Trellix

DATA SHEET

# Trellix Detection as a Service

## Scan content for threats at any point in your workflow

## Highlights

- Detects and prevents known and unknown malware anywhere
- Integrates with all major cloud storage solutions and many web applications
- Protects multiple operating systems, including Windows, Mac, and Linux
- Compiles in-depth analysis details, including MITRE ATT&CK mapping, extracted objects, IOCs, and more
- Supports plug-ins for browsers and cloud storage
- Delivers contextual analysis of detected malware in JSON format

## Introduction

Every company approaches security differently based on their needs, industry, and environment. But to stay safe from dynamic threats coming from everywhere, all organizations need intelligence-backed, validated threat detection capabilities with contextual analysis they can act on.

With Trellix Detection as a Service (formerly Detection On Demand), available through an API, your business can protectively submit files to ensure they're protected against today's threats—whether they exploit Microsoft Windows, Apple OS X, Linux or application vulnerabilities.

Detection as a Service leverages the Trellix Multi-Vector Virtual Execution (MVX) detection engine and multiple dynamic machine learning, AI, and correlation engines to quickly reach a verdict on submitted files. MVX is a signatureless, dynamic analysis engine that inspects suspicious network traffic to identify attacks that evade traditional signature- and policy-based defenses.

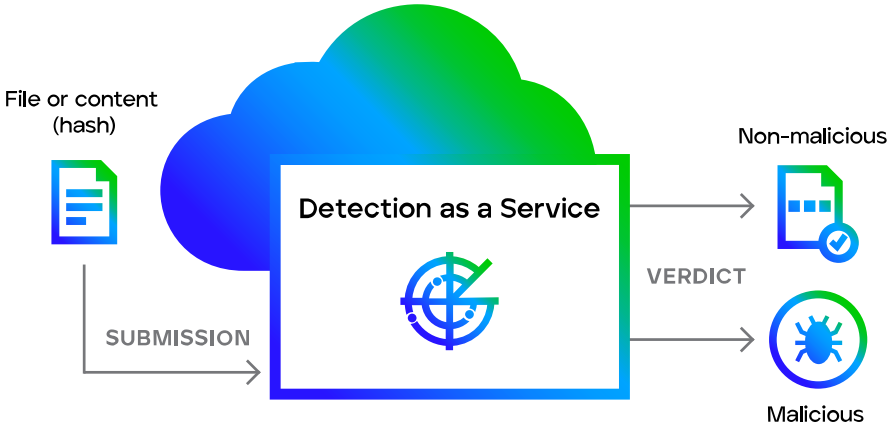
### Premium threat detection in any security architecture

A cloud-native service, Detection as a Service rapidly scans submitted content to identify malware. Unlike file security solutions based on file integrity algorithms, insider threat policy controls, or static check mechanisms, Detection as a Service processes your submissions using the same technologies that power many Trellix offerings.

You can easily configure access to Detection as a Service through an API. And you can integrate it into your security operations center workflow, SIEM analytics, data repositories, customer web applications, and more. The service delivers flexible file and content analysis capabilities wherever you need them to help you identify malicious behavior.

You don't just receive a verdict on each file and piece of content submitted through Detection as a Service. You also get supporting contextual detail, such as file, registry, process, and network changes, as well as MITRE ATT&CK mapping and other relevant findings from continually updated Trellix Dynamic Threat Intelligence.

## How Detection as a Service works



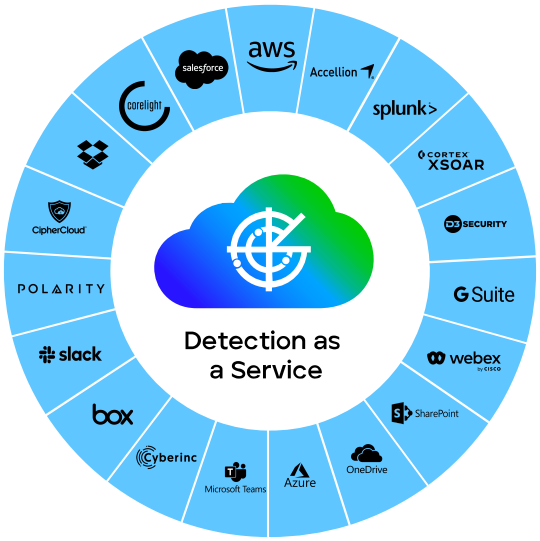

Detection as a Service compares your submission to threat actors' latest known tactics and signatures using static analysis, artificial intelligence, and machine learning. Trellix also determines the possibility of secondary or combinatory effects across multiple phases of the attack lifecycle to discover never-before-seen exploits and malware.

When a document is uploaded or delivered to a collaboration tool, Detection as a Service pulls it off to analyze it. If the file is malicious, it's renamed, sent to a quarantine file, or marked to denote it as a potential threat. And an alert is sent so you'll know if a document needs attention.

## Easy integration with cloud storage solutions and web applications

Detection as a Service integrates with cloud services like AWS, Azure, and Google, and cloud storage tools like Dropbox, Box, OneDrive, and others.

It also integrates with many popular tools like Salesforce.com, Webex, Slack, Microsoft Teams, and much more. You can easily integrate with applications that don't already have a plug-in through our easy-to-use API.




## Get started

Detection as a Service is available through Trellix channels or directly through the AWS Marketplace (for low volume submissions).

When you purchase the service, you specify how many submissions you expect to make during a single year. AWS Marketplace purchases provide a monthly submission quota, billed yearly. File submission rate is limited to 100 per minute. Hash submission rate is limited to 200 per minute. To request higher limits, please contact Trellix support.

Files and other material submitted to Detection as a Service may be assigned a submission value greater than one submission. Trellix will communicate standard submission values to you.

**To learn more about Trellix, visit trellix.com.**

**Trellix**
6220 American Center Drive
San Jose, CA 95002
www.trellix.com

Trellix

**About Trellix**
Trellix is a global company redefining the future of cybersecurity. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix's security experts, along with an extensive partner ecosystem, accelerate technology innovation through machine learning and automation to empower over 40,000 business and government customers.