

# **RSA**Conference2016

San Francisco | February 29 – March 4 | Moscone Center

SESSION ID: CRWD-R12

## **The Gamification of Data Loss Prevention**



Connect **to**  
Protect



#RSAC

**Mark Stevens**

SVP, Global Services



**DIGITAL GUARDIAN**

[www.digitalguardian.com](http://www.digitalguardian.com)

# Topics We'll Discuss



- Overview of Gamification
- Overview of Data Loss Prevention or DLP
- A Relationship that Needs Mending
  - The IT Security Professional & The “End User”
- How to Gamify DLP
- Introducing DG Data Defenders
- Game Demonstration
- How to Make it Happen at Your Organization

# What Is Gamification?



#RSAC

“Gamification is the process of engaging people and changing behavior using game mechanics in a non-game context. It’s taking what’s fun about games and **applying it to situations that maybe aren’t so fun.**”

Gabe Zichermann

# Could Anything Be Less Fun Than...



#RSAC

# DLP

# Why Gamification Is On The Rise



#RSAC

- **It works.** Gamification has proven to be very successful in engaging people and motivating them to change behaviors, develop skills, or solve problems.
- **It's easy to be effective.** Those who use gamification in employee motivation and engagement realize that even a simplistic reward approach (i.e. leaderboards and badges) lead to significant improvements in employee engagement.



## Deloitte.

- Since the integration of gamification in to Deloitte Leadership Academy, there has been a **37 percent increase** in the number of users returning to the site each week.

## OPEN TEXT

The Content Experts™

- OpenText made it possible for their IT team to earn points and badges by sharing information, contributing to discussions, completing assignments and passing tests and the level of active **IT participation was well above 60%** which is significantly higher than the current average in the rest of the company.

# What is DLP?



- Data Loss Prevention is a software solution designed to prevent potential data breach/data ex-filtration by monitoring, detecting and ensure proper sensitive data handling while **in-use** (endpoint actions), **in-motion** (network transmission), and **at-rest** (data storage).
- When poor sensitive data handling is observed, DLP solutions employ data protection controls ranging from log to justify to block and alert **USERS** of their potential and/or past violations.



# USER

{noun} (you-sir)

A word IT Security Professionals use  
when they mean "idiot".



# Typical Security Professionals Interaction With ~~Idiots~~ Users



#RSAC



# Why We MUST Change This Dynamic



#RSAC

- It could take up to 20 years to address the cyber-security skills gap with the worldwide shortage of information security professionals at 1 million openings. *(Source: Cisco 2014 Annual Security Report)*
- 34.5% of security leaders reported significant obstacles in implementing desired security projects due to lack of staff expertise. *(Source: 451 Research)*
- Only 24% of enterprises have 24x7 monitoring in place using internal resources. *(Source: 451 Research)*
- The demand for information security professionals is expected to grow by 53 percent through 2018. *(Source: Bureau of Labor Statistics)*



# BUILD YOUR DATA PROTECTION ARMY

# The Gamification of DLP Can Help!



- If you have, or are considering, DLP software you will have everything you need!
- You can gamify your data protection program by leveraging these core DLP features:
  - Policies/Rules
  - User Prompts
  - Reporting
  - E-mail Alerts



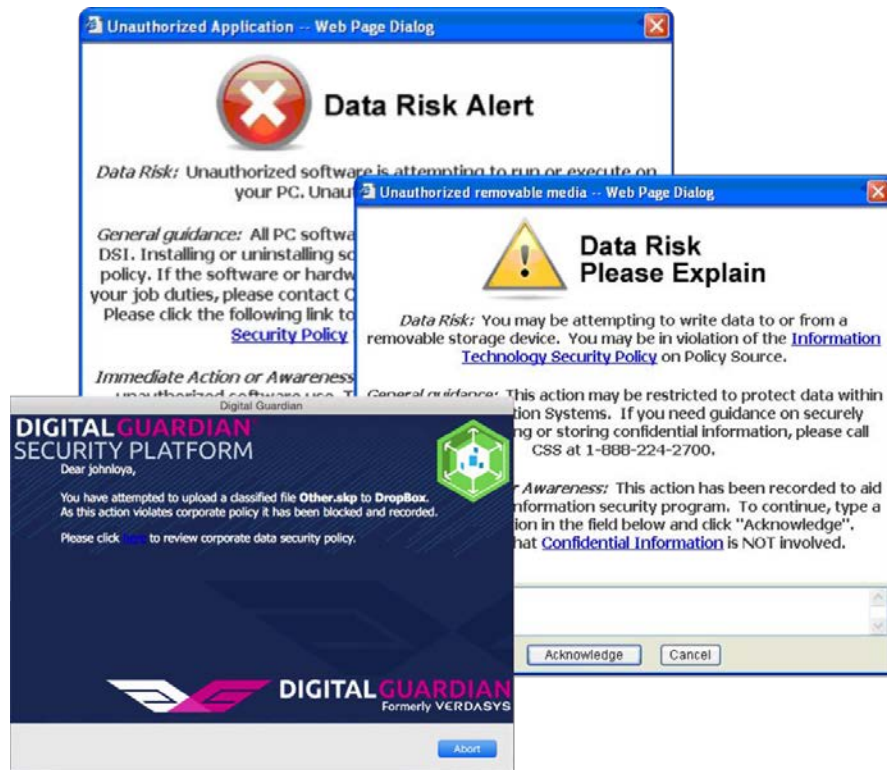
- Set the ground rules for how your employees interact with sensitive data.
- In your DLP system, policies may be packages that contain sets of conditions, which are made up of transport rules, actions, and exceptions that you create in your DLP Management Console and then activate to inspect employee interactions with sensitive data.
- Examples:
  - An employee may not e-mail unencrypted social security numbers.
  - An employee cannot screenshot an R&D file coming from a specified secure data store.

# User Prompts



#RSAC

- A “pop-up” dialogue that allows you to inform employees that they may be about to violate one of your data protection policies.
- Current DLP programs use the “security hand slap” approach, Gamified prompts should take a more positive spin.







- Most DLP solutions have the ability to create custom reports. Typically they are designed to highlight the real or potential “bad stuff,” with our Game we want to highlight the “good stuff” (i.e. compliant behavior that improves data protection).

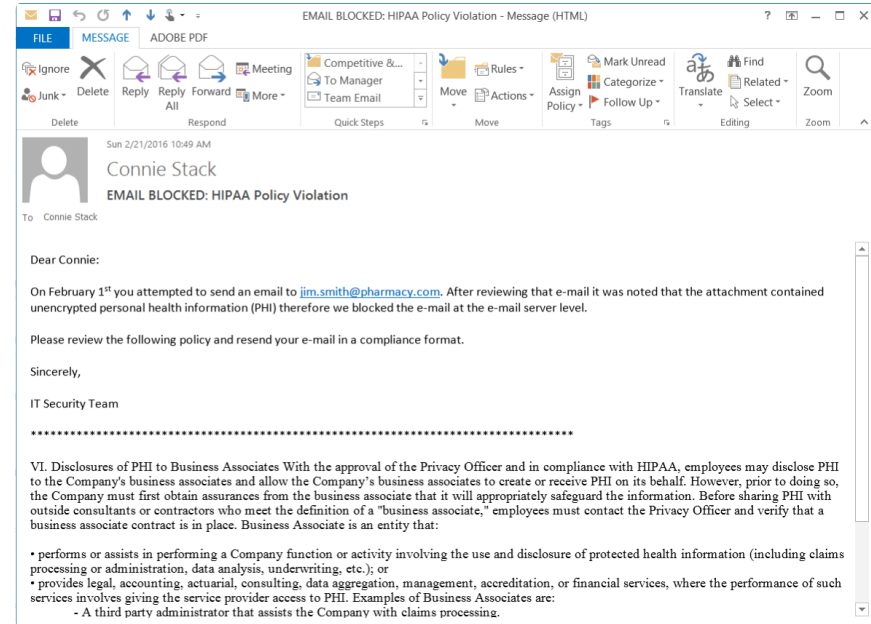


# E-Mail Alerts



#RSAC

- Most DLP solutions have the ability to create e-mail alerts to security team members, managers and/or supervisors.
- Typically they are designed to report policy violations for further investigation, applying gamification requires we highlight compliant behavior that improves data protection as well.





# Key DLP Players...

Gartner

2016 Gartner Magic Quadrant for Enterprise Data Loss Prevention  
Released January 2016



#RSAC



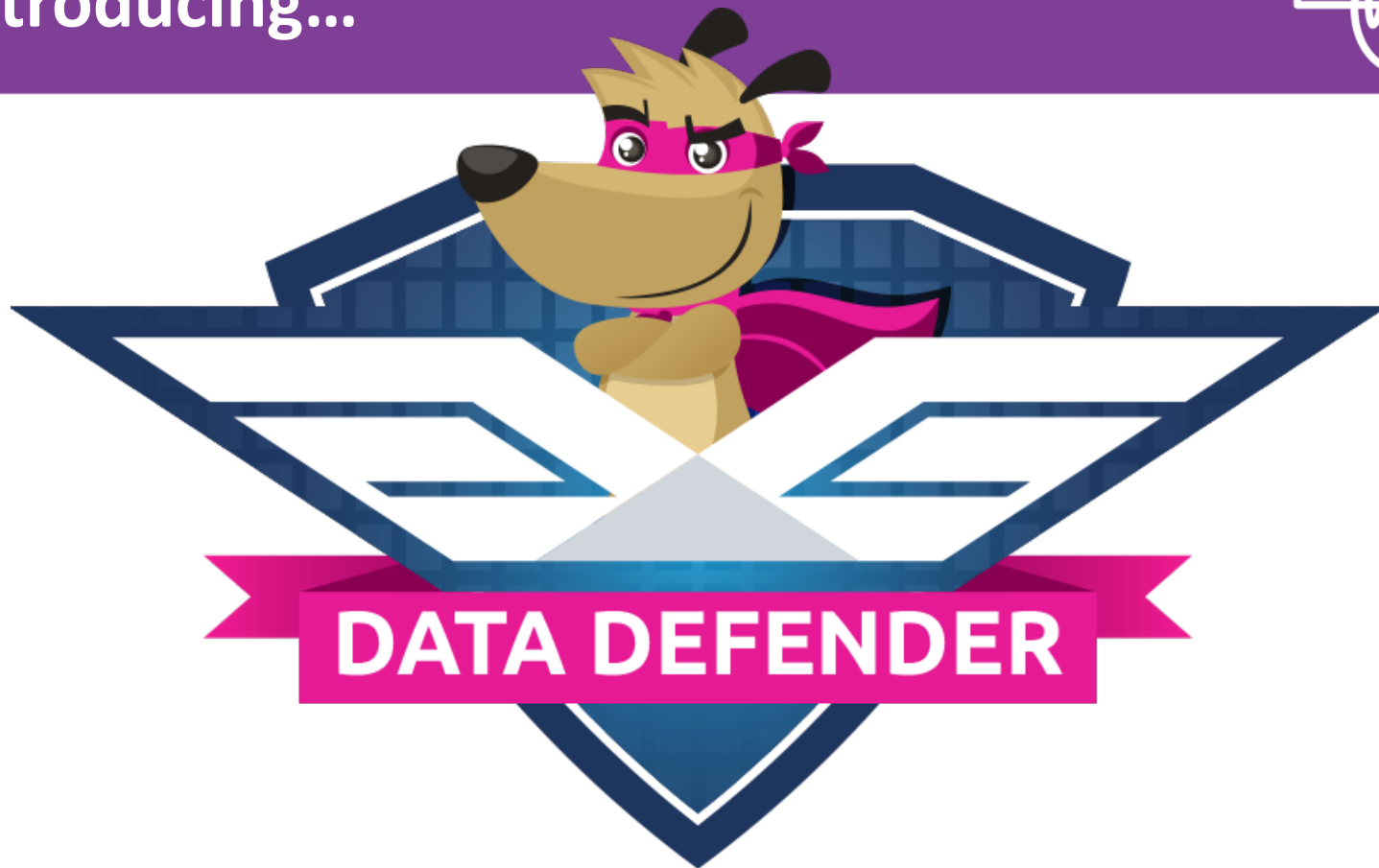
All the 2016 Gartner Enterprise DLP MQ Leaders offer the core features required to replicate our DLP Game, including:

- Policies/Rules
- User Prompts
- Reporting
- E-mail Alerts

# Introducing...



#RSAC



# Objectives of DG Data Defender



#RSAC

1. Address the lack of awareness and individual employee accountability regarding data loss prevention and ultimately change long term behavior.
2. Establish a new data protection “language” and encourage open dialogue when talking about data loss prevention.
3. Engage end users. Data loss prevention is seen as a dry topic, so we’ll establish dynamic, fun and engaging user communications about their positive user behaviors.
4. Measure it’s effectiveness at reducing real data risk.

# Overall Game Premise



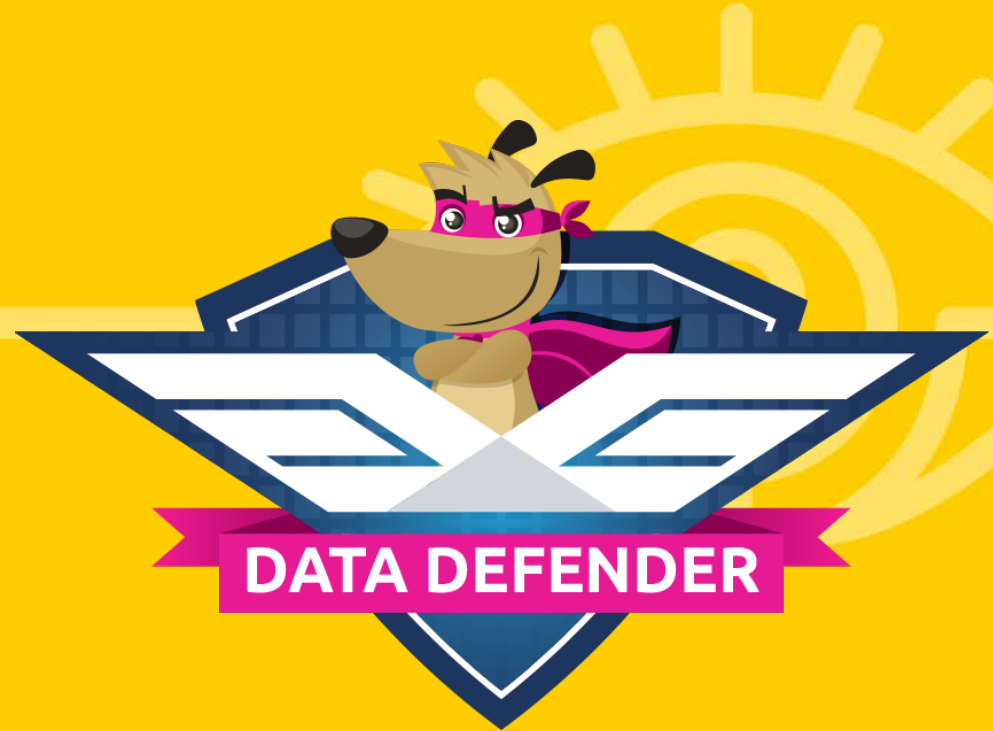
#RSAC

- **Make Users Aware.** Encourage every employee to make good sensitive data handling decisions and follow published data protection policies.
- **Get them Engaged.** Encourage users to display their badges in their workspace (i.e. print them and post in their cube), in e-mail signatures, etc. and engage managers to recognize the good behavior by publishing a monthly Data Defender Leaderboard.
- **Reward Good Behavior.** Provide users the opportunity to earn a series of badges to acknowledge their data protection accomplishment(s) and offer modest prizes once key data protection milestones are met (*done outside DLP platform*).



## Badges & Policies

The Keys To Making DLP Fun



# Baby Data Defender Badge



#RSAC



- Serves as a 'welcome to the data protection game' message and provides the users first badge.
- "Awarded" at first e-mail deployed without triggering a policy violation.
- User Prompt will include the badge image and the printable PDF version of the badge will be automatically emailed from the DLP system to the end user (*ideally to be displayed in their workspace*).

# Secure Sender Badge



#RSAC



- Awarded at the 10<sup>th</sup> e-mail sent without triggering a policy violation.
- Keeps the user engaged as they will likely get two badges on the first day they join the game.

# Cloud Data Protector Badge



#RSAC



- Awarded at the 1<sup>st</sup> use of corporately approved Cloud Storage Engine like Azure, Box or Citrix.





- Awarded at the 100<sup>th</sup> e-mail sent without triggering a policy violation.
- Keeps the user engaged as they will likely get a third badge within a week.



- Awarded at the 1st use of corporately approved, encryption-enabled, external storage device.

# General Data Defender Badge



#RSAC



- Awarded at the 500<sup>th</sup> e-mail sent without triggering a policy violation.
- The number of “clean” e-mails sent can vary, we chose 500<sup>th</sup> so the user prompts did not become too interruptive.

# King's Guard of the Crown Jewels



#RSAC



- Awarded at the 1st use of data obtained from a secure shared drive and correctly stored back on the secure shared drive.
- Particularly useful for departments that regularly handle regulated data (i.e. PII, PHI and PCI) and intellectual property (i.e. trade secrets).



- Awarded upon clean data scan whereby no sensitive data is stored locally on the endpoint.
- Enforces the need to follow good data at rest procedures (i.e. SSN's, credit card data, etc. should never be stored locally on an endpoint).

# Squeaky Clean Badge



#RSAC



- Awarded upon clean system scan where no unapproved applications are present the endpoint.
- Enforces the idea that unapproved applications can be dangerous. A lot of malware infections happen via downloaded web applications (i.e. waterhole attacks) and should be avoided.

# Super Secure Sender Badge



#RSAC

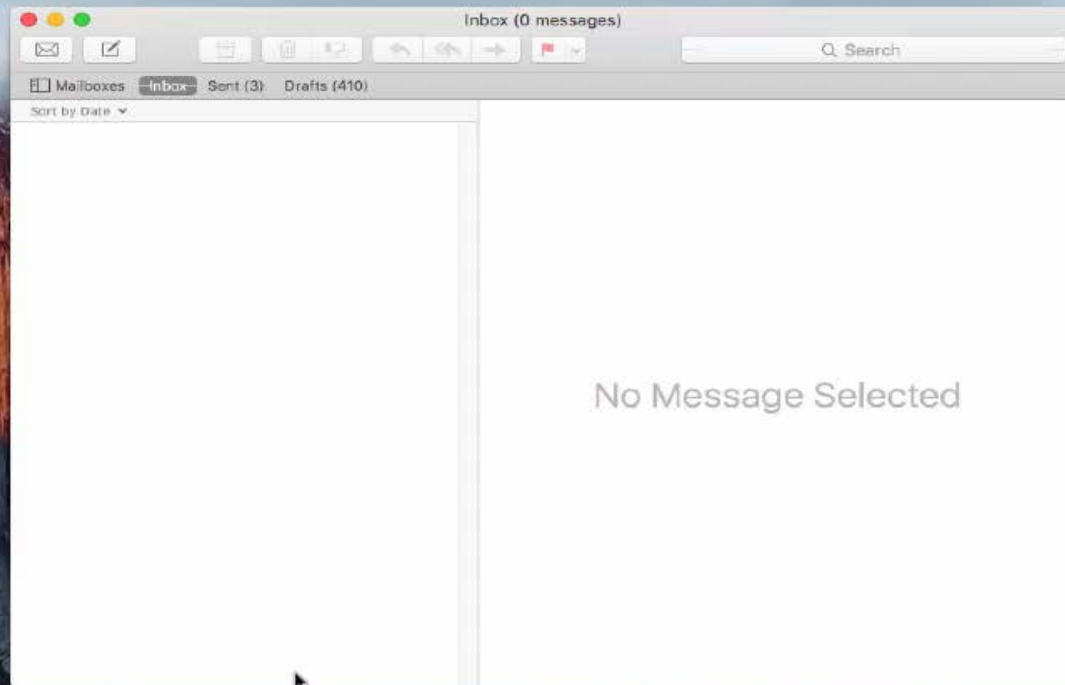


- Awarded at the 1,000<sup>th</sup> e-mail sent without triggering a policy violation.
- Users will be most active in the game through e-mail. Select levels of clean e-mail send badges that are most suited to your organization.



- **Keep It Simple! *Simple Works!***
- Build a leaderboard report in your DLP solution and publish it out to your organization on a regular basis:
  - Display on a monitor in common spaces (*if available*).
  - Send via e-mail.
- Work with HR to offer modest prizes for top performers (i.e. those who accumulate the most badges in a fixed time period):
  - Make them digital for ease of distribution (i.e. digital gift cards that appeal to many tastes – Amazon, iTunes, Netflix, Fandango, etc.)

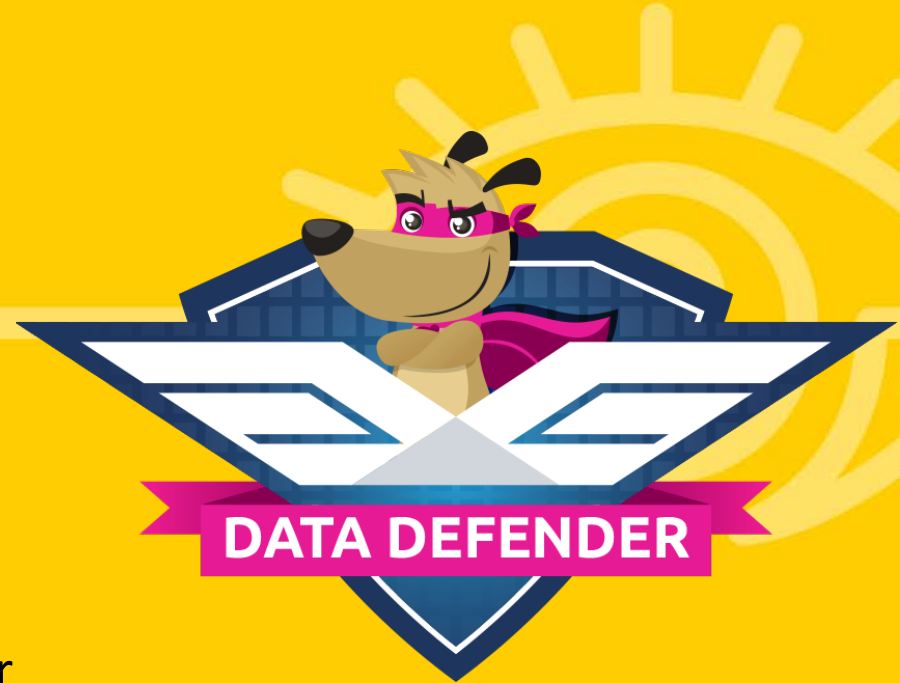






## Gamified DLP *In Action!*

- Justin Bortnick, Sr. Sales Engineer  
Digital Guardian



# Make It Happen At Your Organization



#RSAC

If you currently own and operate a DLP solution from Digital Guardian, Symantec, Intel Security, ForcePoint, etc.:

1. **Policies/Rules:** Start to define your gamified data protection policies that will enforce and reward the actions you want users to take in a positive, non-finger wagging, way. Load policies in your DLP system.
2. **User Prompts:** work with a designer to develop some fun badges that can be presented when the users treat sensitive data in the appropriate way (or just use the ones we developed – I'll share). Upload to your DLP system.
3. **Reporting:** create a dashboard in your DLP management console that can be viewed by the security team and shared with managers and participating users.
4. **E-mail Alerts:** write the copy for the various e-mails to be deployed to users with the badge/certificates attached as PDF's for display in their workspace.
5. **Announce & Promote the Game:** use e-mail, develop posters to display in common areas, etc. and include the prizes that can be earned once you earn a certain level of badges (if you decide to incorporate them).

# Make It Happen At Your Organization



#RSAC

**If you DO NOT currently own and operate a DLP solution from Digital Guardian, Symantec, Intel Security, ForcePoint, etc.:**

1. Consider purchasing and implementing one! 😊



# Thank You!

## Questions & Answers

- Contact Me:  
Mark Stevens, SVP, Global Services  
[mstevens@digitalguardian.com](mailto:mstevens@digitalguardian.com)

