Enhancing security automation
Titus adds intelligence and context to security ecosystems
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 removes these concerns by adding context to data so your security ecosystem is 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 at creation within the flow of work. By identifying your data accurately, Titus empowers DLP solutions 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 organizations can apply policy to prevent data from reaching inappropriate recipients. This is especially useful for industries in which ethical or legal boundaries must exist between departments.

Enforce privacy & compliance

With the public’s rapidly evolving expectations for how their personal data is obtained, held, and shared, 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 solutions that can identify and locate personal information, enhance perimeter security products, and help prevent future incidents.

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, and understand how and why machine learning classifications may differ from user-driven classifications. Aggregate Titus logs to establish baseline risk scores for users and provide real-time intervention from insider threats.

Bring context to cloud security policies

A Cloud Access Security Broker (CASB) has very little chance of knowing if a file without embedded data identification can be placed in 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 identify sensitive data, Titus enables CASBs to quickly determine which, if any, cloud instance(s) can be used as a data destination.

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 build accurate lists 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. Enterprises can use Titus to demonstrate their use of best-of-breed technology and best practices with regards to privacy regulations and the protection of personal data.

© 2019 Titus Inc. ALL RIGHTS RESERVED
Titus 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 can slow business objectives and 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, and involve 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.