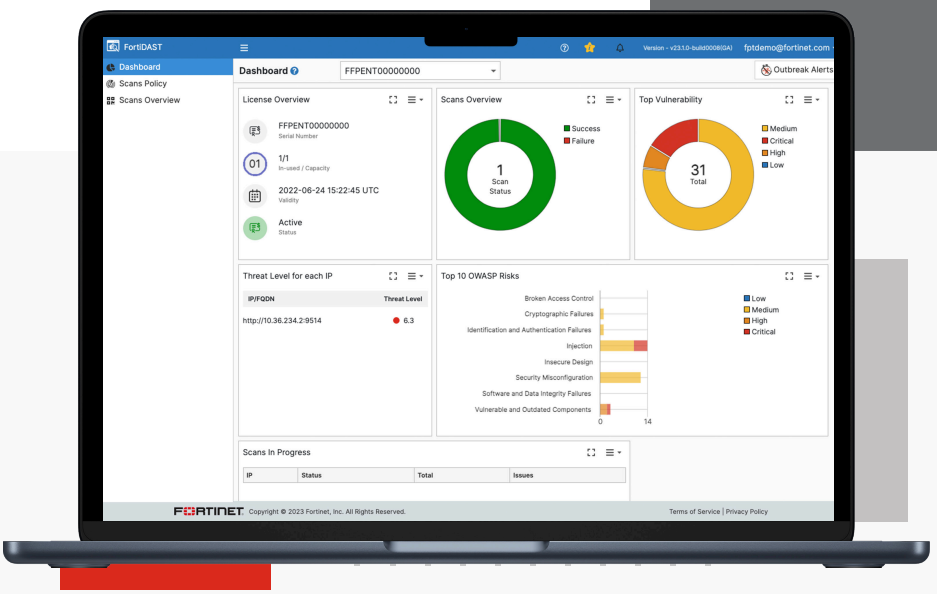
FortiDAST

Available in:

Proxy

Cloud



Highlights

Automate testing of web applications for OWASP Top 10 and other vulnerabilities

Schedule or perform testing on-demand

Get guidance for remediating risks

Easily generate summary and detailed reports on results

Prioritize vulnerabilities for remediation based on threat scores computed from CVSS values

FortiDAST utilizes FortiGuard Labs' extensive threat research and knowledge to enhance efficacy

LABS

Dynamic Application Security Testing

FortiDAST combines advanced crawling technology with FortiGuard Labs' extensive threat research and knowledge base to test target applications against OWASP Top 10 and other vulnerabilities. Designed for Development, DevOps and Security teams, FortiDAST generates full details on vulnerabilities found — prioritized by threat scores computed from CVSS values — and provides guidance for their effective remediation.

Features and Benefits

Black-Box Testing

Automate front-end or black-box testing of web apps against OWASP Top 10 and other vulnerabilities

Integration into CI/CD

Use with FortiDevSec to get full lifecycle coverage of your web applications from inception to production

Advanced Crawling

Use advanced crawling to reach and scan all web application branches and pathways

Vulnerability Scanning

Find run-time application security issues and bugs

Risk Analysis

Analyze threats and misconfigurations that pose risk based on threat scores calculated from CVSS values

Fuzzer Expertise

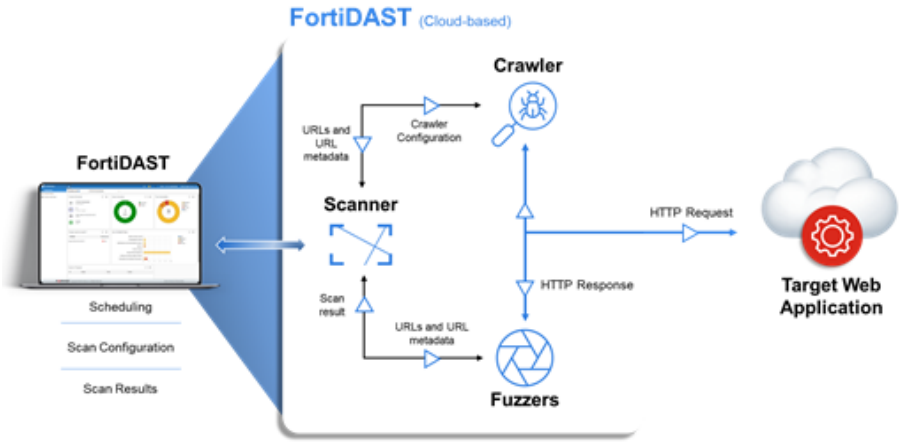
Get top efficacy using fuzzers and tests skillfully written by Fortinet experts

CI/CD Coverage

Get full CI/CD lifecycle coverage through native integration with major CI/CD tools and FortiDevSec

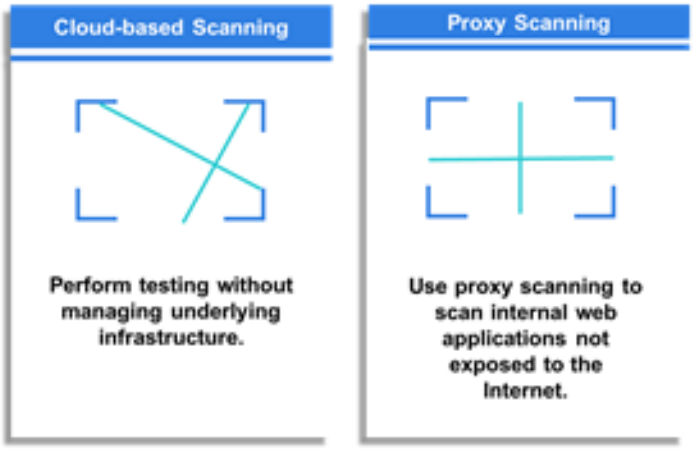
How It Works

FortiDAST employs a powerful crawler and expert-designed fuzzers to crawl and test your web applications for vulnerabilities, simulating tactics threat actors would take in the real world.



Deployment Flexibility

FortiDAST provides multiple deployment options to best fit your organization's needs.



Features

FortiDAST incorporates the following features and capabilities.

DEPLOYMENT FLEXIBILITY	Cloud-based
	Proxy
DISCOVERY	Discovery of existing web assets
SCANNING	Scans for OWASP Top 10 Vulnerabilities
	Scans for Non-OWASP Vulnerabilities
	Scanning of Non-public Internal Assets (1)
	Automatically scans based on triggers
	Recon Engine: Identifies technologies, ports and services on scanned assets
	Exploit Engine: Scans to check the exploitability of n-day vulnerabilities using built-in exploit signatures
SCAN CONFIGURATION	Asset Crawling: Same host or same domain
	User Browser Interaction Simulation (Event Simulation) using Web Automation
	Forced Browsing: Option to upload customer wordlists, inclusion or exclusion lists
	Inclusion/Exclusion Lists
	Crawling Based on API and WADL Definition Files; Detects Websocket Endpoints
	Simple HTTP Request
	Asynchronous HTTP Request
	HTTP Authentication (Basic, Digest, NTLM)
	Login Using Web Auth Module
	Scans Single-page Applications (SPA)
	Scans Authenticated Applications
	Ability to Find Out-of-Band/Blind Vulnerabilities
	API Crawling
	JSON
	YAML
	WADL
	Schedule Scans
	Schedule Recurring Scans (Daily/Weekly/Monthly)
SCAN TYPES AND FEATURES	Supports Quick and Full Scans
	Supports Rescanning
	Scan Comparisons
	Vulnerability Review System
INTEGRATIONS	CI/CD Platforms
	Gitlab CI
	Jenkins
	FortiDevSec
	Other Major Platforms
	Issue Tracking
	Jira
	REST API (for basic and privileged access for automated scanning)
	Fortinet Integrations
	FortiWeb Cloud (Supports Virtual Patching)
	- Ability to generate XML reports to create WAF rules
MONITORING AND REPORTING	Intuitive User Interface/Dashboard
	Customizable Email Notifications
	Summary Reporting
	Detailed Reporting
	WAF Reporting
	Ability to map detected CVEs to FortiGuard OBAs

(1) Supported through Proxy deployment mode.

Features

FortiDAST uses a reconnaissance engine to provide server (host) and web service or application related information to the fuzzer modules to optimize and enhance vulnerability scanning.

FUZZER EXPERTISE	Injection
	Remote Code Execution
	Server-Side Template Injection
	File inclusion
	LDAP Injection
	NoSQL Injection
	SQL Injection
	XPATH Injection
	Code Injection
	XSS (Cross site scripting)
	Insecure file upload and manipulation via WebDAV
	Open Redirect
	Path Traversal
	ORM Injection
	Expression Language (EL) / Object Graph Navigation Library (OGNL) Injection
	Broken Access Control
	Forced Browsing
	Server Side Request Forgery
	Indirect object referencing (IDOR)
	Cryptographic Failures
	SSL Tests
	Weak Ciphers
	Security Misconfiguration
	XML external entity (XXE) injection
	Information Disclosure
PROPRIETARY EXPLOIT ENGINE COVERAGE	Apache HTTP Server
	Apache Struts
	Apache Log4J
	dotCMS
	IIS
	Java Primefaces
	Joomla!
	Microsoft Exchange
	Nginx
	OpenSSL
	PHPUnit
	RomPager
	SAP
	Sharepoint
	ThinkPHP
	WordPress
	ZeroShell

Highlights

Vulnerability Testing

FortiDAST leverages OWASP's Top 10 Web Application Security Risk list as well as separate resources on vulnerabilities to craft a series of tests designed to verify that a target system has been successfully secured against exploit or penetration. FortiDAST can also take advantage of a third-party command and control (C&C) server, allowing security modules to carry blind attacks. Full results are displayed and categorized by their CVSS severity score. Based upon these CVSS scores, an overall Threat Score for the target is generated and displayed.

Advanced Crawler Technology

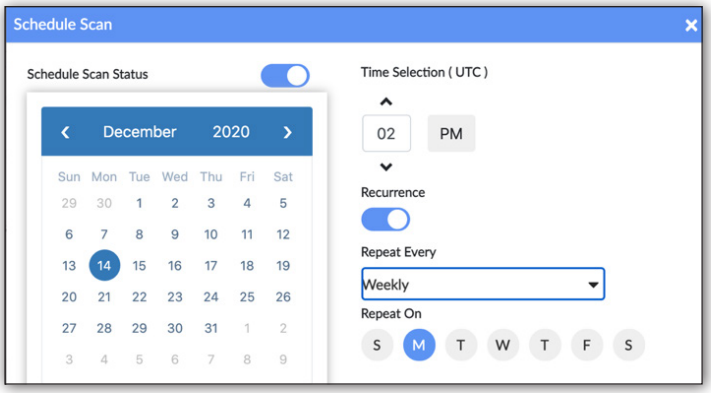
FortiDAST employs an advanced crawler to identify and scan all branches and paths in web applications including JavaScript-heavy web applications. FortiDAST's crawler can also be configured to perform authenticated crawling.

Fuzzer Expertise

Fortinet employs a team of experts skillfully experienced in writing fuzzer rules or tests, further enhancing FortiDAST's efficacy in identifying vulnerabilities.

Schedule Tests at Desired Intervals

Scans can be scheduled for a specific time, or set to recur based on chosen criteria.



Detailed Results with Suggested Remediation

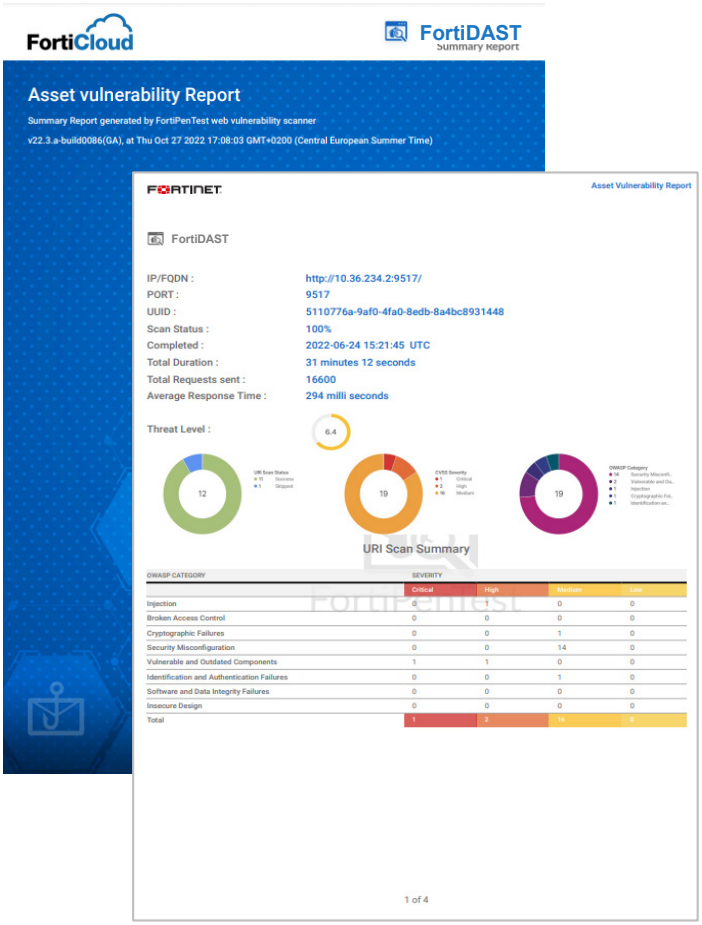
Each vulnerability found can be drilled down to get detailed information on the issue along with suggested remediation steps.

Robust Report Engine

Generate summary and detailed reports for informing leadership of vulnerabilities in web applications and associated risk, or for demonstrating compliance to auditors.

Highlights

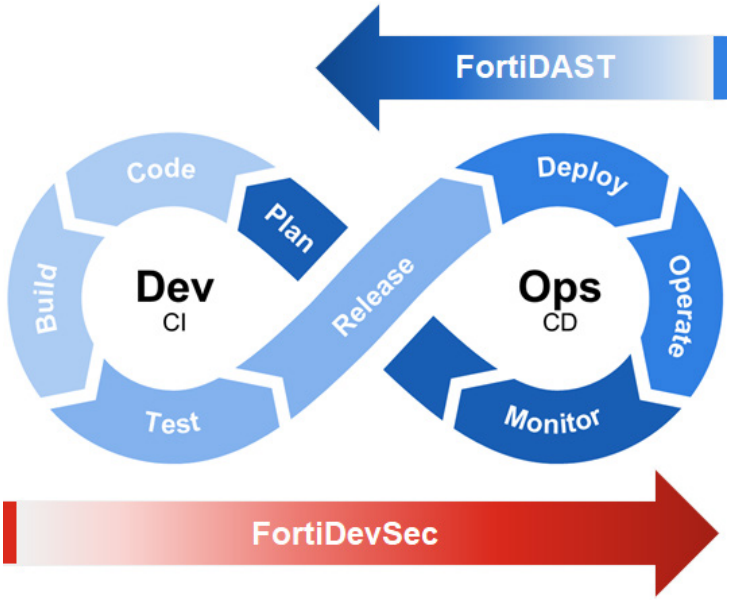
FortiDAST runs a series of tests and attacks to determine what vulnerabilities a target IP address or Fully Qualified Domain Name (FQDN) is susceptible to, then provides full details on not only the vulnerability, but also what you can do about it. Configurable email notifications allow you to choose what you want to be alerted on.



Highlights

Integration with FortiDevSec

FortiDAST is integrated with FortiDevSec for complete CI/CD coverage. FortiDevSec enables developers to detect and remediate security vulnerabilities across the full continuous integration/continuous delivery/deployment (CI/CD) lifecycle. FortiDAST is also natively integrated with other major CI/CD tools.



Fortinet CI/CD Lifecycle Coverage

Ordering Information

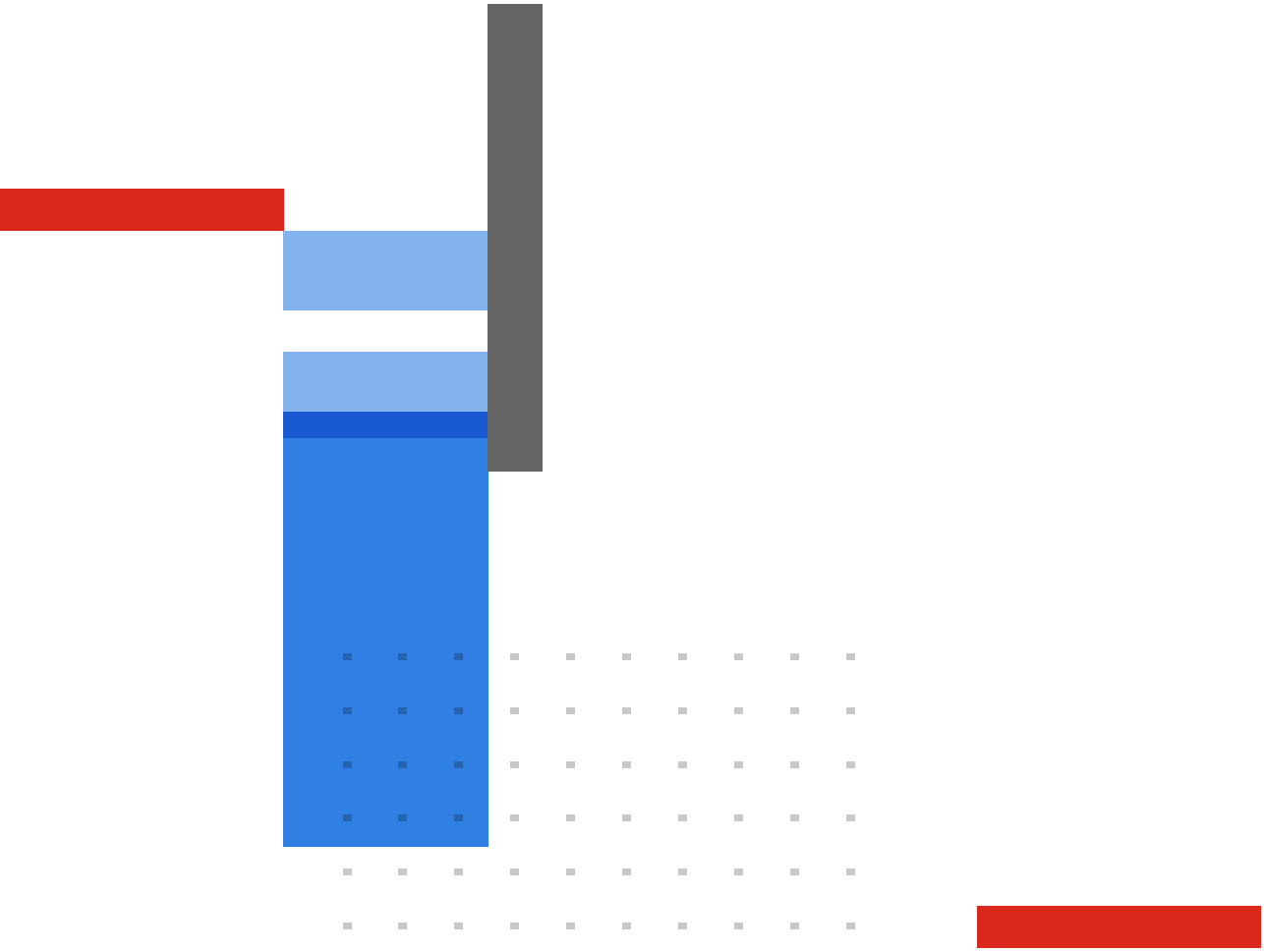
FortiDAST is licensed in blocks of 10 IP/FQDN targets. A trial subscription to FortiDAST is available to FortiCloud Premium subscribers. This trial version is limited to a single IP address / FQDN and will only test to a limited subset of the OWASP Top 10 list.

Product	SKU	Description
FortiDAST	FC-10-FPENT-236-02-DD	This stackable license adds 10 additional IP / FQDN targets to a single FortiDAST cloud account.

Visit https://www.fortinet.com/resources/ordering-guides for related ordering guides.

Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.



FORTINET

www.fortinet.com

September 26, 2024

FDT-DAT-R03-20240926