

# RSA® Conference 2016

Singapore | 20-22 July | Marina Bay Sands

SESSION ID: GPS2-R09

## **Govern every identity, Inspect every packet. Transform IT to the Department of YES**



Connect **to**  
Protect

### **Marco Zhang**

Senior Consultant  
Identity & Access Management, API  
Dell, Inc.

### **Kent Shuart**

Director, SonicWALL Product  
Marketing, Asia  
Dell, Inc.  
Twitter: KentShuart



#RSAC

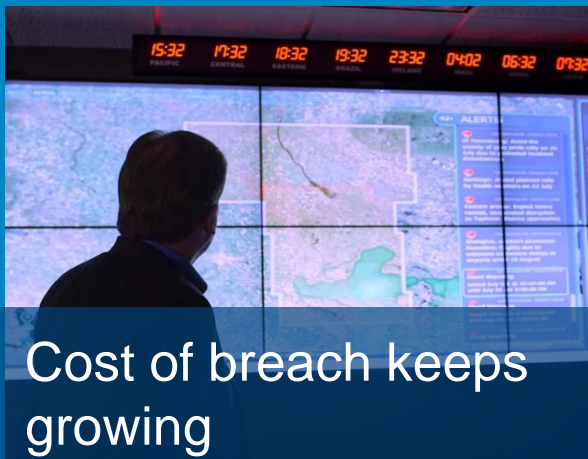
# What you will hear



- Security continues as a key business concern
- Malware continues to become more sophisticated
- A simplified approach to network security
- Why identities are important
- The Questions to ask for identity management
- The right way for identity management



# Growing security concern and costs



**\$3.8M** - Average cost of a data breach. Each lost / stolen record costs \$154.

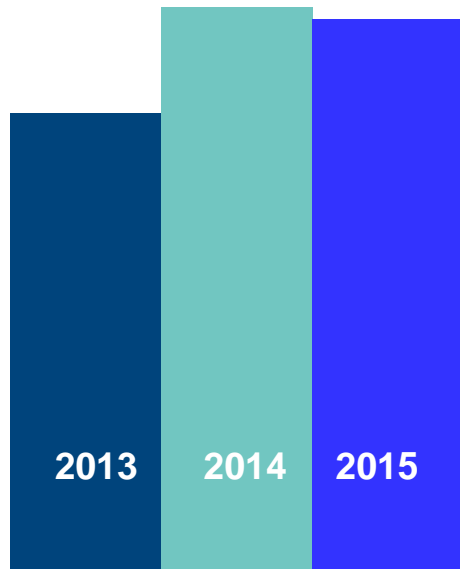


**75%** of CIOs surveyed expect to increase their security spending

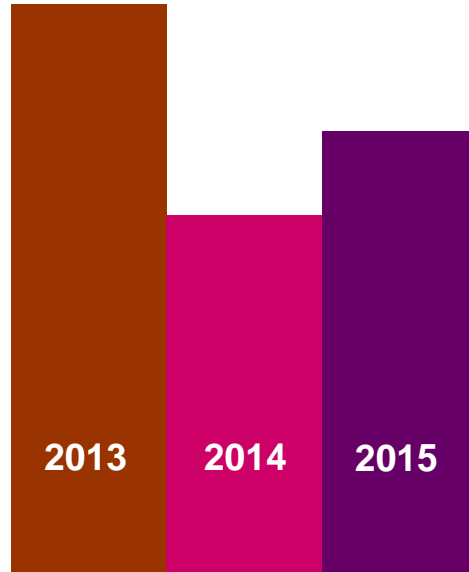


**73%** security professionals believe they will respond to a major threat in 2016

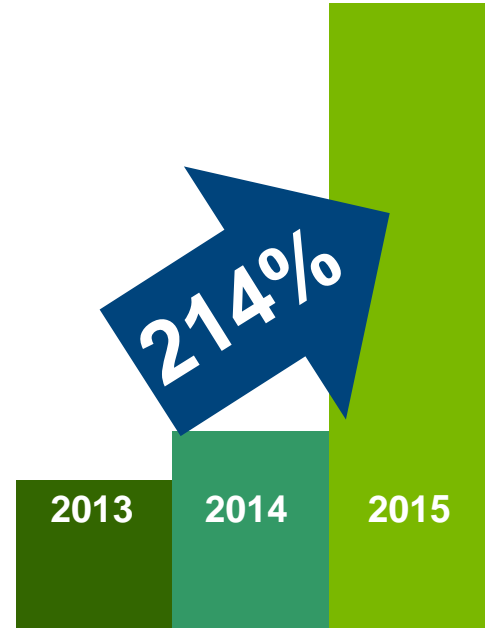
# Malware as a business



Total Breaches



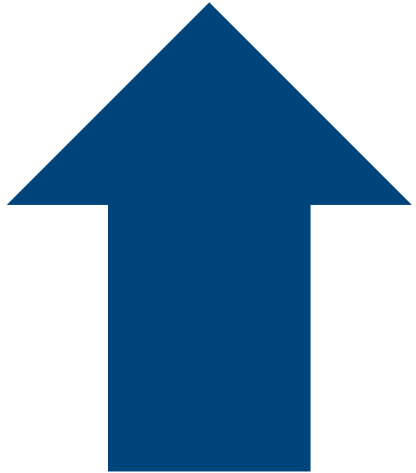
Total IDs exposed



New mobile vulnerabilities



# Malware is evolving



**New malware variants  
2014 to 2015**

INVINCIA ENDPOINT SECURITY BLOG

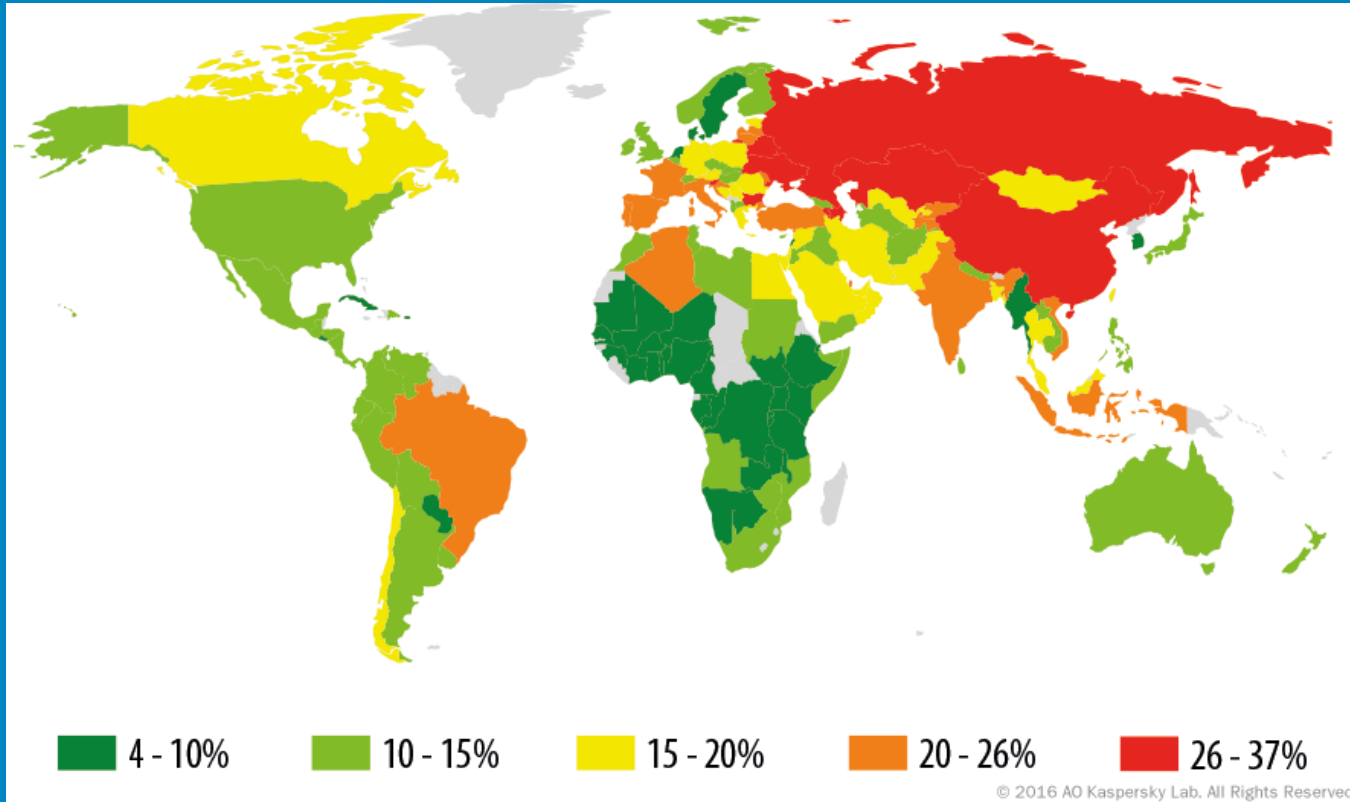
## **Two Attacks for The Price Of One: Weaponized Document Delivers Ransomware and Potential DDoS Attack**

By IKENNA DIKE

May 18, 2016



# Countries where users faced the greatest risk of online infection



Source – Kaspersky Q1 malware report



# Conclusion

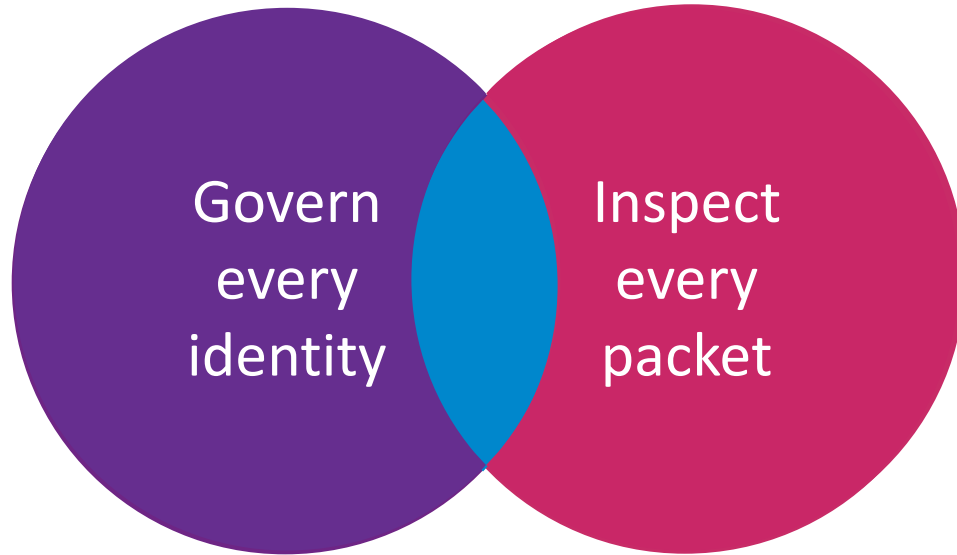
Malware is big business, with sophisticated code  
And improved business models

Eroding confidence in keeping data safe  
Online behaviors will begin to change

Companies will start to scrutinize their partner's  
security capabilities



# Consider a different approach





- The basics
  - NO file size limitations – **OUT OF THE BOX**
  - Inspect encrypted HTTPS files
- Our two factor inspection approach
  - Static
  - Dynamic

## Capturing new threats



## Problems

- There is limited memory available on the firewall
- Encrypted malware
- Malware evades the sandbox analytics
- First time attacks are still effective

## Solutions

- Use the cloud where there are no memory or file size limitations
- Inspect encrypted sessions
- Multiple inspection engines with multiple analysis approaches
- Block suspect files until they are analyzed

# The benefits of inspecting every packet



- Higher security effectiveness
- Faster response
- Protection in the first attack
- Reduced total cost of protection

# Govern Identity - Story mountain analogy



#RSAC

Name:

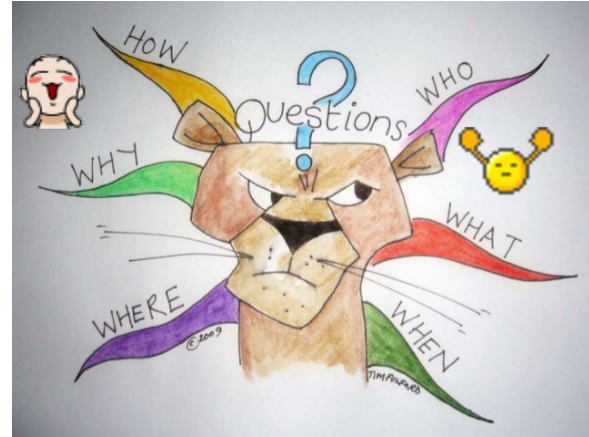
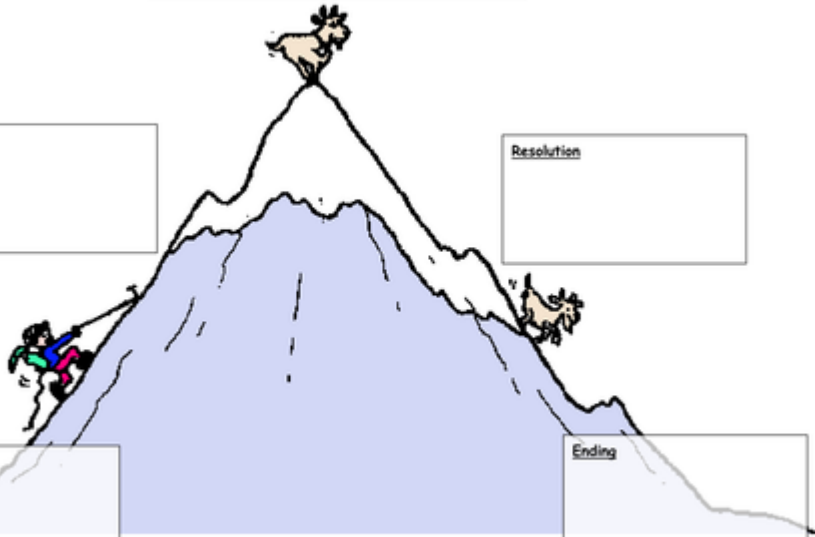
Problem

Build Up

Resolution

Introduction

Ending

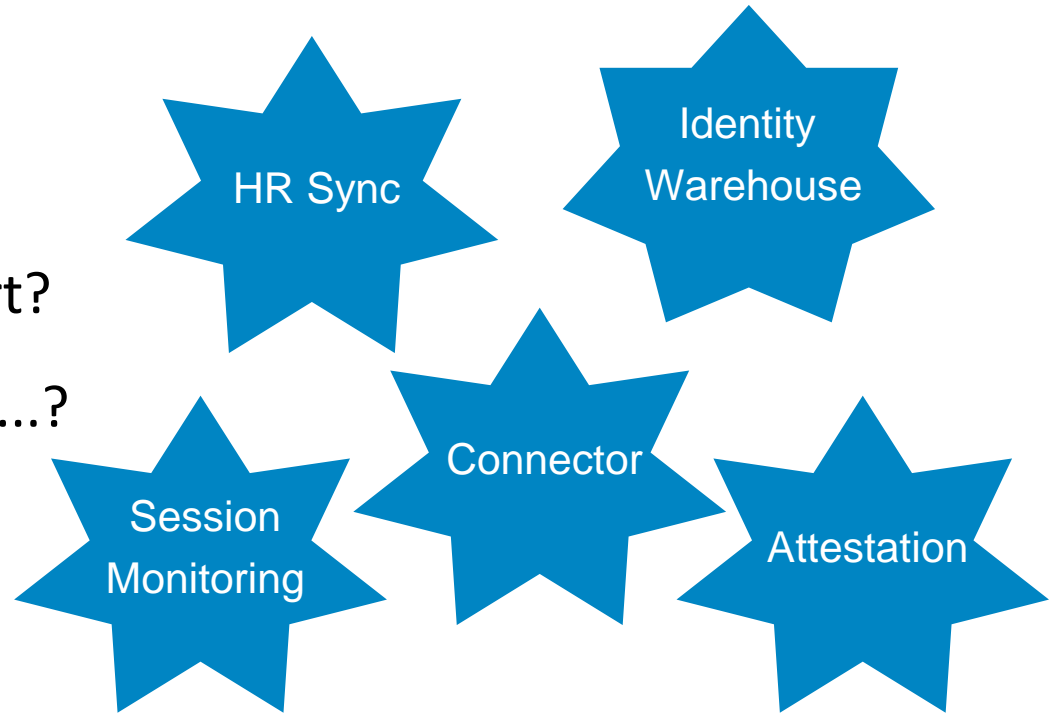


# Govern Identity – The people



#RSAC

- Who is this ...?
- Who does he report to?
- Who are your direct report?
- Who need access on that ...?
- Who did ...?
- What has access on ...?

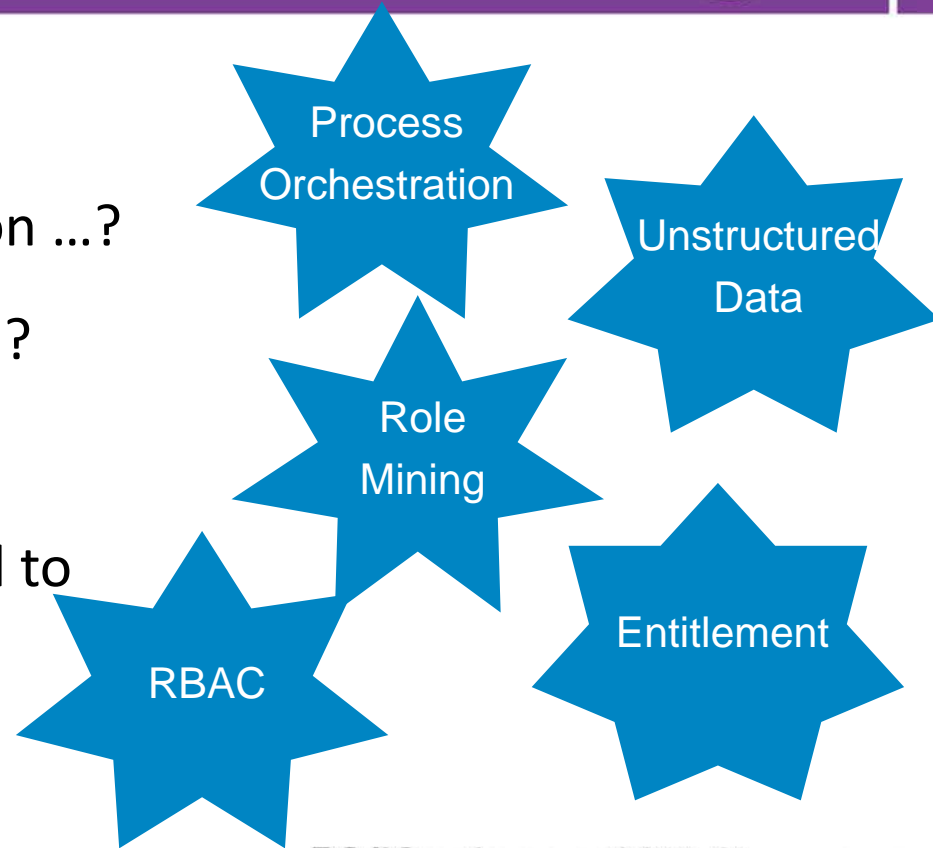


# Govern Identity – The access



#RSAC

- What role does he play in ...?
- What accounts does he have on ...?
- What access rights does this ...?
- What did he do on ...?
- What business processes need to be put in place ...?



# Govern Identity – The timing



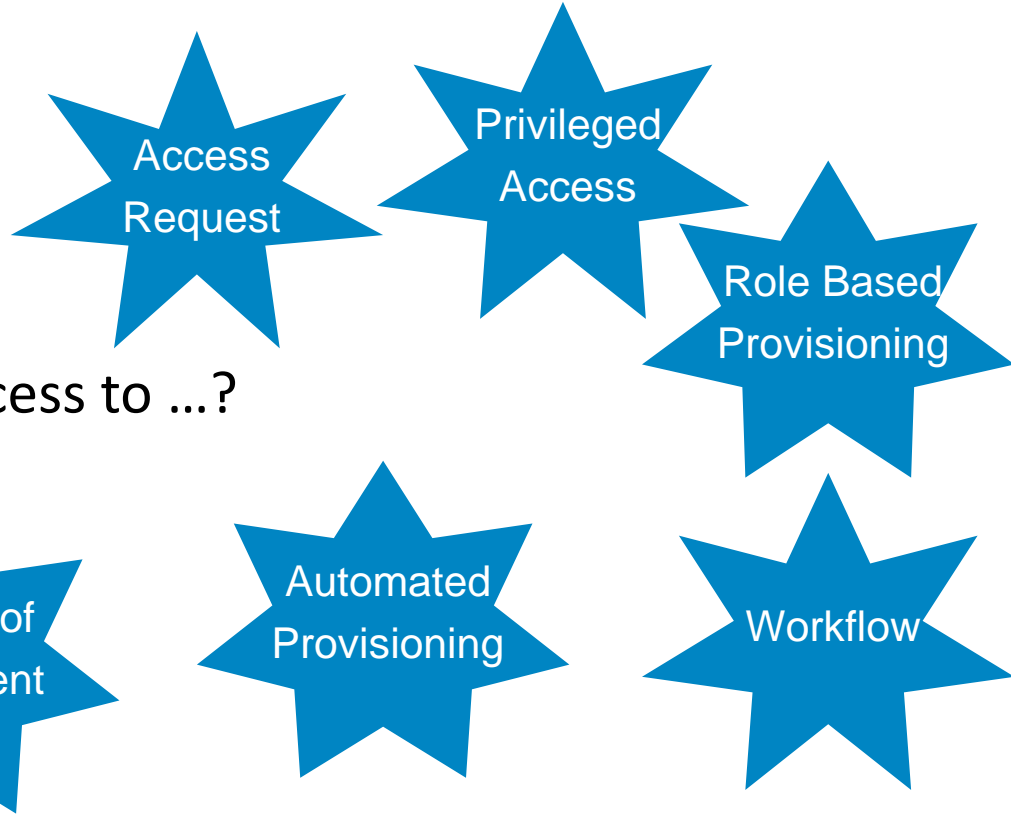
- Where is the access from ...?
- When do you need to access ...?



# Govern Identity – The right way



- How do I get ...?
- How accounts should be provisioned ...?
- How did get he has the access to ...?
- How risky is ...?





# Govern Identity – In a nutshell



#RSAC



The right people



have the right access



to the right stuff



at the right time

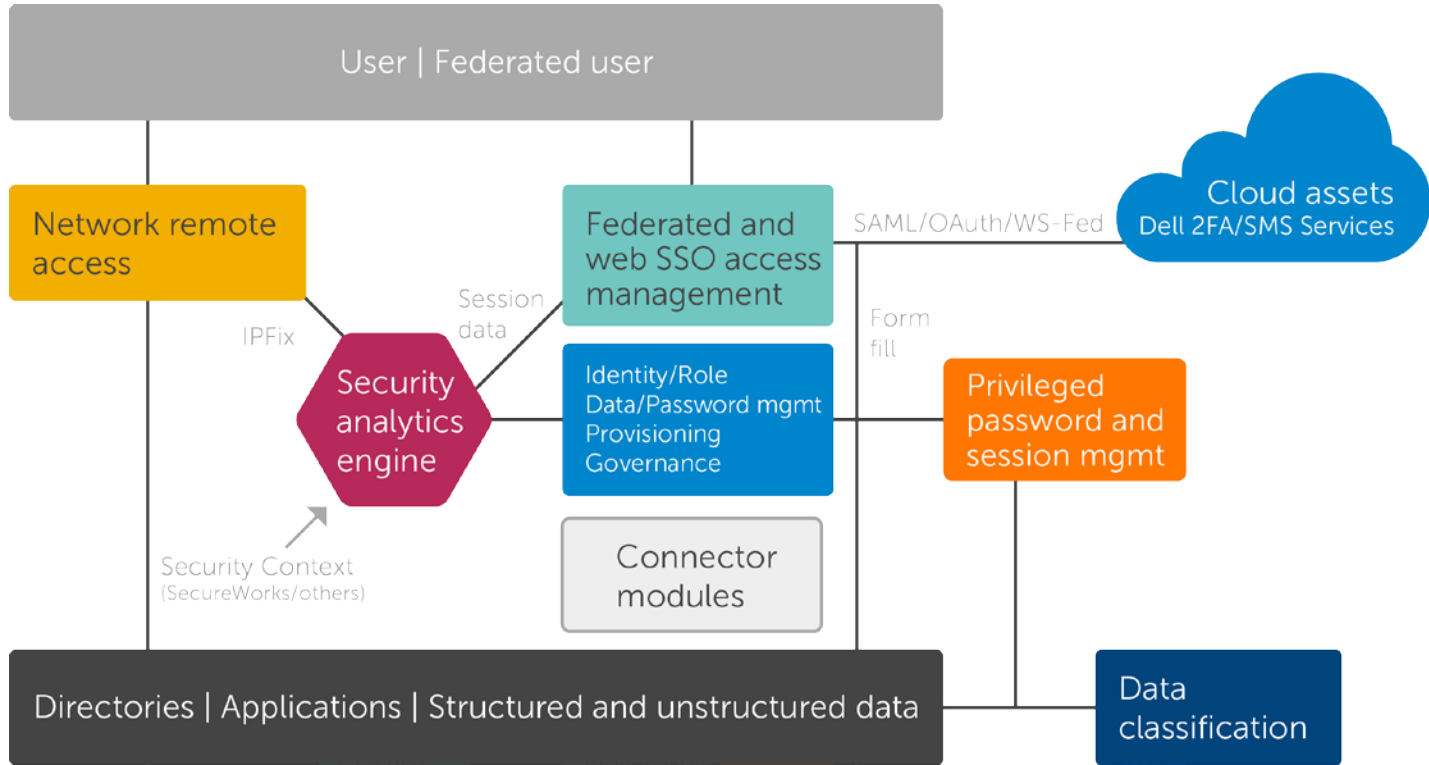


in the right way

# Govern Identity – Reference architecture



#RSAC



# Actions you might consider



- Next week
  - How old is your firewall, is it inspecting encrypted files
  - You need identity governance, so prioritize and pick the low hanging fruit
- Over the next three months
  - Consider a Pen test – by reputable organizations
  - Start educating your staff and partners on security
  - Start planning your IAM strategies

Thank you

DEPARTMENT OF  
YES

# Questions

