




Solution Brief

---

# ORACLE DYN MALWARE PROTECTION

ORACLE® + Dyn

 [dyn.com](https://dyn.com)

 603 668 4998

 @dyn



## Solution Brief:

# Oracle Dyn Malware Protection

Cloud-based, malware protection for websites offered as a 24x7 Managed Security Service

## Overview

Organizations must mitigate the threat of malware upload and delivery to their websites. Oracle Dyn Malware Protection provides the coverage that every business needs.

Many digital businesses allow file uploads via their websites and web applications. Site owners permit (and often require) their customers to upload photos, resumes, insurance claims, sign-up forms, signatures, payments, etc.. Users want a convenient way to share various file types through responsive upload applets. Unfortunately, threat actors leverage the same means as a vector for malware delivery; often turning legitimate websites into malware distribution and infection points.

While there is code that developers can add to secure such applets, many are left unsecured and such code is subject to a host of different vulnerabilities.



## The Solution

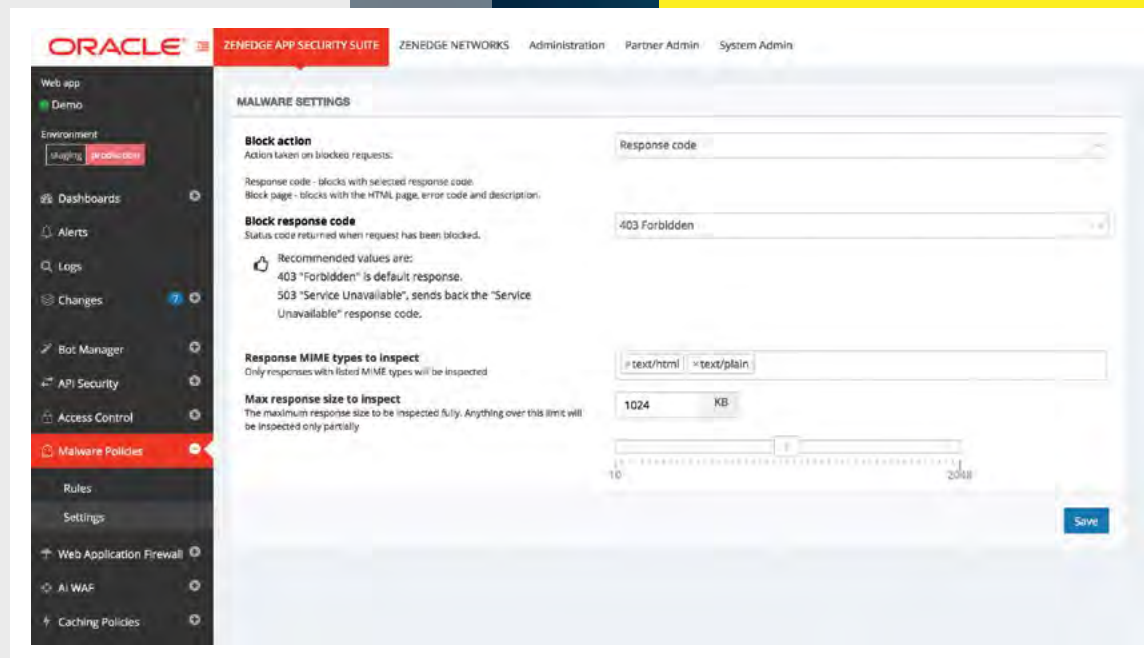
As an inline security control, Oracle Dyn Malware Protection detects malware at the edge - before it reaches your web applications. The solution rejects files upon signature or pattern match in real time and also allows you to apply rate limiting based on various client parameters to further secure web properties. Oracle Dyn Malware Protection gives you the ability to determine the size and naming conventions of uploaded files to conserve network resources, and for ease of file organization.

Going beyond traditional malware solutions available today, Oracle Dyn Malware Protection offers a flexible solution that is easily deployed and continuously managed. This guarantees ongoing malware protection; ensuring the optimized performance and security of your web applications. Oracle Dyn Malware Protection is cloud-based and offered as a 24x7 Managed Security Service. The solution includes advanced dashboard reporting giving you powerful insights into web application uploads, security risks, and critical protections.

Malware Protection Dashboard

## Business Value

- Enterprise-class, cloud-based security solution fully managed 24x7
- Provides unparalleled insight, visibility, and control over uploaded files to websites
- Ensures legitimate traffic only reaches your critical web applications
- Detects and blocks malware and other malicious web traffic
- Ensures uptime, availability, and protection of your critical web applications





Oracle Dyn Malware Protection is part of our cloud-based, managed cybersecurity suite and is seamlessly integrated with our DDoS, Bot Manager, Web Application Firewall, and API Security offerings.

## Key Benefits

- Multiple sources of malware hashes
- Inline malware detection – upstream in the cloud - not onsite
- No performance impact to scan all upload files - doesn't impact websites
- Dashboard statistics – sources of malware IP, user agents, geo's
- Provides visibility into file type blocks/allows
- File type whitelist, length of filename/size, apply naming convention
- Preventing PHP scripts from execution or any other kind of scripts
- Blocks hacker footholds and prevents potential compromise

Customizable Malware Policies

Do you still have questions about Malware Protection?

Learn more at [zenedge.com](https://www.zenedge.com)

The screenshot displays the Oracle ZENEDGE APP SECURITY SUITE interface. The top navigation bar includes 'ORACLE', 'ZENEDGE APP SECURITY SUITE', 'ZENEDGE NETWORKS', 'Administration', 'Partner Admin', and 'System Admin'. A left sidebar lists various security components: Web app, Demo, Environment (staging, production), Dashboards, Alerts, Logs, Changes, Bot Manager, API Security, Access Control, Malware Policies (highlighted), Rules, Settings, Web Application Firewall, AI WAF, Caching Policies, Settings, and Info and Support. The main content area is titled 'MALWARE RULES' and lists several rule categories with their descriptions and configuration options:

Rule Category	Description	Status	Response Action
Anti-debug / Anti-VM	Rules aimed to detect anti-debug and anti-virtualization techniques used by malware to evade automated analysis.	Off	Alert Only, Block
Common Vulnerabilities and Exposures (CVE)	Rules aimed to detect specific CVE.	Off	Alert Only, Block
Crypto	Rules aimed to detect the existence of cryptographic algorithms.	Off	Alert Only, Block
Exploit Kits	Rules aimed to detect the existence of Exploit Kits.	Off	Alert Only, Block
Well-known malware	Rules aimed to detect well-known malware.	Off	Alert Only, Block
Packers	Rules aimed to detect the well-known software packers, that can be used by malware to hide itself.	Off	Alert Only, Block
Webshells	Rules aimed to detect the existence of well-known webshells.	Off	Alert Only, Block
Emails	Rules aimed to detect malicious emails.	Off	Alert Only, Block
Malware Mobile	Rules aimed to detect well-known mobile malware.	Off	Alert Only, Block

Each rule has an 'Enable response inspection' checkbox. An 'Apply' button is located at the bottom right of the configuration area.




# Secure, Intelligent Edge

Oracle Dyn is a global business unit focused on the cloud infrastructure that connects users with digital content and experiences across a global Internet. Dyn, a pioneer in DNS, has now added the Zenedge web application security products to secure applications, networks, databases, and APIs from malicious Internet traffic. Our solutions are powered by a global network that drives 40 billion traffic optimization decisions daily for more than 3,500 enterprise customers, including preeminent digital brands such as Netflix, Twitter, LinkedIn and CNBC.

Copyright © 2018. Oracle and/or its affiliates. All rights reserved. Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners. 1059

ORACLE® + Dyn

 [dyn.com](https://dyn.com)

 603 668 4998

 @dyn