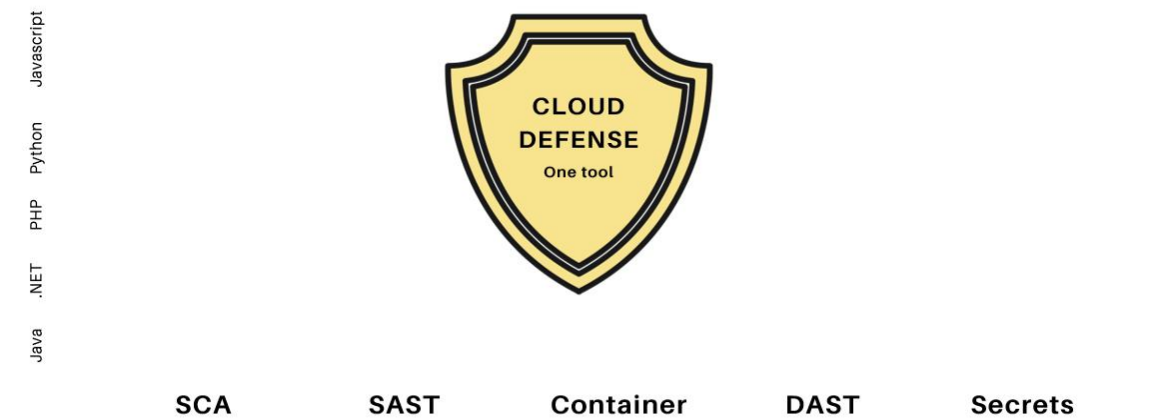
When we showcased our solution to *Facebook*, *Amazon*, and other large companies, they were very surprised to see the simplicity, ease of use and developer-friendliness of CloudDefense.

With our help...

- You don't need multiple expensive tools to manage security of your organizations
- Developers and the Information Security Team can integrate security tools into many build systems and CI/CD tools with a simple few click integration.
- There is a customized view for CISOs, Managers, and Developers so that they can access the risks of their organization and the various applications within it.
- You don't need to be security expert to find security issues in your application. Developers can easily integrate the CloudDefense agent into their build system to get real-time vulnerability details along with auto-fix suggestions.

CloudDefene's helps to simplify the process utilizing one centralized solution to support all languages. No need for multiple tools.

CloudDefense's solution:
One tool for application security. Supports all languages. Single source of truth. Developer friendly.



CloudDefense's Data Quality

We use a proprietary dataset powered by vFeed, which is richer than NVD (national vulnerability database). Our vulnerability dataset refreshes every 12 hours. New vulnerabilities get discovered everyday and it takes approximately 2-4 weeks to reach the NVD database. By integrating CloudDefense’s agent into your build pipeline, new vulnerabilities can be detected in a matter of hours. You can scan all of your applications in real time rather than doing offline or sporadic security scans.

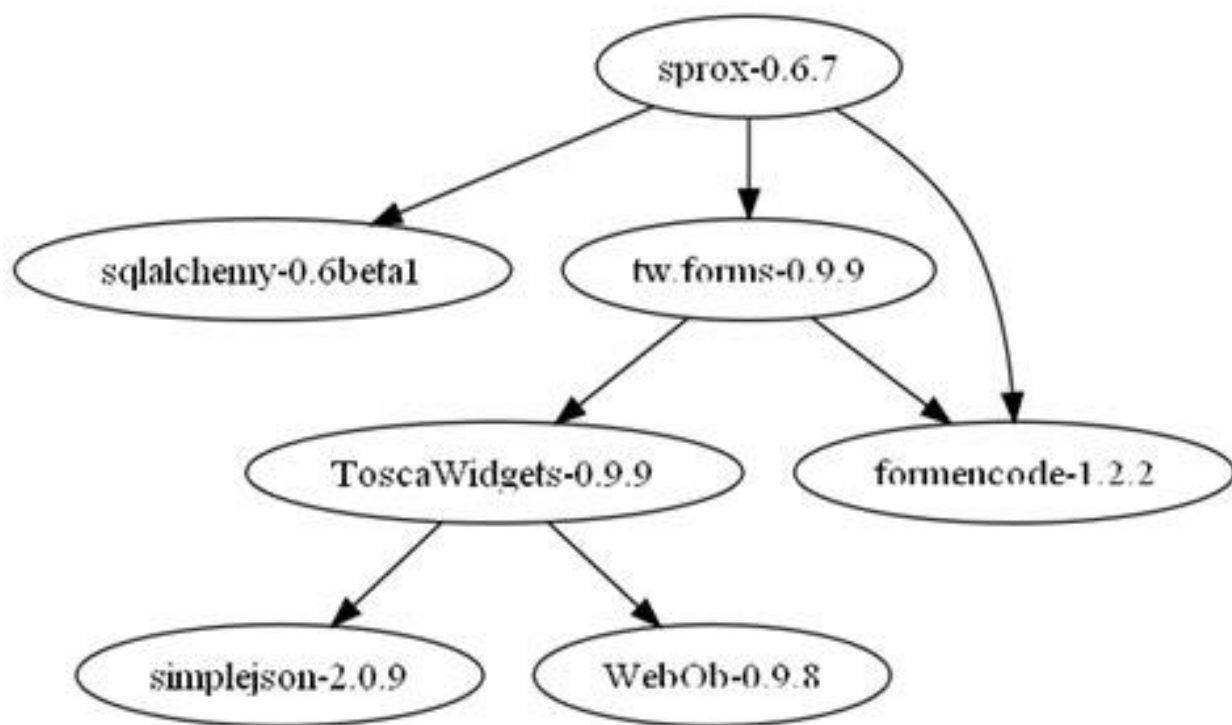
Legal Compliance Issues in Open-Source Libraries

Most software applications use open source dependencies and each open-source library contain many sub-dependent libraries, which makes things complicated as commercial organizations need to declare the licenses used in application release notes..

This raises the following potential issues:

- If there is some vulnerability in a dependent library then your application might be vulnerable, making it possible for hackers to penetrate your application.
- If a sub-dependency is using the software license which is not an open source commercial license, then your organization might have legal liabilities.

In corporations, legal teams spend millions of dollars per year to find the correct licenses for libraries and create release notes so that they can declare the usage of the licenses. Development teams can accidentally use open-source libraries which might not be approved by their legal compliance, which causes liabilities for the organization.



Open-Source License Tree Structure

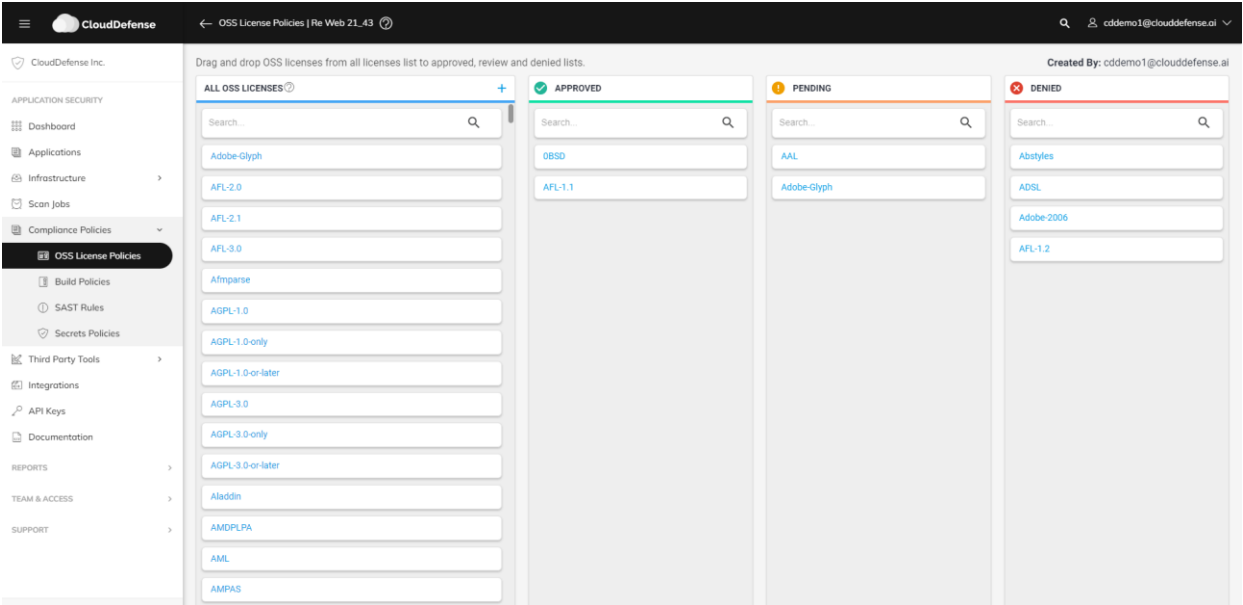
This is how CloudDefense helps!

Automated software license matching

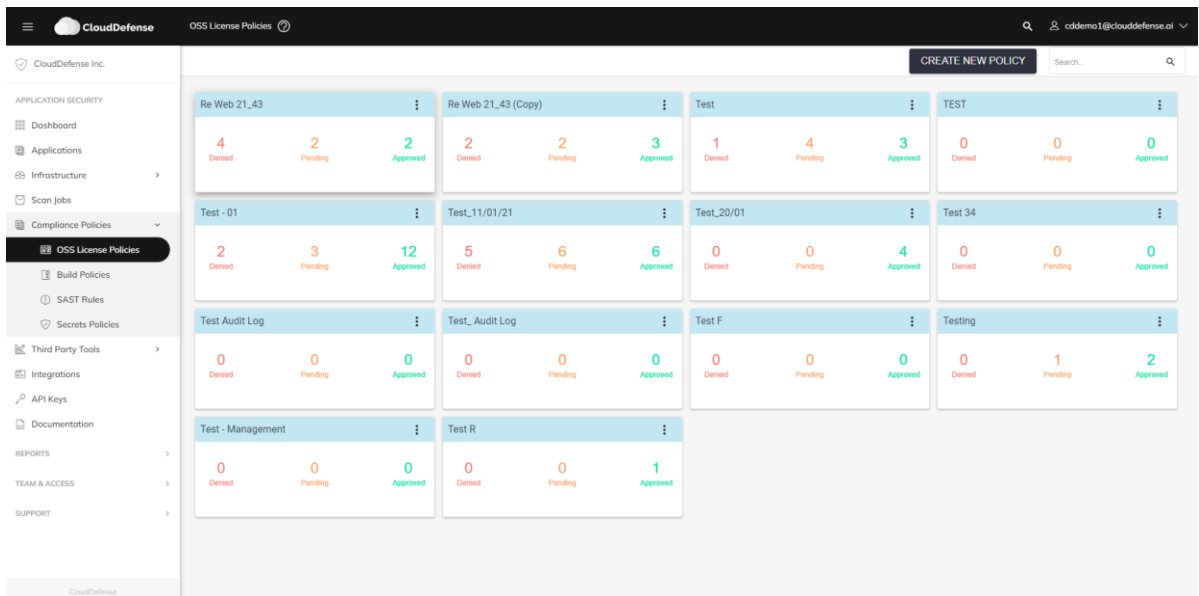
CloudDefense has a centralized, open-source licenses policy-based, system. Your legal teams can create license policies based on your application/organization/team needs by using a simple drag-and-drop interface.

These policies can be attached to an application and tracked in real time. Our patented artificial intelligence system can flag libraries which are violating set policies and you can prevent the accidental usage of “*Non-Approved*” licenses.

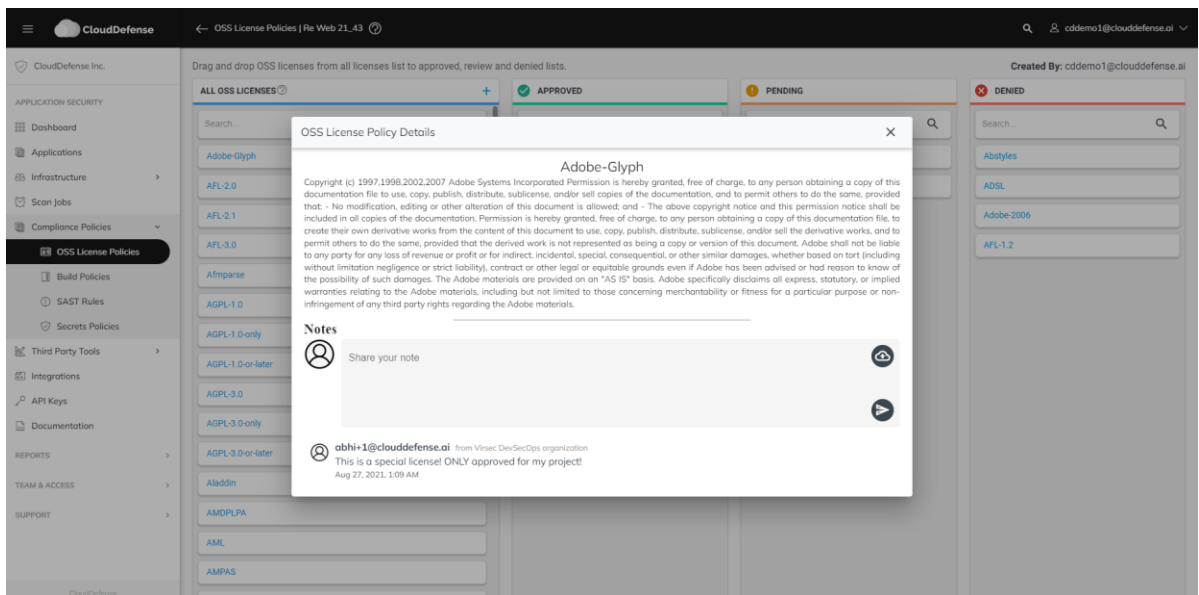
Additionally, release notes to attach to your application can be generated through the click of a button. Our proprietary technology saves you hundreds of manual hours and money spent on license compliance. Additionally, CloudDefense provides an audit trail history so that your teams can take informed decisions.



ALL OPEN-SOURCE LICENSES: DRAG-AND-DROP INTERFACE



APPLICATION USING YOUR PRE-DEFINED LICENSE POLICY



AUTOMATED RELEASE NOTES GENERATION BASED ON YOUR LICENSE POLICY

Prevent Accidentally Slipping Security Issues Into Production

It is a well-known issue that, in the absence of centralized policy-based controls, security issues might slip into production and cause hundreds of millions of dollars of damages. 2019 was a somber year for many companies. Some notable incidents are the [Capital One breach](#) (which occurred due to incorrect AWS configuration settings) and the [Marriott Hotel's data breach](#).

Breaches are expensive to fix and cause extensive and irrecoverable damages.

This is how CloudDefense helps!

Automated build policies

By using our solution, your team can set up an automated build failure policy so that vulnerabilities don't accidentally slip into production without your knowledge. You can set up rules where you want to fail the build, for example, if your application is using any password, AWS keys, encryption keys, Azure and GCP secrets. You can also prevent unapproved licenses and vulnerabilities depending on your needs, all with few simple clicks.

If your application is violating the build policy attached to it, it will break the build and will generate a notification. You can achieve continuous security in real time by using CloudDefense's proprietary technology.

Most security tools available in the market today don't provide continuous security with every code check-in and require manual, offline-execution, to find vulnerabilities.

The screenshot shows the 'Create Build Policy' interface in the CloudDefense application. The left sidebar contains a navigation menu with categories like 'APPLICATION SECURITY', 'COMPLIANCE POLICIES', 'THIRD PARTY TOOLS', 'INTEGRATIONS', 'REPORTS', 'TEAM & ACCESS', and 'SUPPORT'. The 'COMPLIANCE POLICIES' section is expanded, showing 'OSS License Policies', 'Build Policies', 'SAST Rules', and 'Secrets Policies'. The main panel is titled 'Create Build Policy' and contains a form with the following elements:

- Policy Name**: A text input field.
- Policy Description**: A text input field.
- Verify Denied Licenses**: A checkbox with a description: 'This flag is used by scan process to stop the build from promoting next step in CI/CD life cycle e.g. the build will fail when the flag is checked and if denied licenses are found in the dependencies. An alert will be sent to the engineers to review the scan results.'
- Secret Scanning**: A checkbox with a description: 'This flag is used by scan process to stop the build in case some secret keys, passwords, cloud keys are detected in the code. For customization, please check the [documentation](#).'
- Filters / Rules**: A section with a blue link 'Add Filter / Rule'. Below it, a note states: 'Filters are used by scan process to stop the build from promoting next step in CI/CD life cycle e.g. the build will fail when the rule "CRITICAL_SEVERITY_COUNT > 1" criteria is met. An alert will be sent to the engineers to review the scan results.'
- Buttons**: 'CANCEL' and 'SAVE' buttons at the bottom right.

CREATE YOUR OWN CUSTOMIZED BUILD FAILURE POLICIES

Ensuring Security Health of Your Entire Organization

Currently, security teams and CISOs struggle to find the security health of the entire organization. InfoSec compiles security reports from multiple tools and requests security information from each individual application team.

Currently, this process requires a lot of manual time. Much of this time is wasted with back-and-forth data compilation.

This is how CloudDefense helps!

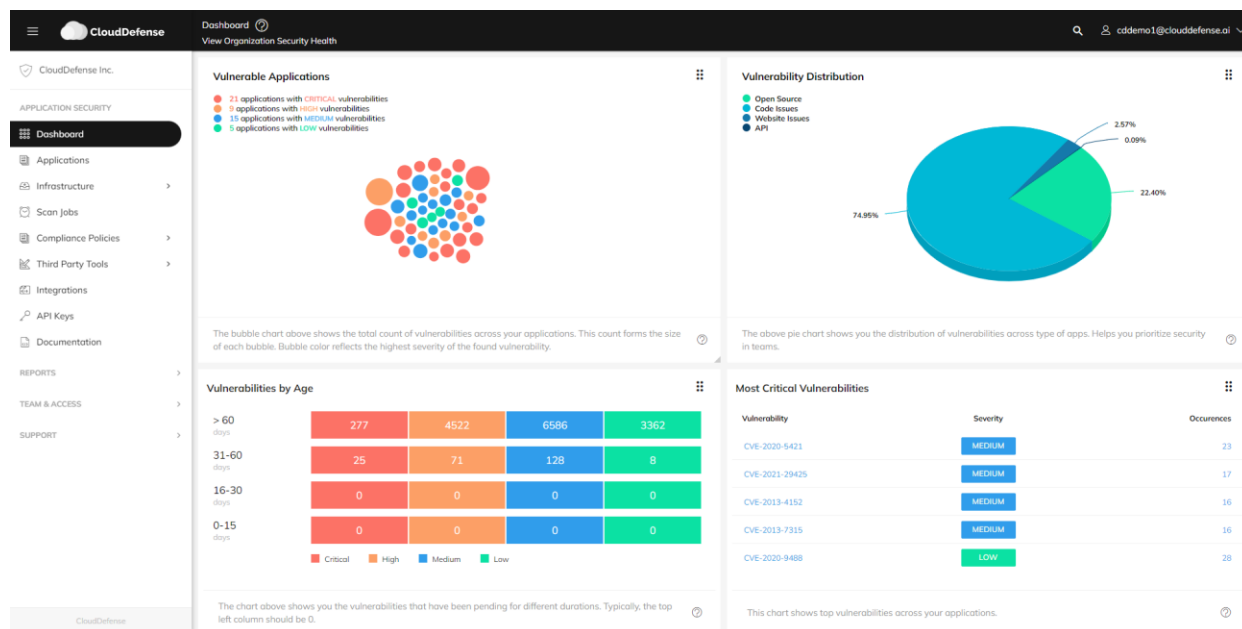
CloudDefense's proprietary technology generates a *"Real Time Dashboard"* for your entire organization. You can also check vulnerability data on a per team basis or per application basis.

By having a comprehensive view, you help your team in *"Increasing Efficiency and Decreasing Cost"*.

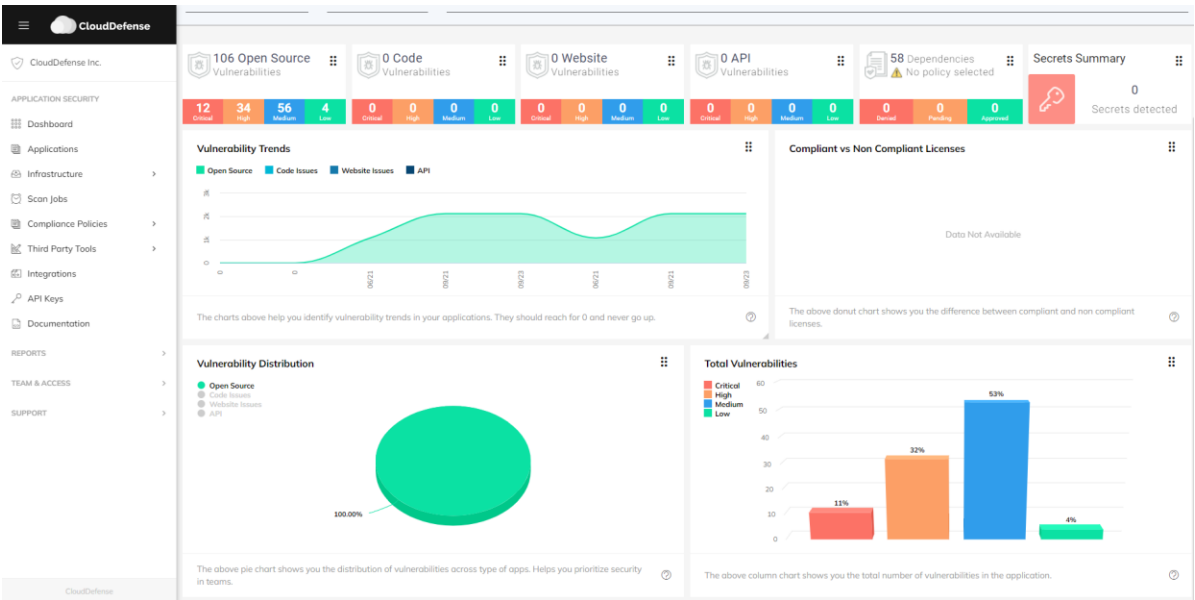
CISO/InfoSec teams can audit the health of organization per team/application basis reducing the need for manual spreadsheets.

One Comprehensive view to see the results:

- Software Composition Analysis (SCA)
- Static Application Security Testing (SAST)
- Pen Testing (DAST)
- Containers
- Hidden Password/Secrets/AWS/GCP/Azure Keys
- APIs
- External tool's SAST/DAST data
- Violated Open-Source License Policies

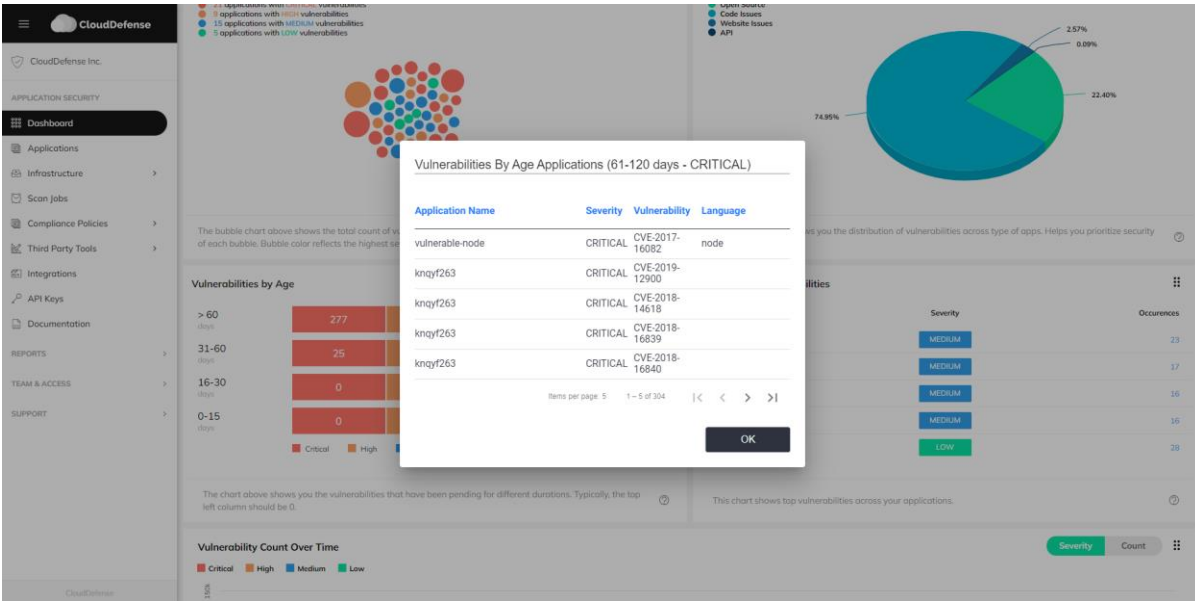


An easy-to-use dashboard with a centralized view for all your applications.



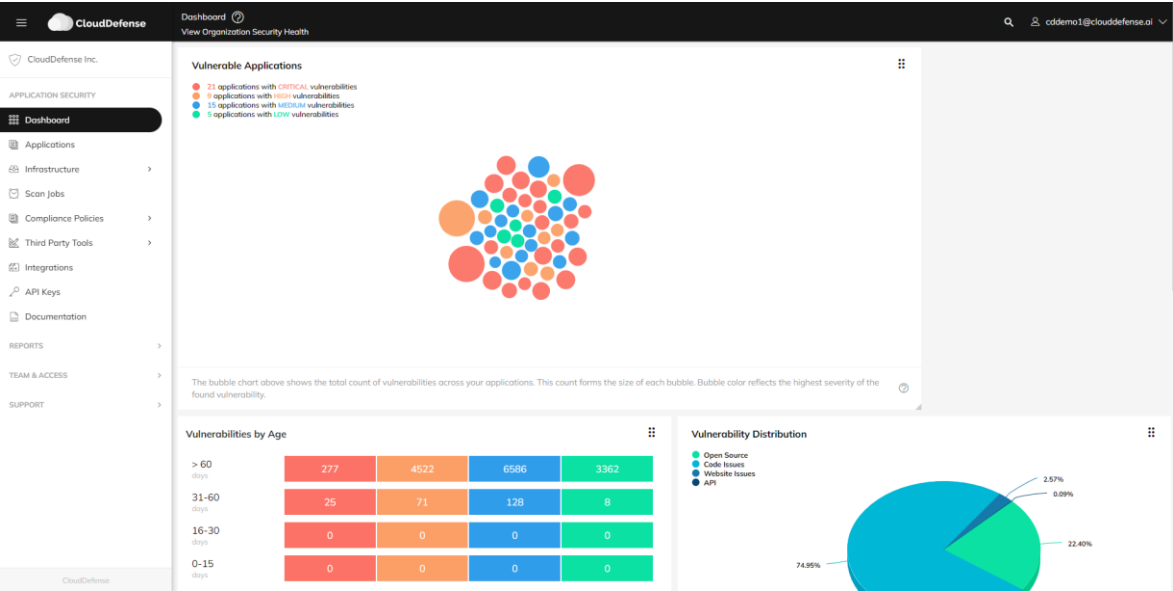
Comprehensive Application Vulnerability View

Vulnerability Aging: Our dashboard also shows Vulnerability Aging Data.



Vulnerability Aging Data Based on Severity

HEAT MAP BASED ON THE VULNERABILITY: We also show a heat-map of a vulnerability spanning across the organization. You can track how many applications are impacted by a single vulnerability. This helps in prioritization across the teams



Vulnerability Spanning Across Many Applications

Prevent Accidental Ippage of Secrets, Passwords in Production

It is very evident that your secret keys such as AWS keys, S3 keys, GCP Keys, Azure keys, passwords can slip into production code leaking customers information and causing huge financial loss to you. During the development process, it's very common to use secret keys for feature development or bug resolution. In the absence of proper code sanitization, keys can be left as part of deployment inadvertently.

Over the last couple of years, we have seen that many times, secret keys, GitHub accounts were found in code causing massive breaches.

This is how CloudDefense helps!

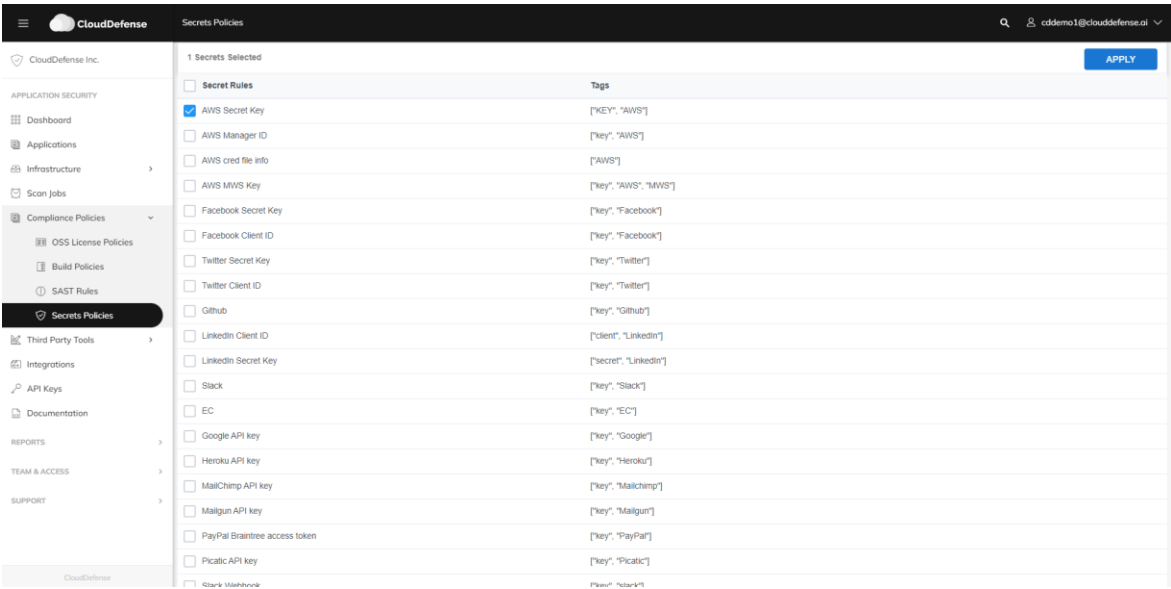
CloudDefense's proprietary technology has inbuilt systems that flag keys based on pre-defined rules. The initial rule set is to prevent all secret keys. That said, you can customize the rules based on application and your organization's needs.

In case a rule is violated, the build breaks and a notification is generated.

We also show which code path you have hidden secret keys in, so that your team can quickly resolve any problems.

Secrets are not stored within the CloudDefense system. Users are only able to see the line number along with the git commit id.

Here is a sample screenshot:



Secrets, Passwords Found in Your Application

Here is a [rule file](#) that can be customized. You can also select the rules that you would like to use from our UI.

```
title = "secrets config"

[[rules]]
    description = "AWS Manager ID"
    regex = '''(A3T[A-Z0-9]|AKIA|AGPA|AIDA|AROA|AIPA|ANPA|ANVA|ASIA)[A-Z0-9]{16}'''
    tags = ["key", "AWS"]

[[rules]]
    description = "AWS cred file info"
    regex = '''(?i)(aws_access_key_id|aws_secret_access_key)(.{0,20})?=[0-9a-zA-Z\\/+]{20,40}'''
    tags = ["AWS"]

[[rules]]
    description = "AWS Secret Key"
    regex = '''(?i)aws(.{0,20})?(?-i)['"]?[0-9a-zA-Z\\/+]{40}['"]?'''
    tags = ["key", "AWS"]

[[rules]]
    description = "AWS MWS key"
    regex = '''amzn\\.mws\\.([0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12})'''
    tags = ["key", "AWS", "MWS"]

[[rules]]
    description = "Facebook Secret Key"
    regex = '''(?i)(facebook|fb)(.{0,20})?(?-i)['"]?[0-9a-f]{32}['"]?'''
    tags = ["key", "Facebook"]

[[rules]]
    description = "Facebook Client ID"
    regex = '''(?i)(facebook|fb)(.{0,20})?(?-i)['"]?[0-9]{13,17}['"]?'''
    tags = ["key", "Facebook"]

[[rules]]
    description = "Github"
    regex = '''(?i)github(.{0,20})?(?-i)['"]?[0-9a-zA-Z]{35,40}['"]?'''
    tags = ["key", "Github"]
```

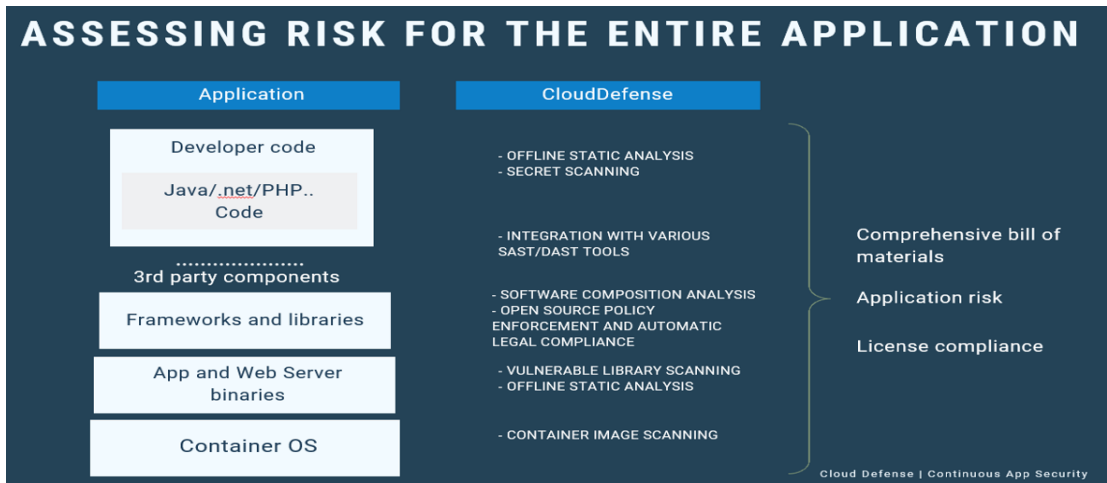
Container Security and Container Registry Scanning

Docker containers and Kubernetes containers are heavily used in organizations and can be downloaded from the public docker repositories. The concern is that public registries might have lots of security vulnerabilities hidden in various containers.

This is how CloudDefense helps!

CloudDefense’s agent can easily scan your docker containers or docker registry. This can also be integrated into your continuous build process. The build-gating criteria is governed by the build policies so that your team can decide when to block the production pipeline in case severe vulnerabilities are discovered.

Our UI also provides detailed analysis of Software Composition Analysis and Licenses used in the docker images. Our UI scans your container, layer by layer, in a nice presentation for your team to review.



API Scanning

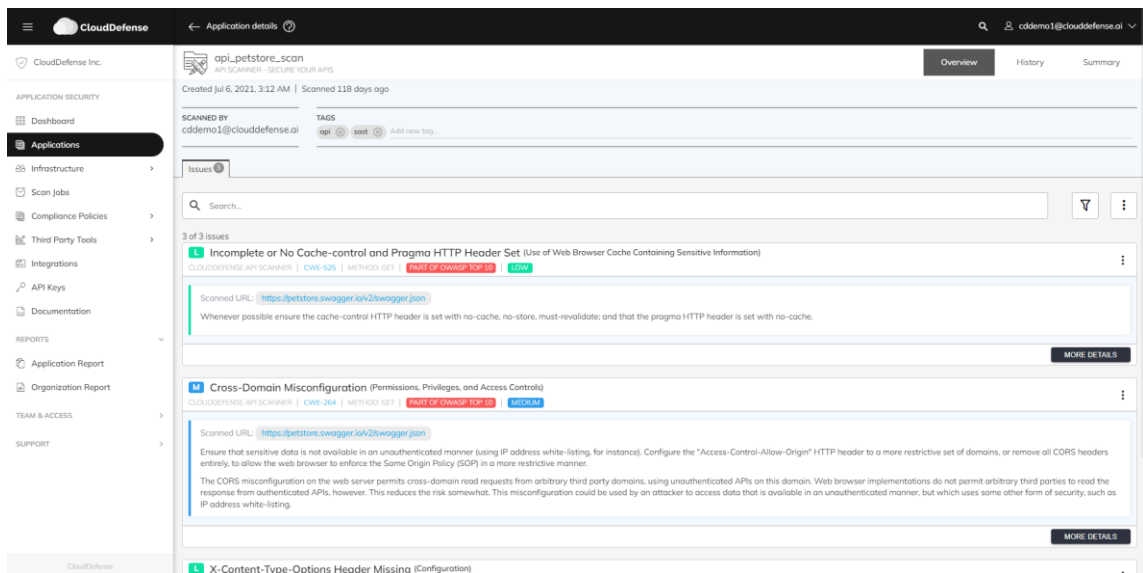
Organizations use hundreds of APIs across many applications. The most popular API specs are Swagger APIs or Open APIs. These APIs can be exposed for upstream and downstream systems - sometimes APIs can be publicly exposed.

APIs might have hundreds of issues such as cross-site scripting, click-hijacking, and much more. In the absence of correct controls, your organization might be susceptible to breaches. The current API vulnerability identification process is heavily manual and requires security expertise. The current process is also not a continuous security scanning process which might lead to the accidental slippage of the issues during the release cycle.

This is how CloudDefense helps!

CloudDefense's simplified agent can analyze your APIs on OWASP Top 10 by simply using a simple command. It can also be integrated as part of your development process so that your team benefits from continuous security. You can also enable build-gating criteria for promoting or failing the build in case vulnerabilities are discovered.

All of this data is compiled and present to your team in a beautiful interface. This also helps you check historical results.



CloudDefense's API Scanning

We analyze APIs on following OWASP Top 10 criteria:

Top 10 Web Application Security Risks

1. [Injection.](#)
2. [Broken Authentication.](#)
3. [Sensitive Data Exposure.](#)
4. [XML External Entities \(XXE\).](#)
5. [Broken Access Control.](#)
6. [Security Misconfiguration.](#)
7. [Cross-Site Scripting XSS.](#)
8. [Insecure Deserialization.](#)
9. [Using Components with Known Vulnerabilities.](#)
10. [Insufficient Logging & Monitoring.](#)

Auto-Remediation for SCA

For SCA, we provide auto-remediation for vulnerabilities discovered in your code so that your developers can generate automated PR to fix the issues.

“Your Developers can leverage Auto Remediation Feature”

CloudDefense’s SCA scan is a tool that provides an end-to-end comprehensive solution for issues in the code that leverage Open-Source components. When you run the SCA scan, the tool scans through not just the code but also related artifacts like containers and registries. It identifies all open-source components and helps detect security vulnerabilities within.

Additionally, the tool then helps prioritize vulnerabilities into CRITICAL, HIGH, MEDIUM or LOW classifications. This way, customers can take informed decisions regarding which vulnerabilities to prioritize for fixing.

Detection and Prioritization is one thing, Cloud Defense takes it one step further by providing what remediation is required to fix these vulnerabilities. Often times, an updated version of the Open-Source Libraries contains the fix for the known vulnerabilities. This insight is provided right in the Scan results.

Developers don't have to go figure out a solution for the vulnerabilities, instead, just use the recommended fix provided in the scan results.

Developers love this feature!

The screenshot displays the CloudDefense Open Source Scanner interface. It lists three vulnerabilities with their details and remediation steps:

- org.postgresql:postgresql (Improper Restriction of XML External Entity Reference)**
 - CVSS: 7.7
 - Introduced through: org.postgresql:postgresql:42.2.5
 - Discovered on: Jun 4, 2020, 8:15 PM
 - License: Unknown
 - Exploit: 2.2
 - Fixed in: 42.2.13
 - Remediation: Upgrade dependency org.postgresql:postgresql@42.2.5 to version 42.2.13
 - Code snippet:

```
1. <dependency>
2. <groupId>org.postgresql</groupId>
3. <artifactId>postgresql</artifactId>
4. <version>42.2.13</version>
5. </dependency>
```
 - PostgreSQL JDBC Driver (aka PgJDBC) before 42.2.13 allows XXE.
 - Buttons: **HIDE FIX**
- org.springframework:spring-web**
 - CVSS: 6.5
 - Introduced through: org.springframework:spring-web:5.1.4.RELEASE
 - Discovered on: Dec 3, 2021, 1:08 AM
 - License: Apache-2.0
 - Exploit: 1.3
 - Fixed in: Not fixed
 - Buttons: **SHOW FIX**
- org.apache.tomcat.embed:tomcat-embed-websocket (Uncontrolled Resource Consumption)**
 - CVSS: 7.5
 - Introduced through: org.apache.tomcat.embed:tomcat-embed-websocket:9.0.14
 - Discovered on: May 29, 2019, 1:29 AM
 - License: Apache-2.0
 - Exploit: 3.9
 - Fixed in: 9.0.35-3.39.1
 - Buttons: **SHOW FIX**















CloudDefense's Auto Remediation

Seamless Integration and Support

CloudDefense integrates into all major languages and CI/CD pipelines. We offer advanced integrations for Cloud and Container coverage allowing your team to connect data sources and get a centralized view putting security front and center.

CloudDefense’s Programming Language Coverage.

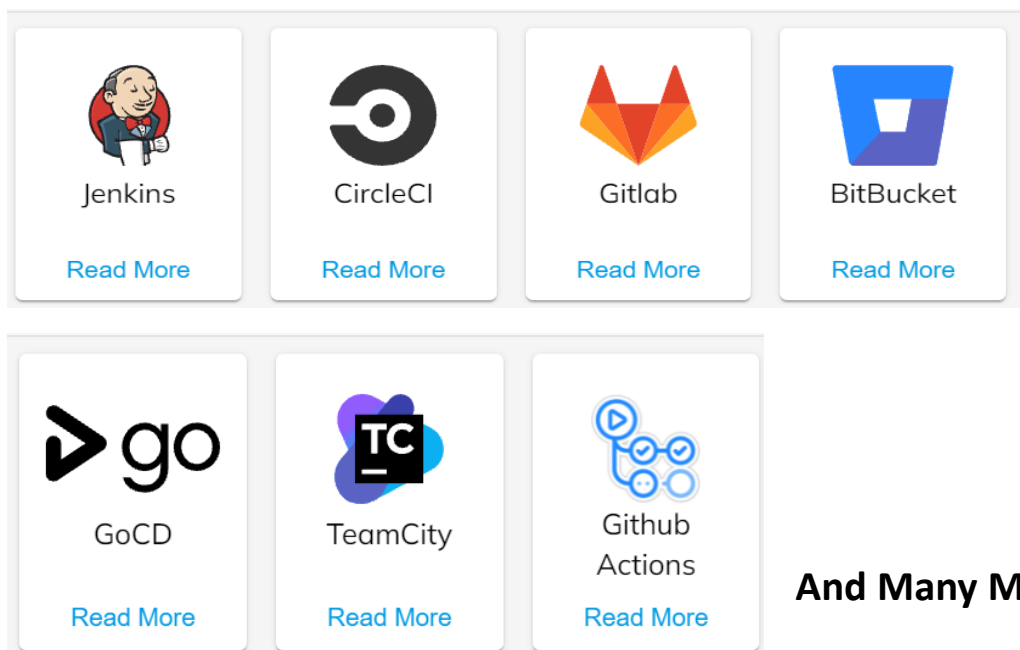
Currently we support the following programming languages. We will be adding additional language (Shift, Kotlin, Objective C) support with further releases.

 Java Read More	 .NET Read More	 Kotlin Read More	 Python Read More	 Swift Read More	 Go Read More	 PHP Read More
 TypeScript Read More	 ObjectiveC Read More	 JavaScript Read More	 C Read More	 Rust Read More	 C++ Read More	 Ruby Read More

Programming Languages Supported

CloudDefense’s CI/CD Coverage:

Currently, we support the following CI/CD. We are continuously adding more CI/CD support. If your team would like any additional CI/CD support then reach out to us at sales@cloudefense.ai



All Major Continuous Integration and Deployment System Supported

CloudDefense's Cloud Coverage:

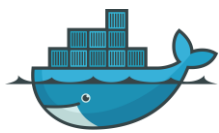
Currently, we support the following Cloud Platform for application security.



All Major Public and Private Cloud Supported

CloudDefense's Container Coverage:

Currently, we support the following containers and container registries. We are adding more registries. If you have additional registries that your team would like any additional container or registry, then reach out to us as sales@cloudefense.ai



docker



kubernetes



Amazon EKS

All Major Container Registries Supported

CloudDefense's Dev Tool Integration:

CloudDefense easily integrates with Slack so that as soon as a scan is run, you receive a notification. We also support JIRA integration so that right from the vulnerability, you're able to create a JIRA ticket..



Seamless Developer Tools Integration

CloudDefense's Solution Types:

“CloudDefense supports SaaS and OnPrem (Docker and Kubernetes) deployment”

“You can choose the solution based on your organizations' need”

- **SaaS Based Service:** CloudDefense provides SaaS based solutions. We also provide tenant isolation for large implementation.
- **On-Prem Version:** CloudDefense has Kubernetes instances which can be setup inside your premise so that everything stays behind your firewall. You're able to configure how frequently your team wants to refresh the vulnerability data.

Vulnerability Database & Reporting

CloudDefense offers automated reporting for teams and executives looking to stay ahead of security concerns. Continuous monitoring allows your team to be informed immediately. Reports can also be generated for team members or executives.

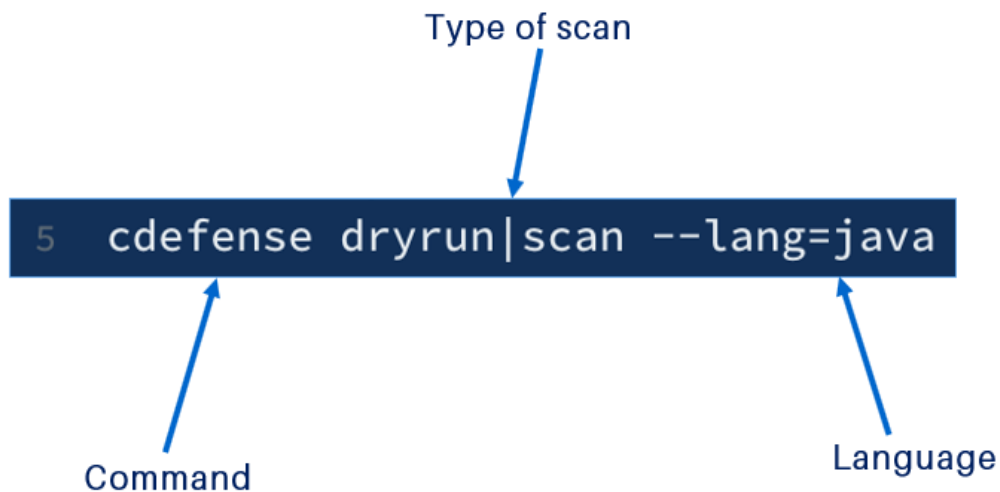
CloudDefense's Vulnerability database:

CloudDefense's vulnerability database is backed by **the vFeed vulnerability intelligence service**, which is one of the industry's top vulnerability databases.

“The vFeed database gets updated 4 times in a day so that as soon as a vulnerability gets discovered, your team can be notified, and your application can be secure. This way, your application is continuously secured, and your data is safe. vFeed ”

“Loved by Developers”

CloudDefense's proprietary technology is easy to use. You don't need to be a security expert to run. Your applications can be secure just by running the following simple command:



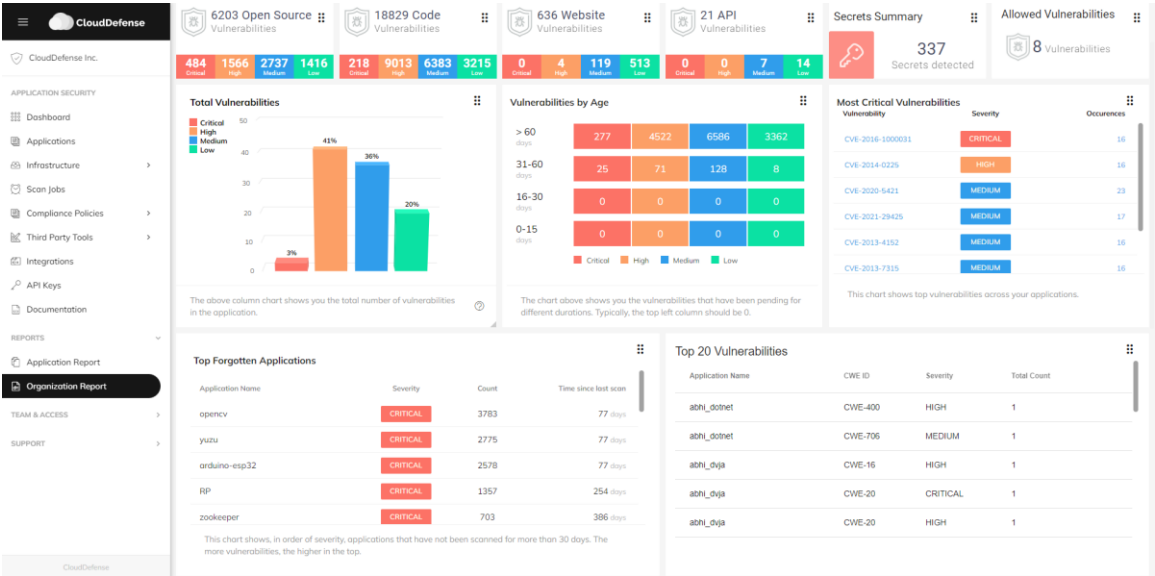
The simple command supports SCA/SAST/DAST/API/Container Scanning. For SCA scans, CloudDefense auto detects the language. With the dry run option, developers can see the vulnerabilities locally, without logging the results to the web console..

Get Started

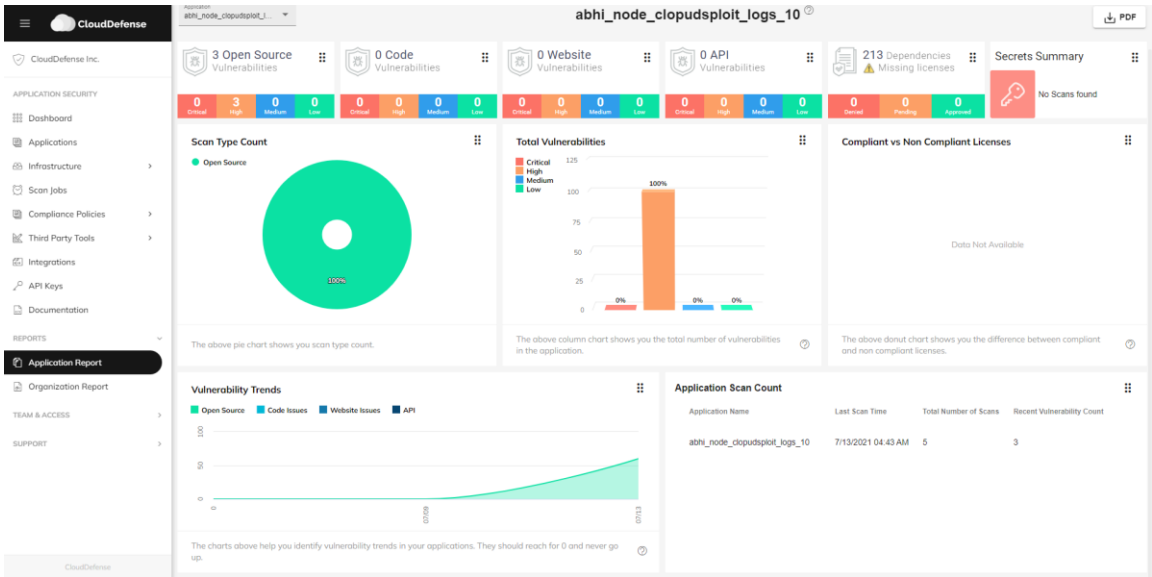
- FREE TRIAL
<https://console.clouddefense.ai/onboarding>
- GET DEMO
<https://www.clouddefense.ai/cd/contact>

CISO/Executive Reports:

CloudDefense provides an executive report which you can review in your team meeting. We provide reports at the organization level or the team level. Individual application reports are also supported. You can schedule the report which will be emailed to your inbox in PDF format.



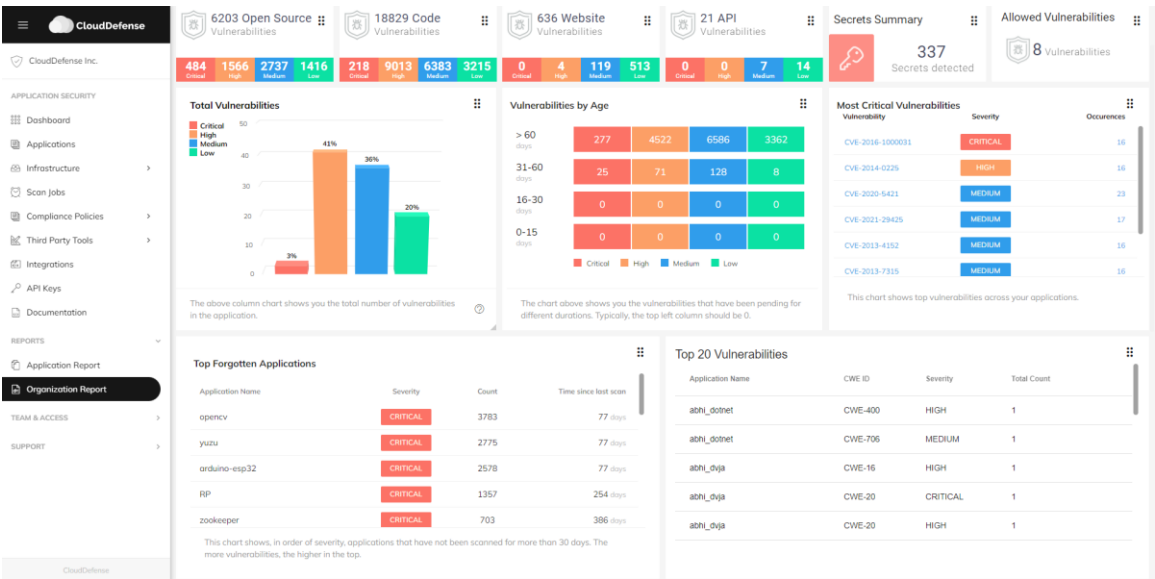
CloudDefense's organization Level Report



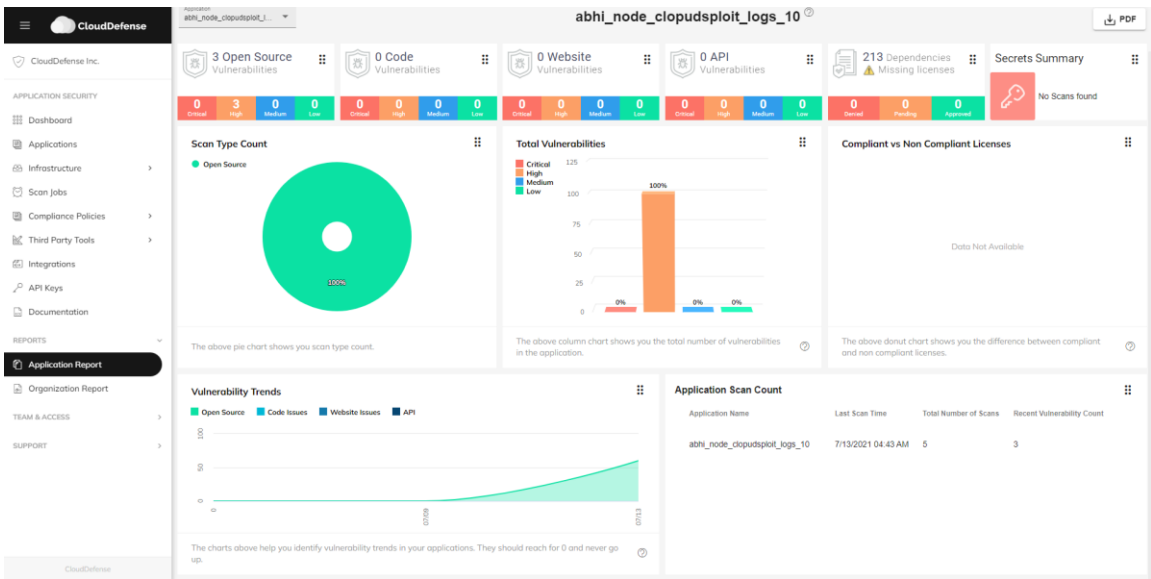
CloudDefense's application-Level Report

CISO/Executive Reports:

CloudDefense provides an executive report which you can review in your team meeting. We provide reports at the organization level or the team level. Individual application reports are also supported. You can schedule the report which will be emailed to your inbox in PDF format.



CloudDefense’s organization Level Report



CloudDefense’s application-Level Report

About CloudDefense Inc.



CloudDefense is the industry's leading application security provider. We bring security closer to the developer so that applications are secured continuously through the development process

Our powerful technology analyzes the security of your application for SCA, SAST, DAST, API, Containers and the data resides in an easy-to-use UI, which can be ingested into your own custom dashboard.

GET DEMO:

<https://www.clouddefense.ai/cd/contact>

QUESTIONS: sales@clouddefense.ai