


Enhancing **security automation**

Titus adds intelligence and context to security ecosystems



The background of the entire page is a dark blue and purple gradient. Overlaid on this is a network diagram consisting of numerous thin, light-colored lines that intersect to form a complex web of triangles and polygons. In the lower-left portion of the image, a hand is visible, holding a pen. The hand and pen are slightly out of focus. In the upper-left corner, there is a large, stylized green arrow pointing towards the right. The arrow has a gradient from a darker green at the top to a lighter green at the bottom.

Securing data cannot be achieved by the act of one technology. The growing volumes and diversity of data require a seemingly disparate set of purpose-built tools working together to make data security achievable. For many, the automation these tools deliver can bring fear, uncertainty, and doubt. Titus provides tools to remove these concerns by adding context to data so your security ecosystem can be better equipped to make accurate and effective data security decisions.



Increase the accuracy and effectiveness of DLP

Data loss prevention (DLP) solutions are often thought of as the first line of defense to address the challenge of insider security threats but can be difficult to implement effectively. Titus adds much needed intelligence to DLP products by applying metadata to data. By giving your data a recognizable identity, DLP solutions are empowered to make better policy decisions.



Connect the identification of data and people

Titus facilitates the use of data identification to allow/restrict access to data or an application based on the user's location, title, role in the business, etc. Data can be automatically classified based on user group, role, seniority, or virtually any other attribute and policy can be applied to prevent data from reaching inappropriate recipients. This is especially useful for industries in which ethical or legal boundaries must exist between departments.



Bring context to cloud security policies

Without the sensitivity of data being identified a Cloud Access Security Broker (CASB) has very little chance of knowing if a file can be placed on the cloud at all, let alone which one. This often results in CASB solutions being overly aggressive; bringing a high volume of false positives, user frustration, and dangerous workarounds. By giving users the power to provide a sensitivity to that data, Titus immediately gives CASBs the information required to decide which, if any, cloud instance(s) data can be placed on.



Enforce privacy & compliance

With the public's expectation for how their personal data is obtained, held, and shared rapidly evolving, governments have been introducing new regulations that carry significant ramifications for non-compliance. Titus helps you assert compliance today while staying ahead of the next regulation with a solution set that can identify and locate personal information and bring visibility to perimeter security products to improve the prevention of possible incidents. Titus policy and labels facilitate compliance across multiple global regulations.



Correlate users, data, and behavior with context

Detailed user activity logs from Titus allow you to report and measure the effectiveness of your security policies and add a level of intelligence to any security information and event management (SIEM) services deployed. Instantly know which users are downgrading classifications or misclassifying data, understand how and why machine learning classifications may differ from user-driven classifications. Aggregate Titus logs to establish a baseline risk scores for users and provide real-time intervention from insider threats.



Trigger rights management based on context

Titus takes the guesswork out of encryption by working with your chosen rights management provider to automatically trigger and configure the correct level of encryption and correct list of safe recipients. Secure and track data based on sensitivity, apply encryption to files at rest, and apply metadata to ensure proper handling on files that lack embedded properties. With Titus, enterprises can demonstrate use of best-of-breed technology and best practices with regards to privacy regulations and the protection of personal data.

Titus removes automation angst turns concern into confidence across your security ecosystem



Concern

Automation represents a loss of control by removing the human element in data security.

New tools often disrupt established workflows and organizational processes.

False positives slowing business objectives and can overwhelm users with unnecessary alerts.

Conflicting or duplicated policies among numerous disparate systems (DLP, CASB, Firewall, etc.)



Confidence

Titus gives you the power, and the freedom, to control your data on your terms. Involving users within the flow of work.

Unlimited schema flexibility is the foundation to a data security solution built around your existing processes and workflows.

Adding intelligence and context to security investments makes them work more accurately and effectively.

Agnostic design brings unmatched inter-operability. Titus acts as the policy broker at the heart of your security automation ecosystem.

About Titus

Titus is a leader in providing solutions that enable businesses to accelerate their adoption of data protection. Millions of users in over 120 countries trust Titus to keep their data compliant and secure, including some of the largest financial institutions and manufacturing companies in the world, government and military organizations across the G-7 and Australia, and Fortune 2000 companies. To learn more about how TITUS can help with CUI and CNSI marking and metadata programs visit www.titus.com.



1 (613) 820 5111 info@titus.com www.titus.com

© 2020 Titus Inc. ALL RIGHTS RESERVED