TITUS
Security & Compliance Solutions

User Driven Classification aduce DLP la viata

Distributor

RSD Reliable Solutions Distributor

Titus Customer Base

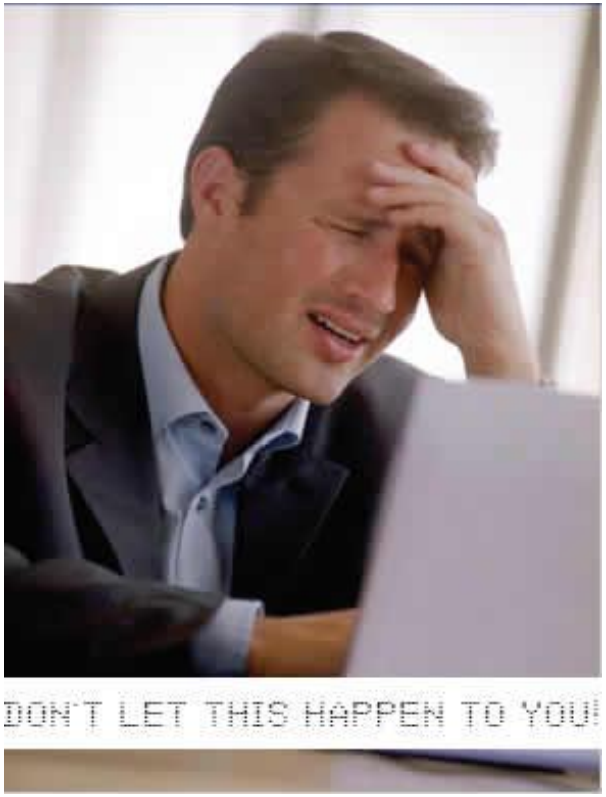
Over 2 Million Users , over than 300 Customers

Military

Government

Commercial

Email este Nr1 in riscul de pierderi de date

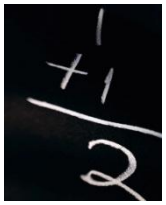


- Pierderi informatii de business (actiuni ale angajatilor care colaboreaza cu concurenta, etc)
- Pierderi informatii confidentiale
- Lipsa compliantei cu standarde, regulamente
- Pierderi informatii cu caracter personal
- Pierderi informatii proprietate intelectuala
- Posibil risc siguranta publica

De ce sa clasificam?

- Companiile creaza si manipuleaza cantitati enorme de informatie
- Nu toata aceasta informatie are aceeasi valoare sau prezinta acelasi grad de risc sau necesita acelasi grad de disponibilitate.

- Clasificare/segmentarea informatiei din companie ajuta la:
  - Asigurarea nivelul corespunzator de politici de securitate si control al informatiei, fiecarei categorii de informatie; acest control este aplicat obligatoriu, transparent si consecvent
  - Asigura ca informatia valoroasa de business este creata si manipulata in conditii de confidentialitate, integritate si disponibilitate in acelasi timp, protejand astfel investitiile companiei.
  - Asigura educarea, responsabilizarea, constientizarea angajatilor, protejarea lor insisi impotriva greselilor si gafelor



De ce clasificare ? Motive:

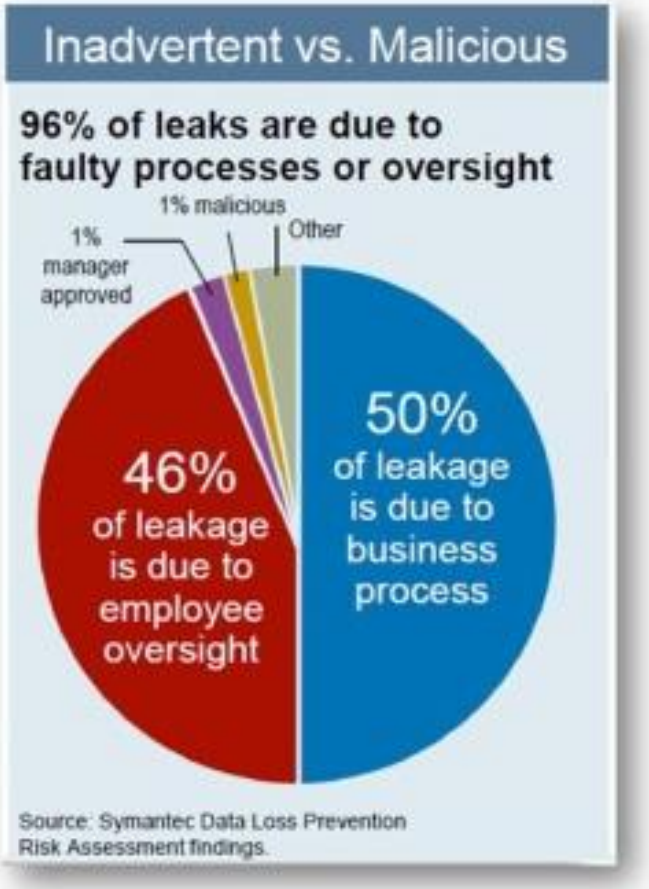
- **Securitate** – clasificarea/etichetarea informatiei (elementele vizuale pe emailur/documente creaza constientizare si responsabilitate in randul utilizatorilor, iar metadata este ulterior refolosita pentru aplicarea politicilor de securitate de catre AD, ADRMS, alte solutii (DLP, arhivare inteligenta, e-discovery, criptare, RMS, document right management, etc).
- **Retentie** – clasificarea permite intreprinderii sa construiasca si sa forteze reguli de retentie, optimizand astfel timpul de arhivare/stocare, mediile de stocare, ceea ce duce la reducerea TCO.
- **E-Discovery** – usureaza modul de regasire a informatei relevante prin folosirea metadatelor create prin clasificare ca si creiteriu de cautare.

Tehnologia singura nu e suficienta

Utilizatorul are un rol foarte important in protejarea informatiei. Prin solutia de clasificare utilizatorul devine:

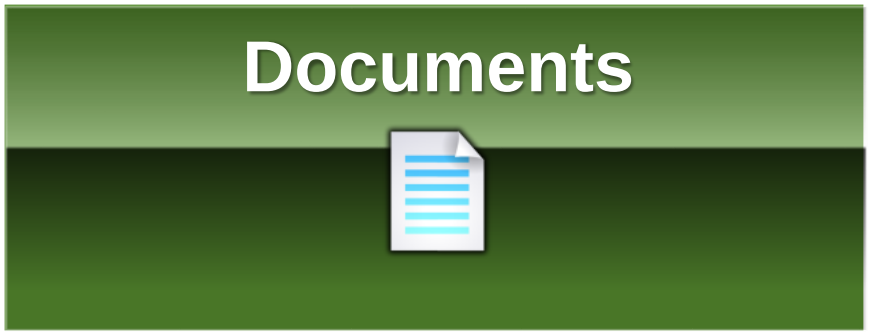
- Constient
- Responsabil
- Educat

Most Data Leaks are Inadvertent



TITUS Classification Solutions

* Titus Message Classification for Outlook (clasifica mesaje, task-uri, appointment);
*Titus Classification for OWA)



* Titus Classification for Office (clasifica fisiere Word, Excel, PowerPoint);
*Titus Classification for Desktop (clasifica orice tipuri de fisiere)
* Titus for LotusNotes

Solutii Titus for SharePoint

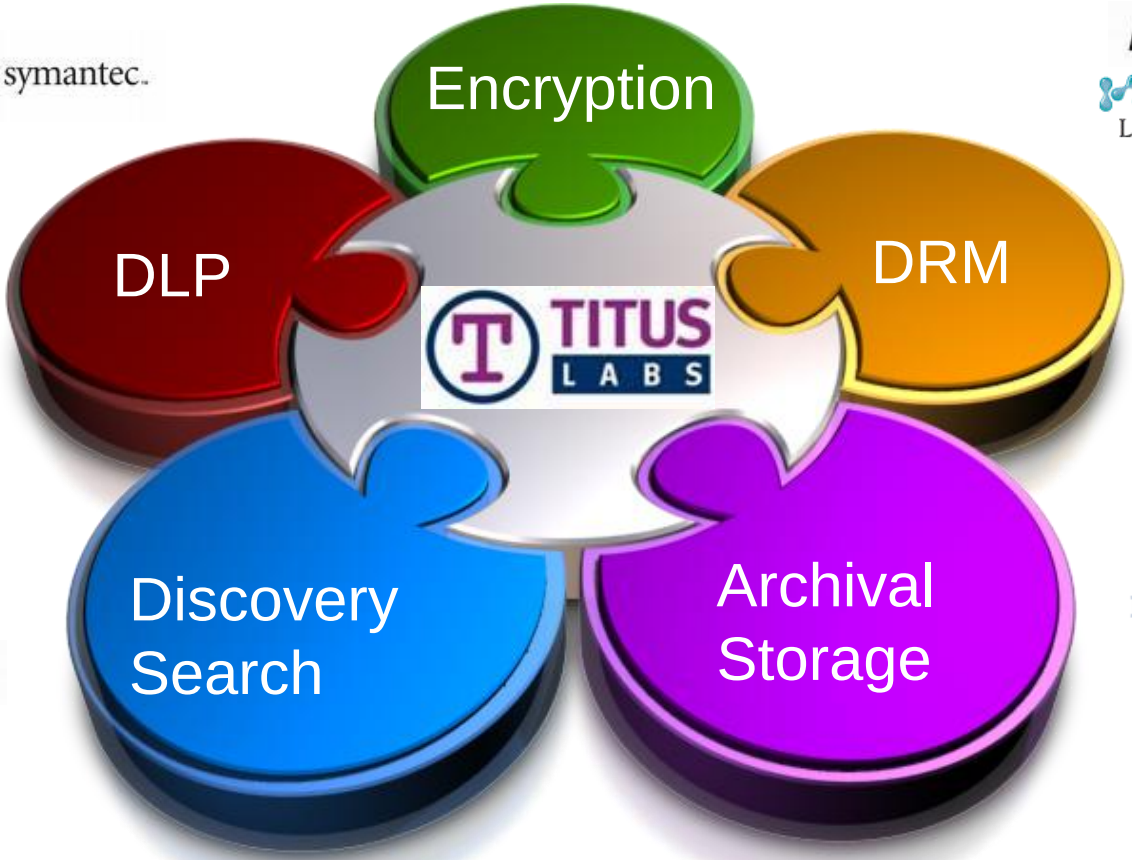
NOU: Solutii de clasificare pentru dispozitivele MOBILE

Classification & policy enforcement at the desktop

Interoperabilitate cu alte solutii

Solutii SIEM

Verdasys



CLASIFICAREA aduce **DLP** la viata.
(DLP – Batteries not included)

TITUS Classification™

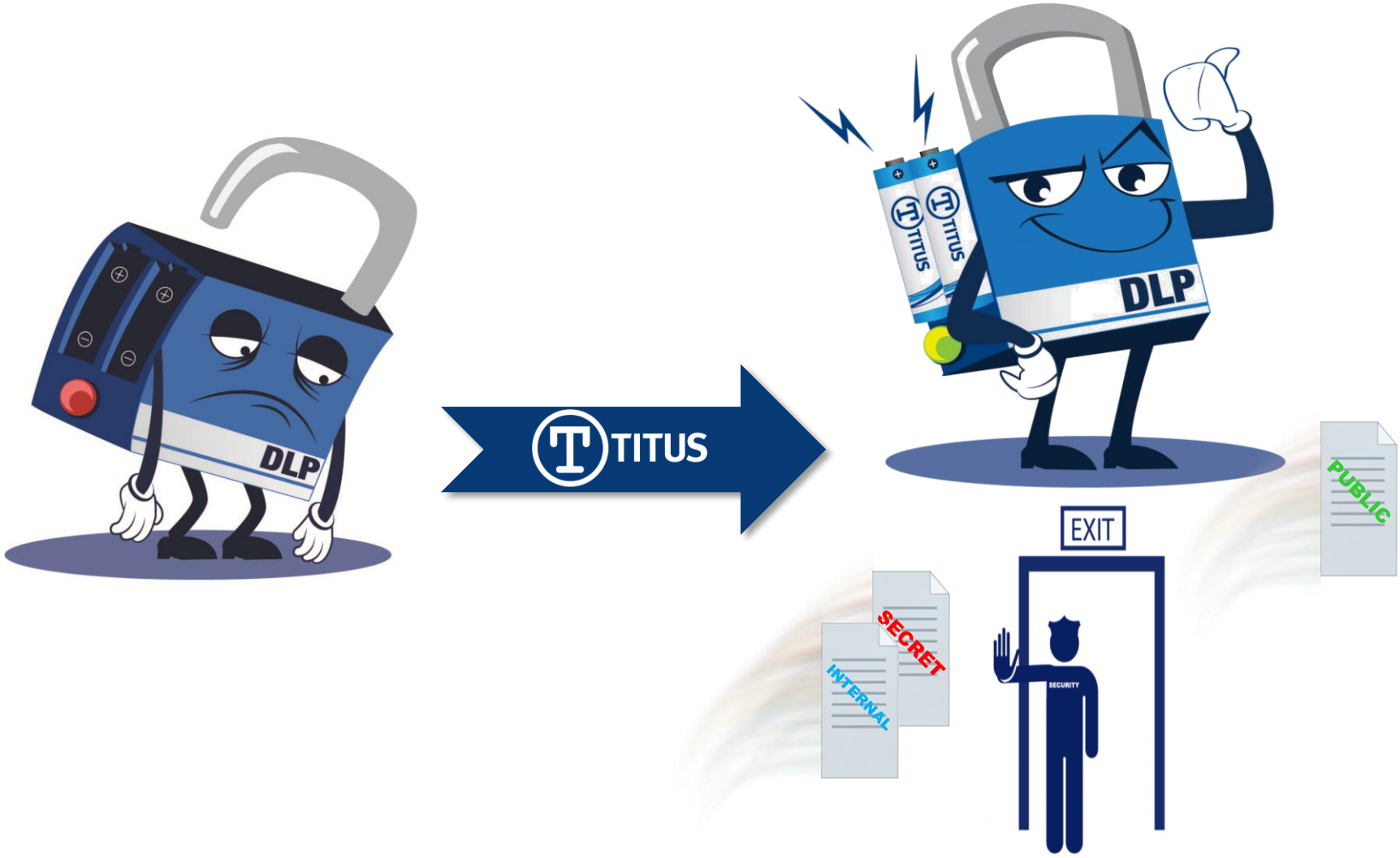
Email

Documente

Fisiere

- Utilizatorii isi clasifica informatia (si in acest fel se protejeaza si pe ei si informatiile companiei)
- Date si sigure si conforme
- Integrare cu solutii third party (si consolidarea acestor solutii)

Classification Brings your DLP to Life!



Protejeaza-ti datele prin Clasificare

TITUS = prima linie de aparare

Identifica sensibilitatea informatiei

- Utilizatorul este fortat sa clasifice fisierele, documentele, email-urile…

Clasifica informatia

- Utilizatorul a clasificat
- TITUS injecteaza Metadata si aplica Politicile de marcare

Protejeaza

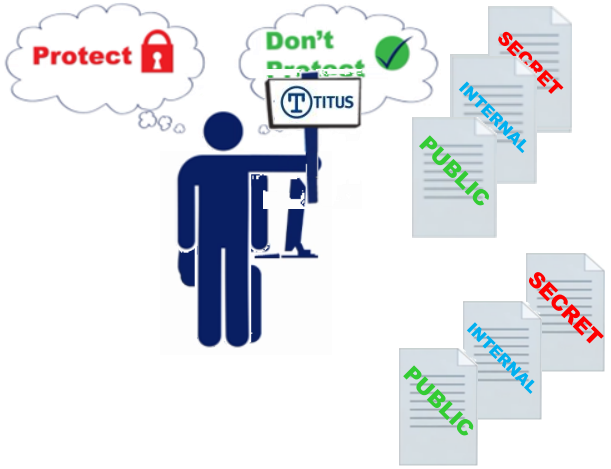
- Se aplica marcaje vizuale pentru constientizare
- Solutiile DLP (host sau Network) declanseaza politici bazate pe continut sau metadate

TITUS = Prima linie de aparare

- Educa utilizatorul
- Creste nivelul de constientizare al utilizatorului
- Avertizeaza utilizatorul
- Previne violarea politicilor
- Permite justificarea utilizatorului
- Protejeaza utilizatorul impotriva

propriilor greseli

Increderea in Utilizator



DLP = A doua linie de aparare

- Carantina
- Blocare
- Raportare
- Recunoaste nevoia de protectie a informatiei clasificate la nivel inalt (prin solutia de clasificare)
- Verifica existenta intentiilor malicioase pe Alte Clasificari
- Analizeaza sabloanele comportamentale ale utilizatorilor

TITUS & DLP

- TITUS cladifica informatia care mai departe poate fi citita de catre DLP
  - Metadate TITUS
  - Marcaje vizuale TITUS

- DLP protejeaza informatia functie de sensibilitatea ei data de clasificarea data de Titus

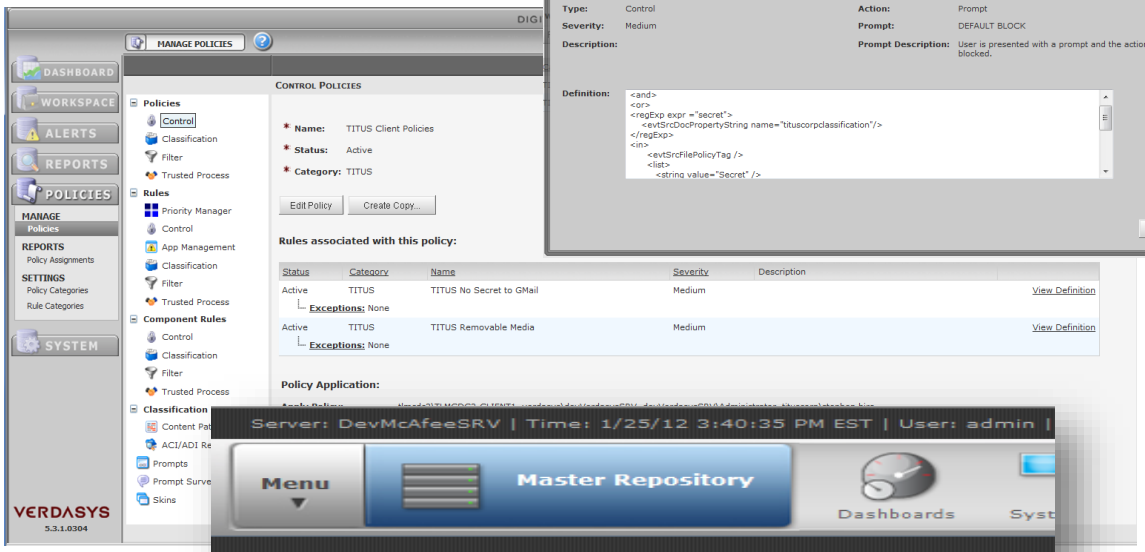
TITUS aduce DLP la viata!

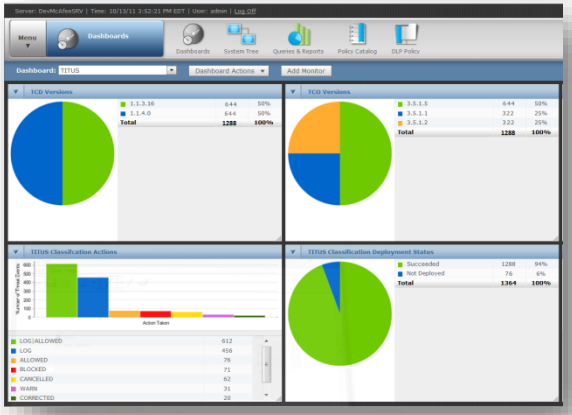
- Titus valorifica puterea DLP
  - Reduce False Positives
  - No more “Monitor Mode”

- TITUS Implica UTILIZATORII
  - Utilizatorii isi pun amprenta si raspunderea asupra informatiei, DLP devenind astfel mai eficient
  - Ii educa pe utilizatori in spiritul politicilor companiei
  - Creste constientizarea si responsabilitatea utilizatorului

Puncte de integrare

- Metadata
- Deployment (agentul ePO)
- Logging & Reporting



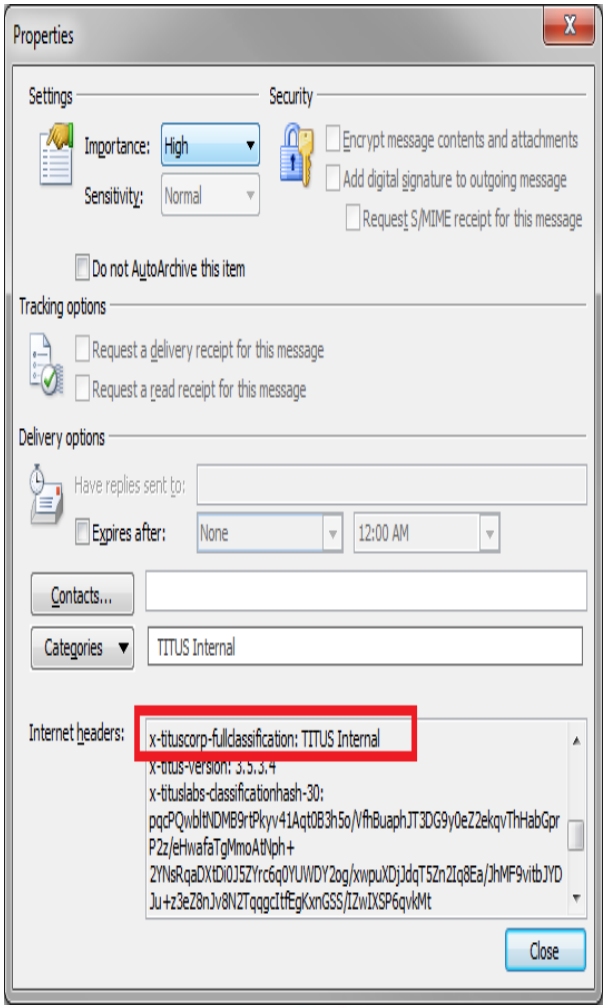


DLP-uri cu care exista experienta de implementare

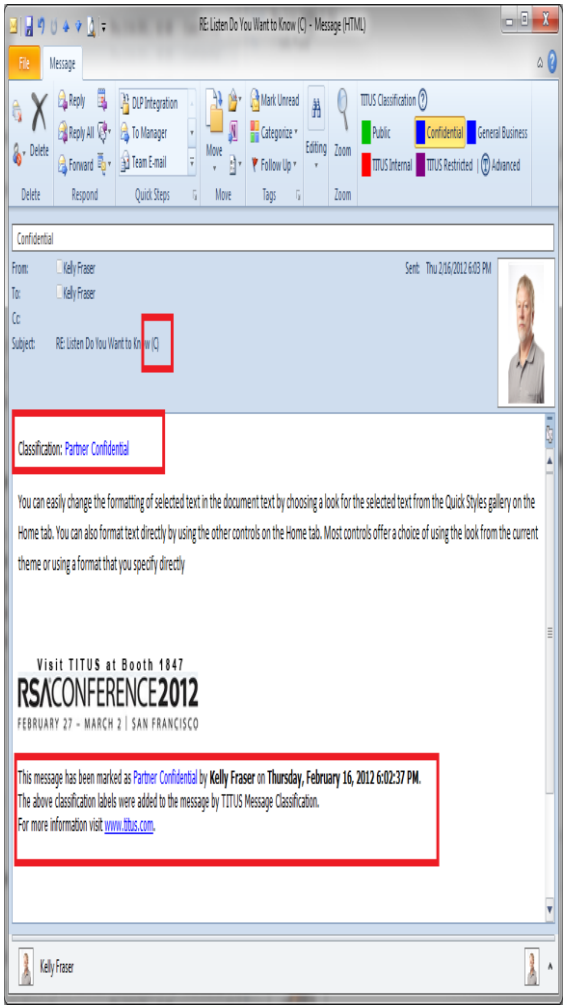
- Working with McAfee
- Working with Verdasys
- Working with Symantec
- Working with WebSense
- Working with RSA
- Working with others.

TITUS Message Classification™ for Microsoft Outlook®

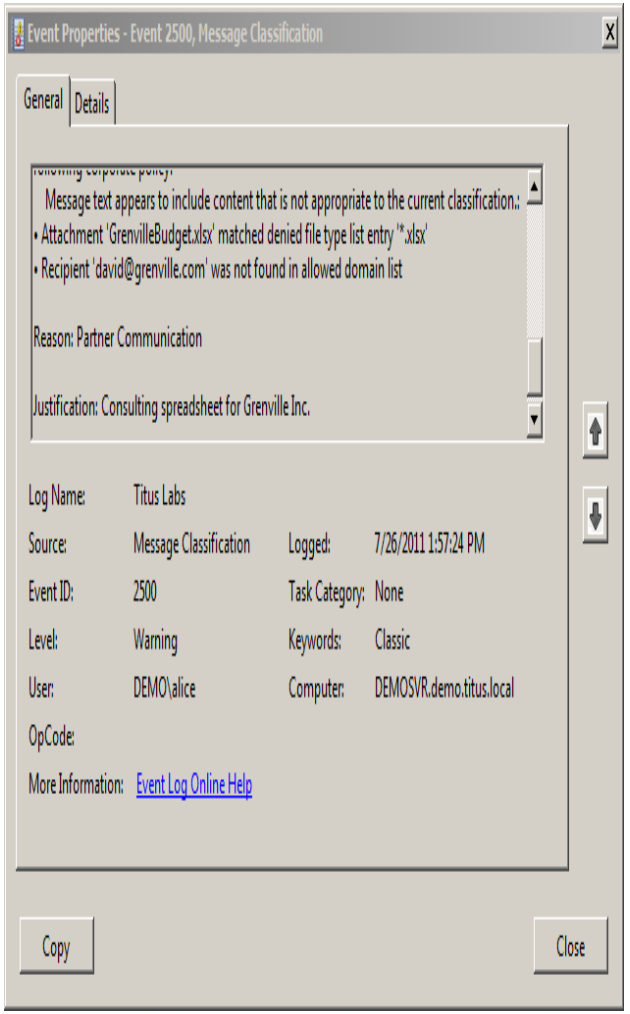
- Metadata



- Marcaje vizuale

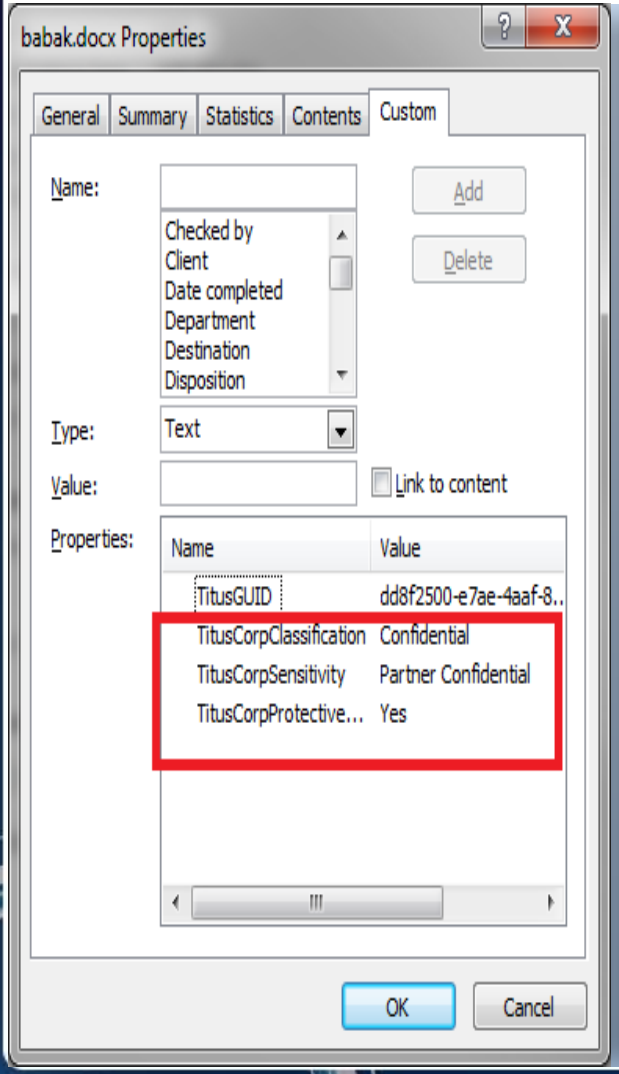


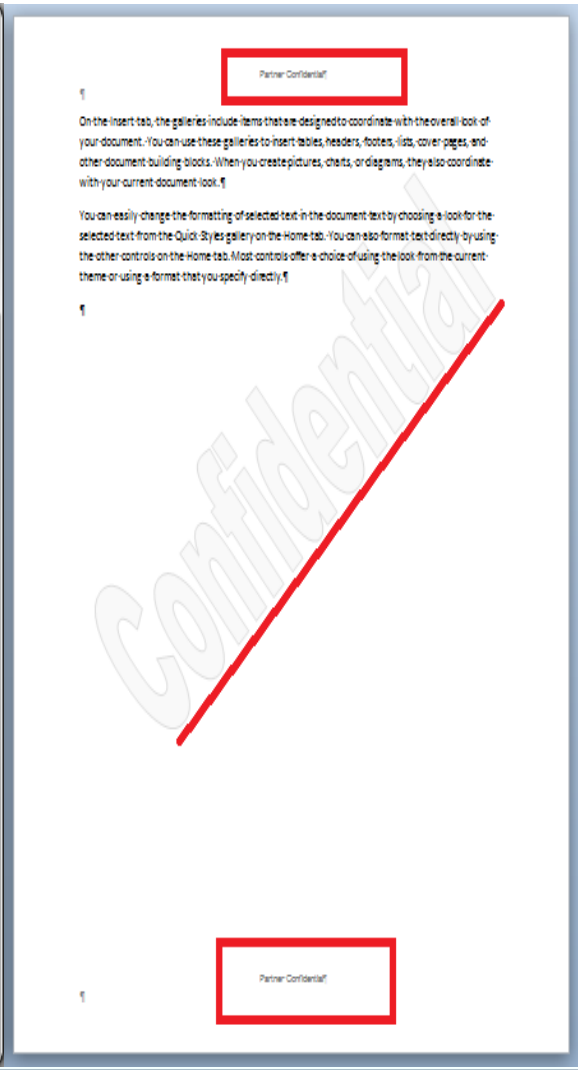
- Logging

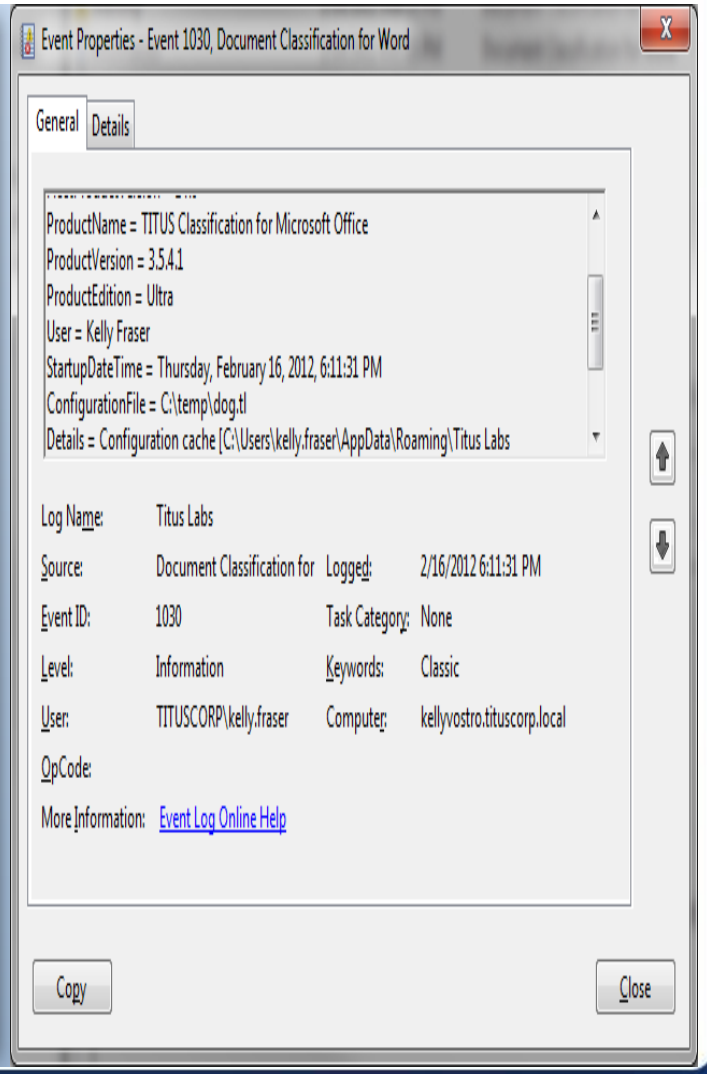


TITUS Classification for Microsoft Office

- Metadata
- Marcaje vizuale
- Logging







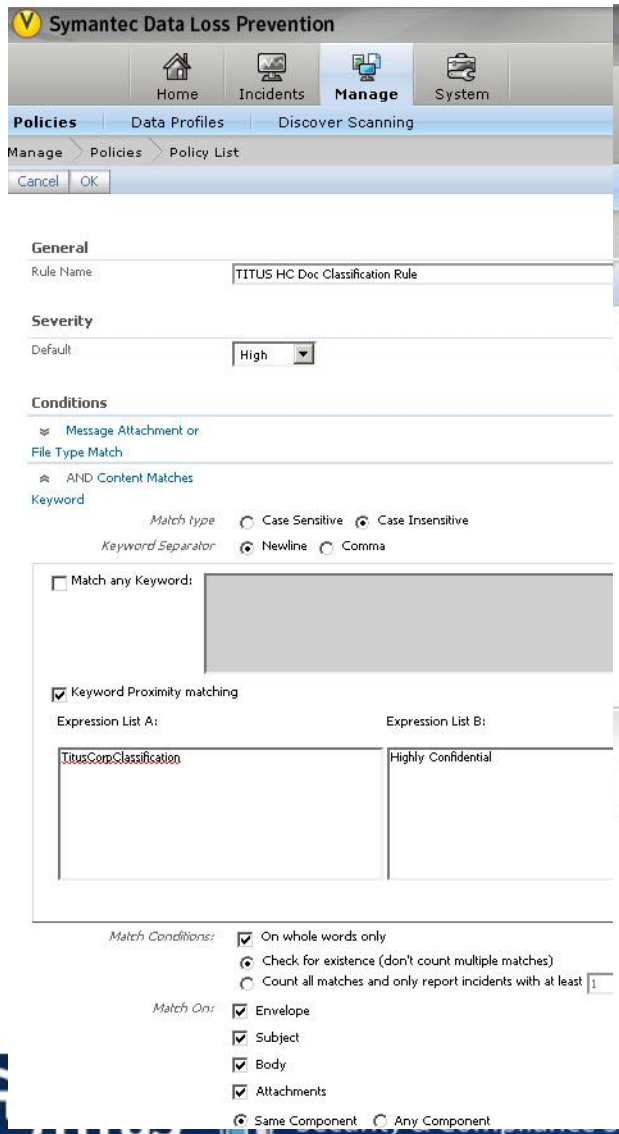
Symantec si TITUS

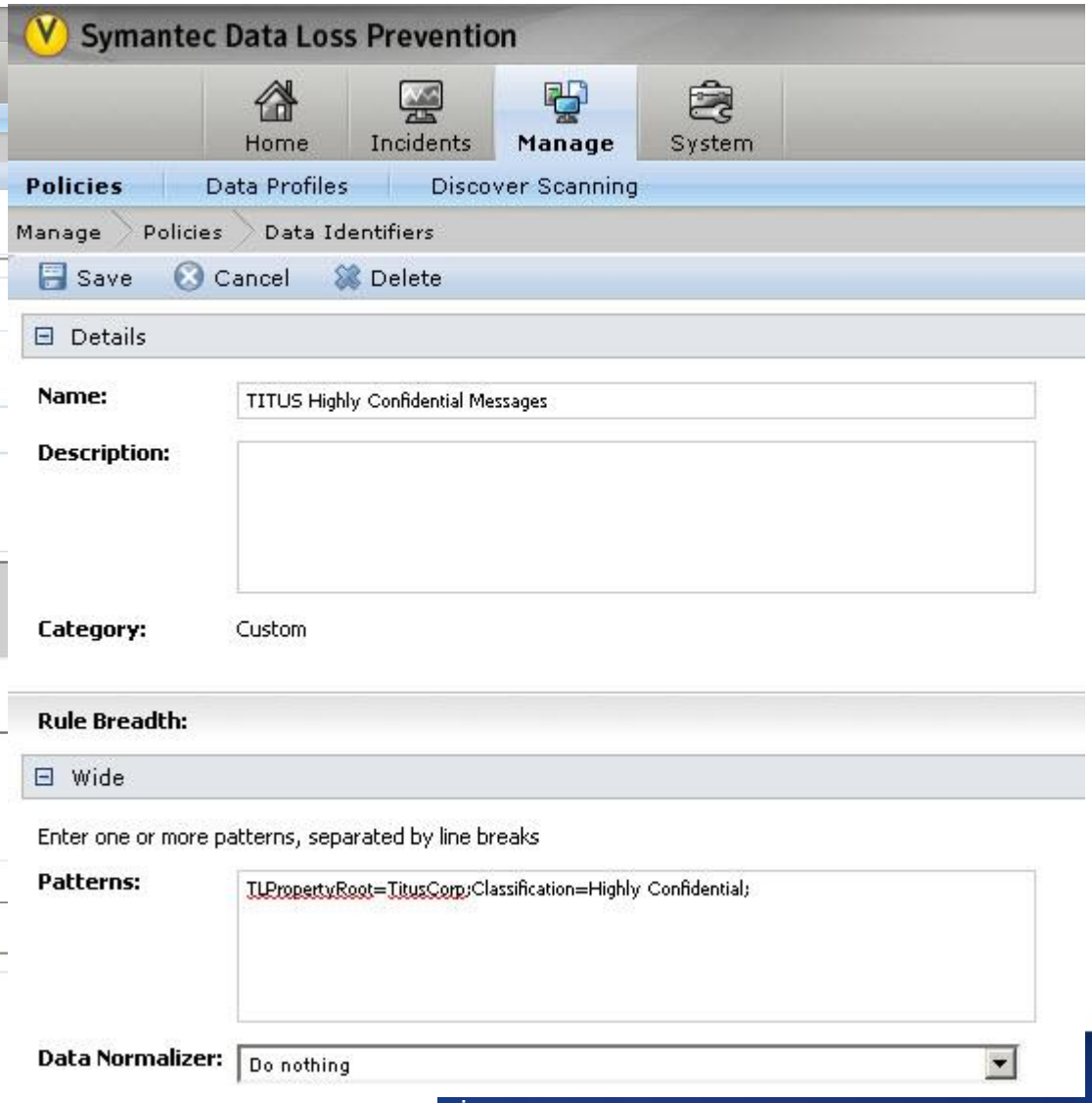
- Interoperabilitate dovedita cu
  - Symantec Enterprise Vault and
  - Symantec PGP
  - Symantec DLP Detection Policies
  - Symantec DLP Incident Response (with FlexResponse)

Integrare cu Symantec

- **Scenarii de detectie multipla:**
  - Descopera toate documentele si/sau email-urile clasificate ca “Highly Confidential”
  - Blocheaza copierea pe medii removable doar daca clasificarea este “Highly Confidential”
  - Contorizeaza numarul de mesaje “Highly Confidential” in tranzit in organizatie

TITUS and Symantec DLP: Detect

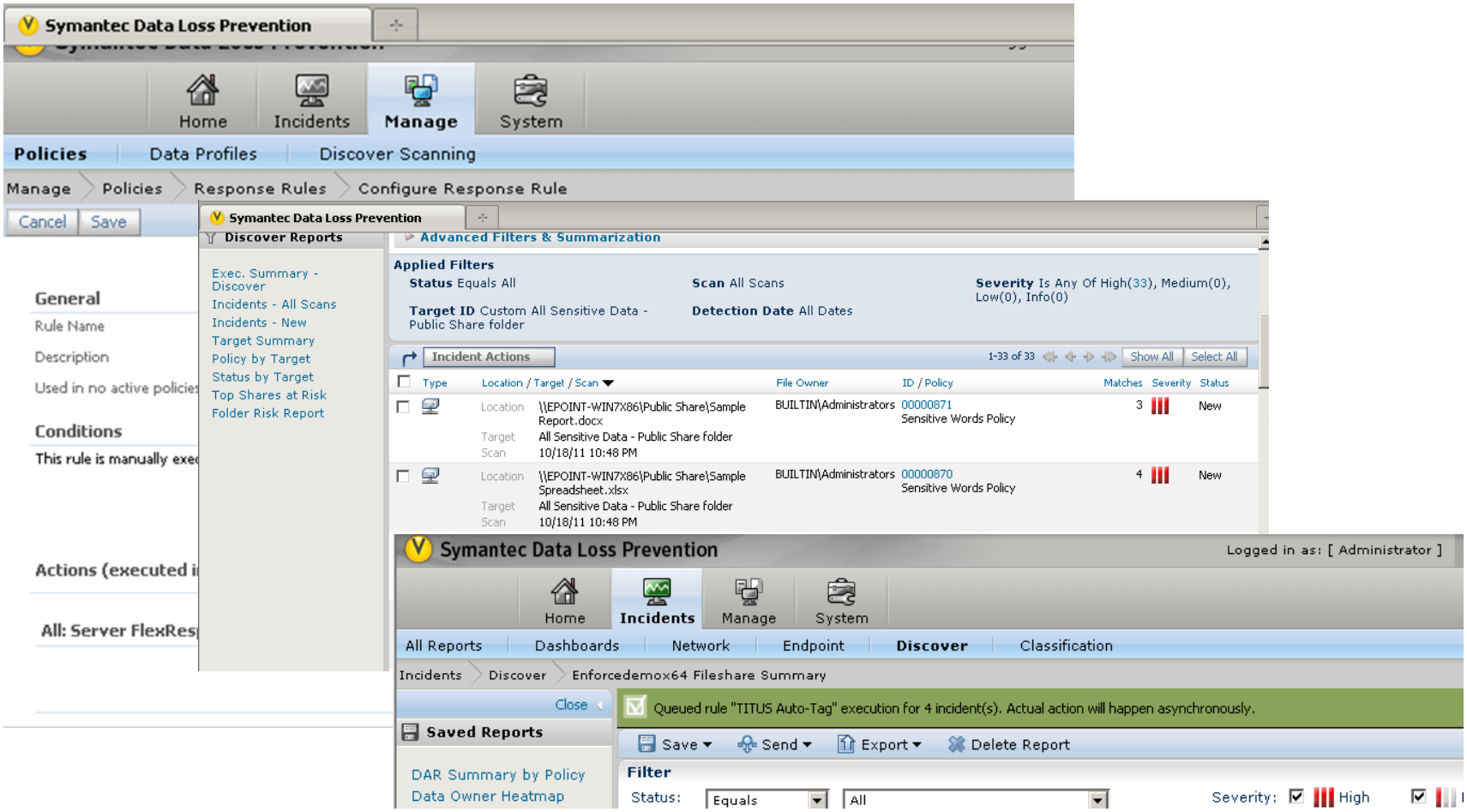




Integrare cu Symantec

- **Scenarii de detectie multipla**
  - Descopera documentele care nu au fost clasificate inca (nu au metadata Titus)
  - Descopera toate documentele care nu sunt clasificate dar contin informatii “highly confidential” si clasifica folosind TITUS

TITUS and Symantec DLP: Apply



TITUS Mobile Solution

Mobile Data Security

- Securitatea informatiilor pe dispozitivele mobile a devenit o prioritate de top pentru organizatii
  - BYOD (Bring your own device) – angajatii aduc propriile dispozitive mobile si le conecteaza in infrastructura companiei
  - Informatia este pretutindeni

- Informatia neclasificata pe dispozitivele mobile este un punct sever de vulnerabilitate

TITUS Mobile Solution ***Coming soon***

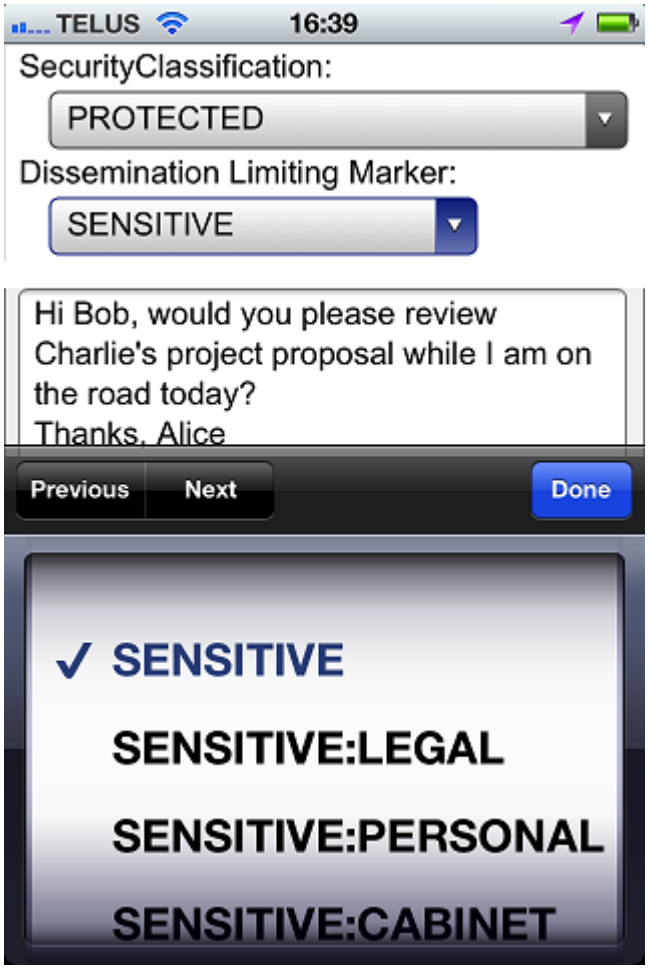
Solutiile de securitate asupra email-urilor de pe dispozitivele mobile protejeaza informatia astfel:

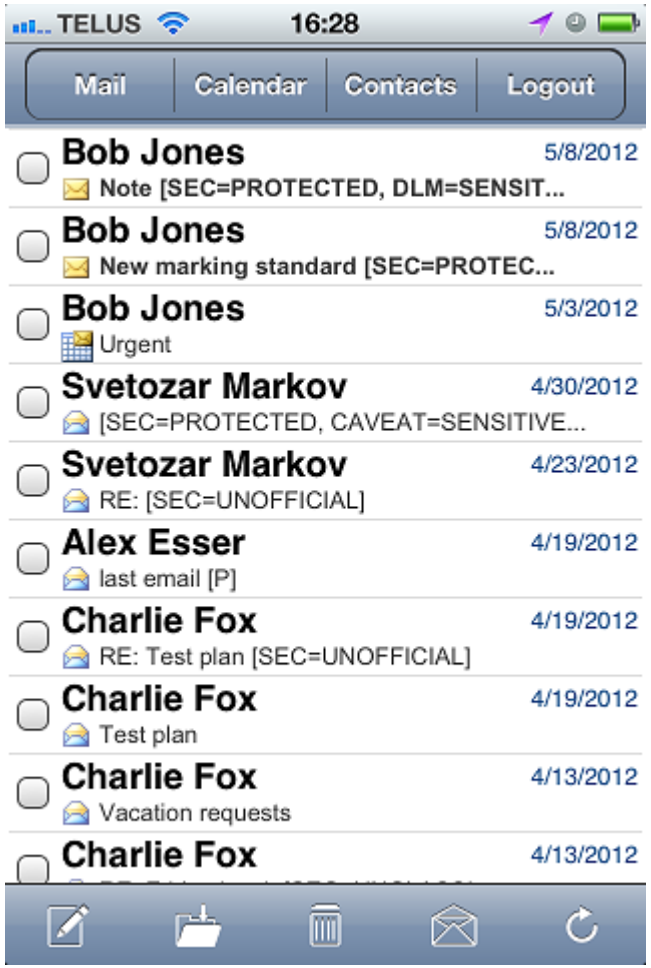
- Forteaza utilizatorii sa clasifice email-urile in mod consistent atat pe desktop cat si pe dispozitivul mobil
- Separa email-urile de business de cele personale
- Controleaza informatia bazandu-se pe sensibilitatea ei
- Lucreaza cu Mobile Device Management

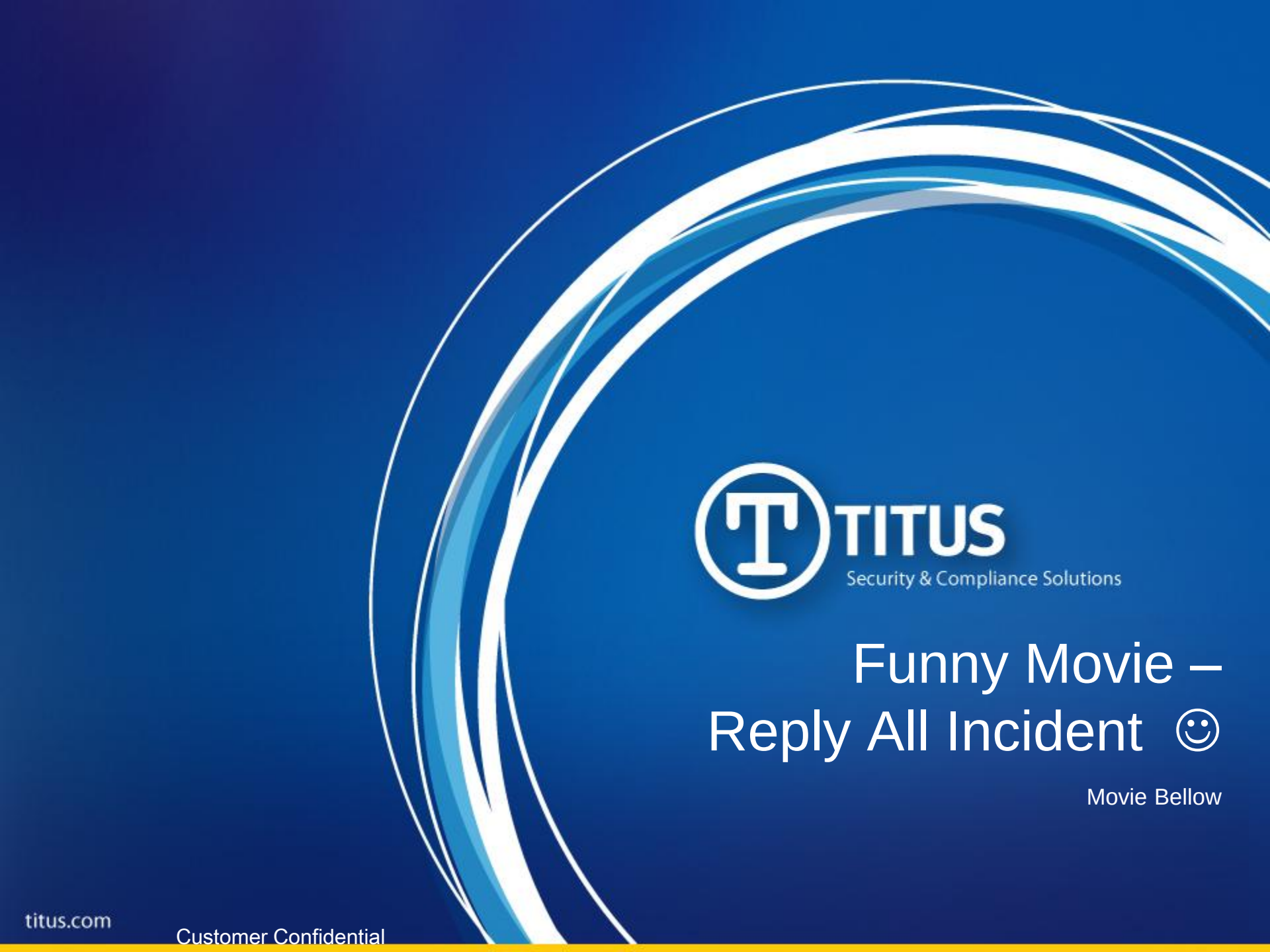
Classification for Mobile Users

- Solutions for BlackBerry Smartphone (available), iPhone (coming soon), Windows Mobile Device (available) and Android Devices

NEW…iPhone







Funny Movie – Reply All Incident ☺

Movie Bellow