



# 內外兼顧，企業資料保護的雙牌

iSecurity Jason / 數位資安 賴銘俊

Date : 2018/03

Confidential

© DIGITAL GUARDIAN INC.

Target: Breach impacted 70 million people

Home Depot Hacked!

USIS security breach undetected for months!

中央社

遠東銀電腦遭植病毒 客戶個資無外洩



中央社



2017/10/06 20:18

# 駭客入侵美俄18家銀行轉帳網路 盜領ATM得手近千萬美元

2017-12-12 發表

Group-IB的研究人員指出代號Money Taker的駭客團體在過去一年入侵至少18家美國

Insider Steals Data of 2 Million Vodafone Customers

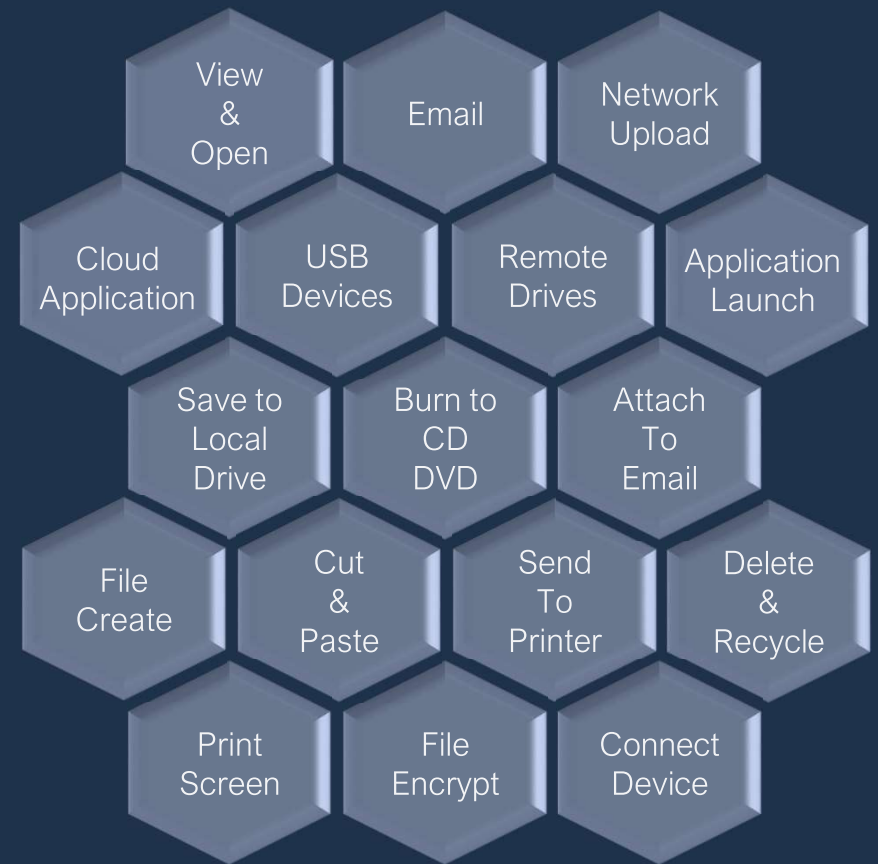
JPMorgan Chase Affects 76 Million

Game-changing attack on critical infrastructure site causes outage

Attack will serve as a blueprint for future attacks on other industrial systems.

ODIN - 12/15/2017, 5:30 AM

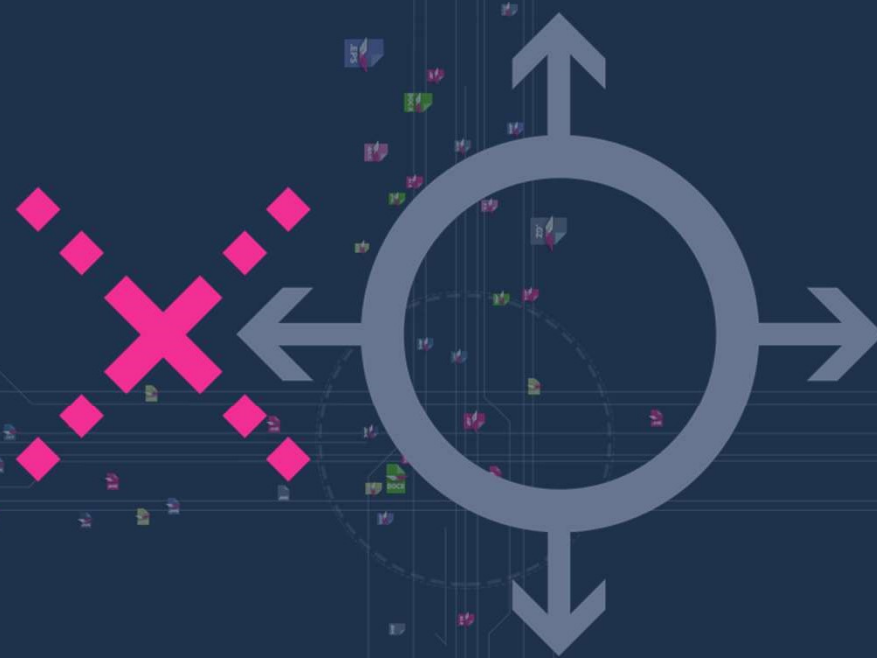
# 如何保護資料? Where、What、When & How



有任何單一agent可以同時保護內賊與外部攻擊嗎？



INSIDER THREATS



OUTSIDER THREATS



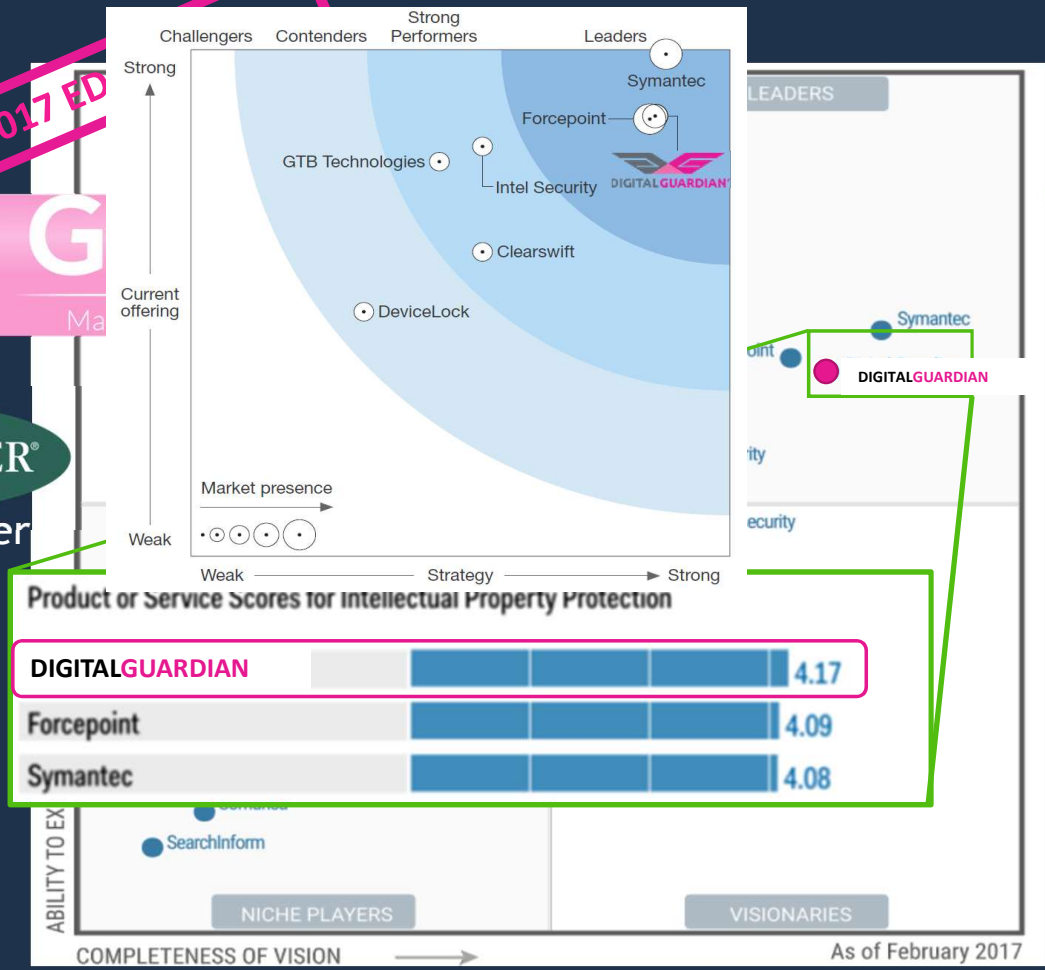
# DIGITALGUARDIAN

- 2003 年由Verdasys公司成立
  - 總部位於麻州波士頓 ( Waltham, MA )
    - London, Amsterdam, Paris, Toronto, Munich, Tokyo offices
  - 已經在六十個國家安裝超過三百萬個agent
  - 取得超過二十個專利技術
  - 數位資安2004年開始代理
- 2017 Gartner 及Forrester評比為領先者
  - 有DLP評比開始，連續六年居於第一象限
  - 企業智慧財產保護的第一名
  - 整合資安法規、內部與外部威脅三大功能之解決方案
  - 前十大專利商有七家使用DG
  - 前十大汽車製造業有七家是DG客戶
- 不間斷的資料保護 (Anytime ,anywhere)
  - Windows, OSX, Linux, offline/online, cloud & mobile
  - Network, Endpoint, Cloud, Database
  - 資料保護、追蹤、加密、應用程式管理、網路行為、周邊管控與事件調查，不受限於平台與連線與否

FORRESTER®  
Wave Leader

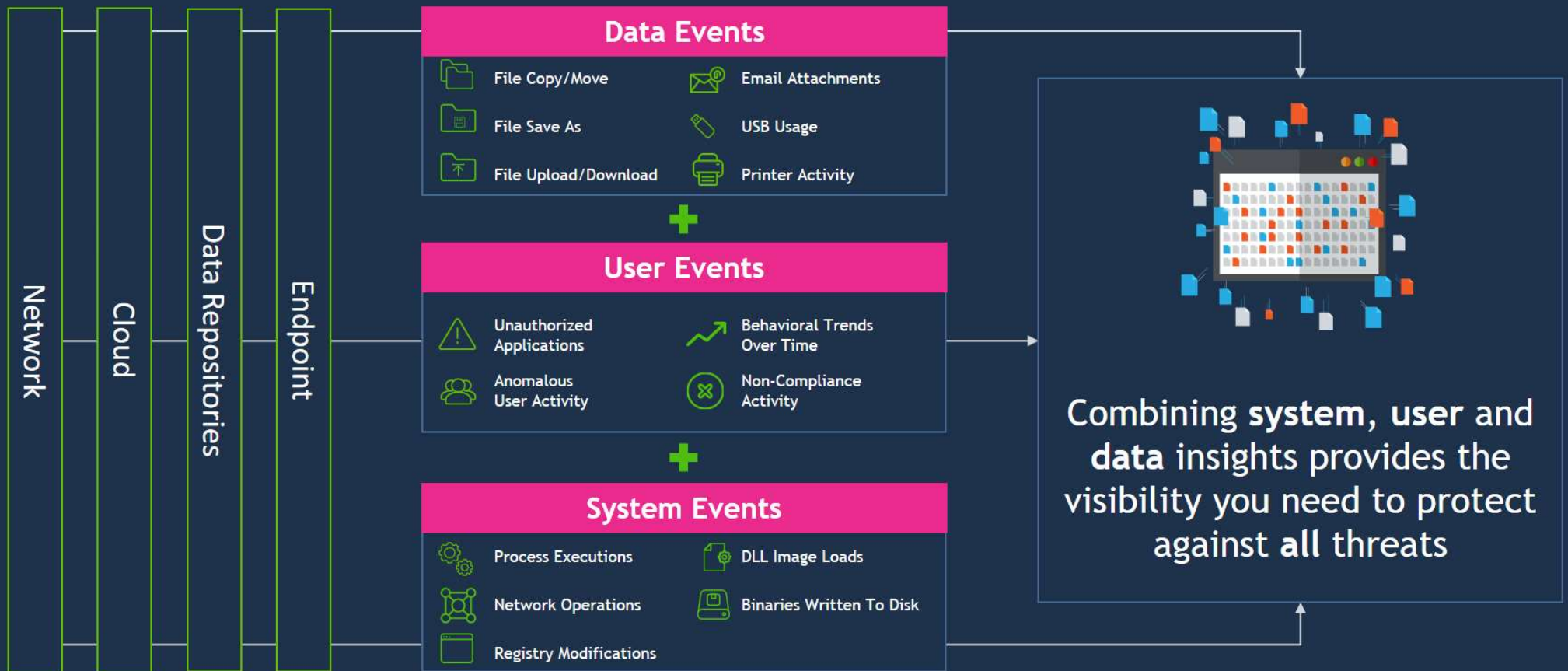
2017 ED

G  
Ma



“Digital Guardian offers one of the most advanced and powerful endpoint DLP agents and its deep native endpoint integration, detection and response (EDR) in a single platform.”

# 最廣的能見度 **Deepest Visibility**



# 使資料免於遭受內部與外來的威脅

## Secure Data from Insider & Outsider Threats

Threat **Aware** Data Protection Secures Sensitive Data Assets

能見度  
**Visibility**



Deepest  
Visibility

Harnessing our:  
識別力  
**Understand**



Real-Time  
Analytics

保護力  
**Protect**



Flexible  
Controls

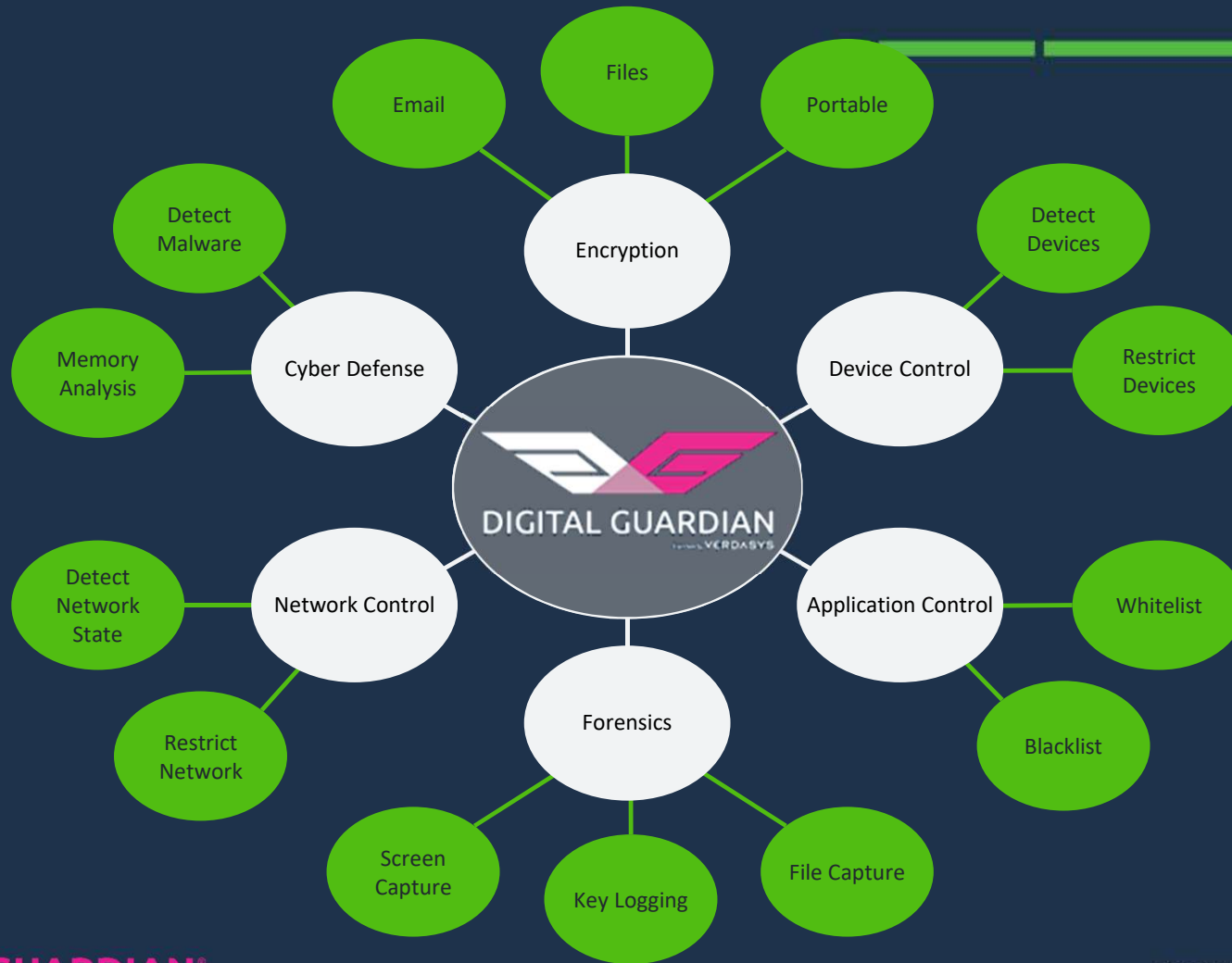
Stops Data Theft From **INSIDER & OUTSIDER** Threats





# DIGITAL GUARDIAN ENDPOINT AGENT Data loss prevention

# 超越傳統的DLP





# DIGITAL **GUARDIAN** FOR ADVANCED THREAT PROTECTION

# Verizon 資料入侵報告

---

- 78% of advanced and targeted attacks involved spear-phishing scams with emails containing malicious attachments
- 23% of users open Phishing messages and 11% click on the attachments
- 95% of malware showed up for less than a month and several didn't last more than 1 week.
- 70-90% of malware samples are unique to one organization
- 15% of incidents still take days to discover.

# DIGITALGUARDIAN<sup>®</sup>

## Advanced Threat Protection



DIGITALGUARDIAN FOR  
ADVANCED THREAT  
PROTECTION

- 運用既有DG Agent的技術
  - Kernel Level Agent
  - Stealth Technology
- 即時行為分析
  - Malicious software
  - System compromise
- 針對APT擴充DG事件類型
  - Deep visibility into events across the user machine, at both the kernel and user level

# DG ATP 的優點

- Visibility into the Full Attack Lifecycle for more effective detection
  - Not just a list of IOCs
- Detects Malware and Non-Malware Based Attacks
  - Not all attacks employ malware
- Detects Known and Unknown Attacks
  - Detects the behavior of the threat, not the specific component
- Continuous endpoint visibility
  - Combination of both Kernel and User mode monitoring gives a 360 degree view

# 進階持續性攻擊(APT)之偵測範例

## Example of Advanced Persistent Threat Detection

Digital Guardian gives you the ability to protect sensitive data from outsider threat

Digital Guardian **protects** by blocking the behavior, quarantining the device, and alerting IT of the phishing attack



User receives a spear phishing email with a PDF attachment claiming to be from HR



User opens the attachment, which is actually an infected PDF in disguise

Digital Guardian **monitors** and **records** those behaviors; identifying them as malicious

Once opened, the file begins executing a series of commands on its own



15

# DG ATP 的保護範圍

- Email Attacks
  - Phishing
  - Spear Phishing
- Web Browser Attacks
  - Watering Hole
  - Drive-by Downloads
  - Malvertising
- Ransomware protection
- Physical Threats
  - Candy Drop
  - Social Engineering
  - Malicious Insider
- Existing Threat Detection
  - Malware actions occurring before ATP was installed
  - Install ATP to gain that visibility





# DIGITAL GUARDIAN Network Appliance

# DG Network Appliance 產品功能

## 掃描 DLP



尋找、矯正機敏資料

- 檔案共享, DBs, SharePoint, CMS, 伺服器與筆電
- 拷貝、移動、刪除

## 網路 DLP



監視/控制網路流量

- EMail, Webmail, HTTP/S, FTP/S, TCP/IP
- 阻攔, 隔離, 加密

整合AD

稽核

事件管理

集中管理平台

報表

Syslog/SIEM

政策管理

## 雲端 DLP

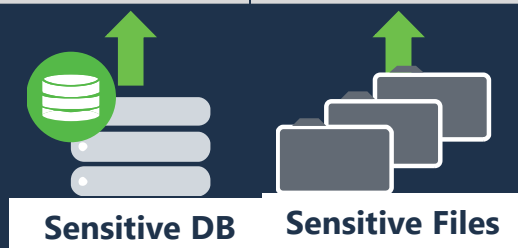


稽核與保護雲端儲存上的資訊

- Box, Sharefile, Egnyte, OneDrive
- 報表、稽核、警示、移動、刪除

# DG Network Appliance 深入的內容辨識

## 高精準度的辨識能力



### Examples

- DB Record Matching** CustName AND (AcctNum OR SSN) from DB
- Partial File Matching** Paragraph match from fingerprinted file
- Patterns** Credit Card Number, SSN, Passport Num
- Regular Expressions** Medical Record Number, Email Address
- Dictionaries** HIPAA Code Sets - NDC, LOINC, HCPCS  
US Addresses



# 使用者分類檔案

# DG User Classification

# How DG Classifies ?



## Content-based

File inspection to identify, tag and fingerprint sensitive data for lowest false positives

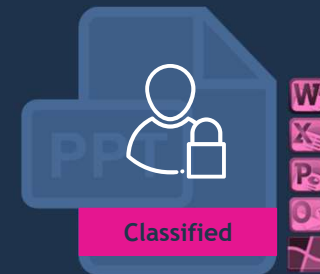
Upload/Download  
User  
Computer  
Classification  
Email  
Session



## Context-based

Identify & tag sensitive data (structured and unstructured) even before you develop policies

Source/Destination  
Application  
Network State  
Operation  
Drive Type  
Time of Day



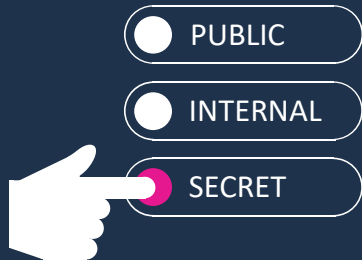
## User-Based

Enable users to classify sensitive data based on business requirements

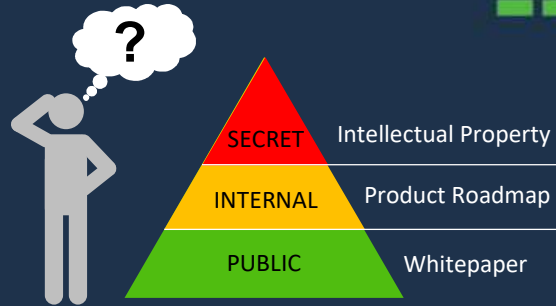
當今最廣泛之資料搜尋與標記解決方案

Most comprehensive data discovery & classification on the market today

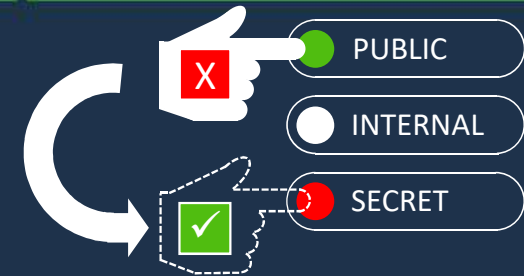
# Use Case: User Classification



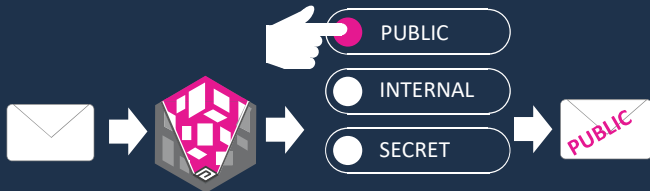
Company wants data owners to determine file & email sensitivity



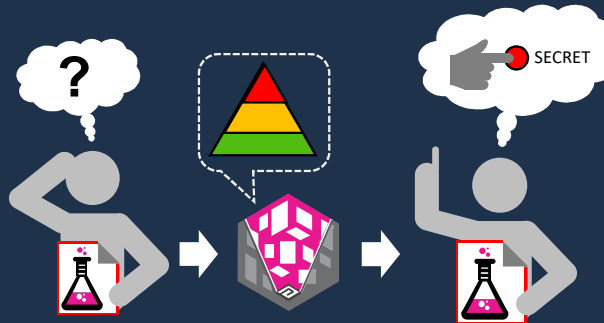
Users must classify data using Company's schema & guidelines



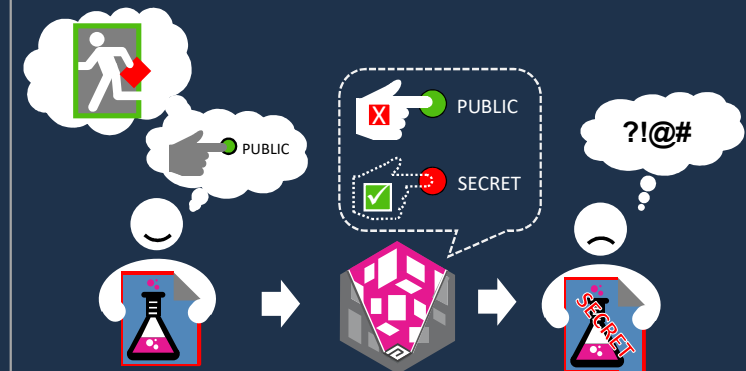
Users must also be audited to prevent misclassification of data



DG requires users to manually classify sensitive files & emails



DG prompts can educate users & guide proper classification



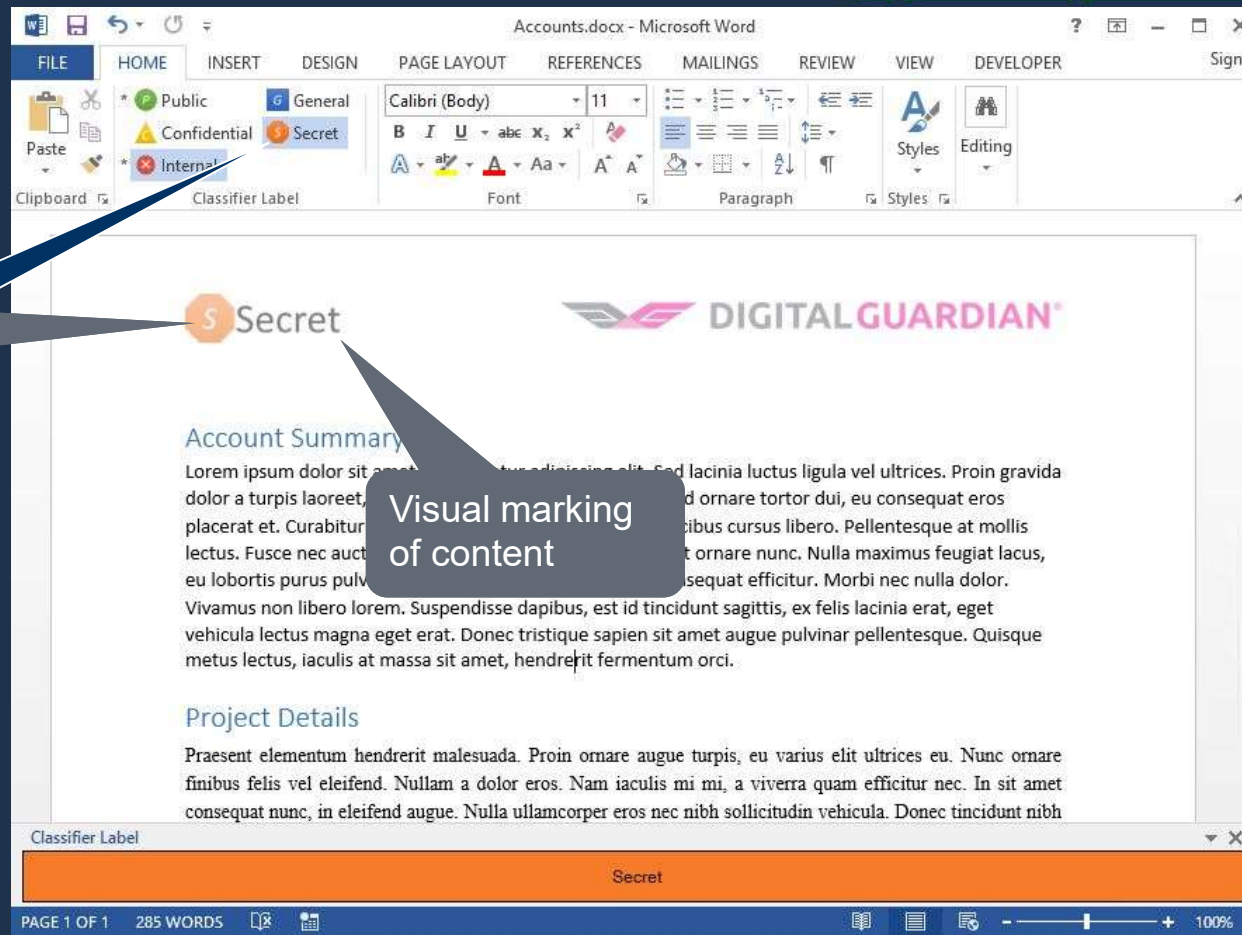
DG's automated rules can confirm & enforce correct classification

# 使用者分類的好處



- 專業—Incorporates data owners into the information security program by using their knowledge to classify data.
- 準確— Increases accuracy of data classification by providing additional context and verification of automated classification.
- 規範— Improves Data Loss Prevention by helping to ensure the right regulated and/or sensitive data is tagged.
- 優先— Increases Advanced Threat Protection efficiency by incorporating accurate data sensitivity context into alert prioritization.
- 全面— Delivers the most complete data classification offering in the industry.

# Classification for Office



Consistent graphics

Visual marking of content



# Classification for Email

The screenshot shows an email client window titled "Account details - Message (HTML)". The "MESSAGE" tab is active, displaying a toolbar with classification options: "Public", "Confidential", "Internal", "General", and "Secret". The "Secret" option is selected, highlighted with a callout box labeled "Classification selection". Below the toolbar, the email header shows "To: myself@personaldomain.com" and "Subject: Account details". An attached file "Accounts.docx (24 KB)" is listed. The email body contains the text "Please see attached for account details." followed by a signature for "Jane Doe | Senior Account Manager (781)555-5555" and the "DIGITAL GUARDIAN" logo. At the bottom of the email content, a "Classifier Label" section shows the word "Secret" in a red box, with a callout box labeled "Visual summary of metadata marking".

Classified Attachment

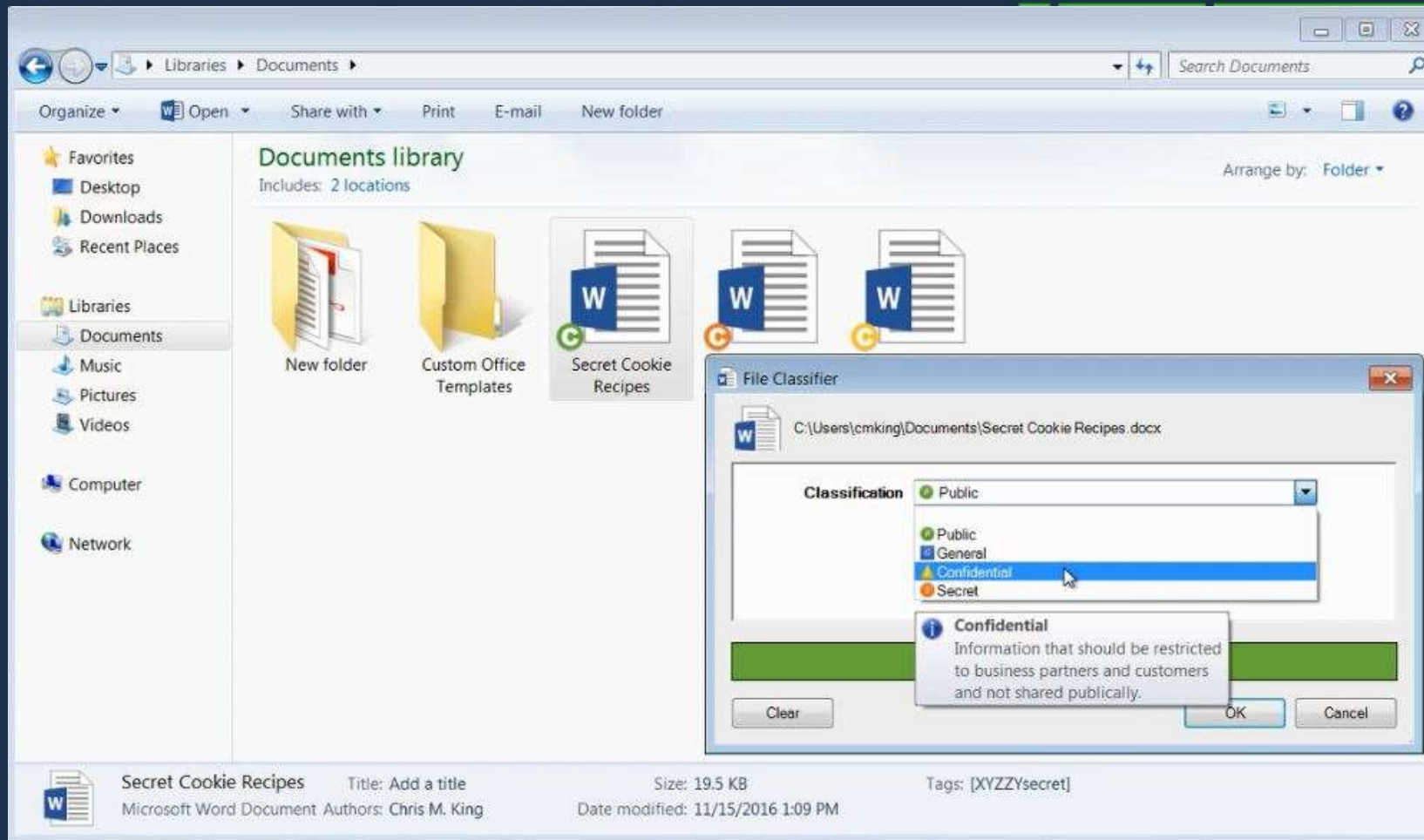
Classification selection

Metadata tag

Visual summary of metadata marking

Classification	
Classification	0
Rule IDs	{D2DBF272-8505-42B2-ABBF-DOF96232CC63} (partnerId=0)
Policy IDs	{22FF716B-D711-4081-B396-6566E51D8062} (partnerId=0) {C0DB2E7C-929A-E6C8-7C2E-DBC09A92C8E6} (partnerId=12) {37E637C8-AF46-8A80-C837-E63746AF808A} (partnerId=12)
Policy Tags	dlp_pci_data_med (partnerId=0) classification_public (partnerId=12) distribution_external (partnerId=12)

# Classification for Files



# DG Prompts and Warnings

The image displays three overlapping screenshots of the Digital Guardian interface. The background screenshot shows a document titled "This is a test.docx - Policy Check" with a "Classification Downgrade" warning: "You may downgrade the classification of this document. Do you have a justification? Do you wish to continue?" Below this is a "Justification" text box and a "Continue" button.

The middle screenshot is a "UC Tag Mismatch" dialog box. It features the Digital Guardian logo and the text: "Dear CMKing, You are attempting to copy/move a sensitive file that has been classified by you as public external. This is required for business purpose, please provide justification for the action and click on continue. If you do not wish to continue, click on Close." Below the text is a "Justification" text box and a "Continue" button.

The foreground screenshot is another "UC Tag Mismatch" dialog box, similar to the middle one, but with the text: "Dear CMKing, You are attempting to email a sensitive file that has been classified by you as public external. If this is required for business purpose, please provide justification for the action and click on continue. If you do not wish to continue, click on Close." It includes a "Justification" text box and "Continue" and "Close" buttons.



# 總結

# DG Products Today



 DG Endpoint Agents (DLP)

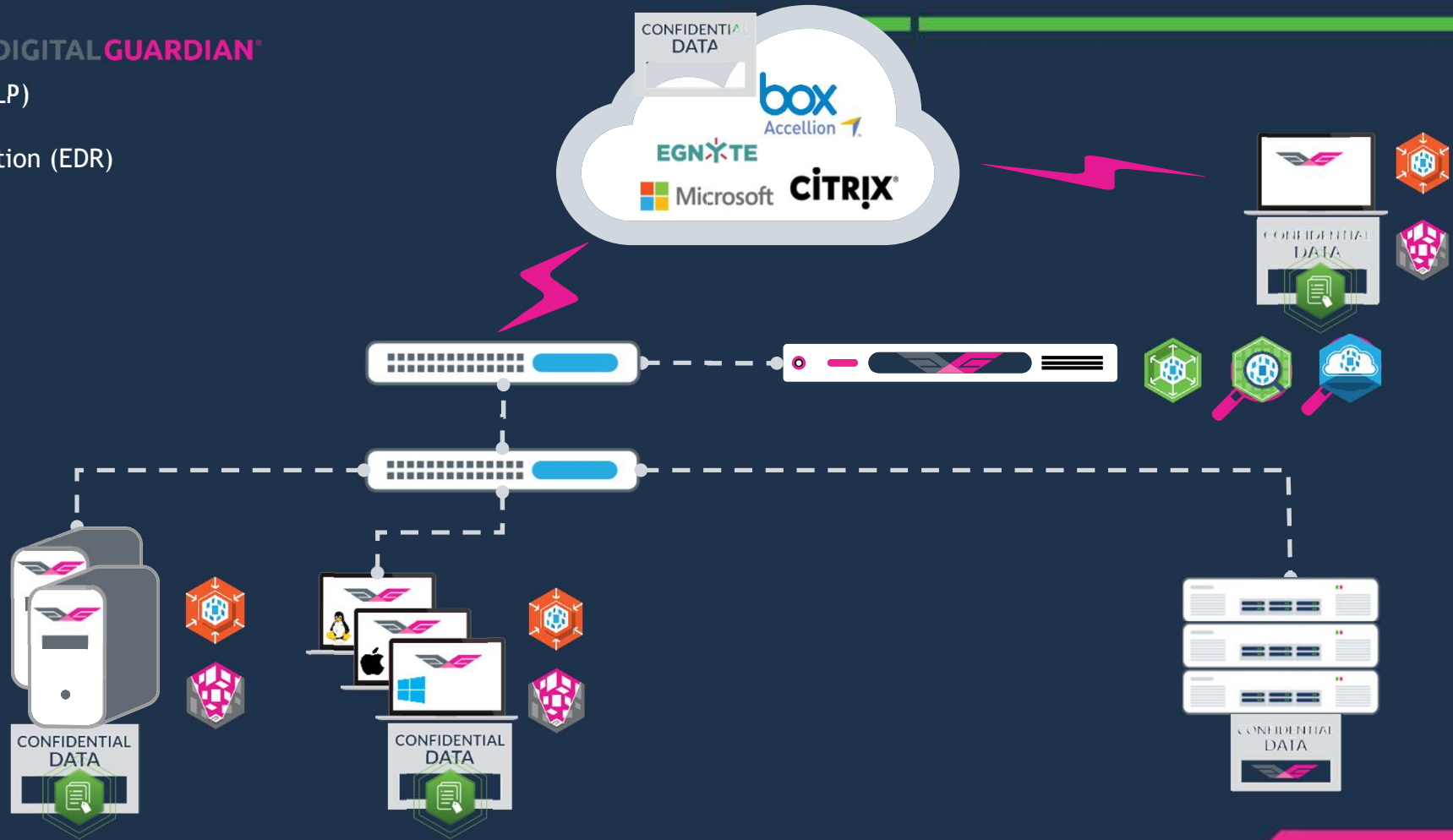
 Advance Threat Protection (EDR)

 Network Appliance

 Data Discovery

 Cloud Data Protection

 Data Classification



# 總結

## DG 解決方案

## 特性

Data loss prevention

- Kernel 層agent，擁有最廣能見度
- 同時支援Windows OSX 及 Linux三大平台
- “Capture all”，不需要事先定義政策

Advanced threat protection

- Not just IOC (Indicator of compromise)
- Behavior based Endpoint detection and response
- Single agent for insider and outsider

User classification

- 強制使用者編輯Office相關檔案及Email時分類
- 可透過按右鍵之方式對一個或多個檔案分類
- 整合與互補內容(content)及屬性(context)標記之不足

Network Appliance

- 於閘道端過濾Web、FTP及SMTP，防範機敏資料外洩
- 事件(event)完全整合於同一管理介面
- 還有Discovery與Cloud之功能

# 總結

---

- 唯一Kernel層的agent
- 唯一不需要事先定義政策
- 唯一完整支援Windows(server/workstation) 、 Mac OS 、 Linux
- 唯一提供三種標記方式的agent
- 唯一同時防範insider與outsider的解決方案
- IP保護的第一名



感謝您的聆聽，如有任何問題，  
歡迎和我們聯繫

**Thank you!**

