Trend Cloud One™ – File Storage Security

Security for cloud file and object storage services

As cloud infrastructure continues to evolve, cloud-native application architectures have incorporated cloud file/object storage services into their workflow. This introduces a new attack vector vulnerable to malicious files. Trend Cloud One™ – File Storage Security protects your downstream workflows through innovative techniques such as malware scanning, integration into your custom cloud-native processes, and broad cloud storage platform support. Benefit from the peace of mind that comes with knowing your data files are not impacting internal systems or external reputation.

Amazon Simple Storage Service (S3)

Microsoft Azure Blob Storage

Google Cloud™ Storage

Key Capabilities

Decrease threat vectors with malware scanning

- **File reputation:** Block known-bad files with anti-malware signatures
- **Malicious software detection:** Uncover Trojan, malware, spyware, worms, and other threats—including known ransomware
- **Variant protection:** Look for obfuscated or polymorphic variants of malware via fragments of previously seen malware and detection algorithms
- **Extensive flexibility:** Trusted scanning support for small and large file sizes, alongside document exploit detection for all file types in Microsoft 365 files and objects
- **Advanced intel:** Over 30 years of cyber threat research and experience

Gain flexibility with integration of custom workflows

- Automates file scanning to be triggered whenever new files are uploaded
- Deploys using cloud deployment templates
- Enables workflow integration through serverless functions
- Provides the option to be deployed as a centralized service, managed by a security team
- Does not require a team to administer nor upkeep of rules
- Provides the option to be deployed as a centralized service (managed by a security team)

Easy-to-adopt implementation options

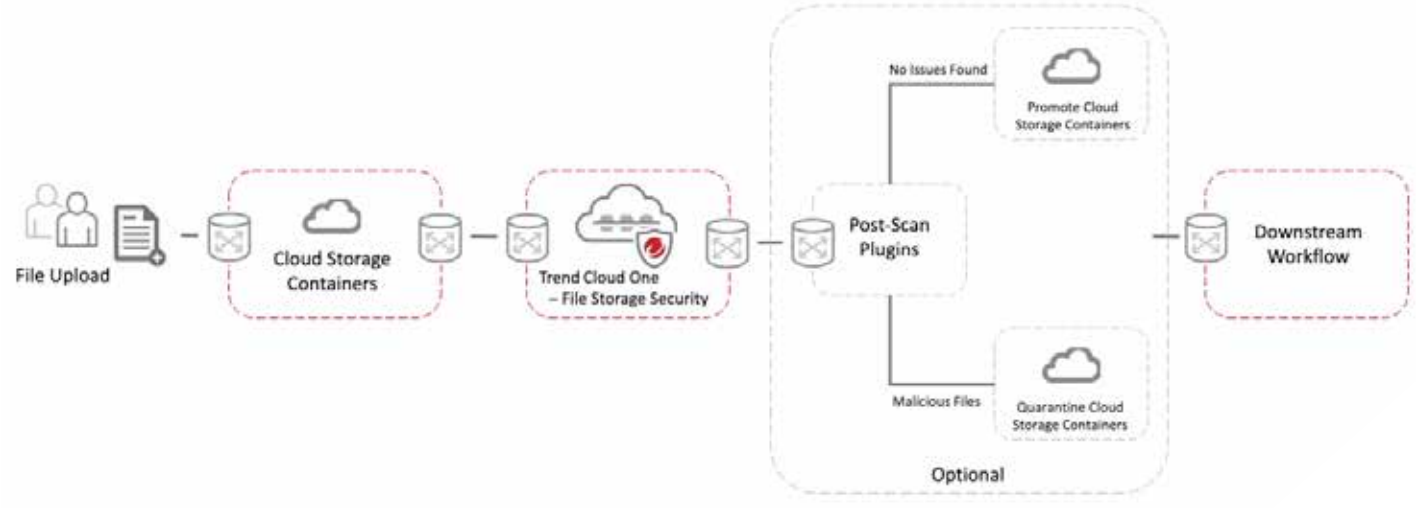
- Supported on Amazon S3, Azure Blob Storage, and Google Cloud Storage
- Allows you to choose between a multi-bucket or blob storage promotional model (a scanning storage unit and a quarantine/clean storage unit) or an efficient single-bucket architecture
- Displays results in the File Storage Security dashboard or from within your Amazon CloudWatch, Microsoft Azure Application Insights, or Google Cloud™ Logging

Deploy via management services. Leverage AWS CloudFormation, Microsoft Azure Resource Manager templates, or Google Cloud™ Shell to deploy the infrastructure, which includes relevant compute functions engineered to scan files uploaded into existing buckets or blob storages.

Ensures data sovereignty is not compromised. During the scanning process, your files will stay within the scanning bucket and will not be sent outside your cloud accounts. The scan is automated and requires no manual intervention.

Manages scanning requirements of any file type and size. Each scan result will be tagged, allowing you to check on specific files or identify malicious files that are detected and quarantined.

Customizable AWS Lambda or Microsoft Azure functions. Determine what happens to the file after it is scanned and if the sender or receiver is required to be notified. Learn how to get started at cloudone.trendmicro.com/docs/file-storage-security/what-is-fss.



Security fueled by leading global threat research

Our 15 global research centers, 450 internal researchers, and over 10,000 external security researchers supporting our Zero Day Initiative™, provide visibility into the entire threat landscape. With teams dedicated to cloud and cloud-native applications, we use our wealth of knowledge to strengthen our products and protect your organization against current and future threats.

Meeting your cloud migration and cloud-native application development security needs

Whether you are serving up images and documents to a browser, storing files for distributed access, or conducting file backup and restore operations, File Storage Security has you covered. You'll receive the confidence of knowing your critical files are protected and that they meet organizational compliance requirements for your file storage service workflow.

File Storage Security is part of Trend Cloud One™, security services for cloud builders.

Our solution includes:

- **Trend Micro™ Cloud Sentry:** Visibility of the threats in your AWS environment with quick, actionable insights in the context of your application
- **Trend Cloud One™ – Application Security:** Security for serverless functions, APIs, and applications
- **Trend Cloud One™ – Conformity:** Cloud security and compliance posture management
- **Trend Cloud One™ – Container Security:** Image scanning in your build pipeline
- **Trend Cloud One™ – Endpoint Security:** Protection, detection, and response across endpoints, servers, and cloud workloads
- **Trend Cloud One™ – Network Security:** Cloud network layer IPS security
- **Trend Cloud One™ - Open Source Security by Snyk:** Visibility and monitoring of open source vulnerabilities and license risks
- **Trend Cloud One™ – Workload Security:** Runtime protection for workloads (virtual, physical, cloud, and containers)

For more information, please visit **trendmicro.com**