



下一代数据资产保护架构

赵树佳 | 解决方案架构师

使用5W2H分析法来解决数据资产安全问题

- (1) WHY——为什么要数据保护？
- (2) WHAT——什么样的数据需要保护？
- (3) WHO——谁？数据的所有者，处理者是谁？
- (4) WHEN——何时？事前，事中，事后？
- (5) WHERE——数据在哪里？是怎么流向的？
- (6) HOW ——McAfee是怎么做的？怎么迭代演进升级的。
- (7) HOW MUCH——如何衡量数据安全投资收益及关注隐性成本。

保护数据资产的动因 (Why)

\$3.79M 是一次数据泄漏的
平均成本



巨额罚款



信誉损害



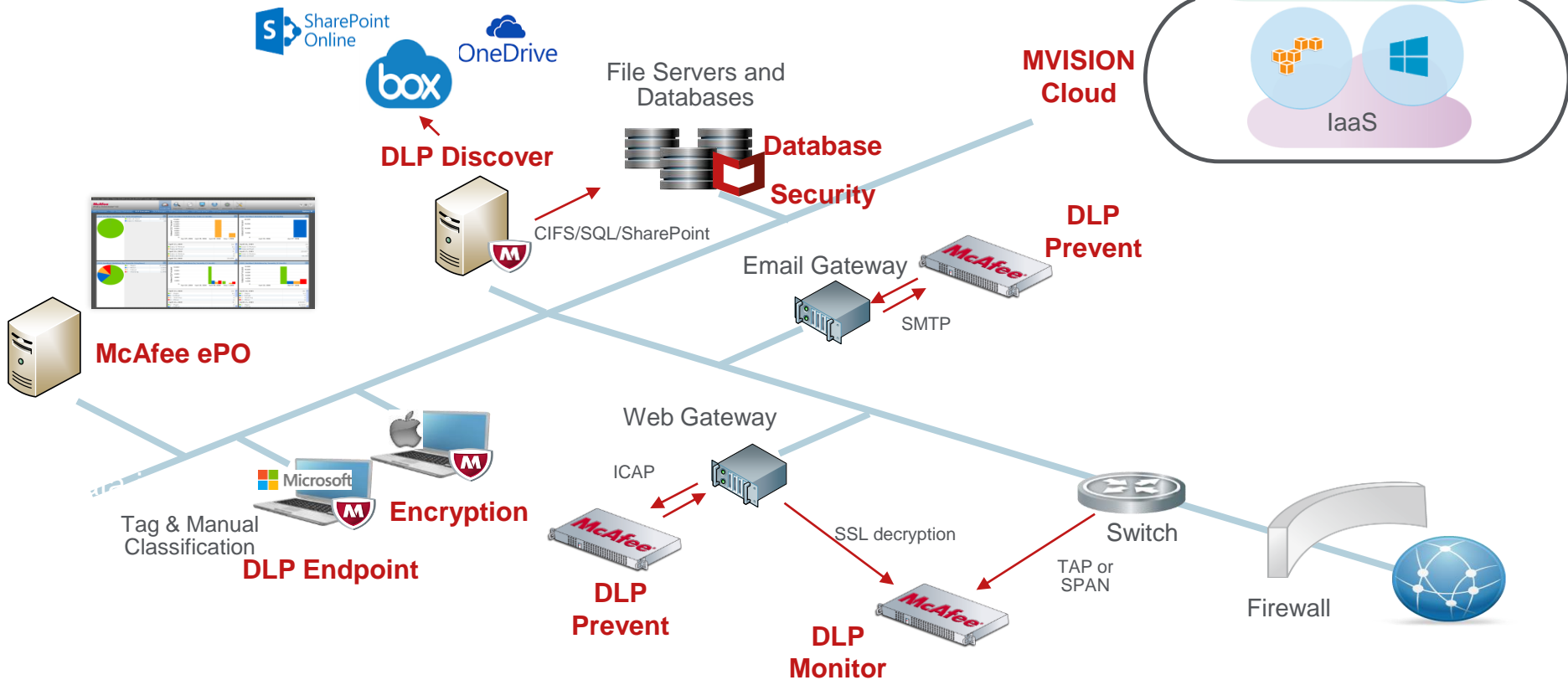
客户及收入
的损失

我们要保护的数据资产是什么？(What)

- 信息可以划分为两大类。
 - 结构化数据：能够用数据或统一的结构加以表示，我们称之为结构化数据，一般存储在数据库中，如客户资料、销售记录等；
 - 非机构化数据：无法用数字或统一的结构表示，如办公文档、图像、声音、网页、设计图纸等，我们称之为非结构化数据。
- 结构化数据的识别技术：关键字、正则表达式、数据字典、指纹库
- 非结构化数据的识别技术：指纹库、标签
 - 非结构化数据不适合使用关键字、正则表达式、数据字典的关键原因在于误报率太高，无法进行精确的阻断。另外要求IT基于对业务数据了解的前提下定制策略，而实际情况几乎是不可能的。



McAfee 下一代数据资产保护架构 (How)



传统终端DLP功能涵盖范围

在用户日常工作中定位危险的行为保护敏感数据.



端点DLP 和 外设控制

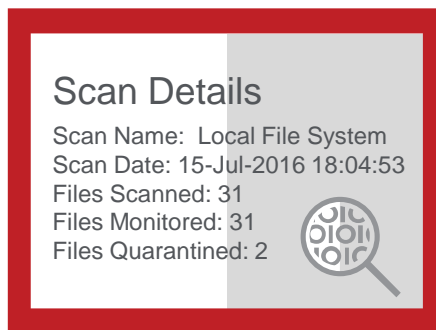
需要教育并监控用户行为 (Who)

手工分类



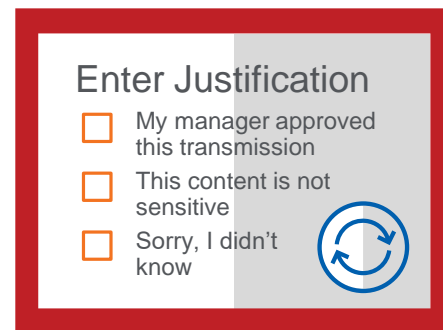
A screenshot of a manual classification interface. On the left, there is a blue icon of a document with a keyhole. To its right, there are three checkboxes: 'Public' (unchecked), 'Confidential' (checked), and 'Partner' (unchecked). The interface is presented in a white box with a red border, set against a grey background.

自修复



A screenshot of a self-repair scan details interface. The title is 'Scan Details'. Below it, the text reads: 'Scan Name: Local File System', 'Scan Date: 15-Jul-2016 18:04:53', 'Files Scanned: 31', 'Files Monitored: 31', and 'Files Quarantined: 2'. On the right side, there is a magnifying glass icon over a binary code pattern. The interface is presented in a white box with a red border, set against a grey background.

实时反馈

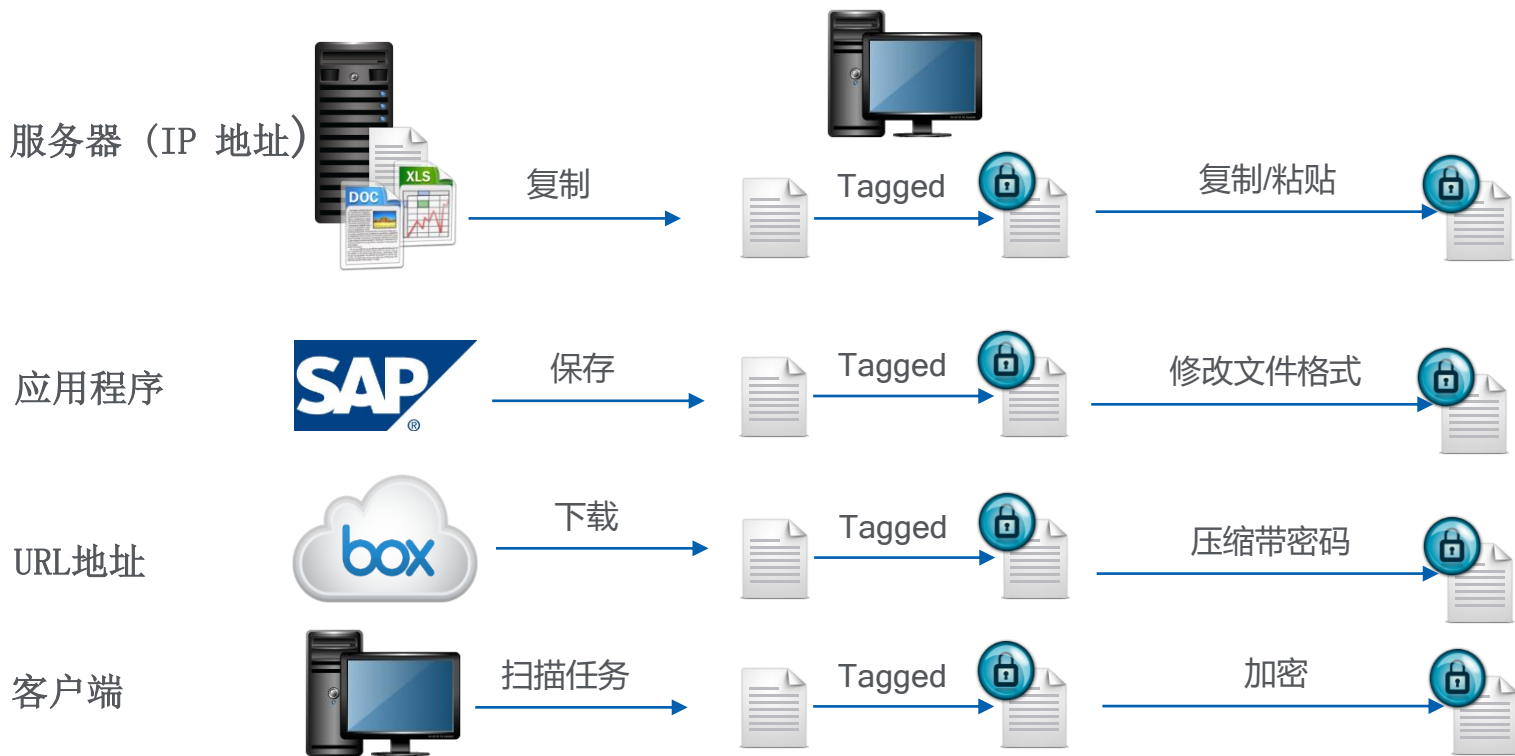


A screenshot of a real-time feedback justification interface. The title is 'Enter Justification'. Below it, there are three checkboxes: 'My manager approved this transmission' (unchecked), 'This content is not sensitive' (unchecked), and 'Sorry, I didn't know' (unchecked). On the right side, there is a circular refresh icon. The interface is presented in a white box with a red border, set against a grey background.

减少超过 ~75% 危险行为

Educates employees; alleviate administrative burden; reduce risky behavior

使用标签技术解决识别数据资产的困难



传统网络DLP解决的问题有限

Data-in-Motion

101101100110101001



网络通讯



Internet

Data-at-Rest

011001101010011011



云存储



数据库

Data-in-Use

1011011001101001



文件共享



邮件/即时通讯

2/3的数据泄露事件发生在传统网络环境中；

1/3的新的数据泄露发生在云架构下，并且这样的趋势在上升



时间问题 (When)



Company

数据外发

DLP 策略

PCI
HIPAA
IP资产
敏感数据

规则匹配



Internet



- 类似于 Google 搜索引擎的数据挖掘能力
- 调查取证历史数据
- 主动的策略调优



事件发生前

- 你必须知道你要保护的内容
- 被动应对数据的变化
- 策略之外漏报的数据没有办法

事件发生时

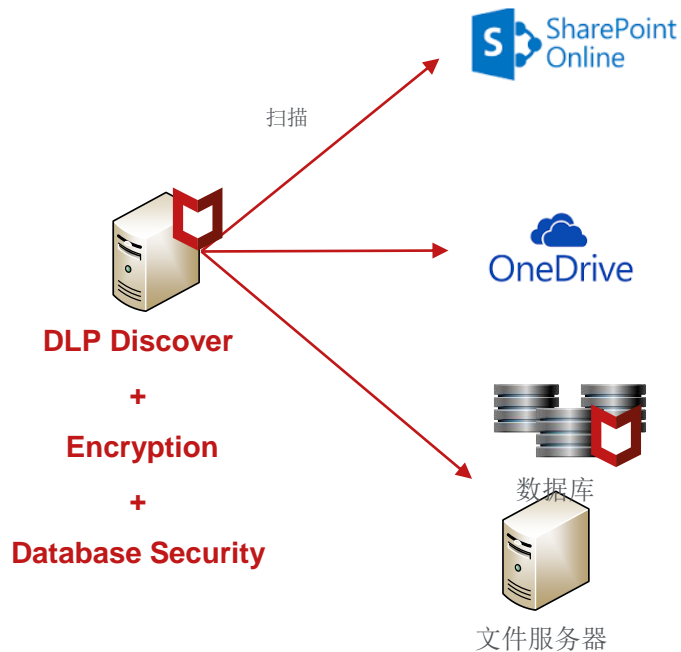
- 拦截/放行, workflow
- 仪表盘报表
- 违规告警提示

事件发生后

- 捕获所有数据
- 无需事先知道你要保护的数据
- 事后进行学习

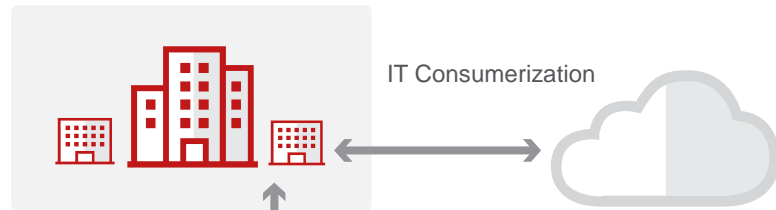
发现需要保护的数据在哪里 (Where)

- 发现敏感数据在各种存储上的分布
- 将敏感数据从公开共享目录中移除
- 发现用户真实数据是否存在于开发测试系统中（未脱敏）
- 对敏感数据进行强制分级（Classification）和加密操作
- 对敏感数据产生指纹，供其它DLP模块使用
- 对数据库的保护日趋重要

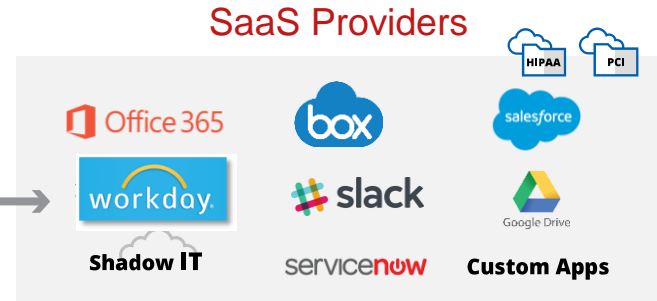


我们要保护的数据资产在去往哪里？ (Where)

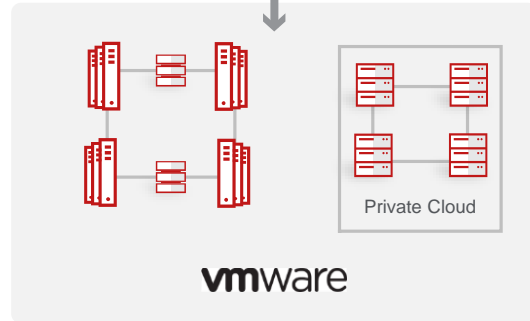
Offices | Remote Sites



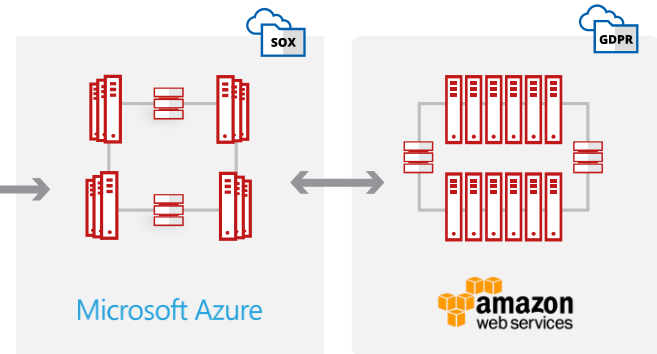
Software Transformation



Infrastructure Transformation



Infrastructure Transformation



On-Prem / Hosted

Cloud IaaS / PaaS

传统数据保护解决方案无法保护数据向云端迁移的场景



- 云端数据缺乏可视化
- 数据不断在云端或未受管理设备上被创建。
 - e. g. Office 365, Box...
- 云端到云端的数据传输无法被发现.

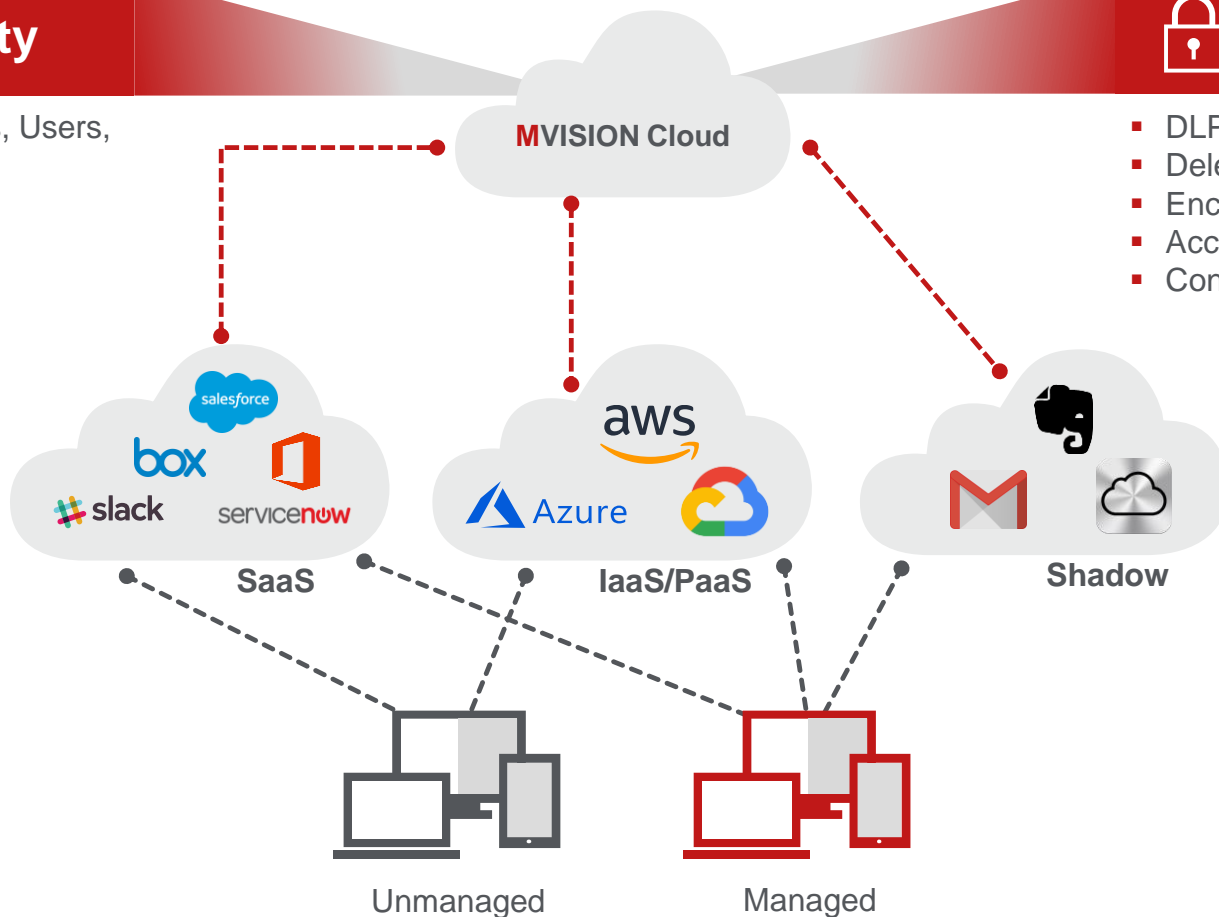
云上的数据安全问题需要用云的解决方案来解决

Visibility

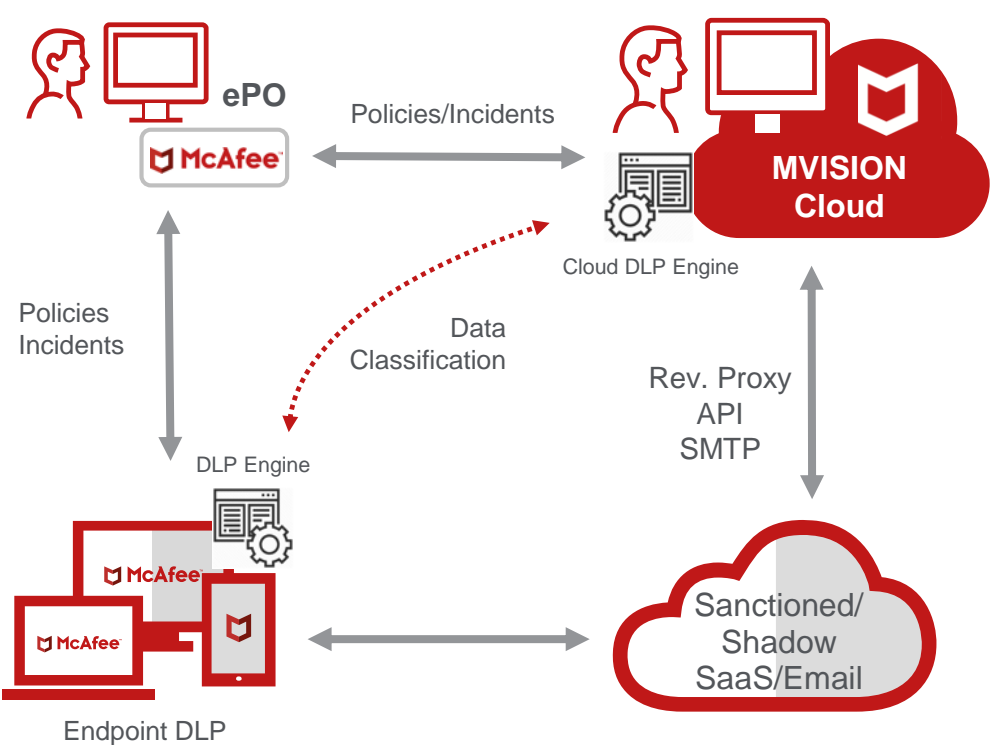
- What: Data, Apps, Users, Devices
- Who
- Where
- When
- Shared

Control

- DLP
- Delete/Quarantine
- Encryption
- Access
- Configuration

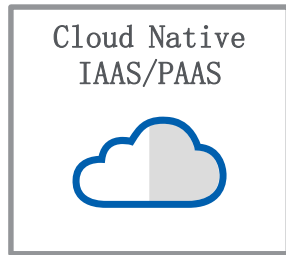
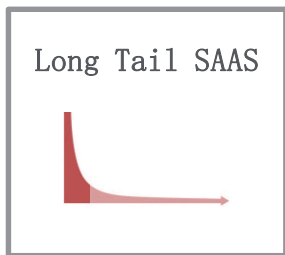


云DLP如何与传统DLP协同工作场景



- 统一的基于ePO的策略管理
- 统一的数据分类
- 统一的事件报警与响应

McAfee MVISION Cloud 保护用户所有云上的数据安全



Common Security Services

Compliance & Risk Assessment

Reporting

Orchestration

DLP

Config Audit

Classification

UEBA

Malware Protection

Access Control

Encryption

Activity Monitoring

Data Protection

Threat Protection

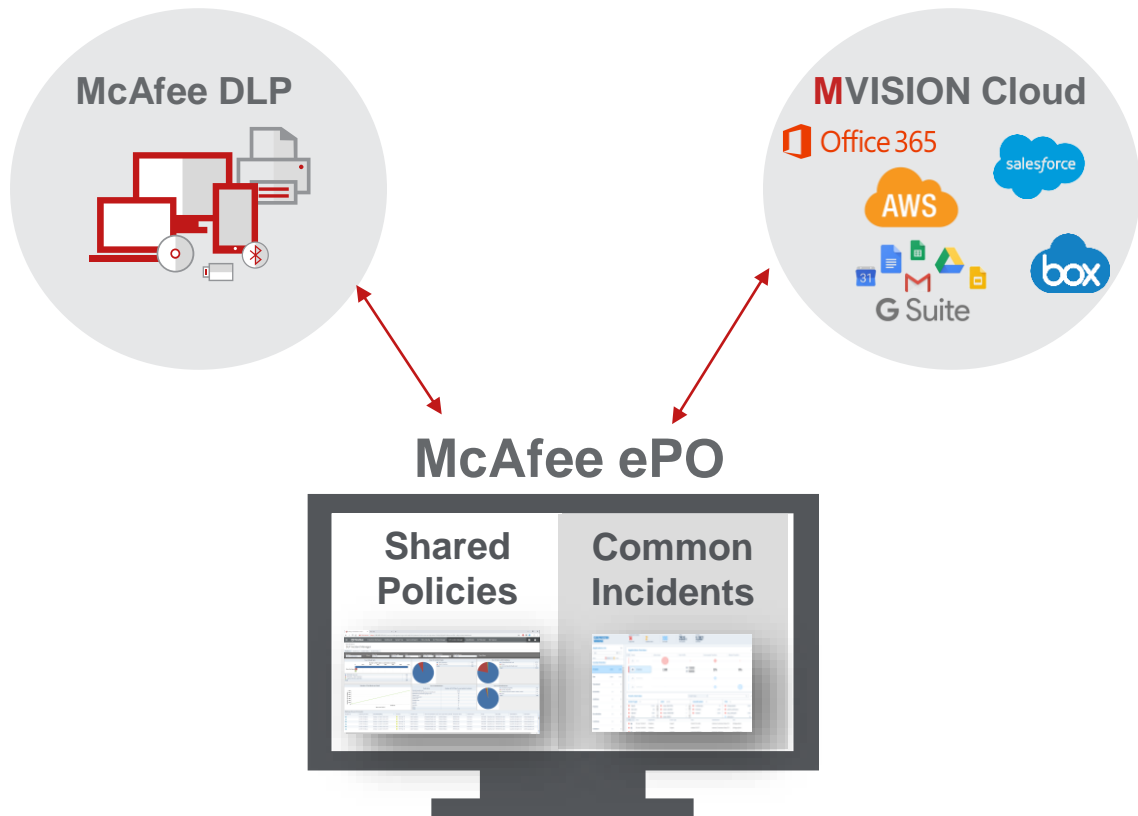
从终端延申到云的完整的解决方案



DLP + MVISION Cloud

基于ePO管理与云端DLP整合

- 一次对数据分类后，在本地和云端持续对数据进行保护
- 统一的视图集中展现数据违规事件
- 一键快速建立统一的数据保护策略



唯有整合的解决方案才能帮助企业获得好的投资回报

案例分享



IDC ExpertROI® SPOTLIGHT

National Bank Minimizes Security Risk and Supports New Business with McAfee Security Solutions

四年累积获利：

四年获利868万美元

投资回报率（ROI）为208%

在20个月内回报

其他获利：

安全事件的解决率提高90%

每年影响安全事件减少77%

由于有影响的安全事件，减少了98%的生产时间

每年产生500万至1000万美元的额外获利

McAfee 数据保护方案的优势

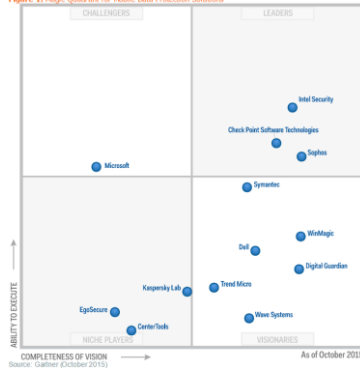
数据保护涉及各个方面

- DLP & Database Security
 - 连续多年位于Gartner Leader象限
 - 获得2018年Gartner的用户最佳选择



Magic Quadrant

Figure 1. Magic Quadrant for Mobile Data Protection Solutions



• 加密

- Gartner排名最靠前的厂商

• CASB

- Gartner、IDC、Forrester三项评测都处于领导者地位

Magic Quadrant

Figure 1. Magic Quadrant for Enterprise Data Loss Prevention



Source: Gartner (February 2017)



Source: Gartner (October 2018)





McAfee, the McAfee logo and [insert <other relevant McAfee Names>] are trademarks or registered trademarks of McAfee LLC or its subsidiaries in the U.S. and/or other countries. Other names and brands may be claimed as the property of others. Copyright © 2017 McAfee LLC.