



RSA Data Loss Prevention (DLP)

Understand business risk and mitigate it effectively

Aris Zikopoulos, Channel Manager ITWAY HELLAS



Definition of DLP

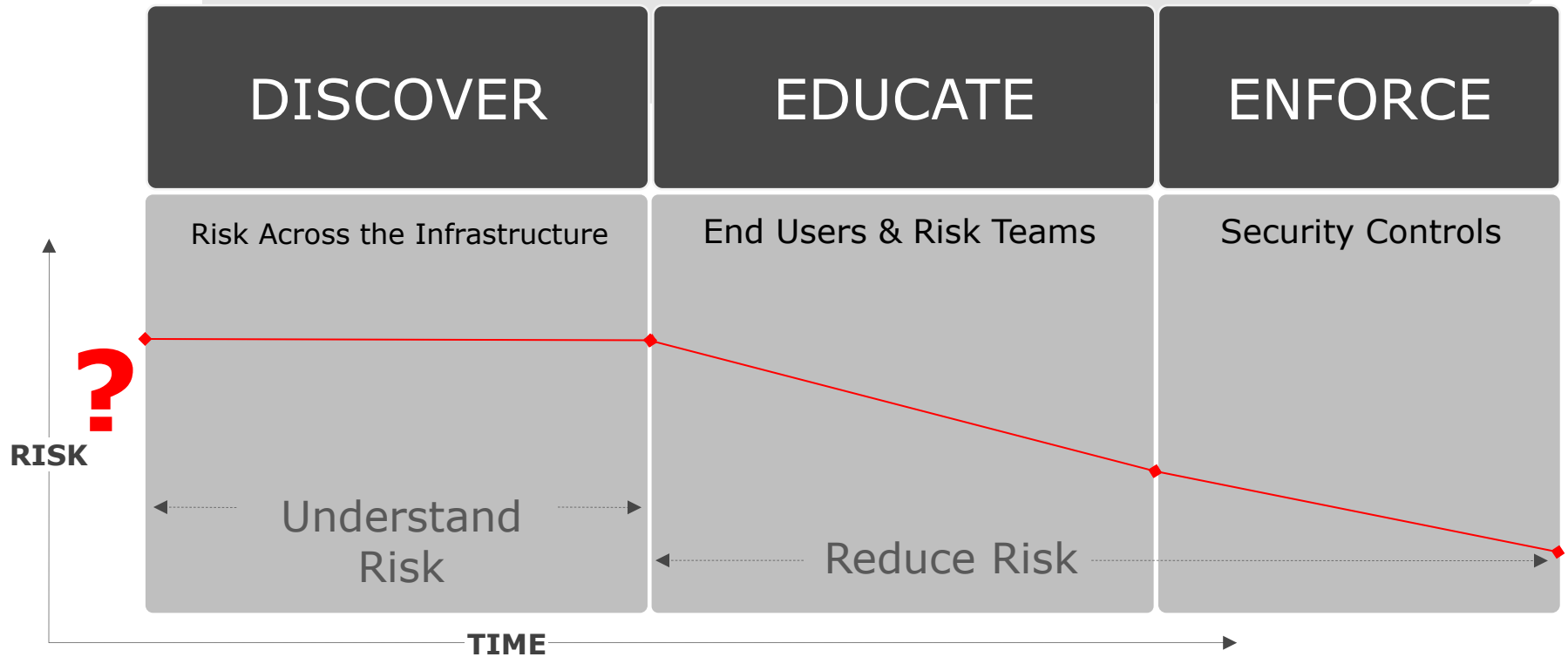
“DLP is a **technology** that helped us
build a **process** to protect our
people from leaking sensitive data”

-CISO, Healthcare Company

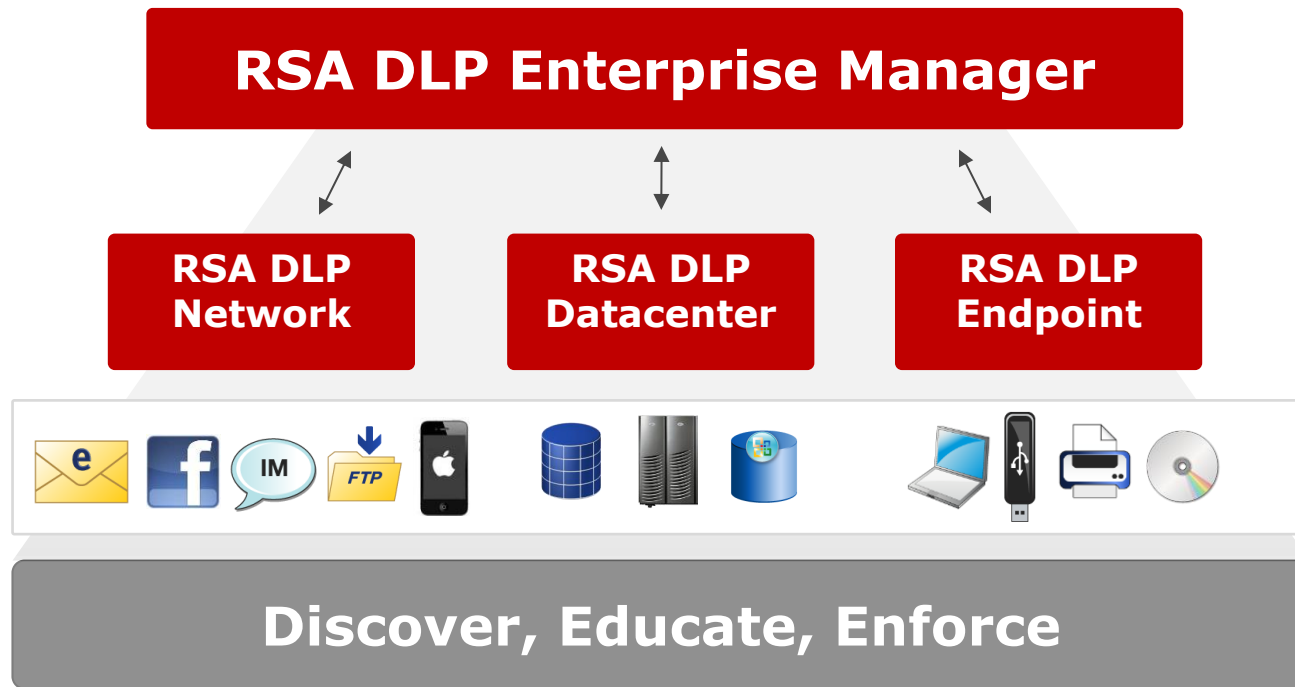
RSA subscribes to this philosophy and encourages customers to focus on people and process and to take a risk based approach in building DLP projects

Establishing a Risk Based DLP Program

DLP Program Lifecycle Management (driven by risk based policies)



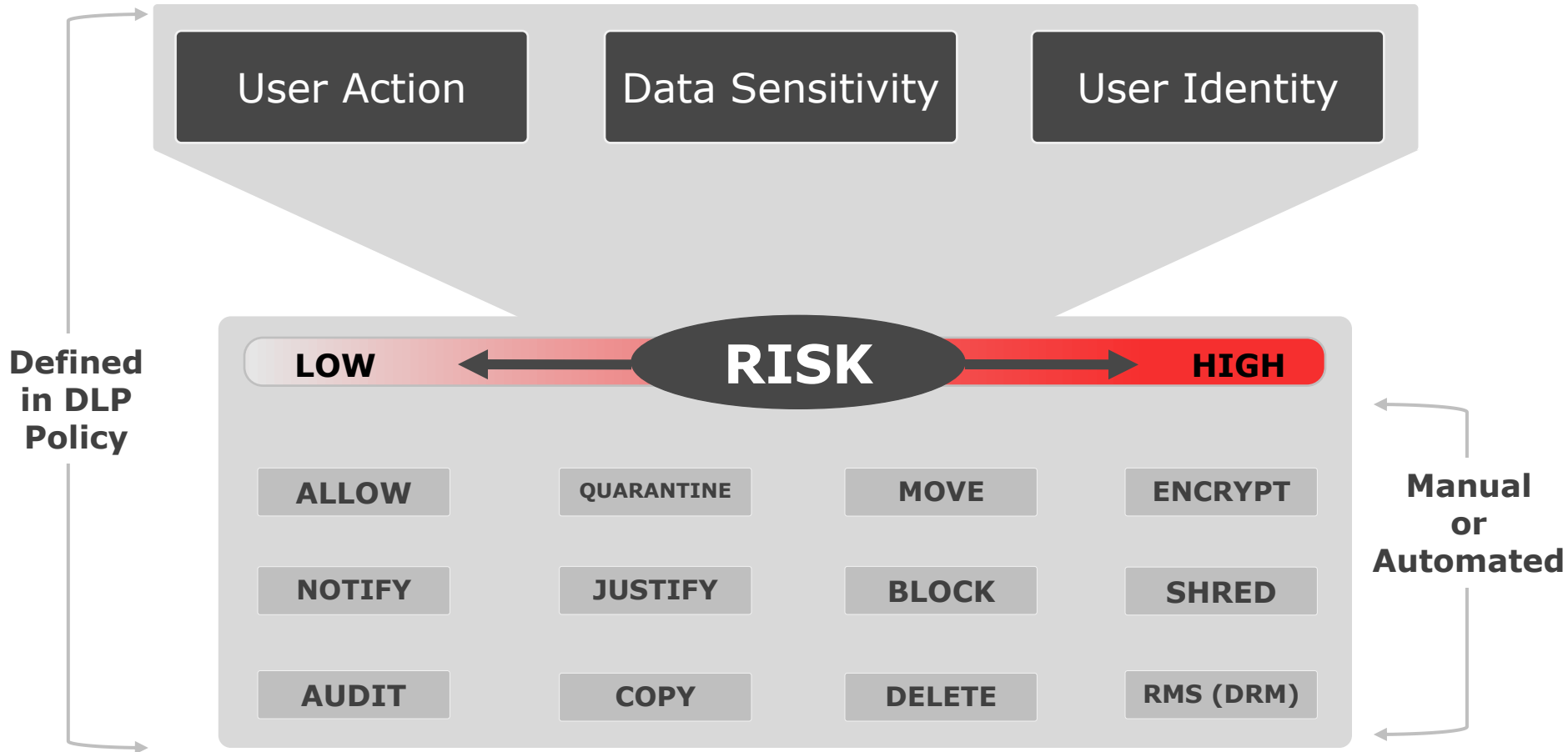
DLP Covers Your Entire Infrastructure



Consistent Classification & Management Across the Board

Risk Based Policy Management

Enforce security controls based on the risk of a violation



bjameson,

!!!! Important !!!! Please read this message carefully and follow the instructions.

An email (or an attachment) that you have attempted to send outside the company may contain sensitive information. The RSA DLP system has automatically blocked the email from being sent.

The email possibly violates the following corporate policies:

- PCI-DSS (Payment Card Industry Data Security Standard)
- California AB-1298

Please review the contents of your email and determine if you still want it to be sent or not:

From: Barbara Jameson
To: patrickCaselton@yahoo.com
Attachments:
Subject: requested info

Hi Patrick,
Here is the information that you requested.

Debbie Brown SSN# 555-44-3333
Credit Card #: 41124940022225
Let me know if you need anything else.

Regards,
Barbara

Please choose one of the following actions:

- Release (the email will be sent)
- Discard (email will *not* be sent)

If you have any questions please contact: petesmith@acme.com

Done

Endpoint Enforce Alert – RSA Data Loss Prevention



Corporate policy analysis

-警告- 您的行動可能違反了公司政策。請輸入行動的理由。

業務需要



---- Select a justification ----

- 業務需要
- 管理部門的要求

業務需要

Must be at least 5 characters

Continue

Cancel

In-Depth Data Analysis Framework

The image shows a screenshot of an email client interface on the left and an Adobe Reader window on the right. The email client shows a message with the subject "Prescription information for patient ID 06135443" and an attachment "Prescription Info.pdf (21 KB)". The email body contains the following text:

Hi Alice,
Please fax the following **prescription** information to

FEXOFENADINE (ALLEGRA) 180 MG Tablet
Dosage: Take 1 Tab by mouth daily.
Prescribed by Joseph A Keeney, MD on 05/03/2011

Please make sure that the information is provided to

Thanks,
Bob

The Adobe Reader window shows the content of the attached PDF, which includes:

FEXOFENADINE (ALLEGRA) 180 MG TABLET
Dosage: Take 1 Tab By Mouth Daily.
Prescribed by Joseph A. Keeney, MD on 06/03/2011

Patient Name: Roger McMillan
SSN: 603-01-1313

Primary Provider: Blue Cross Blue Shield CA
Patient ID: 06135443
Clinic: Stanford Hospital
Address: 177 Bovet Road, San Mateo, CA 94401
Home Phone: 650-528-1620
Credit Card Number: 4378999917456111 e

Red boxes in the email client highlight the recipient list (asmith@acme.com, bob@gmail.com), the subject line, the attachment name, and the word "prescription". In the Adobe Reader window, red boxes highlight the patient name, SSN, patient ID, and credit card number.

Attributes & Identity Analysis

- Email header data
- Attachment type, size, etc.

Content in Email body & Attachment

- General keywords
- Specialized keywords
- Patterns and strings
- Proximity analysis
- "negative" rules

RSA DLP Policy Library & Methodology

170+ built-in policies you can use

Retail

- PCI DSS
- MA CMR 201
- CA AB 1298

Healthcare

- HIPAA
- Caldicott (UK)
- PIPEDA

Telecom/Tech

- CPNI
- Source Code
- Design Docs

Manufacturing

- ITAR
- Patent Apps
- EAR

Financial Serv

- GLBA
- FCRA
- NASD

Other

- NERC
- Global PII
- 401k & 403b

Knowledge Engineering



Sample Profile
of a Knowledge
Engineer

Work Exp: 12 years

Certifications: 18 regulations

Languages : Four

Background: Linguistics,
artificial
intelligence, search
technologies

Education: Library sciences,
Computer science

Dedicated Knowledge Engineering team develops and maintains DLP policies

RSA DLP for Virtualized Environments

Virtualized Servers

- Run RSA DLP management software on virtual machines
- Deploy RSA DLP Network hardware as virtual appliances
- Leverage virtual servers for RSA DLP grid scanning

Virtualized Desktops

- Use RSA DLP Endpoint agent on virtual desktops
- Both Citrix XenDesktop and VMware View are supported
- Scan "Home Drives" without interfering with the desktop

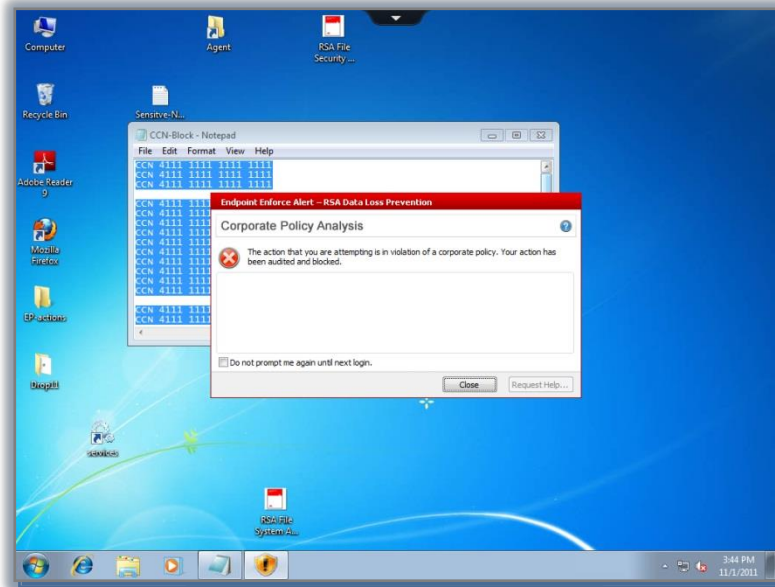
Strategic partnership with major virtualization vendors



DLP for Virtual Desktops & Applications

New Threat Vectors Covered:

- 1) Copying sensitive data from virtual apps & VDI to physical device
- 2) Saving files from virtual apps & VDI to physical device



Key Benefits:

- No agent on endpoints
- Freedom & flexibility to BYOD



Providing Content-Awareness to GRC and SOC

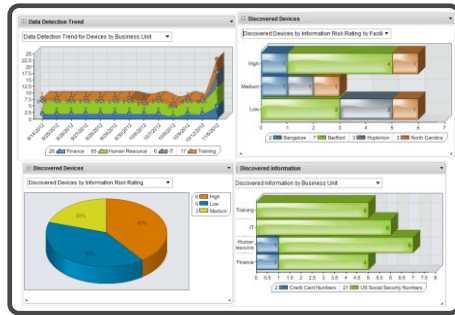
Proactive information risk management & content-aware security analytics



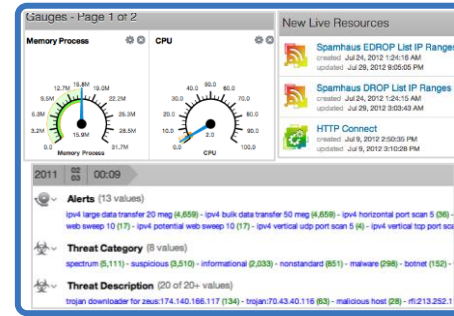
Risk Officer



Business users



RSA Archer
Information Risk Management



RSA Security Analytics
Content-level Intelligence



Security Analyst

RSA Data Discovery



SharePoint



File Servers



Databases



NAS/SAN



Endpoints



Thank You



The Security Division of EMC