WHITE PAPER

Detect malicious content on upload with Trellix Detection as a Service

Stop threats in your cloud infrastructure and SaaS products

Trellix

With the ubiquity of file sharing, companies face an increased risk of ransomware and malware

An attack can take many forms. It could be targeted, where someone intentionally attempts to infect your network with a malicious file. Or a compromised user could be sharing a file they don't know is malicious—and the more it's shared, the more harm it does. Sites could have malicious attributes, such as redirects or ads, or a URL could be malicious to anyone who visits it.

With all these possibilities, and with all the data that's shared back and forth, the challenge is complex. But a simple solution exists.

In this white paper, you'll learn the importance of having a cloud-based detection service that scans the content coming into your cloud, why it's essential to do so quickly before harm is caused, and how your employees can keep working at their own pace while these security measures are applied.

Trouble spot 1: Files, files, and more files

In the current work landscape, millions of files are shared daily.

- Google Drive and Box are the two most used file sharing and storage services, with Google Workplace reporting over 2 billion users.[1]
- 200 zettabytes of data (that's 2 trillion gigabytes) will be stored globally by 2025.[2]

You and your coworkers are constantly sharing and receiving files from customers, partners, third-party file-sharing sites, or fellow employees. Many files come from unknown sources, or you don't know their history.

It's no surprise that you want your team to open and use these files with confidence.

Collaboration tools are not going anywhere either, which means active file-sharing will continue. In fact, 85% of end users report using multiple platforms for collaboration.[5]

With more people working remotely, the use of file-sharing services has gone up:

- Just over 70% of the workforce was still remote at the end of 2020.[3]
- Not all employees are going back to the office soon.
- Many workers want to stay remote.[4]

1. 26 Cloud Computing Statistics, Facts & Trends for 2022, Cloudwards, 2022
2. The World Will Store 200 Zettabytes of Data by 2025, Cybercrime Magazine, 2020
3. How the Coronavirus Outbreak Has—and Hasn't—Changed the Way Americans Work, Pew Research, 2020
4. Just because you can work from home doesn't mean you'll be allowed to, Vox Media, 2021
5. 70 Essential Online Collaboration Software Statistics: 2022 Market Share Analysis & Data, Finances Online, 2022

Trouble spot 2: You could open yourself up to an attack through common collaboration tools

Organizations often use a variety of collaboration tools and channels to share documents. When files are shared, there's an assumption that they're safe to access and use.

Even when relying on built-in security measures in web email hosts and file sharing products, breaches can still happen—making a second layer of content security necessary. Many times, a company doesn't know they've been compromised until they discover it or they're informed externally.[6]

While these services are secure, security at the content level provides much more coverage and assurance.

Your business needs increased monitoring to discover all three threats

There are three main attacks that originate with shared content:

Targeted attacks

An intentional file is sent to a recipient to be accessed either as an attachment or a link.

Compromised users

Users share documents that they don't know are malicious. For example, if the computer is compromised, it could be sending malicious content through all the documents created.

A malicious link embedded in the content of a document

Shared documents might include malicious URLs. Even well-known companies could host malicious code. For example, an advertisement or the site itself could be compromised. The user doesn't know the URL is malicious when sharing documentation, and visitors to the site can get infected.

[6] M-Trends Report 2021, Mandiant, 2021

Enterprises benefit from advanced threat detection capabilities

SaaS security solutions often don't offer your organization the advanced capabilities to find difficult-to-detect threats.

In the past, using a static antivirus service may have been enough. But those services don't provide the level of detection needed to catch threats at a content level.

Documents enter an organization's network through popular collaboration tools from reputable brands. For example:

- Slack was released in 2013.
- Box is among the top ten file-sharing apps.[7]
- Microsoft Teams incorporates with SharePoint and other trusted Microsoft apps.
- For Amazon Web Services (AWS) customers, Amazon Simple Storage Service (Amazon S3) is a go-to repository where files are stored once shared.

Sometimes these channels are approved for enterprise use, while other times they're used ad hoc or only in certain departments. Of course, the more files that are shared, the higher the security risk to your organization.

Knowing a file is there and who sent it is one thing, but knowing what's in the document is another piece of information paramount for security. Your company may have numerous files that should be scanned before they go into a trusted zone.

Virtual machines allow you to detonate files in an environment separate from your company's internal network and see how they behave on the internet.

Here's how this works:

- The file is detonated in the sandbox.
- The file then runs on multiple versions of various operating systems.
- The sandbox also allows for the deobfuscation of scripts and can tell you what the file is doing on disk, memory, the registry, and the network stack.

How to use a cloud-based threat detection service in your organization

The most common use of cloud-based threat detection capabilities is for research forensics by security operations center (SOC) analysts. These analysts put a lot of effort into building virtual machines (VMs) and a sandbox to explore files.

For the sandbox to work on the VM, there must be a separate internet connection from a public ISP, but still within the corporate network. This process is both complicated and time-consuming.

With a packet capture, your SOC team can capture the connection and communication between the VM and the internet. They'll also know where the payload will beacon quickly and which parameters are getting passed into processes. For example, it can capture macros inside Microsoft Word docs.

This process is far easier than if you tried to do this by hand. Deobfuscation is difficult, but it saves significant time—up to 90 minutes.

[7] 10 top file-sharing services: Dropbox, Box, Google Drive, OneDrive, and more, Computer World, 2021

Trellix Detection as a Service: Scan content for malware

Trellix Detection as a Service, formerly known as Detection On Demand, is a cloud-native threat detection service that rapidly scans submitted content to identify resident malware. To protect your cloud infrastructure, you must be able to actively monitor files for the presence of malicious content. Detection as a Service uncovers harmful objects in the cloud.

It also delivers flexible file and content analysis capabilities to identify malicious behavior wherever your business needs it. For example, it can be integrated into your SOC workflow and used for security information and event management (SIEM) analytics, data repositories, or customer applications.

Detection as a Service features:

- Available through an API connection to many popular collaboration tools and enterprise services, including Amazon S3, Box, Polarity, Salesforce, Slack, and Microsoft Teams
- Protection of multiple operating systems, including Windows, Mac, and Linux
- Quick detection of new files, which are intercepted and analyzed before they can execute malware
- Near real-time analysis to determine the exact nature of the potential threat
- An alert system that lets you know when a document has potentially malicious content

> Detection as a Service integrates with multiple services to add further protection to enterprise environments.

With detailed analyses and context of detected malware in easy-to-consume JSON format, you'll get supporting details, including file, registry, process, and network changes. Each submission renders a verdict, so you'll know what's happening in your environment every time.

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 in some way to denote it as a potential threat. An alert is sent so you'll know if a document needs attention.

With Detection as a Service, you can detect and prevent known and unknown malware anywhere with a simple API. Trellix has the capabilities of a sandbox in the cloud, so it's more affordable and faster, with a more robust graphical user interface (GUI) and stronger reporting.

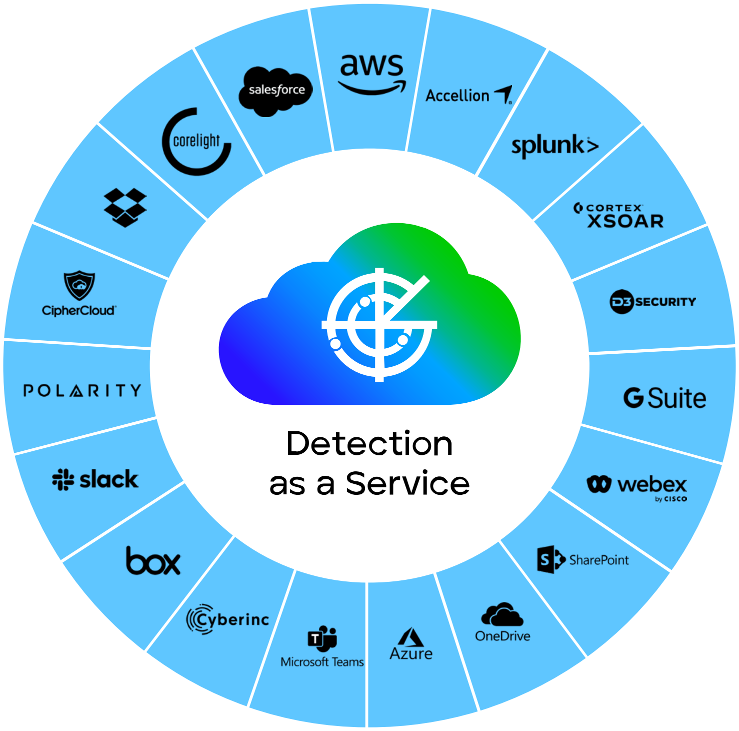
How customers are using Detection as a Service

Across many industries, Detection as a Service helps SOCs and their sandbox operations make informative discoveries to keep their systems secure from both outside and inside threats, so workers can accomplish higher-value tasks. Some examples:

- A document publishing company uses Detection as a Service to run millions of untrusted files uploaded by third parties each month.
- A financial services company uses the Detection as a Service API via its security orchestration, automation, and response (SOAR) solution to analyze files from its endpoints.
- A fast-food company uses the Detection as a Service API to get screenshots of suspicious URLs.
- A cloud security vendor uses Detection as a Service to analyze suspicious content from its cloud infrastructure.
- A bank uses Detection as a Service to analyze files from Box.com repositories.
- Trellix EDR – Forensics uses Detection as a Service to analyze suspicious files from endpoints.

About Trellix and Amazon Web Services (AWS)

Trellix Detection as a Service enhances the security of Amazon S3 buckets from ransomware and malware. The file and object scanning ensures you are not bringing malicious items when you migrate to the cloud and keeps them out of your ongoing business operations.



Detection as a Service also works with Amazon Macie, which can discover and protect your sensitive data on AWS using machine learning and pattern matching, and through a searchable inventory of your Amazon S3 buckets. Get protected in minutes with a one-month free trial of Detection as a Service via the AWS Marketplace.

To learn more about cloud security, visit trellix.com.

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

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.