



FORCEPOINT

LGPD

COMO USAR A TECNOLOGIA ADEQUADA?

William Rodrigues
Senior Sales Engineer

A woman with long, dark, wavy hair is looking off to the side with a serious expression. She is wearing a light pink, textured blazer over a dark top. A small, colorful brooch is pinned to her lapel. The background is a blurred clothing store with racks of garments.

**PROTEJA SEU ATIVO MAIS VALIOSO
O PONTO HUMANO**

TECNOLOGIAS MUDAM



PESSOAS SÃO A CONSTANTE EM SEGURANÇA

Lei	Por Lei/Regulamentação
Geral	Amplo Alcance
Proteção	Privacidade
Dados	Dados Pessoais (PII)

O SISTEMA HUMAN POINT



Identificar dados pessoais em uma organização distribuída



Mapear, Gerenciar e Controlar o fluxo de dados pessoais



Detectar e responder de forma rápida à incidentes de dados



FORCEPOINT
Protecting the human point.

FORCEPOINT
Protecting the human point.

Protecting the human point.

GDPR Technology Mapping Guide

PERSONAL DATA INVENTORY

FORCEPOINT
Protecting the human point.

Protecting the human point.

GDPR Technology Mapping Guide

DATA FLOW MAPPING & CONTROL

FORCEPOINT
Protecting the human point.

Protecting the human point.

Solution Brief - Part 3

GDPR Technology Mapping Guide

DETECT & RESPOND TO A DATA INCIDENT



PRÉ-VAZAMENTO



PÓS-VAZAMENTO

Inventário de Dados Pessoais

Mapear, Gerenciar e Controlar Fluxo de Dados Pessoais

Responder à incidentes de dados de Forma Rápida

Tecnologias mapeadas para o LGPD

Data Loss Prevention/CASB

User & Entity Behavior Analytics (UEBA)

User Activity Monitoring

COMO A TECNOLOGIA PODE AJUDAR?

INVENTÁRIO DE DADOS PESSOAIS



DLP: Discover, Cloud, Endpoint

MAPEAR, GERENCIAR E CONTROLAR FLUXO DE DADOS PESSOAIS

Who	What	Where	How	Action
Human Resources	Source Code	Evernote	File Transfer	Confirm
Customer Service	Credit Card Data	Dropbox	Web	Block
Marketing	Personal Data	Business Partner	Instant Messaging	Notify
Finance	M&A Plans	Facebook	Peer-to-Peer	Remove
Accounting	Employee Salary	OneDrive	Email	Encrypt
Sales / Marketing	Financial Report	Malicious Server	Print	Quarantine
Legal	Customer Records	Removable Media	File Copy	Custom
Technical Support	Manufacturing Docs	Competitor	Print Screen	Audit
Engineering	Research	Customer	Copy/Paste	Notify



DLP: Network, Endpoint Web & Email Security modules

PREPARAR PARA REPORTAR EM TEMPO HÁBIL



Security Manager & Insider Threat Command Center

Inventário de Dados Pessoais

DLP

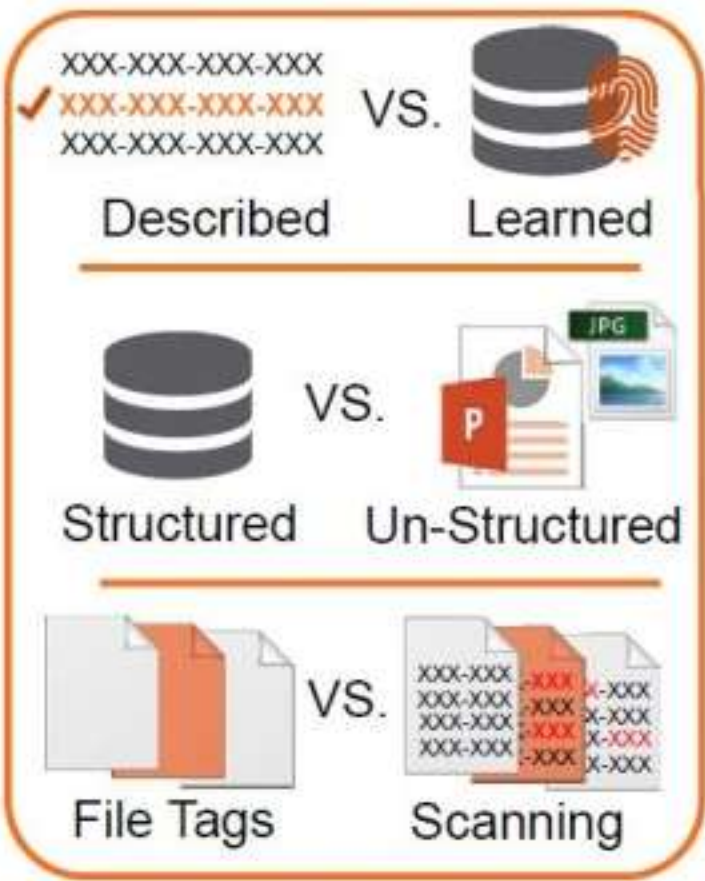
Entender a exposição da empresa ao LGPD

Entender a superfície de ataque da empresa

INVENTÁRIO DE DADOS PESSOAIS



OS DADOS ESTÃO EM TODO LUGAR



ESSES DADOS NÃO SÃO SIMPLES DE ACHAR



ALEM DE PERDIDOS, DADOS TAMBÉM PODEM SER ROUBADOS

PRODUTOS FORCEPOINT: DLP DISCOVER & DLP ENDPOINT

POLITICAS PRÉ-DEFINIDAS DE DADOS PESSOAIS

FORCEPOINT Security Manager WEB **DATA** EMAIL MOBILE admin | Log O

Role: Super Administrator **Deploy**

Main Manage Discovery Policies

Add Edit Delete Show Disabled Rules More Actions Refresh

Listed below are the policies in your organization.
Expand the tree to view a policy's rules and exceptions. Highlight a policy, rule or exception to see its details.
Click a button in the toolbar to add or edit a policy, or hover over the policy and select options from a pull-down menu.

2 Policies (enabled rules: 4, total rules: 4) Policy version: 138

- Confidential
- LGPD
 - CPF
 - RG
 - Nomes

Políticas PII

Description:

Rules (enabled: 1, total: 1)

- [Confidential](#)

Monitorar, Gerenciar & Controlar o Fluxo de Dados Pessoais

DLP + CASB

Garantir que dados pessoais sejam processados de acordo com as políticas de proteção de dados

Gerenciar o fluxo de dados pessoais para fornecedores e outros destinos aprovados

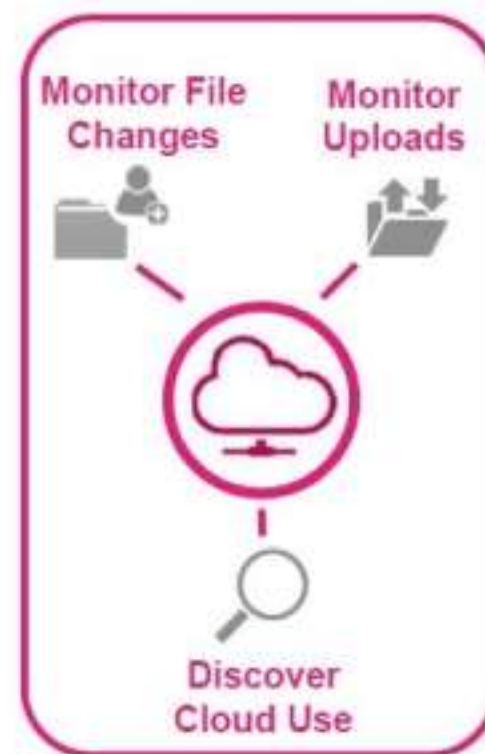
CONSIDERAÇÕES PARA MONITORAMENTO DE FLUXO DE DADOS



NETWORK
Data in Motion



ENDPOINT
Data in Use
& in Motion



CLOUD
Data In Use
& in Motion

PRODUTOS FORCEPOINT: DLP NETWORK, DLP ENDPOINT & DLP CLOUD, WEB SECURITY + CASB

MAPEANDO FLUXO DE DADOS

The screenshot displays the Forcepoint Triton APX interface. At the top, it shows the user name 'admin' and the role 'Super Administrator'. The main content area is titled 'DLP Data Incident Report' and shows a table of incidents. The table has columns for Incident ID, Incident Time, Source, Policy, Channel, Destination, Severity, Action, Transaction Size, and Status. A specific incident is highlighted in yellow, and its details are shown in a pane below. The details pane shows the incident ID '7667629', severity 'Medium', action 'Permitted', and channel 'Network email'. The message body is visible, showing a subject line 'Automatic Email Subject with <keyword>' and a body containing a URL. Annotations in green boxes point to specific parts of the interface: 'Origen' points to the Source column, 'Canal' points to the Channel column, 'Destino' points to the Destination column, 'Ação' points to the Action column, and 'Forense' points to the Message Body field in the details pane.

Incident ID	Incident Time	Source	Policy	Channel	Destination	Severity	Action	Transaction Size	Status
3.1	2016-11-24 20:44:20	Nathalia Doby	PCI, Finance Fraud...	Network email	brasil@admsistemas...	High	Permitted	27.3 KB	Done
3.1.1	2016-11-27 12:37:02	Nathalia White	Email to Comput...	Network email	alicia@admsistemas...	High	Quarantined	330.58 KB	Done
3.2.2	2016-11-09 10:43:42	Linda Jackson	Suspicious Mail In...	Network email	linda.jackson@77...	Medium	Quarantined	24.50 KB	Done
3.4	2016-11-24 11:58:44	10.0.140.102	Web-DLP Policy: P...	HTTP	www.fedex.com	High	Blocked	1.25 KB	Done
3.5	2016-11-23 17:41:02	10.0.140.102	SP Product Number	HTTP	software.com	Medium	Permitted	23.67 KB	Done
3.6	2016-11-20 16:58:21	10.0.140.102	Gartner Note 7 det...	FTP	29.41.2.67	Medium	Permitted	6.47 KB	Done
3.7	2016-11-08 12:04:08	10.0.151.31	Forbidden File	HTTP	19.41.2.72	High	Permitted	1.22 KB	Done
3.2	2016-12-22 16:54:15	Nathalia White	Information Leak...	Network email	nathalia@admsistemas...	Medium	Permitted	281.34 KB	Done
OneDrive	2016-11-08 11:32:50	rsal@admsistemas...	PCI, Credit Card	File Sync and Share...	rsal@admsistemas...	High	Risk Mitigated	460 B	Done
84%	2016-11-03 16:42:34	Linux1	PCI, Credit Card...	Enclined LAN	\\192.168.100.100\...	High	Blocked	54.3 KB	Done

Annotations:

- Origen: Points to the Source column in the incident table.
- Canal: Points to the Channel column in the incident table.
- Destino: Points to the Destination column in the incident table.
- Ação: Points to the Action column in the incident table.
- Forense: Points to the Message Body field in the incident details pane.

VISIBILIDADE SOBRE O USO DE CLOUD APPS NÃO HOMOLOGADAS

The screenshot displays the Forcepoint Triton APX interface, which is used for cloud application discovery and risk management. It is divided into several key sections:

- Applications Panel:** Shows a list of discovered cloud apps with columns for Risk Level and Cloud App name. Apps listed include Hub, Cloud Medical, Caspio, Easy Office, Autodesk, CoreTree, Art-On Software, Easy Office Phone, eFax, and WhatsApp.
- Cloud App Details:** Provides information for a specific app (Cloud Vertical), including its description, provider (Digital Hero Limited), location (Cantact, Ireland), domain, and service type (CloudFinance).
- Cloud App Risk:** A detailed view of security risks associated with the app, such as "Content cannot be shared with users who do not have accounts in the app" and "Users cannot track their own usage history".
- Cloud App Summary for eptrillio:** A horizontal bar chart titled "Top 10 Cloud Apps Used by eptrillio". The x-axis represents the number of requests, ranging from 0 to 170. The apps and their approximate request counts are: Easy Office Phone (~165), Cloud Aspects (~100), ServCorp (~45), FreshBooks (~45), Clicksor (~45), AdDataExpress (~45), eFax (~45), CoreTree (~45), CobWeb (~45), and Cloud Vertical (~45).
- User Summary Report for Dremus:** A vertical bar chart titled "Top 10 Users of Dremus". The y-axis represents the number of requests, ranging from 0 to 200. The users and their approximate request counts are: adgman (~195), 10.203.145.19 (~100), Manoj (~45), and reportUser (~45).

Identifies usage of cloud apps that can represent risk to an enterprise

Reportar um Incidente de Dados

DLP + UEBA + UAM

Entender e aprender com a exposição da empresa ao LGPD

INVESTIGANDO UM CASO DE VAZAMENTO DE DADOS



UTILIZE ANALÍTICOS DE SEGURANÇA E DE SCORING DE RISCO PARA PRIORIZAÇÃO DO PROCESSO DE RESPOSTA



REVISE RESULTADOS HISÓRICOS DE INVENTÁRIO DE DADOS PESSOAIS



Who	What	Where	How	Action
Security Operations	Security Alerts	Security	Web Monitor	Quarantine
Customer Service	Credit Card Data	Employee	Web	Block
Marketing	Personal Data	Business Partner	Instant Message IM	Notify
Finance	MLA Plans	Facebook	Post to Post	Remove
Accounting	Employee Salary	Website	Email	Encrypt
HR - Payroll	Financial Report	Malicious Email	Print	Quarantine
Legal	Employee Records	Employee Email	Print	Quarantine
Business Support	Marketing Data	Competitor	Print Screen	Audit
Engineering	Network	Customer	Print Screen	Notify

REVISE INCIDENTES PARA ADEQUAR POLITICAS DE VIOLAÇÃO DE FLUXO DE DADOS

PRODUTOS FORCEPOINT : SECURITY MANAGER, INSIDER THREAT COMMAND CENTER, UEBA CONSOLE

EXAMPLOS DE RELATÓRIOS QUE AUXILIAM NA INVESTIGAÇÃO

Identifique os casos de incidents de dados de alto risco

Identifique usuários de alto risco & contexto

User	Position	Title	Department	Manager	High	Medium	Low	Total
James Brown	Product Engineer	Product Engineer	Product	James Brown	High	Medium	Low	High
Jane Smith	Product Engineer	Product Engineer	Product	Jane Smith	High	Medium	Low	High
John Doe	Product Engineer	Product Engineer	Product	John Doe	High	Medium	Low	High
Jane Smith	Product Engineer	Product Engineer	Product	Jane Smith	High	Medium	Low	High
John Doe	Product Engineer	Product Engineer	Product	John Doe	High	Medium	Low	High
Jane Smith	Product Engineer	Product Engineer	Product	Jane Smith	High	Medium	Low	High
John Doe	Product Engineer	Product Engineer	Product	John Doe	High	Medium	Low	High
Jane Smith	Product Engineer	Product Engineer	Product	Jane Smith	High	Medium	Low	High
John Doe	Product Engineer	Product Engineer	Product	John Doe	High	Medium	Low	High
Jane Smith	Product Engineer	Product Engineer	Product	Jane Smith	High	Medium	Low	High
John Doe	Product Engineer	Product Engineer	Product	John Doe	High	Medium	Low	High
Jane Smith	Product Engineer	Product Engineer	Product	Jane Smith	High	Medium	Low	High
John Doe	Product Engineer	Product Engineer	Product	John Doe	High	Medium	Low	High
Jane Smith	Product Engineer	Product Engineer	Product	Jane Smith	High	Medium	Low	High
John Doe	Product Engineer	Product Engineer	Product	John Doe	High	Medium	Low	High
Jane Smith	Product Engineer	Product Engineer	Product	Jane Smith	High	Medium	Low	High
John Doe	Product Engineer	Product Engineer	Product	John Doe	High	Medium	Low	High
Jane Smith	Product Engineer	Product Engineer	Product	Jane Smith	High	Medium	Low	High
John Doe	Product Engineer	Product Engineer	Product	John Doe	High	Medium	Low	High
Jane Smith	Product Engineer	Product Engineer	Product	Jane Smith	High	Medium	Low	High
John Doe	Product Engineer	Product Engineer	Product	John Doe	High	Medium	Low	High

IRR utiliza Machine Learning e Analíticos de Segurança para agrupar incidentes em casos

Incidents by Severity

Incidents by Action

INVESTIGANDO UM INCIDENTE DE VAZAMENTO DE DADOS

**Workflow - DPO
Remediação
Escalar Incidente**

Incid...	ID	Incident Time	Source	Policies	Channel	Destinations	Severity	Action	Transaction Size	Status
1.1	5099195	2018-11-14 20:44:26	Nathalie Derby	PCI; Peoples Repu...	Network email	barackadana@yahoo...	High	Permitted	17.5 KB	New
1.2.1	7605210	2018-11-17 12:37:02	Barbara White	Email to Competit...	Network email	adriola@ediliza-p...	High	Quarantined	330.66 KB	New
1.2.2	3440707	2018-11-09 18:45:42	Linda Jackson	Suspected Mail to...	Network email	linda.jackson1976...	Medium	Quarantined	14.95 KB	New
1.4	5846287	2018-11-14 11:36:44	10.0.140.183	Web DLP Policy; R...	HTTP	www.fishrepper.com	High	Blocked	1.15 KB	New
1.5	3683221	2018-11-13 17:01:30	10.0.140.183	3M Product Number	HTTPS	safeflowing.goss...	Medium	Permitted	13.97 KB	New
1.6	3679239	2018-11-10 16:56:21	10.0.140.183	Golser Note 7 doc...	FTP	10.11.2.67	Medium	Permitted	8.47 MB	New
1.7	7098214	2018-11-10 12:16:28	10.0.151.51	Password files	HTTP	10.11.2.72	High	Permitted	1.13 KB	New
1.8	7667628	2018-12-02 16:34:15	Barbara White	Information Gover...	Network email	knrdsm@pacch201...	Medium	Permitted	283.84 KB	New
OneDrive	3275851	2018-11-06 11:32:06	(cloud) forcecloud...	PCI; Credit Cards	File Sync and Sharing	forcecloud-vr.sha...	High	File deleted	400 B	New
8MS	3211253	2018-11-03 19:12:34	QAT	PCI; Credit Cards...	Endpoint LAN	V1310.20.80\VOL09B_1	High	Blocked	34.5 KB	New

Origem (Source) → **Canal** (Channel) → **Destino** (Destination) → **Ação** (Action)

Forense (Forensics)

Incident: 7667628 | Severity: Medium | Action: Permitted | Channel: Network email

Rule: 3G Toolkit: DOB and Name

- Date of Birth near UK Names

Forensics: Properties History

From: Barbara White | Sent: 20 Jan, 2017, 1:02:40 AM

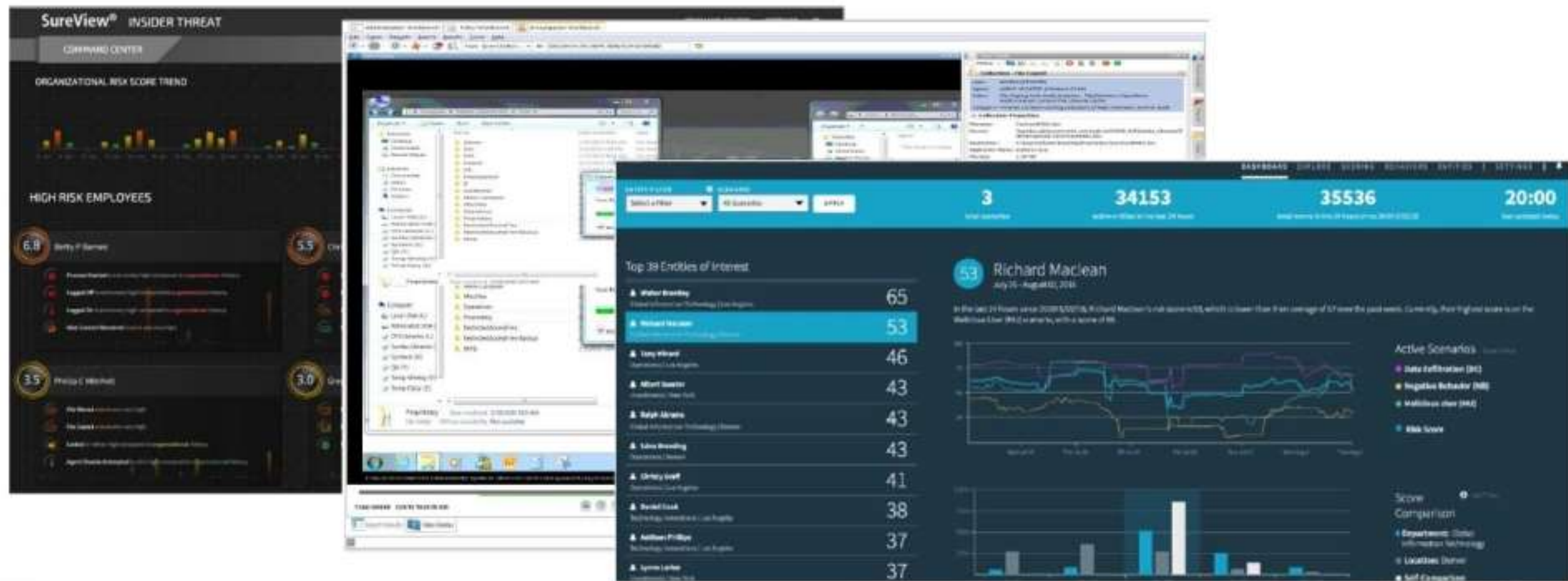
To: isellen@pacch2018.vrtm

Subject: Automatic Email Subject with <keyword>

Attachments: copora_reflow_with_con_sate_newdownwar_cvt31_clocR&@262.88 KB

0 Message Body

NOTIFICAÇÃO DE VAZAMENTO DE DADOS – SCORE DE RISCO PARA COMPORTAMENTO DE USUÁRIOS & INVESTIGAÇÃO COM FORCEPOINT INSIDER THREAT E FORCEPOINT UEBA





DEMO

PERGUNTAS?

The background of the slide features a complex network of green dots connected by thin lines, creating a mesh-like structure that resembles a molecular or digital network. The dots and lines are more prominent in the lower half of the image and fade into the dark background towards the top.



WILLIAM RODRIGUES
Senior Sales Engineer
wrodrigues@forcepoint.com

OBRIGADO

WWW.FORCEPOINT.COM

FORCEPOINTBLOG.COM.BR

