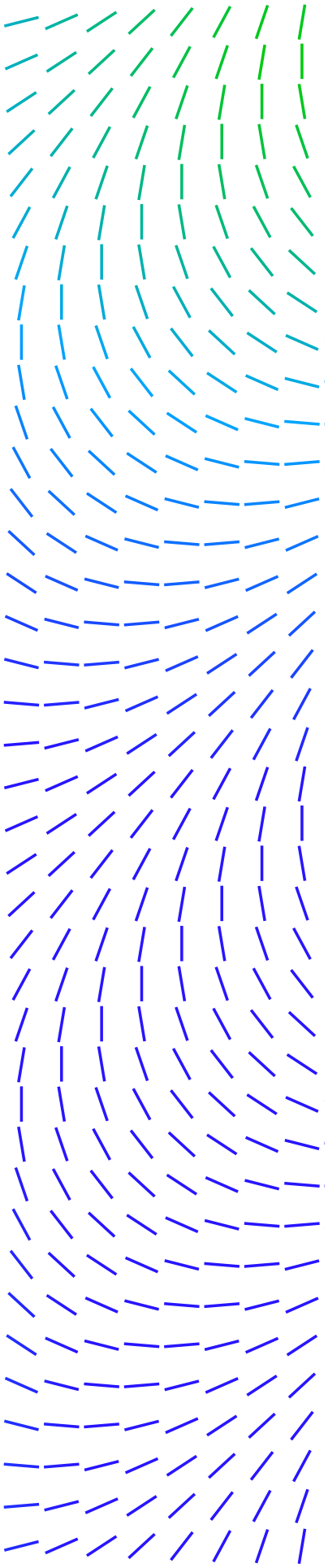


WHITEPAPER

aws PARTNER

Detect Malicious Content on Upload with Trellix Detection as a Service

Detect threats in your cloud infrastructure and SaaS products.

Trellix

Table of Contents

04 Trouble spot #1: Files, files, and more files

05 Trouble spot #2: You could be opening yourself up to an attack through common collaboration tools

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

08 Trellix Detection as a Service: scan content for malware

09 How customers are using Trellix Detection as a Service

With the ubiquity of file sharing, companies are facing an increased risk of ransomware and malware.

Attacks can take many forms. It could be targeted, where someone intentionally attempts to infect your network with a malicious file. A compromised user could be sharing a file that they don't know is malicious—the more it's shared, the more harm is done. Sites could have malicious attributes, such as re-directs or ads, or a URL could be malicious to anyone who visits it.

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

In this white paper, learn the importance of having a cloud-based detection service that scrutinizes the content coming into your cloud, why it's important to do so quickly before harm is caused, and how your employees can keep working at their own pace.

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]
- Your documents are among them—shared and received.

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

It is no surprise that you want assurances and confidence before letting your team open and use these files. You want to know that they aren't malicious. And yet, they could be malicious in various ways.

> Usage of file-sharing services has gone up with more people working remotely.

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

Collaboration tools are not going anywhere, either, which means active file-sharing will continue. In fact, there has been a 176% increase in collaboration app installations on enterprise devices since May 2020 alone. The number may be higher today.[5]

TROUBLE SPOT #2:

You could be opening yourself up to an attack through common collaboration tools

It is common for organizations to use a variety of collaboration tools and channels to share documents. When files are shared, there is an automatic assumption they are safe to access and use.

Indeed, all these collaboration programs have built-in security. But despite built-in security functions for web email hosts and file-sharing products, a second layer of content security is necessary. Even when relying on built-in security measures and taking proactive precautions, breaches can still happen.

Many times, a company doesn't know they've been compromised until they discover it, or they are informed externally.[6]

While these services are secure, security at the content level provides much more coverage and assurance. There are three main attacks that originate with shared content:

- **Targeted attacks:** An intentional file sent to another recipient to be accessed either as an attachment or a link.
- **Compromised users:** In this case, 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 docs created.
- **A malicious link embedded in the content of a document:** Documents that are shared might have malicious URLs, where the URL might be malicious for a day, a week, or a month. Even well-known companies could host malicious code; for example, an advertisement, or the site itself, could be compromised. The user does not know it is malicious when sharing documentation, and visitors to the site can get infected as well.

Increased monitoring is needed to discover all three threats.

Enterprises benefit from advanced threat detection capabilities

Oftentimes, SaaS security solutions do not offer the advanced capabilities to find threats to your organization that are extremely difficult to detect.

In the past, using a static antivirus service may have been enough, yet now those services do not provide the level of detection needed to catch threats at a content level.

Documents enter an organization's network through popular collaboration tools. There are many collaboration tools that are popular and come from reputable brands. For example:

- Slack has existed for eight years.
- Box is among the top ten file-sharing apps.
- 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 for where files are stored once shared.

Sometimes these channels are approved for enterprise use, while other times, they are 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 is on the document is another paramount level of information and security. Your company may have numerous files that should be scanned quickly before they go into a trusted zone.

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

The most common first use of cloud-based threat detection capabilities is with security operations center (SOC) analysts, who use it for research forensics. These analysts put a lot of effort into building a virtual machine (VM) and sandbox to explore files.

The virtual machines are instrumented to detect what is happening on the VM. For it to work, 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.

Virtual machines offer the ability to detonate files in an environment separate from the company's internal network and see how it acts on the internet. How it works:

- Detonation opens the file.
- When the file is detonated, it is run on multiple versions of various operating systems.
- The sandbox also allows for the deobfuscation of scripts.
- It can tell you what the file is doing on disk, memory, the registry, and the network stack.

With a packet capture, the user can capture the connection and communication between the VM and the internet. They will also know where the payload will beacon quickly and which parameters are getting passed into processes. can also capture macros inside of 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 roughly 90 minutes.

Trellix Detection as a Service: scan content for malware

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

Detection as a Service delivers flexible file and content analysis capabilities to identify malicious behavior wherever your business needs it. For example, it can be integrated into the SOC workflow, used for SIEM analytics, data repositories, or customer applications.

With detailed analyses and the context of the detected malware in easy to consume JSON format, customers benefit from supporting details, including file, registry, process, and network changes. Each submission renders a verdict, so you will know what is happening in your environment every time.

When a document is uploaded or delivered to a collaboration tool, Trellix Detection as a Service pulls it off to analyze it. If the file is malicious, it is renamed, sent to a quarantine file, or marked in some way to denote it as a potential threat. An alert is sent so you will know if a document needs attention.

With Trellix 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 on the cloud, so it is more affordable and faster, with more robust graphics (GUIs) and stronger reporting.

Trellix 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 Teams.
- Protection of multiple operating systems, including Windows, Mac, and Linux.
- Quick detection of new files—they 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.

aws PARTNER
- Public Sector
- AWS Marketplace Seller
- Authority to Operate
- Security Software Competency

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 it out of your ongoing business operations.

Trellix 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.

Trellix Detection as a Service is available in AWS Marketplace.

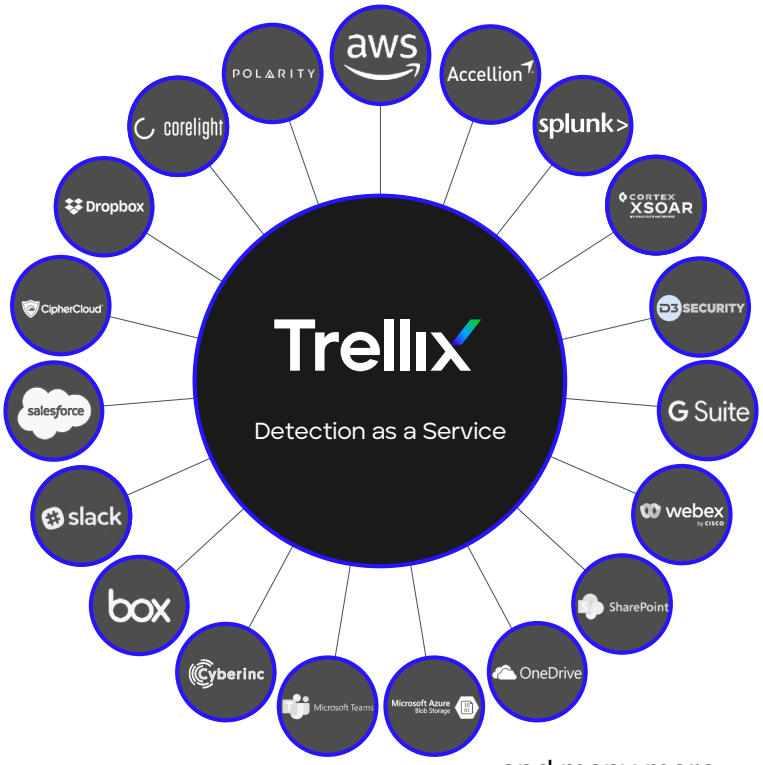
How customers are using Trellix Detection as a Service

Trellix Detection as a Service integrates with mulitple services to add further protection to enterprise enviornments

Across many industries, Trellix 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 that workers can accomplish higher-value tasks. Some examples include:

- A document publishing company uses Detection as a Service to run millions of untrusted files uploaded by third parties a month.
- A financial services company uses the Detection as a Service API via their Security Orchestration Automation and Response (SOAR) solution to analyze files off their endpoints.
- A fast-food company uses the Detection as a Service API to get a screenshot of suspicious URLs.
- A cloud security vendor is using Detection as a Service to analyze suspicious content from their cloud infrastructure.
- A bank is using Detection as a Service to analyze files off Box.com repositories.
- Trellix's Endpoint Security solution is using Detection as a Service to analyze suspicious files from endpoints.

aws PARTNER
- Public Sector
- AWS Marketplace Seller
- Authority to Operate
- Security Software Competency



Get protected in minutes with our deep integration with AWS, including Amazon S3. Click here to start your one month free trial of Detection as a Service via the AWS Marketplace.

1. Cloudwards, https://www.cloudwards.net/cloud-computing-statistics/
2. The World Will Store 200 Zettabytes Of Data By 2025, Cybercrime Magazine, June 8, 2020, https://cybersecurityventures.com/the-world-will-store-200-zettabytes-of-data-by-2025/
3. How the Coronavirus Outbreak Has—and Hasn't—Changed the Way Americans Work, Pew Research, December 9, 2020, https://www.pewresearch.org/social-trends/2020/12/09/how-the-coronavirus-outbreak-has-and-hasnt-changed-the-way-americans-work
4. Just because you can work from home doesn't mean you'll be allowed to, Vox Media, April 21, 2021, https://www.vox.com/recode/22387529working-from-home-return-to-office-remote-work
5. Finances Online, https://financesonline.com/online-collaboration-statistics-analysis-of-trends-data-and-market-share/
6. M-Trends Report 2021, Trellix, https://content.Trellix.com/m-trends/rpt-m-trends-2021

aws PARTNER

- Public Sector
- AWS Marketplace Seller
- Authority to Operate
- Security Software Competency

Trellix

Visit Trellix.com to learn more.

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.