PREVOTY Datasheet

Automate defense and intelligence for applications and services

Data theft and tampering, fraud, compliance, and a host of other threats weigh heavily on every information security team. With a dizzying array of software controlling and automating all aspects of every organization, runtime application security that detects and responds to threats is critical for reducing risk.

Prevoty offers a simple-to-use, DevOps-oriented application security solution that automates protection and provides unprecedented levels of actionable visibility into production attacks. Use Prevoty to keep applications and data safe against cyber threats.

With Prevoty installed, applications run in either Monitor or Protection mode:

Application Monitoring: Prevoty's monitoring capability delivers unparalleled insights into the threats that are actually hitting an application at runtime, giving real-time threat intelligence from inside your applications. Monitor mode is useful for software evaluations, and extremely instrumental in exposing previously unknown vulnerabilities within enterprise applications.

Application Protection: Protection mode is the next tier above everything within monitoring mode, plus it actually sanitizes all incoming data - removing malicious queries and invalidating tokens, all the while delivering authenticated input to applications - to keep data safe and applications secure.

Increase Visibility

What do applications see afterthey've been deployed? Gain continuous, actionable insights into unusual behavior and view correlated network, database and application analytics on every attempted attack and threat, in real-time. Focus on what counts, with fewer false alarms.

Discover Unknown Risks

Increase threat intelligence and eliminate guesswork with application monitoring. Expose inherent vulnerabilities and take necessary corrective action. Reduces noise and delivers uniform, reconciled insights - eliminating distractions so that resources are deployed only where and when needed.

DevSecOps Scalability

Rapid scaling using orchestration tools and platform-based deployments makes Prevoty the first seamless and DevOps-friendly deployment for application security. Plugs directly into existing Continuous Integration / Continuous Deployment processes to analyzes data input and state changes at runtime.

Real-Time Protection

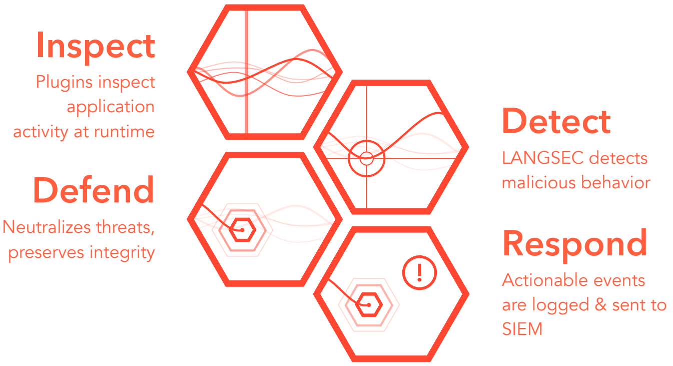
Inspect, detect, alert and respond - all at once. Unlike security testing, which finds hypothetical vulnerabilities, Prevoty inspect payloads in real-time to sanitize user input, prevent exploits and reduce production application risk. Eliminate security holes in legacy systems, third party applications and new development.

How Prevoty Works

The Prevoty solution accurately identifies and neutralizes application-level attacks in real-time by using a patented language security-based input analysis technology called LangSec. LangSec processes and evaluates all incoming application data with no dependence on definitions, patterns, regular expressions, taint analysis or behavioral learning.

By understanding how data will execute in an environment, it effectively sees through any obfuscation or fuzzing of data input. Threats are **sanitized within-context**, **nullified** in **real-time**, and **logged**, within safeguarding confidential data and protecting users.

Applications call the LangSec engine using via either Prevoty Plugins or Software Development Kits (SDKs), which communicate directly over secured network protocols via an open API.



Inspect
Plugins inspect application activity at runtime

Detect
LANGSEC detects malicious behavior

Defend
Neutralizes threats, preserves integrity

Respond
Actionable events are logged & sent to SIEM

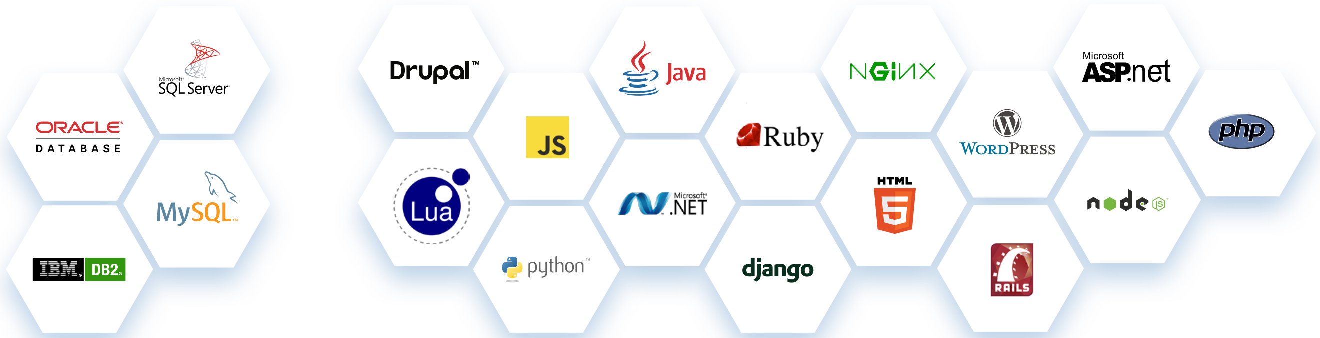
Plugin Highlights

- No coding changes required, allowing for easy installation
- Compatible for use with both new and legacy applications
- Only vulnerable data paths are monitored for malicious activity, minimizing performance impact
- Available for multiple platforms including: .Net, Java, Rails, Drupal and Lua

SDK Highlights

- Standardized to allow for maximum compatibility
- Easy integration into key locations of existing applications via an API call
- Performs the same analysis and returns the same intelligence data as the Prevoty plugins
- Available for a wide variety of languages and frameworks including: C#, Java, Node.js, Go, PHP, Python, and Ruby

Compatible Databases & Frameworks



Identified Threat	Solution
SQL Injection (SQLi) OWASP A1	Even the most sophisticated SQL injections can be prevented, including those that originate via other APIs, partner applications, RSS feeds, synthesized queries, and more.
OS Command Injection (Ci) OWASP A1	Organizations have the ability to target specific applications more prone to Ci attacks, securing them down to specific application-level processes and allowing only the pre-approved system commands.
Broken Authentication Protection and Session State Management OWASP A2	Prevoty detects and blocks HTTP response objects that contain invalid basic authentication headers, and protects against sessions or credentials being sent over an unencrypted link preventing broken authentications and ensuring secured session states.
Cross-Site Scripting (XSS) OWASP A3	Prevoty offers unprecedented defense against injected scripts or script fragments, either through unvalidated input in the Document Object Model (DOM), 'reflected' or stored XSS scripts, and via XML External Entities (XXE). Incoming code is effectively analyzed, including HTML, CSS, XML and JavaScript, whether it's a full document, plain text or mixed content.
Sensitive Data Protection OWASP A6	Protection against sensitive data exposure, uncaught server errors, and missing cache control headers within the HTTP Response Object, keeping confidential information such as credit card numbers, national ID numbers, etc. safeguarded.
Cross-site Request Forgery (CSRF) OWASP A8	Prevoty generates and validates cryptographically unique tokens to prevent CSRF attacks by identifying malformed, expired and replayed tokens, preventing user identity theft and fraud.
Invalidated Redirects/Forwards OWASP A10	Prevoty prevents improper phishing, unvalidated redirects and protects against unauthorized URL forwards, eliminating this threat in its entirety.
HTTP-Response Splitting	HTTP-Response Splitting is successfully detected and eliminated, ensuring that the intended payload returned by the application is secured and authentic, protecting output presented to clients and client interactions.
Path Traversal Protection (PT)	Prevoty protects against unauthorized PT file access by canonicalizing URL paths, and ensuring the directories and subdirectories exist on a predefined approved whitelist, preventing unauthorized access.

Solution Benefits

Vulnerability Mitigation in Real-Time

Prevoty automatically modifies and/or blocks payloads in real-time - cleaning up not just malicious but also malformed inputs before they hit the application or database, with fewer false positives. The "Detect, Report, Fix" cycle takes a new meaning since the "Fix" is performed at runtime by the Prevoty engine, rather than waiting on developers to patch a vulnerability.

Continuous, Correlated Security Intelligence

The security analytics available through an array of SIEMs/Log Managers such as Splunk, QRadar, and others, help to connect the dots between application vulnerabilities, attempted threats, the network and the user, providing correlated data between each of these points for greater overall security intelligence.

High-Performance Speeds

With high-functioning algorithms designed for large-scale use, Prevoty comfortably processes tens of thousands of requests per second, which is 30-50x faster than traditional pattern-matching approaches.

DevSecOps Transformation

Prevoty powers the first seamless, scalable and DevOps-friendly deployment for runtime application security. Think one-click installations and no external dependencies. DevOps teams can now automatically harden and deploy applications to any environment and at any scale -- mitigating critical security issues without the endless retest cycle.

Protection for Legacy Systems

Existing legacy applications with known vulnerabilities can be fully protected and have state-of-the-art security protection as newer applications and development.

Partners

Prevoty is proven, trusted, and employed throughout multiple Fortune 50 companies and other enterprises spanning the global banking and financial industries, education and university campuses, retail corporations, and entertainment networks.

Prevoty also maintains strategic partnerships and technological alliances to amplify its range of capabilities and enable businesses to be more intelligent, sophisticated, and proactive with their application security strategies.

amazon web services
docker
Pivotal
CHEF
puppet
ANSIBLE

WhiteHat SECURITY
DENIM GROUP
ASTECH consulting
GOTHAM DIGITAL SCIENCE A STROZ FRIEDBERG COMPANY

splunk>
QRadar
intel Security
SECURONIX

Complimentary Proof of Value

We encourage you to reach out to our staff with any questions, or to arrange a complimentary proof of value session to demonstrate how Prevoty's application security solution can be of value to your organization.

Prevoty, Inc.
11911 San Vicente Blvd. #355
Los Angeles, CA 90049 U.S.A.

+1 310-499-4714
+1 866-940-2540 (toll free)

support@prevoty.com
prevoty.com