



Distributor



titus.com

Customer Confidential

**User Driven Classification aduce
DLP la viata**

Titus Customer Base

Over 2 Million Users , over than 300 Customers

Military



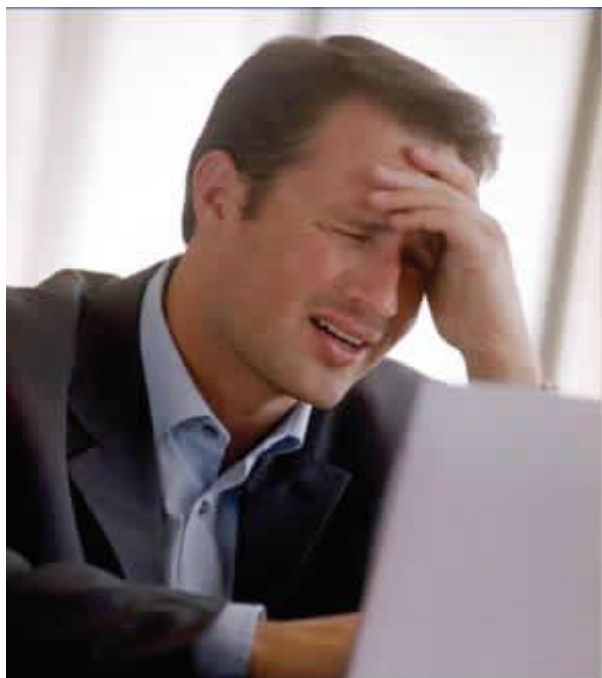
Government



Commercial



Email este Nr1 in riscul de pierderi de date

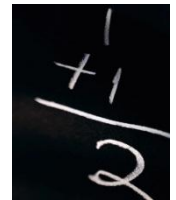


DON'T LET THIS HAPPEN TO YOU!

- 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 creeaza 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 nivelului 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 re folosita 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 informatiei relevante prin folosirea metadatelor create prin clasificare ca si creiteriu de cautare.

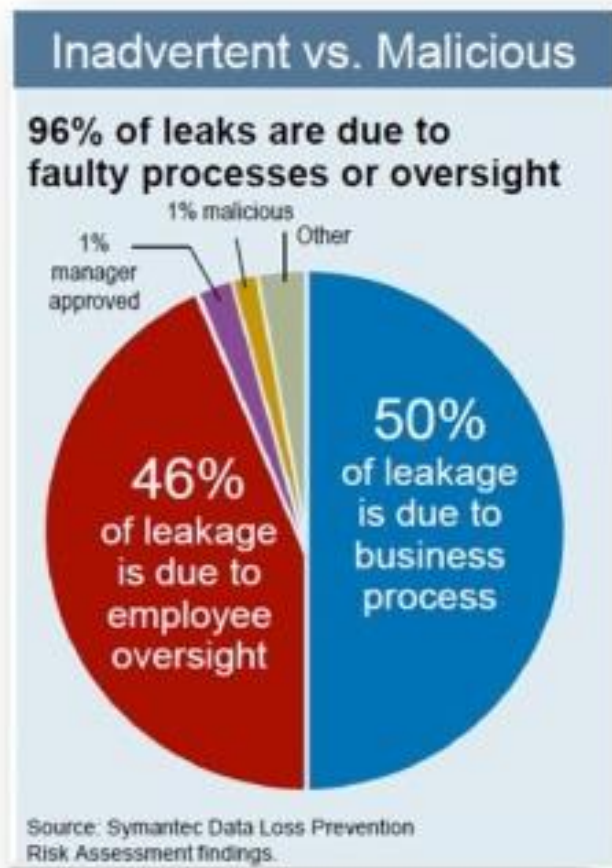
Tehnologia singura nu e suficienta



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

E-Mail



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

Documents



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

SharePoint



Solutii Titus for SharePoint

NOU: Solutii de clasificare pentru dispozitivele MOBILE

Classification & policy enforcement at the desktop

Interoperabilitate cu alte solutii

McAfee®

Verdasys

VeriSign®

Entrust®
Securing Digital Identities
& Information

Voltage
SECURITY

Solutii SIEM

RSA®

The Security Division of EMC

symantec.

Microsoft®



LIQUID MACHINES

The Freedom of Security.™

EMC²

where information lives®



Microsoft Office
SharePoint

EMC² | documentum

Quest®
Archive Manager

Kazeon®

Microsoft

Discovery
Search

Archival
Storage

TITUS
LABS



Security & Compliance Solutions



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

TITUS Classification™

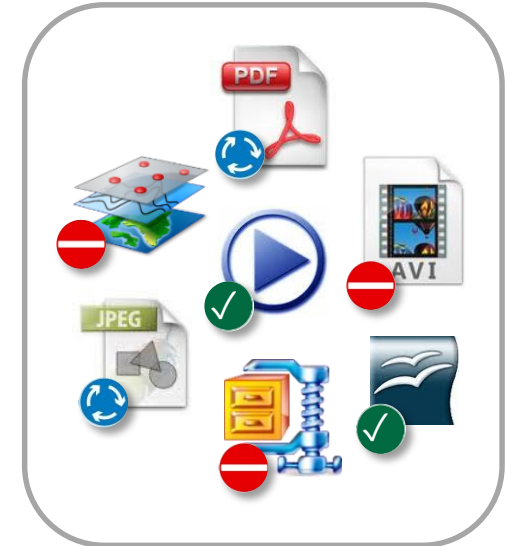
Email



Documente

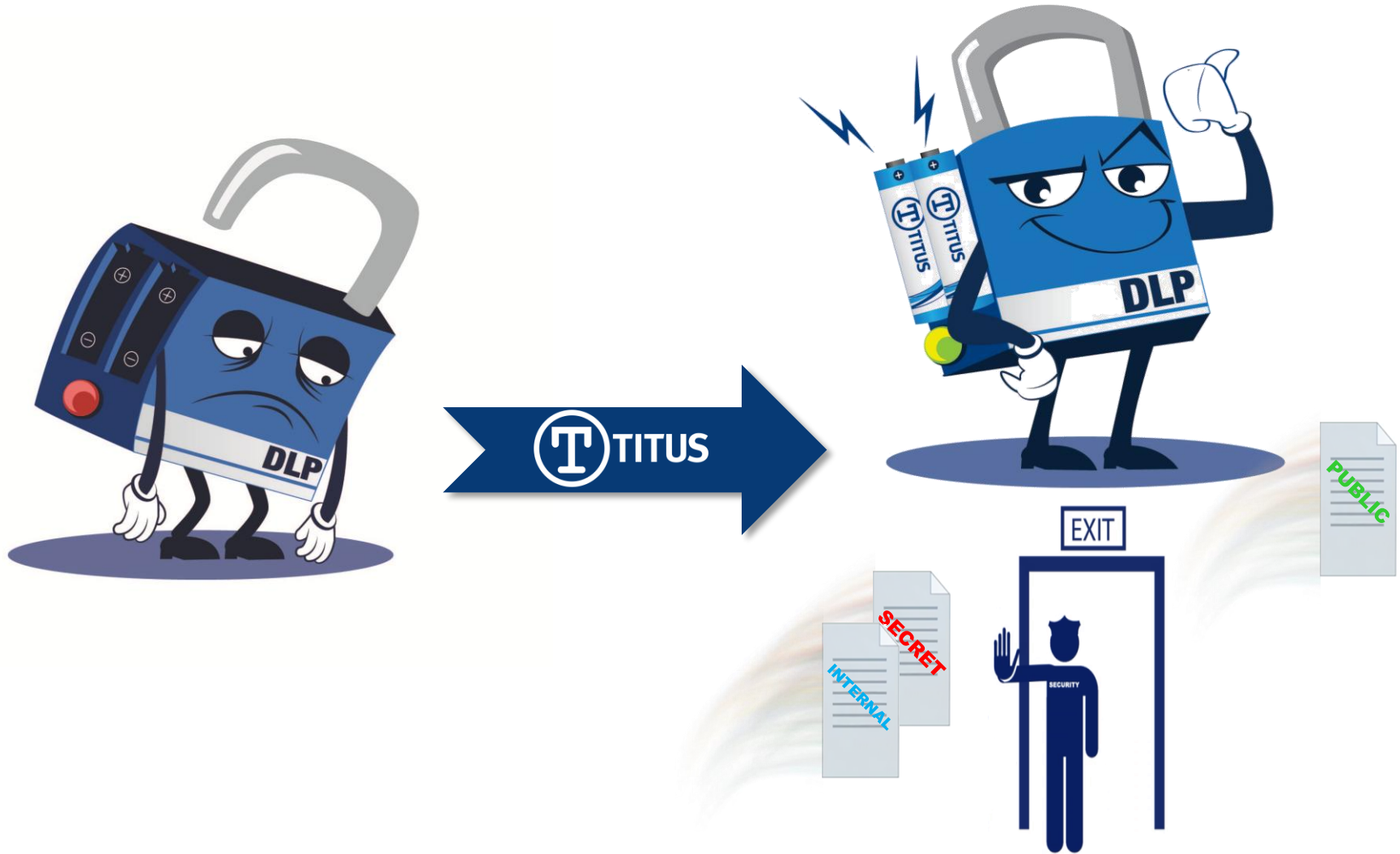


Fisiere



- 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)

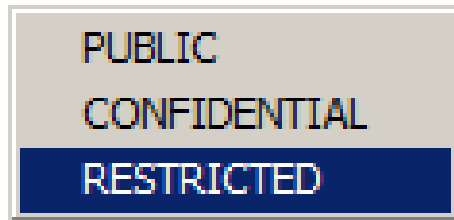
Classification Brings your DLP to Life!



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

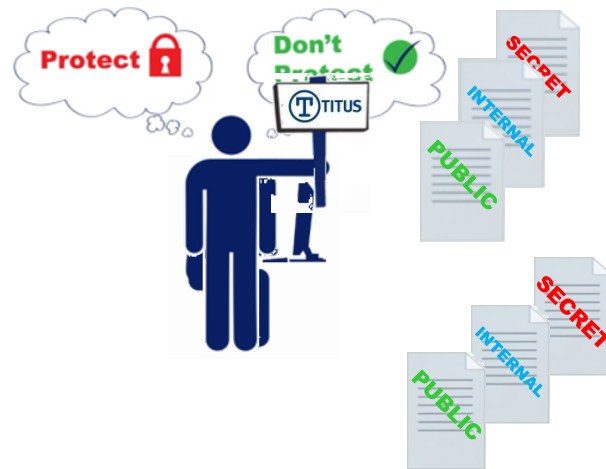


- Se aplica marcaje vizuale pentru constientizare
- Solutiile DLP (host sau Network) declanseaza politici bazate pe continut sau metadata

TITUS = Prima linie de aparare

- Educa utilizatorul
- Crește nivelul de conștientizare al utilizatorului
- Avertizează utilizatorul
- Previne violarea politicilor
- Permite justificarea utilizatorului
- Protejează utilizatorul împotriva propriilor greșeli

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 clasifica 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
 - li educa pe utilizatori in spiritul politicilor companiei
 - Creste constientizarea si responsabilitatea utilizatorului



Puncte de integrare

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

Rule Definition

Name: TITUS No Secret to Gmail Status: Active
 Category: TITUS Modified by: DMC Users/layadmin
 Type: Control Action: Prompt
 Severity: Medium Prompt: DEFAULT BLOCK
 Description: Prompt Description: User is presented with a prompt and the action is blocked.

```

Definition:
<and>
<or>
<regExp expr="secret">
<evtSrcDocPropertyString name="tituscorpclassification"/>
</regExp>
</or>
<evtSrcFilePolicyTag />
</and>
<string value="Secret" />
    
```

Rules associated with this policy:

Status	Category	Name	Severity	Description
Active	TITUS	TITUS No Secret to Gmail	Medium	View Definition
Active	TITUS	TITUS Removable Media	Medium	View Definition

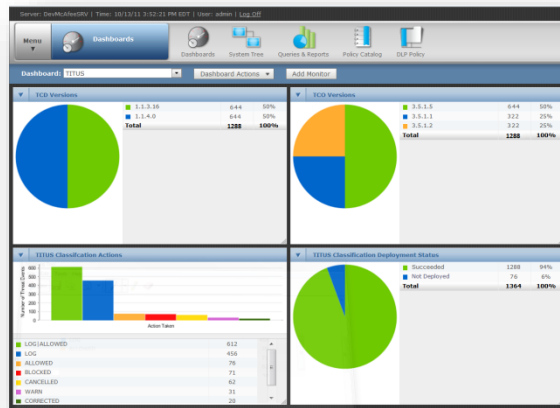
Server: DevMcAfeeSRV | Time: 1/25/12 3:40:35 PM EST | User: admin

Menu Master Repository Dashboards System

Packages in Master Repository

Preset: All Branches

Name	Status	Type	Version
ePO Agent Key Updater	OK	Plugin	4.6.0
Host Intrusion Prevention Content	OK	DAT	7.0.0
McAfee Agent for Linux	OK	Install	4.5.0
McAfee Agent for Mac OS X	OK	Install	4.5.0
McAfee Agent for Windows	OK	Install	4.5.0
McAfee Data Loss Prevention	OK	Install	9.1.0
Rogue System Sensor	OK	Install	4.6.0
TalkNow	OK	Install	2.0
Titus Classification for Desktop	OK	Install	1.1
Titus Classification For Office	OK	Install	3.5
Titus Message Classification	OK	Install	3.5



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

The screenshot shows the 'Properties' dialog box in Outlook, with the 'Security' tab selected. The 'Importance' is set to 'High' and 'Sensitivity' is 'Normal'. There are checkboxes for 'Encrypt message contents and attachments', 'Add digital signature to outgoing message', and 'Request S/MIME receipt for this message'. Under 'Tracking options', there are checkboxes for 'Request a delivery receipt for this message' and 'Request a read receipt for this message'. Under 'Delivery options', there is a field for 'Have replies sent to:' and an 'Expires after:' dropdown set to 'None' at '12:00 AM'. At the bottom, there are 'Contacts...' and 'Categories' dropdowns, with 'TITUS Internal' selected. The 'Internet headers' section is expanded, showing a list of headers. The first header, 'x-tituscorp-fullclassification: TITUS Internal', is highlighted with a red box.

- Marcaje vizuale

The screenshot shows an Outlook message window. The message is from Kelly Fraser, sent on Thursday, February 16, 2012 at 6:03 PM. The subject is 'RE: Listen Do You Want to Know (C) - Message (HTML)'. The message content includes a 'Confidential' classification label, which is highlighted with a red box. Below the message content, there is a red box containing the text: 'Classification: Partner Confidential'. At the bottom of the message, there is a red box containing the text: 'This message has been marked as Partner Confidential by Kelly Fraser on Thursday, February 16, 2012 6:02:37 PM. The above classification labels were added to the message by TITUS Message Classification. For more information visit: www.titus.com.'

- Logging

The screenshot shows the 'Event Properties' dialog box for 'Event 2500, Message Classification'. The 'General' tab is selected. The 'Log Name' is 'Titus Labs'. The 'Source' is 'Message Classification' and the 'Logged' time is '7/26/2011 1:57:24 PM'. The 'Event ID' is '2500' and the 'Task Category' is 'None'. The 'Level' is 'Warning' and the 'Keywords' are 'Classic'. The 'User' is 'DEMO\alice' and the 'Computer' is 'DEMOSVR.demo.titus.local'. The 'OpCode' is empty. The 'More Information' is 'Event Log Online Help'. There are 'Copy' and 'Close' buttons at the bottom.

- Metadata

babak.docx Properties

General Summary Statistics Contents Custom

Name: Add

Checked by: Client
Date completed:
Department:
Destination:
Disposition:

Type: Text

Name	Value
TitusGUID	dd8f2500-e7ae-4aaf-8...
TitusCorpClassification	Confidential
TitusCorpSensitivity	Partner Confidential
TitusCorpProtective...	Yes

OK Cancel

- Marcaje vizuale

Partner Confidential

On the Insert tab, the galleries include items that are designed to coordinate with the overall look of your document. You can use these galleries to insert tables, headers, footers, lists, cover pages, and other document building blocks. When you create pictures, charts, or diagrams, they also coordinate with your current document look.

You can easily change the formatting of selected text in the document text by choosing a look for the selected text from the Quick Styles gallery on the Home tab. You can also format text directly by using the other controls on the Home tab. Most controls offer a choice of using the look from the current theme or using a format that you specify directly.

Partner Confidential

- Logging

Event Properties - Event 1030, Document Classification for Word

General Details

ProductName = TITUS Classification for Microsoft Office
ProductVersion = 3.5.4.1
ProductEdition = Ultra
User = Kelly Fraser
StartupDateTime = Thursday, February 16, 2012, 6:11:31 PM
ConfigurationFile = C:\temp\dog.tl
Details = Configuration cache [C:\Users\kelly.fraser\AppData\Roaming\Titus Labs]

Log Name: Titus Labs
Source: Document Classification for Word Logged: 2/16/2012 6:11:31 PM
Event ID: 1030 Task Category: None
Level: Information Keywords: Classic
User: TITUSCORP\kelly.fraser Computer: kellyvostro.tituscorp.local
OpCode:
More Information: [Event Log Online Help](#)

Copy Close

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

Symantec Data Loss Prevention

Home Incidents **Manage** System

Policies Data Profiles Discover Scanning

Manage > Policies > Policy List

Cancel OK

General

Rule Name: TITUS HC Doc Classification Rule

Severity

Default: High

Conditions

Message Attachment or File Type Match

AND Content Matches

Keyword

Match type: Case Sensitive Case Insensitive

Keyword Separator: Newline Comma

Match any Keyword:

Keyword Proximity matching

Expression List A:	Expression List B:
TitusCorpClassification	Highly Confidential

Match Conditions:

On whole words only

Check for existence (don't count multiple matches)

Count all matches and only report incidents with at least 1

Match On:

Envelope

Subject

Body

Attachments

Same Component Any Component

Symantec Data Loss Prevention

Home Incidents **Manage** System

Policies Data Profiles Discover Scanning

Manage > Policies > Data Identifiers

Save Cancel Delete

Details

Name: TITUS Highly Confidential Messages

Description:

Category: Custom

Rule Breadth:

Wide

Enter one or more patterns, separated by line breaks

Patterns: TLPropertyRoot=TitusCorp:Classification=Highly Confidential;

Data Normalizer: Do nothing

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

The screenshot displays the Symantec Data Loss Prevention (DLP) console interface. The top navigation bar includes 'Home', 'Incidents', 'Manage', and 'System'. The main menu shows 'Policies', 'Data Profiles', and 'Discover Scanning'. The breadcrumb trail indicates the current location: 'Manage > Policies > Response Rules > Configure Response Rule'. A 'General' sidebar on the left lists various report types like 'Exec. Summary - Discover' and 'Incidents - All Scans'. The main content area is titled 'Discover Reports' and shows 'Advanced Filters & Summarization' with applied filters for status, target ID, and severity. Below this is a table of incident actions.

Type	Location / Target / Scan	File Owner	ID / Policy	Matches	Severity	Status
<input type="checkbox"/>	Location: \\EPOINT-WIN7X86\Public Share\Sample Report.docx Target: All Sensitive Data - Public Share folder Scan: 10/18/11 10:48 PM	BUILTIN\Administrators	00000871 Sensitive Words Policy	3	High	New
<input type="checkbox"/>	Location: \\EPOINT-WIN7X86\Public Share\Sample Spreadsheet.xlsx Target: All Sensitive Data - Public Share folder Scan: 10/18/11 10:48 PM	BUILTIN\Administrators	00000870 Sensitive Words Policy	4	High	New

A notification banner at the bottom of the console states: 'Queued rule "TITUS Auto-Tag" execution for 4 incident(s). Actual action will happen asynchronously.' The notification includes options to 'Save', 'Send', 'Export', and 'Delete Report'. The filter section at the bottom shows 'Status: Equals All' and 'Severity: High' selected.



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

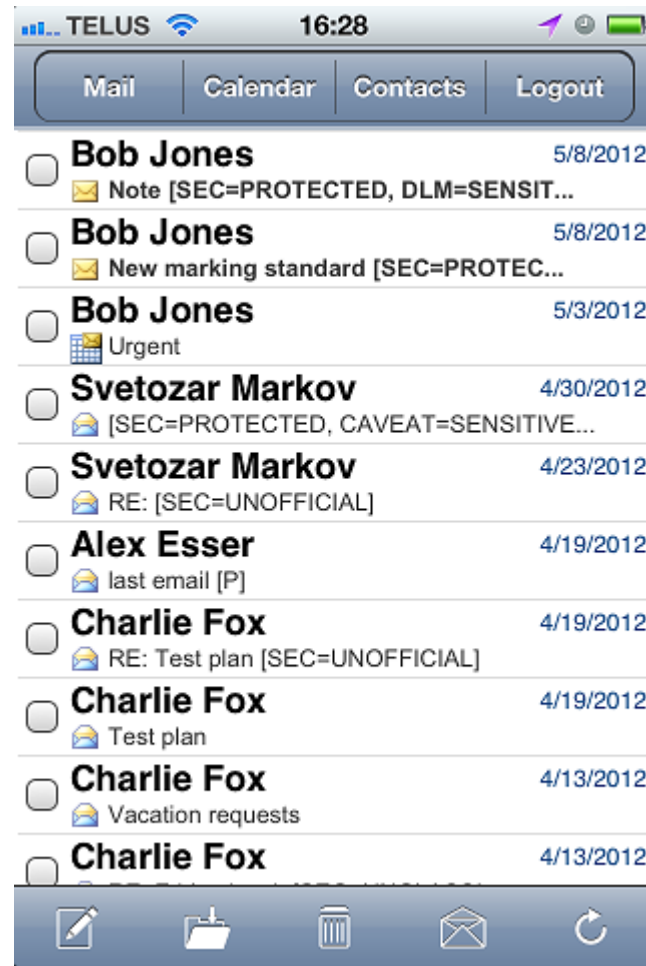
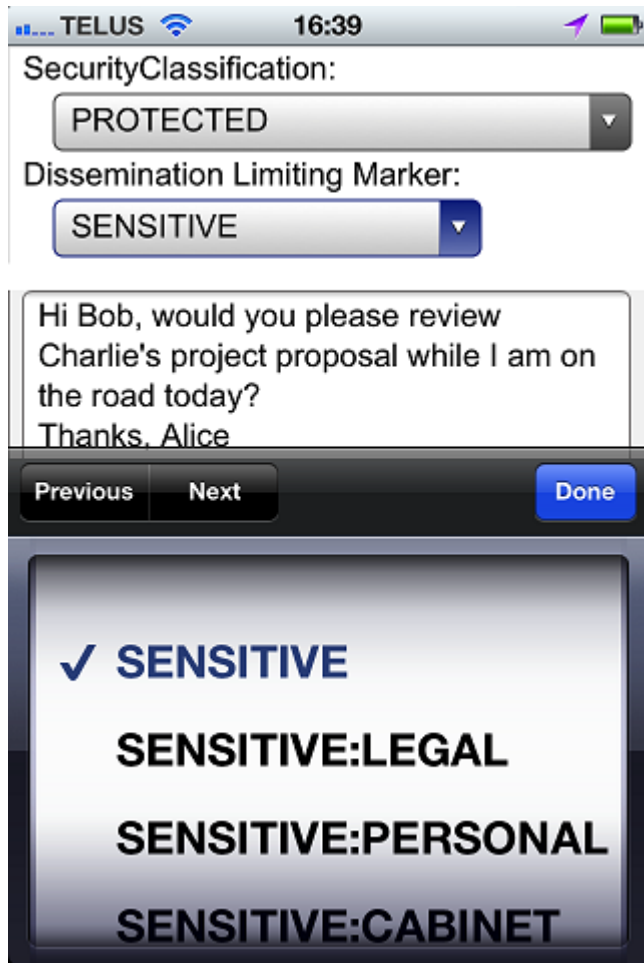


Classification for Mobile Users



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

NEW...iPhone





Funny Movie – Reply All Incident 😊

Movie Bellow