Netskope and TITUS

The growing volume of unstructured data, coupled with the expanding use of cloud services, has increased the risk of data loss in the cloud. Netskope and TITUS protect sensitive data in the cloud by classifying business data and gaining granular visibility and control of this data as it moves into the cloud.

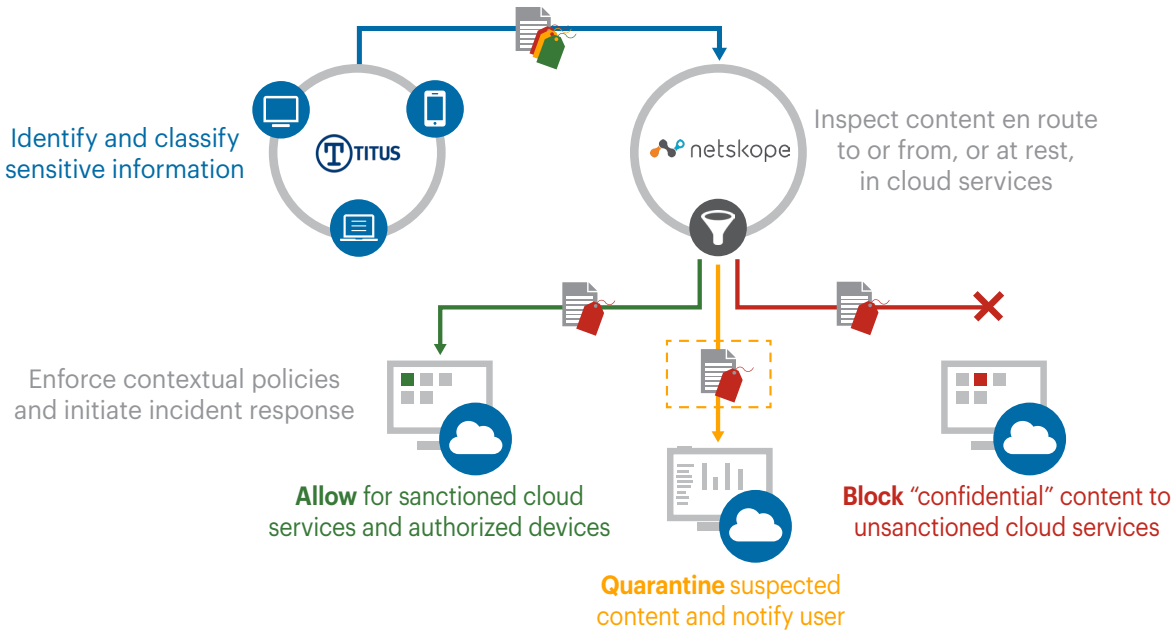
QUICK GLANCE

- Assign automatic, system-suggested, and user-driven data classifications
- Apply visual markings and persistent metadata to classified files
- Gain complete visibility of data movement in the cloud
- Protect sensitive data with precise, granular controls

NETSKOPE AND TITUS

With the use of cloud services growing rapidly and more data moving to the cloud, organizations need to take a comprehensive approach to address the risk of data loss from the cloud services they are using. Netskope and TITUS together provide a robust solution to identify and protect sensitive data in the cloud. Data identification starts with TITUS, a proven platform that provides automated, system-suggested, and user-driven classification tools for unstructured data in the enterprise. TITUS applies both visual markings and persistent metadata to classified data. Metadata markings supplement the advanced, automated content inspection capabilities in Netskope DLP, delivering highly accurate DLP detection with very low false positives. Combined with Netskope's unique vantage point across all cloud services and deep contextual information about cloud usage, the combined solution enables the creation of precise, granular policies to protect sensitive data in the cloud.

NETSKOPE AND TITUS



KEY CAPABILITIES

Flexible options to assign data classifications

TITUS helps users make better security decisions when creating, handling, or sharing information. TITUS starts by scanning information with configurable data identification rules and intelligent content analysis. Based on the analysis of the content, author, and other document attributes, TITUS can automatically classify data or make suggestions to the end user within the productivity application being used. By classifying documents at creation in key productivity apps, organizations can add structure and context to the vast number of documents being created and shared every day.

Data classification visible to users and systems

TITUS data classification is applied as both visual markings within key productivity apps and as persistent metadata. Visual markings in headers, footers, and watermarks, as well as user involvement in classifying data, help promote security awareness and responsibility for data protection. Persistent metadata provides system-level visibility which is used to increase the accuracy and effectiveness of other security and archiving solutions, including Netskope's advanced, cloud DLP.

Advanced, cloud DLP

TITUS complements Netskope DLP, which protects sensitive data in the cloud with accuracy and precision, and has the ability to inspect data at rest in sanctioned cloud services as well as data en route to and from all cloud services. Sensitive content is detected across 1,000+ file types and across structured and unstructured data, using 3,000+ data identifiers, metadata extraction, proximity analysis, fingerprinting, exact match, and more. Netskope DLP can use TITUS metadata to trigger policy actions, and can also be used to verify that documents have been correctly classified by TITUS users.

Full visibility of data and activities in the cloud

Netskope provides an all-mode architecture capable of covering all cloud traffic whether users are on premises or remote, using a web browser, mobile app, or sync client. Combine this unique cloud vantage point with Netskope DLP and TITUS Data Classification to gain full visibility and control of sensitive data across all of your cloud services.

KEY CAPABILITIES (CONT.)

Granular control for data protection

Netskope can apply granular policies to all of your cloud services, by combining deep cloud context with flexible options for policy enforcement. Rather than take a coarse-grained approach by blocking services, set security policies based on user, device, location, app, activity, and data. Choose from actions such as block, alert, bypass, encrypt, quarantine, and coach for policy enforcement. With Netskope, enforce policies such as "automatically encrypt data classified as 'confidential' being uploaded to a sanctioned cloud storage service," or "block public sharing of data classified as 'company internal.'"

Netskope and TITUS Features

FEATURE	DESCRIPTION
Data classification	• User-driven classification within key productivity applications • System-suggested classification • Automatic classification based on content, author, and other document attributes
Visual markings	• Visual markings applied in headers, footers, and watermarks to clearly identify information • Increase security awareness and promote proper handling of sensitive data
Persistent metadata	• Data classification selections stored with document as persistent metadata • System-level visibility can be used by DLP, security, and archiving solutions
Advanced, cloud DLP	• Control sensitive data in and en route to and from all cloud services • Get the highest degree of accuracy with fingerprinting, exact match, and more
Multi-mode architecture	• Gain full visibility of sanctioned and unsanctioned cloud services • See traffic whether users are on premises or remote, using browsers, sync clients, or mobile apps
Granular visibility and control	• Understand use and enforce policies across cloud services based on identity, app, activity, data • Policy actions include allow, block, user alert, quarantine, and encrypt • Mix and match policy elements to carve out risk without blocking services

ABOUT TITUS

TITUS solutions enable organizations to discover, classify, protect, analyze, and confidently share information. Organizations use TITUS to meet regulatory compliance requirements by identifying and securing unstructured data—on the desktop, on mobile devices, and in the cloud. Millions of users in over 120 countries trust TITUS to keep their data compliant and secure.