# IONIC SECURITY

Be fearless.

# “Start with the Data”

## Sensitive Data Protection Landscape and Requirements

Security Interest Group Switzerland (SIGS)
Technology Summit 2015

23 June 2015
Bern, CH

Allen Vance, VP, Product Management

# Agenda

- Executive Summary
- Sensitive Data Protection: Traditional Approaches
- Challenges to these Approaches
- A New Model
- Key Requirements
- Summary
- Discussion

# Executive Summary

- Sensitive data generation is growing exponentially
- Traditional protection approaches are failing
- Consequences of failure are rising
- A new approach is needed, which must provide:
  - Distributed data defense with ultra-scale, automated crypto key orchestration
  - Protection for **any** kind of data on **any** device, on **any** network, **anywhere**
  - Data federation without loss of control
  - Unified platform approach vs. point solutions
  - Near zero end user friction
  - Open architecture, open code, open protocols and APIs

# Traditional Approaches - 1

"The Vault"

- Keep the data in a defined "location" (servers, networks)
- Use system-type access controls (ACLs for file, device, other objects)
- May or may not have encryption
- Advantages:
  - Relatively straightforward to set up and manage
  - Some level of (or at least sense of) control
- Disadvantages:
  - Collaboration across boundaries is difficult; often achieved only by weakening controls
  - All the data is in one place – high negative impact if compromised
  - Privileged *system* access = privileged *data* access (when it should not)

# Traditional Approaches - 2

Public Key Cryptography (PKI)

- Establish key pairs and bind accordingly to devices, users, applications
- Advantages:
  - Allows for more data movement (‘out of the vault’)
  - Strong crypto controls do provide protection
- Disadvantages:
  - Inflexible – devices, users, applications change frequently
  - Complex to deploy and maintain; user friction = training & support costs → $$$
  - Policy adjudication and enforcement is not real time
  - Provides no real inherent visibility – must be added on
  - Difficult to federate across org boundaries

# Traditional Approaches - 3

## Digital Rights Management (DRM)

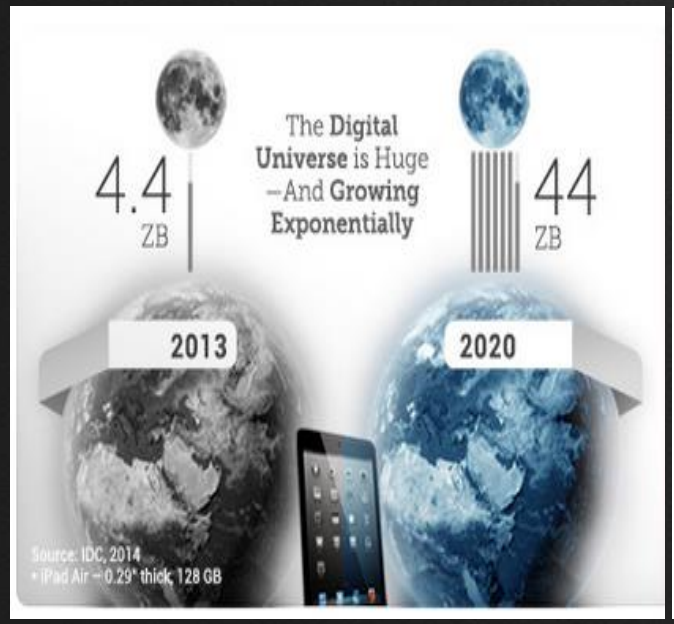
- Significant improvement over the vault model
- Data (at least of certain types) can move relatively freely
- Has access rights ‘baked in’ to the objects (usually files) with a policy server
- Advantages:
  - Somewhat easier to manage
  - Supports some levels of collaboration and external sharing and control
- Disadvantages:
  - Typically very limited in object types: usually MS Office and PDF only
  - Rights have to be ‘pushed out’ – this policy ‘latency gap’ can be exploited
  - Proprietary platforms – have to adopt the whole ecosystem (+ $$$) to work

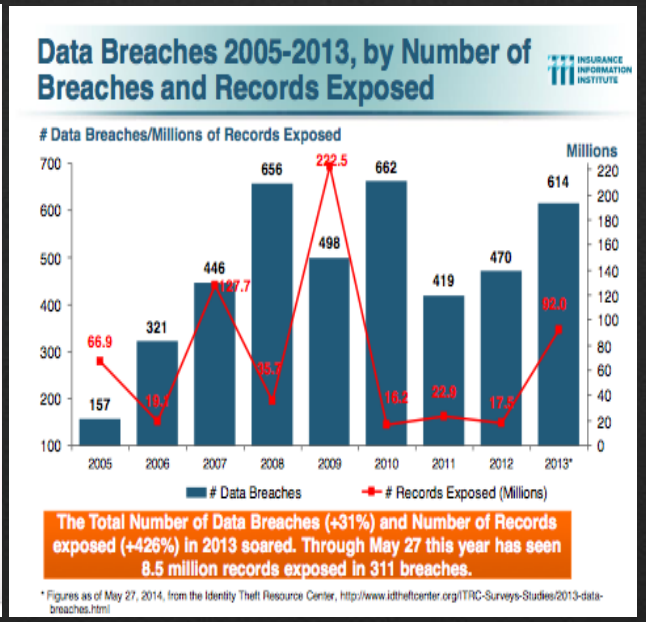
# Challenges to Traditional Approaches

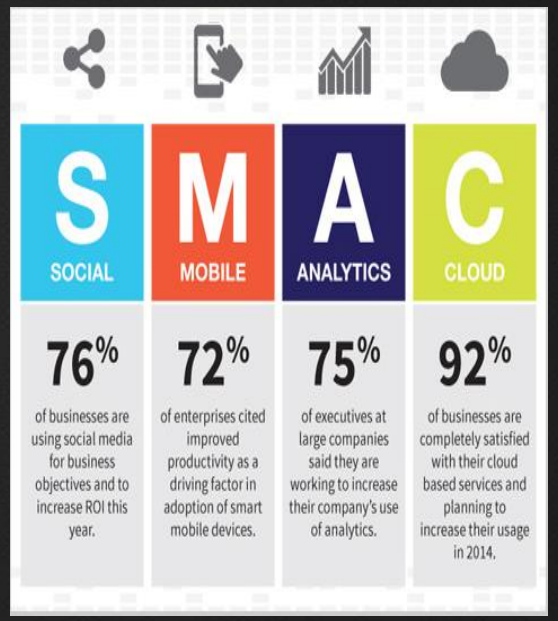
Data is exploding (1,000% growth in 7 years)

Number and cost of breaches are growing

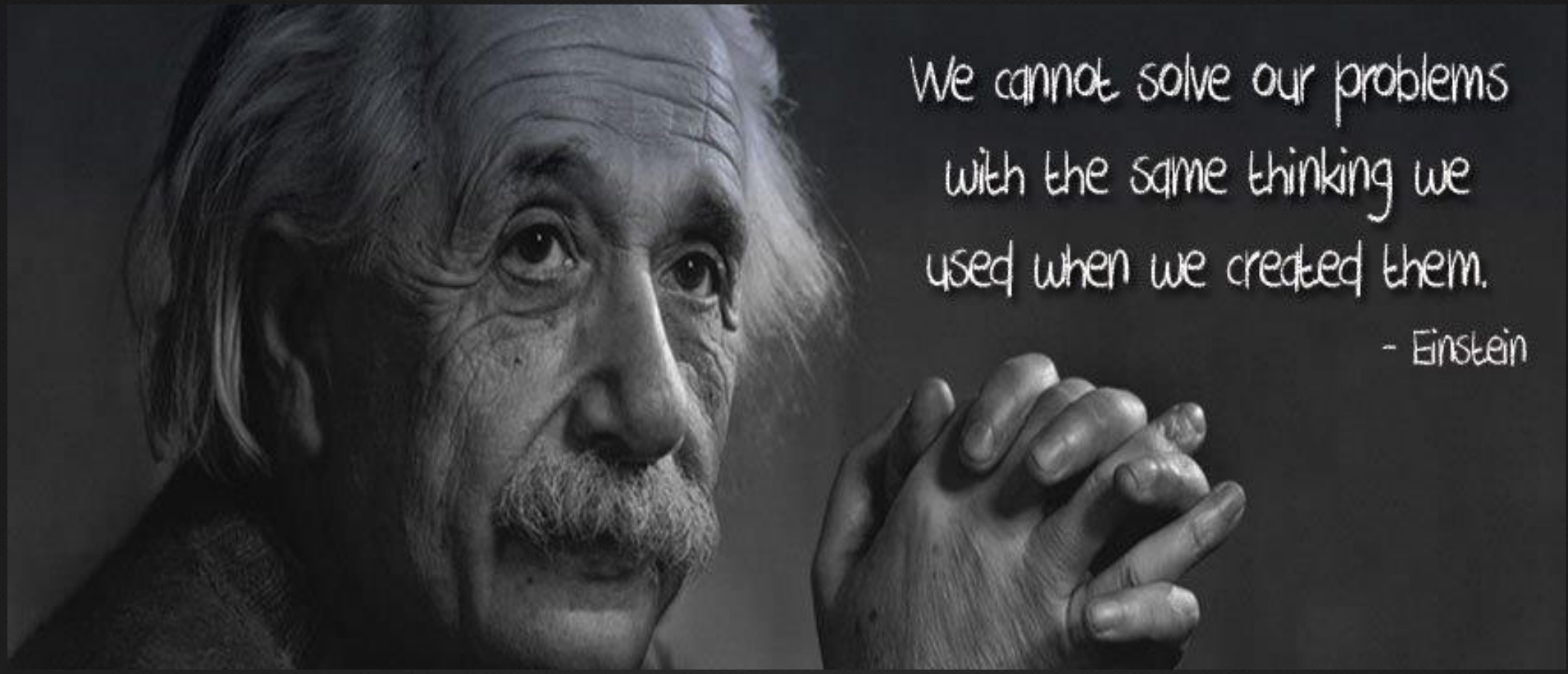
Organizations need agile tools for collaboration



# We need to start from a different premise



# Visibility + Real Time Policy Enforcement


# Key Requirements

# Visibility

- Analytics for Internal and External Threat Detection
  - Detect when endpoint is accessing data outside of normal expectations
    - » Very fast access attempts, access attempts on files ‘in order,’ etc.
  - Detect when user is attempting to access data outside normal expectation
    - » Time of day, location of access, user’s scope of duties, age of information, etc.
    - » What other users in their peer group (organic, not predefined) access
- Analytics for Data Spillage Detection
  - Detect high to low movement, whether accidental or deliberate
- Federated Analytics
  - Policy-based ability to share access analytic data across org boundaries

# Protection - 1

- Secure Key Exchange
  - Securely exchange keys across infrastructure assumed to be compromised
  - **Force attacker into less desirable economics of compromising each endpoint**
- Unified protection across both:
  - devices (operating systems on server/desktop/mobile)
  - formats (files, ‘web’ applications, near-real-time messaging solutions, etc.)
    - Must be **open** – authoring, distributing, and publishing are not security - and these functions should not be “mandatory” for security, nor should proprietary data formats
    - and **neutral** or if I may, “Switzerland”, with regard to data objects and the operations performed upon them.

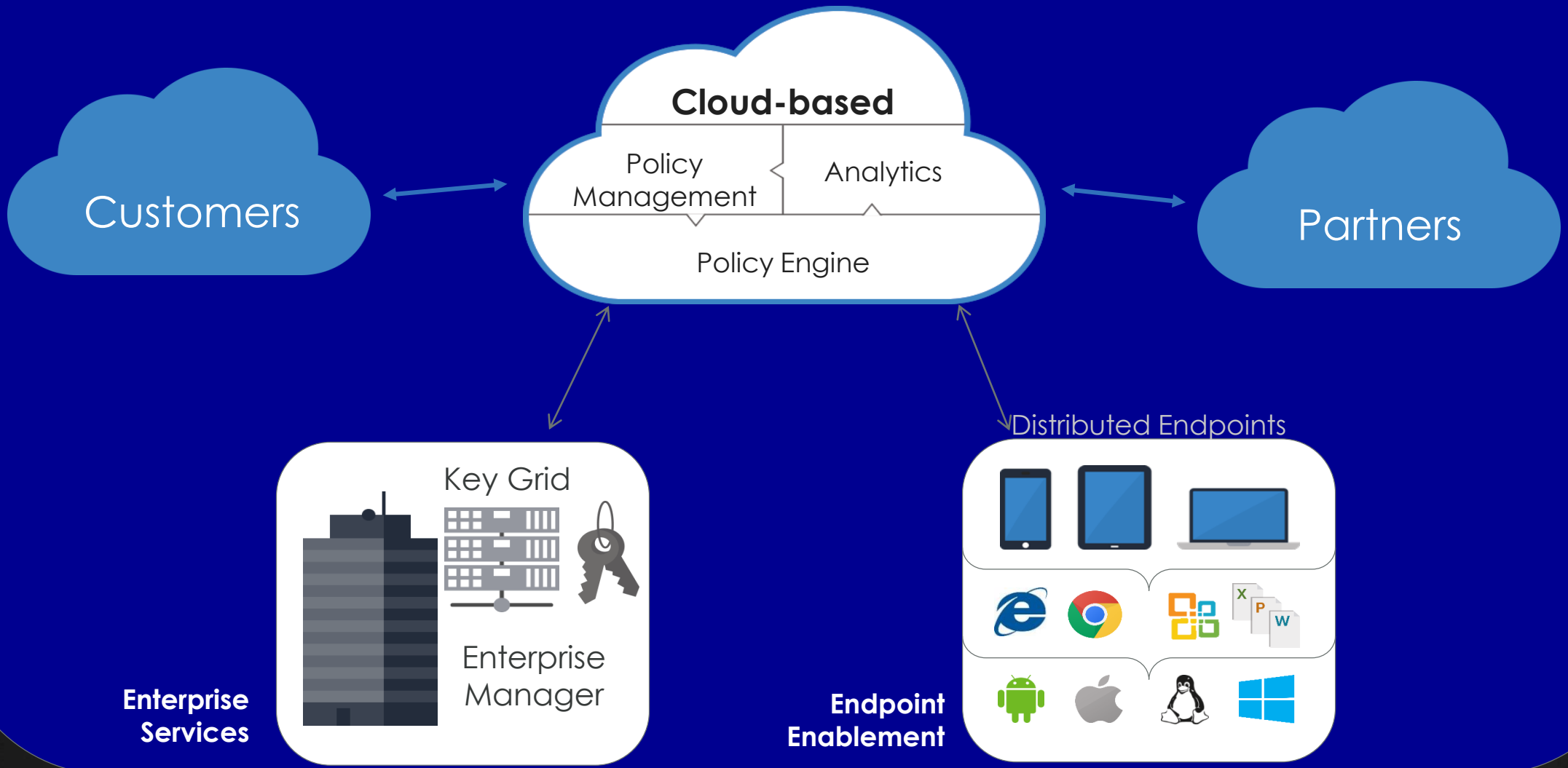
# Protection - 2

- Modular Cryptographic Libraries
  - Ability to change algorithms or key lengths to protect data
- Unique Key for each data object
  - Possible by ultra-scale and autonomous key management
  - Minimizes damage if a key is compromised (no “master key” scenarios)
- Flexible and sophisticated key-based use cases:
  - Key Retirement (disallow any and all access to a data object)
  - Rotating/Re-Keying (for improved protection over time)
  - Cryptographic Shredding (truly, completely, irrevocably purge a data object)

# Control

- Policy based on multiple attributes
  - Time, User, Location, Device
  - Classification (of data), Action (open/preview/etc.)
  - Device health (integrate with other endpoint security systems)
- Authentication based on multiple attributes
  - MFA: Know - Secret (password or key); Have -Token (badge or mobile); Be (Biometric)
  - Location Beacon (physical or network based)
- Federation with each federated org controlling its own
  - Policies
  - Key Grid with org-controlled Key Nodes

# Hybrid PaaS Model for Sensitive Data Protection



# Summary

- Traditional models for sensitive data protection are failing due to:
  - exploding data volume
  - increased need for secure sharing and collaboration
  - ever higher consequences of data leakage
- New thinking is required
- An effective and sustainable model must be ***data-centric, real time, flexible, open and extensible, federated, and  device agnostic***
- This model can provide owners of sensitive data:

  critical ***visibility, protection*****, and *contro***/ for success

# Questions?