

RSACONFERENCE2014

FEBRUARY 24 - 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

The Network Alone Can't Protect Your Data

SESSION ID: STU-T07B

Elliot Lewis

Chief Security Architect
Dell / Dell Software Group
@elliotdLewis

Chad Skipper

Senior Principal Engineer
Dell / End User Computing
@chadskipper



Agenda

1

The Data Journey

2

Powerful Disrupters: Data is More Connected

3

The Network Alone Can't Protect Your Data

4

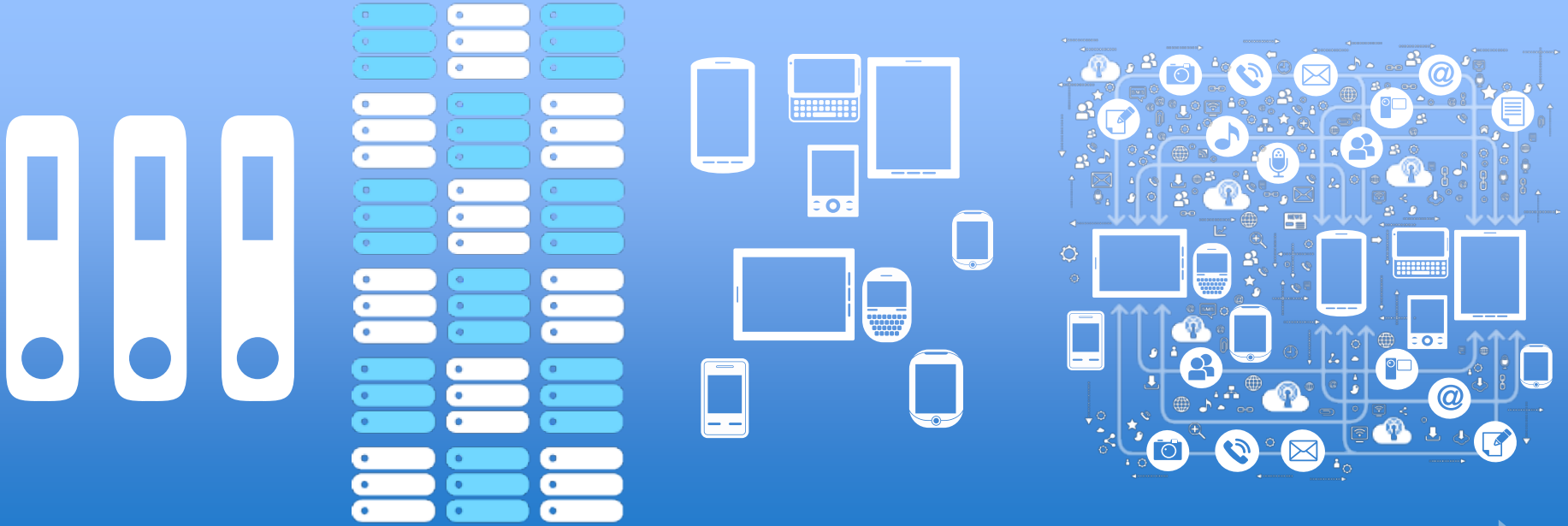
Data Access Risk Models

5

Data Protection Reference Architecture







The Data Journey



From mainframe to client server to distributed to *risk everywhere*



Powerful Disrupters: Data is More Connected

Cloud		85%	Use cloud tools
Big Data		35	Zettabytes by 2020
Mobility		5X	Increase in personal owned devices
Security & Risk		79%	Experienced significant security incident



#RSAC

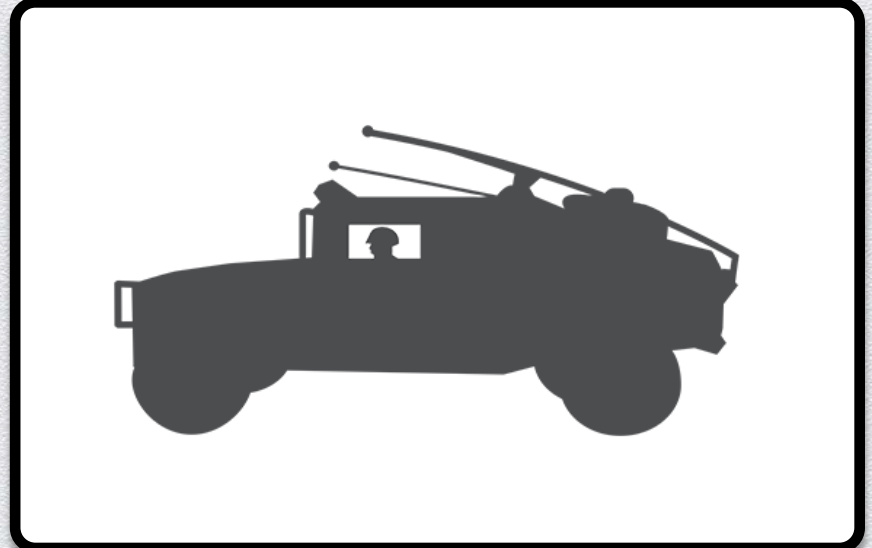
RSACONFERENCE2014

Two Kinds of Protection

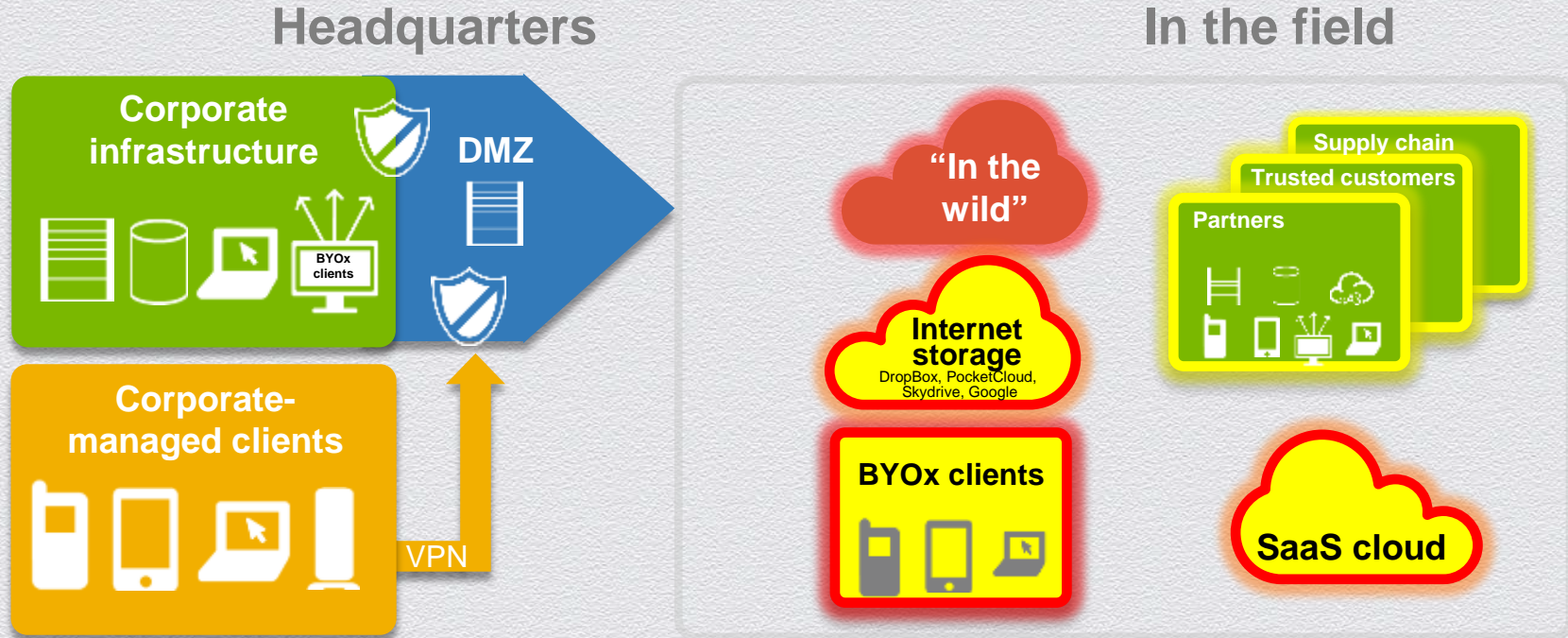
Headquarters



In the field



The Network Alone Can't Protect Your Data

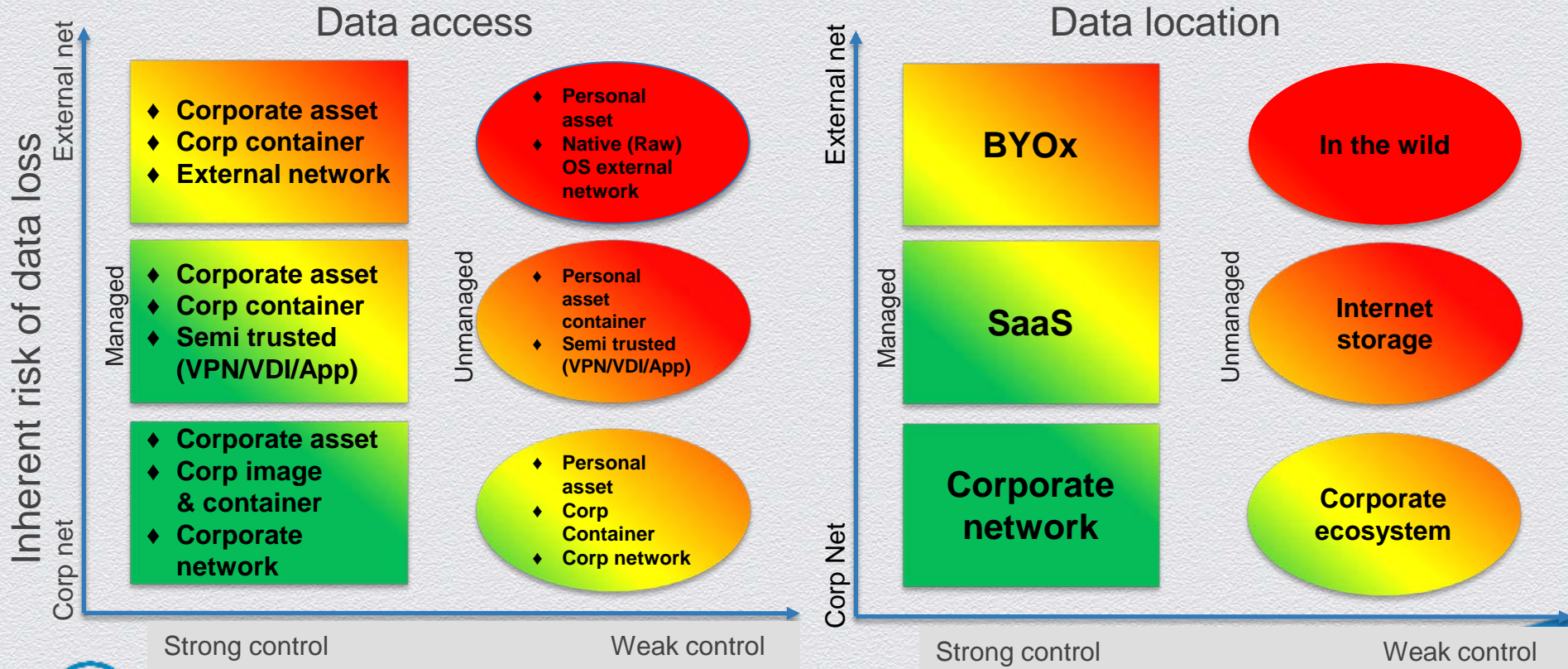


How does one prepare data for external protection?

#RSAC

RSACONFERENCE2014

Data Risk Models



Mitigation control weakness



Contextual Access Assessment



Device, location and access method

- ◆ **Identification processing**
 - ◆ Who should be allowed to start the assessment process?
- ◆ **Endpoint platform assessment**
 - ◆ What kind of device are they on?
 - ◆ What OS type?
 - ◆ Managed/unmanaged?
- ◆ **Connection allowance assessment**
 - ◆ What connectivity do they have?
 - ◆ Corporate or public network?
 - ◆ Wireless or wired?



Data Access Policy & Identity Verification Process



Who, proof, authorization and RSOP

- ◆ **Data classification access assessment**
 - ◆ Assessment proceed based on data classification?
- ◆ **Identity verification**
 - ◆ If sensitive is 2F verification required?
- ◆ **Policy selection**
 - ◆ Which policy best applies to access parameters?
- ◆ **Resultant Set of Policy Resolution (RSOP)**
 - ◆ Which policy takes precedence?
- ◆ **Policy conflict resolution**
 - ◆ Which policy should take effect in a conflict?



Enforcement Controls



Location, what device, access method & data integrity

Multiple enforcement mitigations from which to choose:

- ◆ Firewall
- ◆ DLP
- ◆ AV/AM
- ◆ Network segmentation
- ◆ Sandboxing
- ◆ Containerization
- ◆ VPN
- ◆ Virtualization
- ◆ Secure browser



Encryption Processing



Encrypt, decrypt, key management

Encryption state assessment

↳ Key management

↳ Platform assessment

↳ Decryption processing

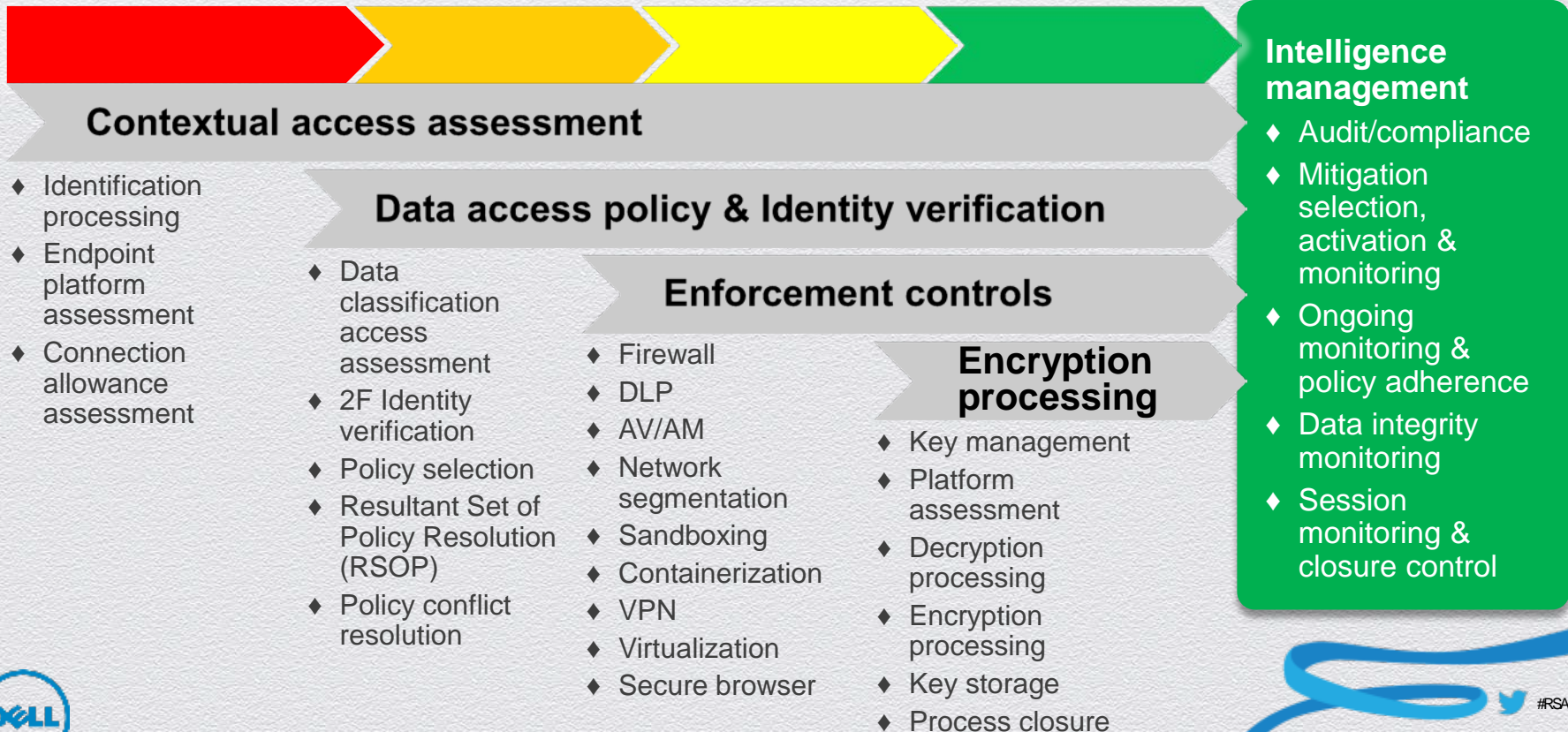
↳ Encryption processing

↳ Key storage

↳ Process closure



Data Risk Assessment Process



Data Protection Reference Architecture

Crowd sourcing
Common threats

Open source intelligence
Government /
private intelligence

Security-as-a-
Service providers

Regulatory &
compliance controls

External interfaces & intelligence

Public APIs

Risk Analysis Fabric

Data
access
request

Contextual
access

Identity
verification

Data
access
policy

Enforced
controls

Encryption
processing

Intelligence
mgmt

Access
result

Private
API's

Private
API's

Private
API's

Private
API's

Private
API's

Device

- ◆ Managed laptop
- ◆ BYOD container
- ◆ Unmanaged BYOD

Identity

- ◆ Employee
- ◆ Contractor
- ◆ Customer

Access

- ◆ Full access
- ◆ Read access
- ◆ View access

Enforcement

- ◆ Firewall
- ◆ VPN
- ◆ Virtual

Access result

- ◆ Data downloaded
- ◆ Container access
- ◆ Data streaming



#RSAC

RSACONFERENCE2014

RSACONFERENCE2014

FEBRUARY 24 - 28 | MOSCONE CENTER | SAN FRANCISCO



Thank You