# Table of Contents

- **Executive Summary** ........................................... 4
- **Product Overview** ........................................... 5
- **Network Deployment Options** .............................. 8
- **Application Modes: Monitor and Protect** ............... 9
- **What Threats Does Prevoty Protect Against?** ........... 10
- **Performance Impact** ........................................ 14
- **Product Benefits** ............................................ 15
- **Complimentary Proof of Value** ............................ 16
- **Summary** ..................................................... 16
- **Additional Support** .......................................... 17
Executive Summary

With the wealth of confidential data needing protection, application security has become of the utmost importance and a central focus to maintaining safe business practices across an ever-changing internet-centric global landscape.

The frequency and impact of hacking attempts against websites and applications continue to rise to extraordinary levels, creating a significant impact on enterprises. The most common attacks according to OWASP\(^1\) and numerous industry studies\(^2\), include Cross-site Scripting (XSS), Command Injection (Ci), SQL injection (SQLi), and Cross-site Request Forgery (CSRF).

Unfortunately, these types of attacks are also the most devastating with the highest risk and most potential for serious damage. When successful, these attacks can lead to many issues including brand defacement, exfiltration of confidential data, user ID theft and a host of other serious problems stemming from hackers and cybercriminals having unfettered access to applications and data services (caches, databases, filesystems, etc.) behind the firewall.

“It is estimated that 90% of reported security incidents result from exploits against defects in the design or code of software.”\(^3\)

Prevoty has developed a unique product set that provides an unprecedented level of protection, using LANGSEC methodology to operate at runtime and inside the applications themselves. Prevoty’s application security solution identifies and eliminates all of these attacks, keeping organizations’ and their software safe.

This paper provides a technical overview of the components that make up the Prevoty solution.

---

\(^1\) Open Web Application Security Project (OWASP), [http://www.owasp.org](http://www.owasp.org)


\(^3\) Dept. of Homeland Security’s Software Assurance Program ([https://buildsecurityin.us-cert.gov/software-assurance](https://buildsecurityin.us-cert.gov/software-assurance))
Product Overview

Prevoty has developed a unique product set that provides an unprecedented level of protection, using LANGSEC methodology to operate at runtime and inside the applications themselves. Prevoty’s application security solution identifies and eliminates all of the most common cyber-attacks, keeping organizations’, their data, and their software safe.

How Prevoty Works

Prevoty provides a comprehensive application security solution designed to protect organizations against the top application security threats from an easily deployable runtime service. This solution consists of three main components:

- **Prevoty Engine**
  A fast, distributed system comprised of a number of modular services that inspect data using patented LANGSEC and other analysis techniques.

- **Prevoty Plugins/SDKs**
  Agents that monitor application behavior, routing data payloads to the Prevoty Engine for analysis.

- **Prevoty Manager**
  A web-based console for configuring application security controls, policies, and plugin configuration settings.

Prevoty Security Engine

The Prevoty solution is based on a highly unique and efficient security analysis engine, which accurately identifies and neutralizes application-level attacks in real-time by using a patented language security-based input analysis engine, 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 prevents any obfuscation or fuzzing of data input. Identified threats are sanitized *with-context*, nullified in *real-time*, and logged, thus safeguarding confidential data and protecting users. The engine is called by applications via either Prevoty plugins or SDKs, which communicate over secured network protocols.
The Prevoty Engine also provides high visibility into what is actually going on in the applications during runtime, by providing in-depth information on each attempted threat. These data metrics may be transmitted to custom data stores, made directly available to logging tools or fed into a Security Information and Event Management (SIEM) by communication predefined JSON payloads via TCP/UDP.

Examples of compatible logging tools include: syslog, Unix socket, Splunk, IBM QRadar, HP ArcSight, or information may be exported as a CSV for further reporting and analysis.

Prevoty Plugins/SDKs
Applications communicate directly with other Prevoty components via an open API that is called from pre-built plugin frameworks, or from the business logic of the application via Prevoty software development kits (SDKs). Applications can either be centralized or distributed, allowing for a fully scalable enterprise-wide security solution, offering protection for new development, legacy applications and 3rd-party integrations.

Prevoty Plugins
Prevoty plugins are available and supported for .NET, JAVA, Nginx and Kong. The Java framework is implemented as servlet filters and agents, and the .NET framework is implemented as an HTTP module. Below are several highlights of implementing using one of the Prevoty plugins:

- No coding changes are required within source code, allowing for easy integration.
- Plugins enable applications to intercept malicious content in a minimally invasive manner.
- Compatible for use with new and legacy applications.
- Only vulnerable data paths are monitored for malicious activity, minimizing any impact on application performance.

Prevoty Software Development Kits (SDKs)
Prevoty SDKs allow developers to quickly add Prevoty security into their applications. A single API call is added to the application whenever analysis is required, for example using GET and POST requests, or preceding a SQL query. Highlights of implementing with one of the Prevoty SDKs include:

- Standardized to allow for maximum compatibility.
- Easy integration into key locations of existing applications.
- Calls into the SDKs perform the same analysis as the Prevoty plugins, and return the same comprehensive intelligence data.
- SDKs are available for a wide variety of languages and frameworks.

<table>
<thead>
<tr>
<th>Programming Language</th>
<th>Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>C# (compatible with Classic ASP 2.0)</td>
<td>2.0 - 4.6</td>
</tr>
<tr>
<td>Java</td>
<td>1.5.0 - current</td>
</tr>
<tr>
<td>Node.js</td>
<td>0.11, 0.12, 4.0</td>
</tr>
<tr>
<td>Go</td>
<td>1.3 - current</td>
</tr>
<tr>
<td>PHP</td>
<td>5.3 - 5.6</td>
</tr>
<tr>
<td>Python</td>
<td>2.7</td>
</tr>
<tr>
<td>Ruby</td>
<td>2.0 - current</td>
</tr>
</tbody>
</table>

Prevoty Manager

Prevoty Manager provides a single web-based interface for managing application security control settings, creating plugin configurations, updating Java WAR files, and more.

Through Manager, users can easily create customized security policies that encompass a span of applications or narrow settings down to individual applications. Once created, these policies may be downloaded via configuration files and instantly applied within the applications, keeping enterprise security up-to-date with this intuitive and easy-to-use management tool.

Figure 2. Prevoty Manager Database Security Policy Page

Copyright © 2017 Prevoty. All Rights Reserved.
## Network Deployment Options

The Prevoty Solution is a highly-flexible, scalable system which can be integrated into a number of network architectures, based on the specific enterprise needs and requirements.

Each deployment option implements Prevoty as a Runtime Application Self Protection (RASP) solution, embedded within the application (using either Plugins or SDKs). The most common deployment configurations include:

- On-premises in a customer data center using RPMs or a pre-built virtual appliance
- SaaS (Software as a Service) using a Prevoty cloud or an organization’s private cloud
- Amazon Marketplace Instance (AMI) available through the Amazon Marketplace.

The main variance between the implementation options is deciding the best method for applications to interact with the Prevoty security analysis engine. The engine can exist externally, as in the cloud and on-premises architectures, or it can exist internally as a completely self-contained implementation.

Regardless of where the security analysis engine is hosted, the performance and accuracy are exactly the same, aside from minimal latency necessitated by the network communication.
Application Modes: Monitor and Protect

Users have the ability to configure each individual application to run in either of the available application modes:

- **Monitoring**: This mode detects and logs any identified threats. Monitoring mode may be useful for software evaluation purposes to prove the effectiveness of the Prevoty solution, and can also be instrumental in exposing the potential vulnerabilities within enterprise applications.

- **Protection**: This mode detects, logs, and nullifies identified threats. Protection mode is the next step above monitoring, as it provides everything within monitoring mode, plus it actually sanitizes incoming data, removing malicious queries and invalidating tokens, all the while delivering authenticated input to applications, keeping data safe and applications secure.

Switching between the two modes is seamless within the Prevoty Manager, and provides organizations greater opportunity to test, verify, and deploy the Prevoty solution with minimal impact on production.

<table>
<thead>
<tr>
<th>Application Mode</th>
<th>Monitor</th>
<th>Protect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ability to identify specific threats and sources</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Real-time notification of application security threats</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Integration with SIEMs and log management software</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Centralized security policy management across all applications, regardless of application type</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Data exfiltration prevention</td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>Content sanitization</td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>Token &amp; session ID management</td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>Man-in-the-middle protection</td>
<td></td>
<td>✔️</td>
</tr>
</tbody>
</table>
What Threats Does Prevoty Protect Against?

To meet the ever growing and changing needs of application-security, Prevoty has developed a solution that detects, monitors, and protects against the following types of attacks.

- Preventing SQL Injection (SQLi)
- Broken Authentication Protection and Session State Management
- Preventing Cross-site Request Forgery (CSRF)
- XML External Entity Protection (XXE)
- Database Access Monitoring
- Blocking OS Command Injection (Ci)
- Cross-Site Scripting (XSS)
- Sensitive Data Detection and Protection
- Prohibiting Invalidated Redirects/Forwards
- Eliminate Http-Response Splitting
- Path Traversal Protection

Preventing SQL Injection (SQLi)

The Prevoty security engine analyzes database queries and protects popular relational databases (Oracle, MySQL, IBM DB2, MSSQL, etc.) from SQL injections using advanced proprietary query virtualization, tautologies, and lexical analysis that can audit parsed fields, tables, functions and subqueries. Even the most sophisticated SQL injections can be prevented, including those that originate via other APIs, partner applications, RSS feeds, synthesized queries, etc.

The engine analyzes and compares SQL query parse trees, post-lexical analysis, to the relevant configuration that has been created (constraint solving). Reconciliation with the configuration reveals whether or not the query is planning to access a field that it should not, invoke a function call that it should not, attempt to access a database table that it should not and perform an invalid join/subquery.

Through the Prevoty Manager, security and development teams can further refine and customize database security policies with specific directives to allow or disallow access to specific tables, fields and functions. This feature provides protection for OWASP A1.

Blocking OS Command Injection (Ci)

Another level of protection that Prevoty offers, is protection against OS Command Injection attacks. These vulnerabilities enable an attacker to craft a payload that causes applications to execute other applications on the system, potentially giving control over to the attacker. Typically, these attacks take the form of a web application input that is insecurely passed and executed.

OWASP lists injection attacks as being one of the top threats to website security, and states
that injection flaws are very prevalent, particularly in legacy code. Unfortunately, many of these
attacks result in severe data loss, compromised systems, and network failure.

Prevoy stops Command Injection attempts by identifying every incoming application
command, and evaluating it prior to passing the code through for execution. With the Prevoty
game, organizations have the ability to target specific applications more prone to Command
Injection attacks, securing them down to specific application-level processes and allowing only
the pre-approved system commands.

During runtime, the Prevoty engine does a comparative analysis against an approved ‘whitelist’
of predefined application-level commands, which organizations create and customize
specifically towards their needs. This protection also addresses OWASP A1.

Broken Authentication Protection and Session State Management

The Prevoty solution will detect and block HTTP response objects that contain invalid basic
authentication headers, and detect and protect against sessions or credentials being sent over
an unencrypted link.

This feature offers protection from broken authentications and ensures secured session states
for users, which addresses OWASP A2.

Cross-Site Scripting (XSS)

Cross-Site Scripting (XSS) attacks are widespread and occur when malicious users inject scripts
or script fragments, either through unvalidated input in the Document Object Model (DOM),
through ‘reflected’ or stored XSS scripts, or via XML External Entities (XXE). While these
variations overlap in some areas, each type of XSS attack employs specific scripting methods
thereby requiring a solution that offers complete XSS protection.

The Prevoty solution is designed to protect against and eliminate each type of XSS attack, and
offers unprecedented defense against all levels of cross-site scripting. Prevoty effectively
analyzes all incoming code, including HTML, CSS, XML and JavaScript, whether it is
fragmented, a full document, plain text or mixed content.

All content is lexically formed and transformed. Based on the analysis of the content, the
Prevoy security engine predicts web browser executions, then pinpoints and surgically
removes bad content while preserving data fidelity. By being within the control flow of an
application, the Prevoty engine provides a rich statistical data structure containing key security
metrics that allow a developer to make decisions on what actions to take. This protection
addresses OWASP A3.
Sensitive Data Detection and Protection

This feature within the Prevoty solution, minimizes and protects against sensitive data exposure. Confidential information such as credit card numbers, national ID numbers, etc. are detected and the data is prevented from being logged and stored.

This capability also detects and prevents uncaught server errors and offers the ability to serve a selected default URL. In addition, plugins will also detect and insert missing cache controls headers within the HTTP Response object. This protection addresses OWASP A6.

Preventing Cross-site Request Forgery (CSRF)

The Prevoty security engine can generate and validate cryptographically unique tokens to prevent CSRF attacks by identifying malformed, expired and replayed tokens, preventing user identity theft and fraud. Prevoty’s token management guarantees two distinct levels of trust:

1. An application can trust that users are exactly who they claim to be

2. A user can trust that an application knows exactly when he/she is performing a state changing action (e.g. login, checkout, etc.)

The engine does this by keeping track of individually generated tokens and ensuring that they are only used as specified, through a Prevoty technology called SmartCache.

As an example, if a large organization is using Prevoty token management with their mobile applications, when a user logs in for the very first time, their mobile application calls home to retrieve a persisted token. Then for every state changing activity that the user does, the Prevoty engine actually does the “bucket brigading”: sending the timed token back and validating the request. If the timed token is valid, it executes; otherwise it sends a new timed token back that’s bound to the next request that the user is about to take.

In this way, an organization can make sure that users are who they say they are prior to taking the state-changing activity in the application. No forgery, no replayed tokens, no (successful) man-in-the-middle attacks. This protection addresses OWASP A8.

Prohibiting Invalidated Redirects/Forwards

Web applications that employ URL redirects or forward users to other web pages, are potentially vulnerable to this type of threat. Typically the destination URL is determined using untrusted data, and without proper validation, attackers can redirect users to malware sites or use forwards to access unauthorized pages and information.

Prevoty prevents improper phishing and redirects, by validating the information being passed.
and ensuring that users arrive on the intended page. User authorization is also verified which prevents unauthorized access to restricted pages. Using these methodologies, Prevoty both prevents unvalidated redirects and protects against unauthorized URL forwards, eliminating this type of threat. This protection addresses OWASP A10.

Eliminate Http-Response Splitting

Http-Response Splitting, while not one of the more common attacks, can have devastating effects when it does occur. To mount a successful attack, the vulnerable application must allow input that contains CR (carriage return, also given by %0d or \r) and LF (line feed, also given by %0a or \n) characters.

Attackers manipulate these characters to return malicious data in an HTTP response header, giving them control of the response the application intends to send, and allows them to create additional responses entirely under their control.

The Prevoty solution successfully detects and eliminates Http-Response Splitting, ensuring that the intended payload returned by the application is secured and authentic, thereby protecting output presented to clients and the subsequent client interactions.

Path Traversal Protection

A path traversal attack (also known as directory traversal) aims to access files and directories that are stored outside of the application’s root folder. By manipulating variables that reference files with “dot-dot-slash (../)” sequences and attempting common variations of file paths, it may be possible to access arbitrary directories stored on file system thereby giving unauthorized access to application source code, configurations, and critical system files.

Prevoty protects against unauthorized PT file access, by canonicalizing URL paths to each file being called by the web application, and ensuring the directories and subdirectories exist on a predefined approved list of url paths (whitelist). This whitelist gives organizations the ability to secure directories and protect file systems, preventing unauthorized access via unauthorized PT attempts.

XML External Entity (XXE) Protection

As part of the Content (XSS) filter, Prevoty now offers protection against XML External Entity Injection (XXE) attacks. XXE attacks occur when XML input containing a reference to an external entity is processed by a weakly configured XML parser. Entities are defined within the XML document with an <entity> tag, and access local or remote content via a declared system identifier. Entities are a large security risk which can leave organizations vulnerable to the disclosure of confidential data, denial of service, server side request forgery, port scanning
from the perspective of the machine where the parser is located, and have other negative impacts.

Database Access Monitoring

Prevoty’s Database Access Monitoring (DAM) tool offers greater visibility into applications by monitoring the traffic and requests sent to a database. DAM operates within the application itself and reports the who/what/when a query is being made, the actual query itself, and metadata of the rows affected. Legacy systems and unusual database architectures may benefit from this type of monitoring tool, due to the greater insights into which data is being accessed, how often, and by whom. Through reporting on cluster hits, HTTP request info, connections and user credentials, DAM provides a greater level of overall visibility and security intelligence for Cassandra databases.

Performance Impact

The Prevoty solution was designed for high performance large-scale use, and comfortably processes tens of thousands of requests per second, per enterprise. Research shows that LANGSEC processes inputs 30-50x faster than pattern-matching / regular expressions. Advanced design and high-functioning algorithms enable the security engine to process complex payloads in less than a millisecond.

- The performance impact of an API call when a payload is being processed varies based on deployment.
  - On cloud-based SaaS, round-trips typically take around 50-60ms.
  - On-premises deployments typically results in round-trips of only 2-3ms.

These processing time have been tested using the SaaS Prevoty Cloud, and on-premises with engine and application servers in the same data center, being secured with a high-speed pipe, positioned either at the app server tier or the web server tier.

---

Product Benefits

➢ Runtime Application Protection
Dramatically reduces opportunities for security breaches by eliminating top OWASP runtime threats such as XSS, SQLi, CSRF breaches, and Http-Response Splitting, thereby reducing the risks of data exfiltration, user ID theft and fraud, and brand defacement.

➢ In-depth Threat Intelligence
The Prevoty solution captures details regarding every attempted hack and threat, and logs them in real-time. These metrics enable security teams to understand application vulnerabilities, and take any necessary corrective actions.

➢ Real-time Threat Prevention
The “Detect, Report, Fix” cycle takes on a whole new meaning since the “Fix” is done in runtime by the Prevoty engine while the application is running, rather than waiting on developers to patch a vulnerability.

➢ Ease of Implementation
The Prevoty solution is delivered as a fully scalable software-as-a-service cloud or as RPMs for on-premises deployment. Application integration is available as .NET or Java plugins which require no code changes, or as standardized SDKs.

➢ Protection for Legacy Systems
Existing legacy applications with known vulnerabilities and security holes, can be fully protected and have state-of-the-art application security protection.

➢ Eliminate Zero-day Attacks
Prevoty’s patented contextual, behavioral and lexical analysis engine has automatic detection of malformed and malicious data, and then fixes or rejects the threat without the need for blacklisting, dramatically reducing the potential for zero-day attacks.

➢ Distributed and Dynamic Applications
The Prevoty solution will process data input and state changes, regardless of where it originates (the cloud, web services and API calls, RSS feeds, user generated content, mobile devices, etc.), ensuring protection even for the most complex applications.
Complimentary Proof of Value

Prevoty is committed to ensuring success every step of the way by providing world-class products and customer support.

We encourage you to reach out to our staff with any questions, or to arrange a complimentary “Proof of Value” session with a solutions architect to demonstrate how Prevoty’s application security solution can be of value and benefit to your organization.

Summary

Prevoty is proven, trusted, and employed throughout multiple Fortune 50 companies spanning the global banking and financial industries, education and university campuses, retail corporations, and entertainment companies. Our mission is to protect enterprises and their users by delivering innovative application security using technologies that are: real-time, in-application, and provide active defense.

Being consistently recognized as a leader in the application-security industry, Prevoty has been highlighted and showcased through these awards as well as our work with select partners:
Additional Support

Prevoty is committed to ensuring your success every step of the way by providing world-class products and customer support, and by ensuring that clients have access to all the latest software releases, features, optimizations and bug fixes in a timely manner.

Our staff of highly-qualified technical engineers and solution architects, helps end users of all technical levels and abilities understand and successfully employ the Prevoty products.

If you have any questions or issues, please visit our support website and search the Prevoty knowledge base, read through documentation, or submit a support ticket. We also encourage you to reach out to our support staff by selecting the most convenient method below.

Address:
11911 San Vicente Blvd. #355
Los Angeles, CA
90049 U.S.A.

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

Web:

https://support.prevoty.com

At Prevoty, we welcome your feedback, value your comments and encourage you to contact us with any concerns or suggestions.