Prevoty

Document Portal PDF

Prevoty Runtime Application Security

Technical Overview

Prevoty, Inc. HQ

11911 San Vicente Blvd. #355

Los Angeles, CA 90049

prevoty.com

support@prevoty.com

310.499.4714

Version Number: 6.0

Version Date: Jan 2018

VERSION: 6-182501

Table of Contents

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 continues to rise to extraordinary levels, creating a significant threat to enterprises. The most common attacks according to OWASP[1] and numerous industry studies[2], include Command Injection (Ci), SQL injection (SQLi), Cross-site Scripting (XSS), and Broken Authentication.

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 autonomous application security 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;
[2] "*Recent Ponemon Study on Application security*" (http://info.prevoty.com/ponemon-report-enterprise-app-risk);
[3] Dept. of Homeland Security's Software Assurance Program (https://buildsecurityin.us-cert.gov/software-assurance)

Product Overview

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 system comprised of a number of modular services that inspect data using patented LangSec and other analysis techniques.

Prevoty Plugins/SDKs

Plugins that monitor application behavior, analyze incoming user-input and data payloads, detect threats and sanitize data for safe execution within the application(s).

Prevoty Manager

A web-based console for configuring application configuration settings, creating security policies, and event logging visualization.

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 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) system. Examples of compatible logging tools include: Splunk, Elastic, QRadar, ArcSight, syslog, Unix socket, where options exist for information to be exported as a CSV for further reporting and analysis.

Prevoty Plugins

Applications communicate directly with other Prevoty components via pre-built plugin frameworks. Applications can either be centralized or distributed, allowing for a fully scalable enterprise-wide security solution that offers protection for new development, legacy applications and 3rd-party integrations.

Prevoty plugins are available and supported for multiple languages including; .NET which is implemented as an HTTP module via a .msi file, Java which is implemented as servlet filters using .jar files, and several other languages all built from an internal proprietary native code base.

Plugin Highlights

Below are several highlights of implementing with one of the Prevoty plugins:

- No coding changes are required within the source code, allowing for easy integration.
- Customizable application security protection with the ability to select/deselect parameters and settings within the configuration file.
- Compatible for use with new, legacy, and 3rd-party applications.
- Plugins enable applications to intercept malicious content at runtime, in a minimally invasive manner.
- Only vulnerable data paths are monitored for malicious activity, minimizing any impact on application performance.
- Detailed event information is tracked and logged for increased security intelligence.

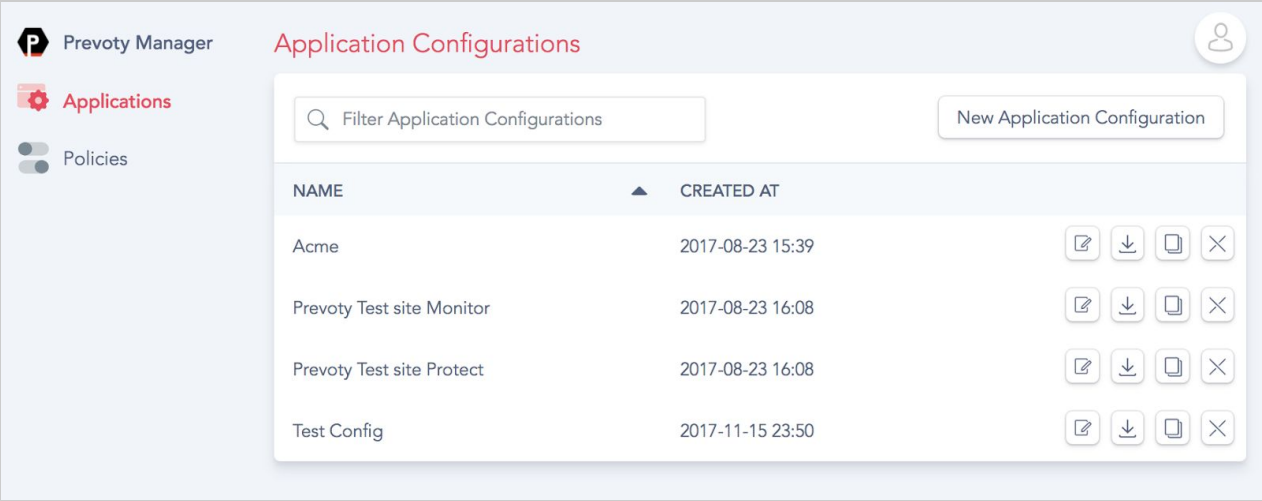
Prevoty Manager

Prevoty Manager provides a single web-based interface for managing application configuration files, creating security policies, viewing Prevoty event data, and API key management.

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

In addition, Prevoty Manager can help users understand event data through a logging visualization tool. This tool offers a glimpse into a specific set of logged events, and can provide increased understanding through a mix of data-collaboration points, charts, and graphs.

Figure 1. Prevoty Manager Home Page



Network Deployment Options

Prevoty 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 any of the available application modes:

- **Disabled**: This mode will turn off Prevoty's monitoring and protection services on the application(s).
- **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 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 1. Application Running Mode Features

Application Mode	Disabled	Monitor	Protect
Ability to identify specific threats and sources		✔	✔
Real-time notification of application security threats		✔	✔
Integration with SIEMs and log management software		✔	✔
Centralized security policy management across all applications, regardless of application type		✔	✔
Data exfiltration prevention			✔
Attack blocking/sanitization			✔
Token & session ID management			✔

What Threats Does Prevoty Protect Against?

Prevoty's threat protection is grouped into security modules that guard against many of the top threats as identified by OWASP, as well as additional security vulnerabilities that can be commonly overlooked. One or more modules may be employed, and each module contains numerous options and settings allowing for highly-specific customization to meet demanding security needs.

Content Injection Module

The Content Injection Module is designed to protect against and eliminate each type of Cross-site Scripting (XSS) attack, and offers unprecedented defense against all levels of XSS. These 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.

This module effectively analyzes all incoming code for Cross-site Script injections, including HTML, CSS, XML, JSON and JavaScript, whether it is fragmented, a full document, plain text or mixed content. This content is lexically parsed and transformed, identifying potential threats. Based on the analysis, the Prevoty security engine predicts web browser executions, then pinpoints and surgically removes bad content while preserving data fidelity. This protection addresses OWASP 2017: A7.

Cross-site Request Forgery (CSRF) Module

The CSRF Module 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 that a user can trust the application knows exactly when he/she is performing a state changing action (e.g. login, checkout, etc.) and their session is safe from any request forgery attempts.

The CSRF Module intelligently inserts and cryptographically verifies individually generated tokens and ensures that they are only used as specified during any events requiring state changes. 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. This protection addresses OWASP 2013: A8.

SQL Injection Module

The Prevoty SQL Injection Module analyzes database queries and protects popular relational databases (Oracle, MySQL, IBM DB2, MSSQL.) 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.

In addition to the out-of-the-box SQL Injection protection, the engine optionally 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 or 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 2017: A1.

Command Injection Module

Prevoty stops Command Injection attempts by identifying every incoming application command, and evaluating it prior to passing the code through for execution. WIth the Prevoty engine, 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.

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. 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 2017: A1.

Path Traversal Module

A Path traversal (PT) 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.

Request/Response Module

The Request/Response module includes protection for HTTP and HTTPS header objects that are used when generating web pages, and helps to secure all dynamic or static code, as well as validates data from user-based interactions. Web applications become vulnerable to attack when header objects are missing, out-dated, or implemented incorrectly. The following vulnerabilities are addressed within this module:

Broken Authentication Protection and Session State Management
Prevoty detects and blocks HTTP response objects that contain invalid basic authentication headers, and detects and protects 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 2017: A2.

Content-Security-Policy (CSP) Support
The CSP Options header is a HTTP response header that determines whether or not a web page should load dynamic resources including JavaScript, Images, CSS, fonts, AJAX requests, Frames, and HTML5 Media. Prevoty plugins prevent attacks based on CSP vulnerabilities, by determining if the CSP header tag exists and then adding the CSP header string value, which is defined within Prevoty Manager. This value can be customized as needed to meet security policy requirements, and may consist of one or more directives, separated with a semicolon.

Sensitive Data Detection and Protection
This feature minimizes and protects against sensitive data exposure. Confidential information such as credit card numbers, national ID numbers, etc. is 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 2017: A3.

Prohibiting Invalid 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 unvalidated 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. This protection addresses OWASP 2013: 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 use 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. Prevoty 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.

XML External Entity (XXE) Protection

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. This protection addresses OWASP 2017: A4.

X-Frame Options (XFO) Support

XFO is a HTTP response header that determines whether or not a web page may be rendered within a <frame>, <iframe>, or <object> tag. Often times this header is not set, which may pose a vulnerability to the overall web application. This attack occurs when an attacker uses a transparent iframe in a window to trick a user into clicking on a button or link, which then sends the unsuspecting user to another server with an identical looking window. Any further user input, interactions and data is unknowingly captured by the imposter website. Prevoty supports XFO by determining if the XFO header tag exists and then sets it accordingly to prevent frame-sniffing and click-jacking attacks.

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.[2]

Advanced design and high-functioning algorithms enable the security engine to process complex payloads in less than a millisecond.

[2] "*Visualizing Security via LangSec*" Kunal Anand, AppSec California 2016 (https://www.youtube.com/watch?v=OYlWhhdoKRY)

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 under 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, XXE injection, and many others, 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 an on-premises deployment. Application integration is available through Prevoty 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 automatically detects 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

Put your applications to the test! Find out if your applications are secure or if threat vulnerabilities exist, with a complimentary "Proof of Value" (POV) session.

During a POV, a Prevoty Solutions Architect will employ our monitoring software on an in-house application to demonstrate whether or not Prevoty would be beneficial in protecting your applications. You'll gain real-time visibility and see not only the amount of suspicious events, but also the types of threats your applications are experiencing.

After this session, the architect can help determine if Prevoty would be of value and benefit to your organization, and provide an application security plan. Call our offices at 310-499-4714 to schedule a POV.

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, entertainment and other industry sectors. 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:

RSAC Innovation Sandbox 2016 FINALIST

IBM Business Partner

amazon web services

DENIM GROUP

Contact and Support Information

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.

Headquarters Address:	11911 San Vicente Blvd. #355 Los Angeles, CA 90049 U.S.A.
Telephone: +1 310-499-4714 +1 866-940-2540 (toll free)	The standard business hours for Customer Support are M-F 6:00 am – 6:00 pm Pacific Time, excluding holidays. Calls outside of business hours will be responded to the following business day. If you attempt to contact Customer Support via telephone during *Normal Business Hours* and are directed to voicemail, please leave a message and a Customer Support Engineer will respond shortly.

	Severity 1 issues may contact support 24/7 via the toll-free number.
Support Email: support@prevoty.com	When a problem is submitted via email, you will receive an auto-reply from the ticketing system acknowledging receipt and assigning the ticket a case number for future tracking. To ensure proper tracking of your ticket, please either reply to the automated email for all subsequent communications on the particular issue or enter the ticket number in the Subject line of any new email you send pertaining to this particular issue.
Online Support Portal: https://support.prevoty.com	The support portal provides logged-in users access to FAQs, the Knowledge Base, and online documentation. Users can also enter support issues directly into a **Case Management System (CMS)**. The CMS allows users to submit, view, and check the status of cases at any time. The CMS is the preferred method for submitting support cases – users can avoid waiting on the phone, document a question in detail at any hour, and have questions directed to the most appropriate support engineer.

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