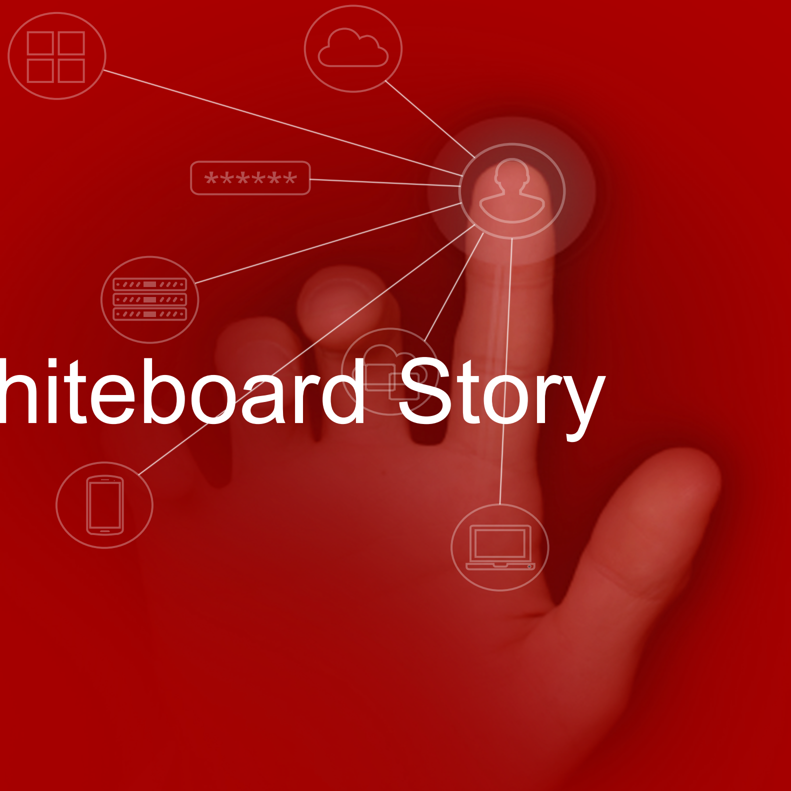
Centrify®



Identity Platform Whiteboard Story

Version 2.0

January 2016

Author: Mark Gibson

Introduction

Good morning and thank you for sharing your time with me today.

(SALES PROLOGUE)
In preparing for our meeting today, I tried to put myself in your shoes and think of some of the questions I thought you might have for me.

I thought you might want to know:

1. How familiar are we with compliance in your industry?
2. Who else have we helped that is in your industry?
3. What are the best-practices for managing identity in your industry?

1 Are these some of your questions?
Do you have any others? (Write their questions on the whiteboard – not the 3 you thought they might have)

It will take about X minutes to address your questions; then, if its OK with you I'd like to ask you some questions to figure out if we can help you.
(Answer their questions: Facts, Images, Stories)

Did I answer your questions?
I have a question for you….

2 What do you see as the the biggest security threats to your business? (capture them on the whiteboard)

3 Verizon's 2016 DBR report says >63% of all data breaches are caused by weak, stolen or default passwords.
Write #1 attack vector, compromised identity (in red).

4 Why don't I draw up the axes for a conversation around identity risk. I'm going to shake it up a bit because this chart will go from high risk to low. (Draw, label axes and title - Identity risk)
The biggest risk factors in protecting identity are privilege and passwords.

5 Hackers are indiscriminate, threats can come from anywhere, targeting any and all users Draw threats in red

OBJECTIONS
We are already working with CYBERARK/OKTA/BeyondTrust/PING

RESPONSE:
How's that working for you?

Great, so you've got 100% risk protection for all user identities across Cloud, Mobile and DC?
(If the buyer says yes- ask them what they have done to achieve it)

Introduction

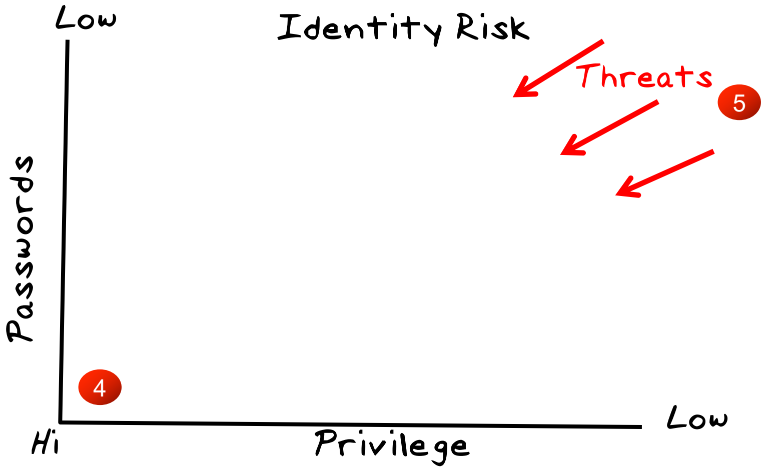
Questions 1

1. ....
2. ....

Threats- 2

#1 Attack Vector 3

Compromised Identity



Identity and Risk

Lets talk more about identity and risk in light of this constant threat.

1 Draw in the danger zone.
The password danger zone is entered when we use simple username and passwords or single factor authentication, there are too many passwords and too many privileged accounts sharing passwords.– this is how hackers got into Home Depot.

2 **Have you thought about how many identities an individual has at your company?** Identity silos are high risk. (write in danger zone).

3 The Privilege danger zone is entered when users can access more infrastructure and are authorized to do more on those resources than they need to do their job. Too much access is another major risk factor (write it in danger zone).

4 Without role-base access control it is difficult to give users the rights they need to do their jobs, whether they are employees, contractors 3rd. Parties or outsourced IT. There is no differentiation between privileged and ordinary users. With no policies to provide context for controlled access and with no auditing it is impossible to have complete visibility across what users can do and what they have done.

Insight:

Policies can provide context through granular authentication for end-users, step-up access for App admin; commands are time-based, geo-based, outside IP range for privileged users),

Identity and Risk

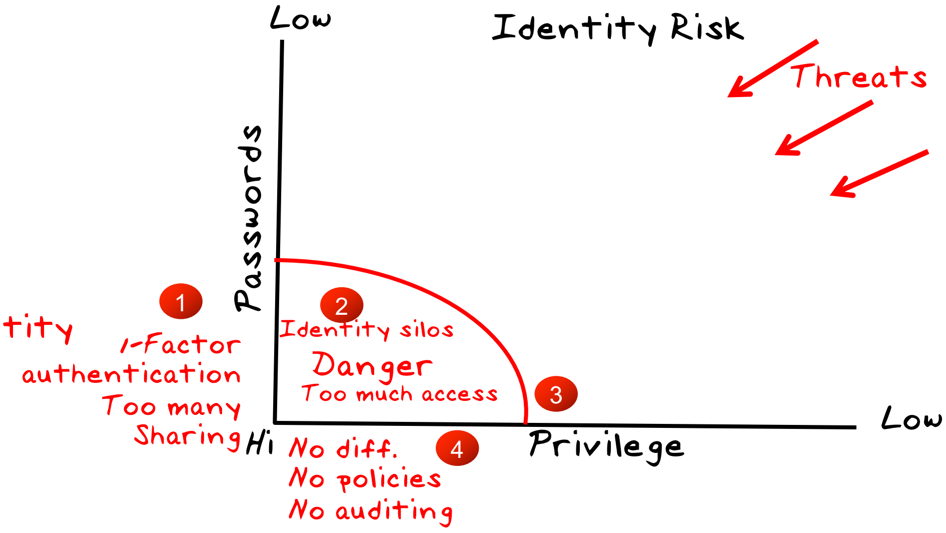
Questions

1. ....
2. ....

Threats-

#1 Attack Vector

Compromised Identity



The Enterprise Perimeter

Why don’t I quickly draw a typical Data Center and we can build our risk discussion from here.

1 Draw the data center, servers, storage, administrator.
Write the names of their major apps.
(You should know the major on-prem apps they use based on your pre-call prep)
Are you using Multi Factor Authentication to protect these applications?

2 This is the Firewall and traditional perimeter defense for the data center.

3 Draw in the Admin: This admin and their privileges are the prime target for hackers as they hold the keys to the kingdom

What about BIG DATA? Is it on-prem or Cloud based? (Write BIG DATA in the picture if they have it)

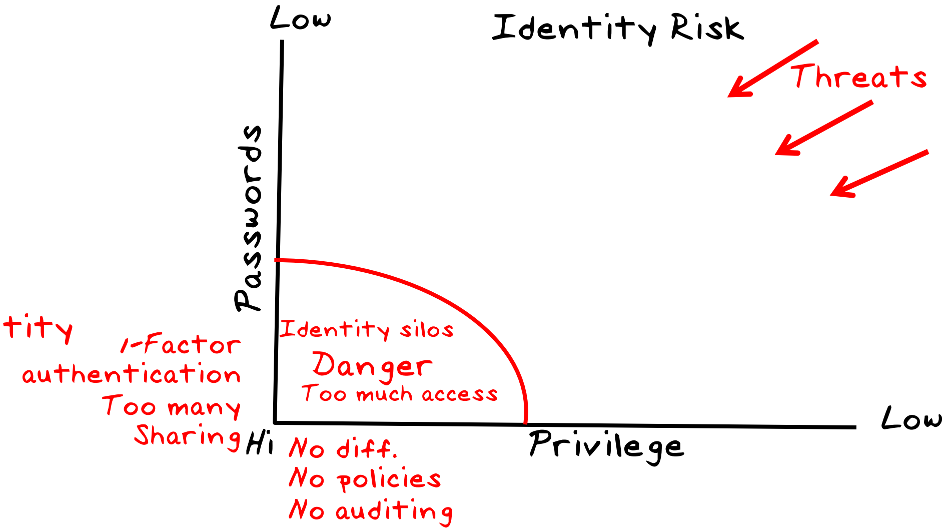
Encourage the customer to contribute to the whiteboard

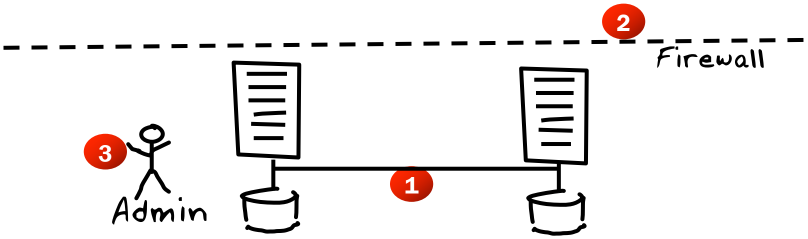
The Enterprise Perimeter

Questions
1. ....
2. ....

Threats-

#1 Attack Vector
Compromised Identity





A Changing Landscape

1 Draw the cloud and label it SaaS, IaaS

Are you adopting Infrastructure as a service (IaaS)?
What are your biggest challenges in moving to the Cloud?
Where are you with O365?

2 Draw the users. Write Employees, Contractors, 3rd parties, Outsourced IT
Are you outsourcing IT or application development? How would you know if one of your ITO providers had malware on their Laptop?

3 **Are you using a VPN to provide remote access for IT administrators?** Write VPN
In a recent Forrester survey 100% of companies outsource some of their application development and infrastructure. Ninety-seven percent of decision-makers claimed that they allow employees and outsourced vendors privileged access using a VPN, or shared access method.

4 **Are you enabling on-demand privileged access to your administrators?**

BONUS QUESTIONS
Are you planning password federation with any external parties –(indicates CIS potential)

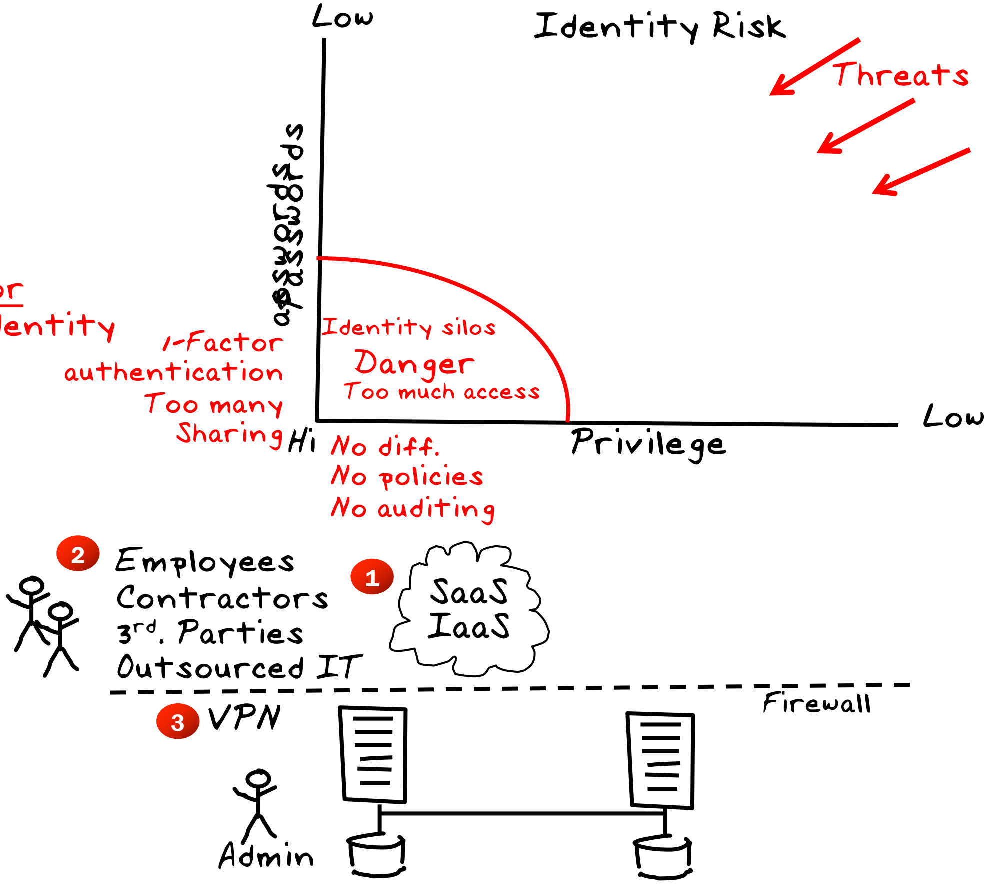
What about big data?
- (indicates CSS potential)

A Changing Landscape

Questions
1. ....
2. ....

Threats-

#1 Attack Vector
Compromised Identity



Threats and Impact

Earlier you stated the biggest threats to your business are XXX and YYY (you wrote this down earlier).
Lets talk about these risks by way of example, (take Home Depot - or your own stories in region)

1 The Home Depot breach is instructive. (draw the hacker and the arrows in red for each step)
Hackers landed a malware Phish on an outsourced IT administrator's PC.

2 They accessed the network via the VPN using a Trojan to steal passwords, (red arrow)

3 Once inside the network they were able to elevate privilege, (red arrow)

4 Access the POS network and place malware on POS systems, (red arrow)

5 And exfiltrate credit card data. (red arrow and $dollar)

Hackers came through the front door dressed as business partners.
How do you assess what happened at Home-Depot? Is there a concern that it could happen here?
They had insurance, but the bigger issue is damage to their brand and the class-action law-suits.

An even worse story involves a certain motion picture company in Los Angeles (Rhymes with Pony).

We had multiple proposals on the table over several years with this company. They got really excited about our offering for Multi Factor Authentication, but the now ex-CIO declined our proposals and chose to do nothing. "It won't happen here and I am prepared to take the risk" are famous last words.

This company announced they were breached in Nov. 2014. Multi Factor Authentication could have prevented the Sony, Home Depot, Anthem, OPM and hundreds of other breaches. What will this cost them?

How do you rate your ability to control administrative privilege on scale of 0-10, where 0 is no control and 10 is, - users only have the access they need to do their jobs? (put an X indicating their score along the X axis)

How do your rate your protection against compromised passwords on a scale of 0-10; where 0 is - users have multiple passwords, passwords are being shared, and basic authentication is all that is

QUESTIONS

What about compliance audits, when was your last one?

How did you fair?

Are auditors asking you who can do what" and to explain what they can do with elevated privilege?

Threats and Impact

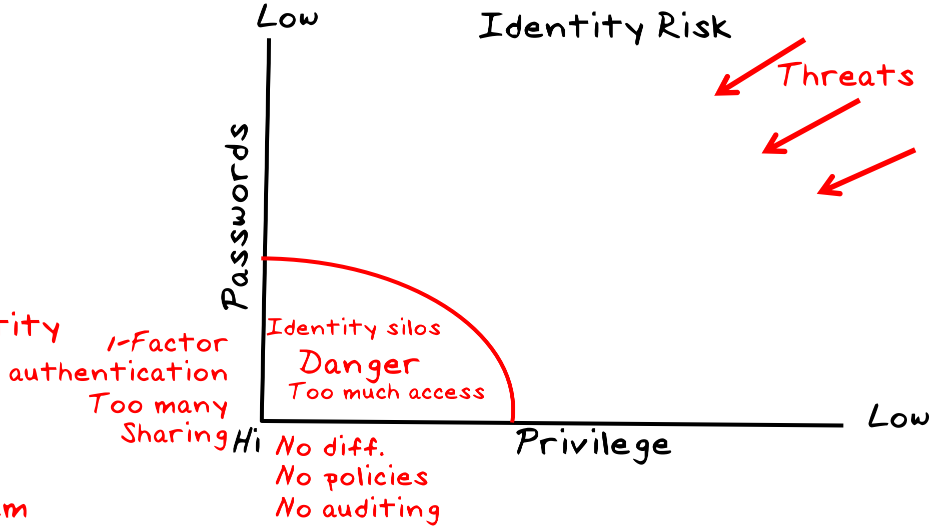
Questions

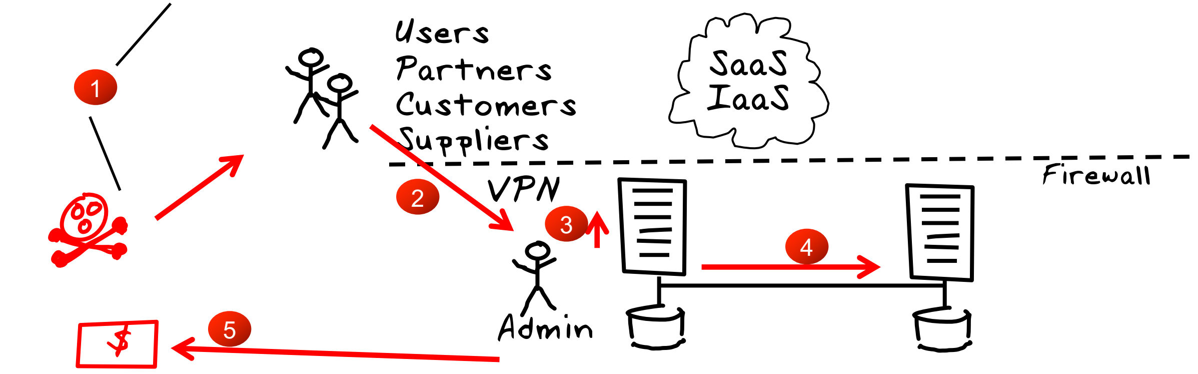
1. ....
2. ....

Threats-

#1 Attack Vector

Compromised Identity





Best Practices - Case Study

We all know that at some point hackers will get in. To reduce risk, we need to protect the identity of all users and systems against attack. But how?

1 A case study of one of our customers, a regional US bank could be useful.

(Situation) IT security administrators at a regional US bank were struggling to provide context in granting outsourced IT contractors privileged access to infrastructure.

(Complication) Offshore IT contractors were considered a high risk– the bank wanted to restrict privilege and more tightly control access to certain systems.

(Turning Point) The Bank used Active Directory and wanted to centralize control and implement a single identity to reduce risk. They evaluated point solutions, but they added complexity and left security gaps. They decided to implement our privilege service.

2 (Resolution) We helped them implement Multi Factor Authentication on Server login and on privilege elevation. Draw green check marks

3 Users login as themselves with a single identity, no shared accounts and MFA to login and elevate privilege.

4 The bank adopted policy to provide context and least privilege and access: (administrators only get credentials for,- and access to, that which they maintain). With our privileged session monitoring and access reporting, audit & compliance efforts for privileged accounts are more efficient and effective.

5 Point products provide good, but fragmented protection, and add complexity (draw black arc, write good)

6 Best-practices require an integrated holistic approach to managing identity. (Draw the green arc, write Best).

7 We helped our customer to reduce risk and move from the danger zone to the best zone (Draw green narrow)

INSIGHT
Tie your case study back to their relevant pain, don't try to hit every point.

Be prepared to discuss Google's BeyondCorp initiative. Google no longer trusts the network, they are going totally Cloud. They are Implementing all of Gartner's identity best practices recommendations and more.

Google are building their own identity solution, but you can buy it from Centrify

OBJECTIONS

Best Practices - Case Study

Questions

1. ....
2. ....

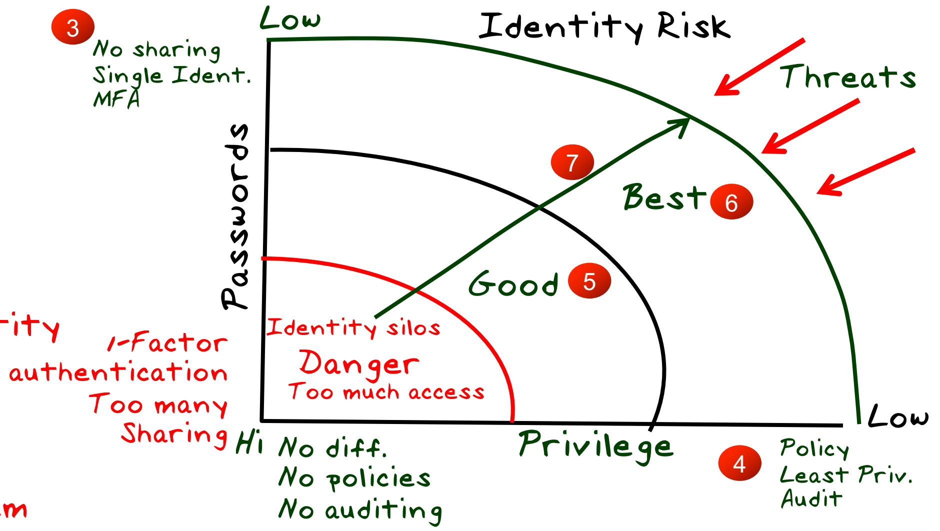
Threats-

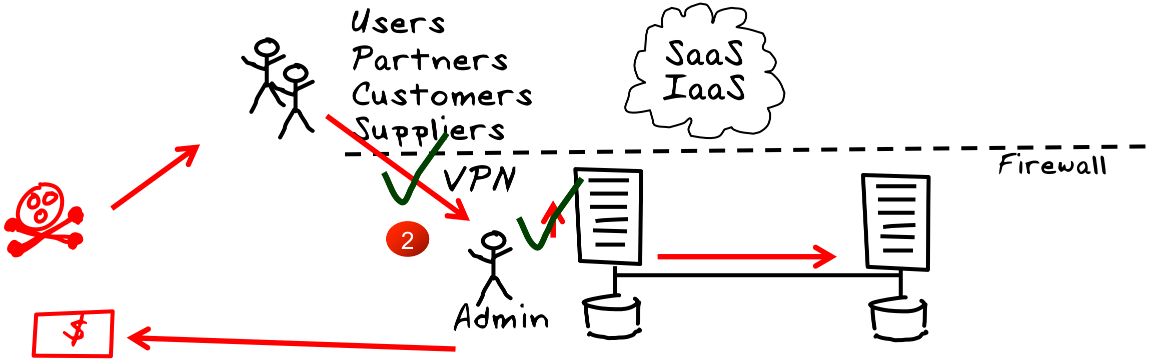
#1 Attack Vector

Compromised Identity

Home-Depot/Anthem

1 Case Study





Centrify Solution

1 In summary, we believe that Identity is the new perimeter (Draw green circle around everything)

2 We unify identity and protect access to on-premises and cloud-based infrastructure for employees, contractors, 3rd parties, and outsourced IT to reduce the risk of your organization being breached.(put a green check mark over the users, Cloud and all the red arrows and put a squiggly line over the money leaving the circle)

3 Cross platform MFA protects your infrastructure. If a privileged credential is stolen, an in progress attack will be stopped on remote session initiation, server login or when leveraging privilege.

4 Because we capture all privileged sessions centrally, and tie activity to an individual we are able to provide better visibility over "who did what" for regulatory compliance and forensic investigation.

5 This enables Centrify customers to secure access to infrastructure, reduce risk of data breach, and reduce the complexity of managing security in today's hybrid IT world.

6 I'd like to propose the following Next Steps

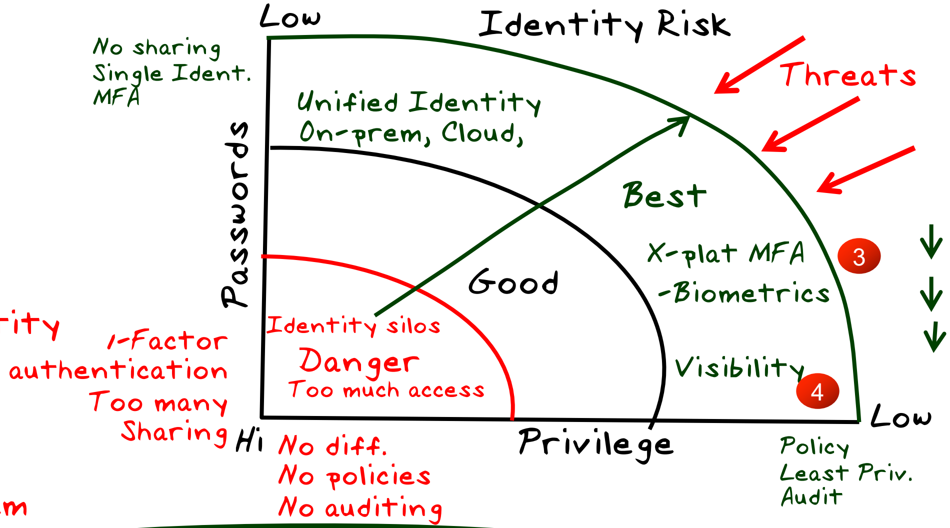
OBJECTIONS

Centrify Solution

Questions
1. ....
2. ....

Threats-

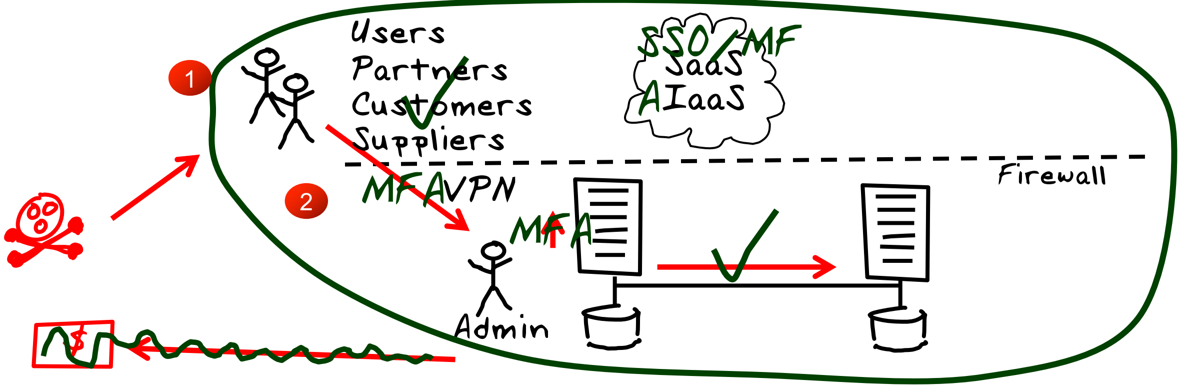
#1 Attack Vector
Compromised Identity



Case Study

Centrify
Protect Identity
↓ Risk
↓ Complexity
↓ Hassle
5

Home-Depot/Anthem



6 Next Steps

Appendix: Maturity Level Privileged A/Cs

Advanced

- Centralized personal accounts, roles/rights
- Non-human priv. A/C’s Competitive SAPM in place, (Centrify CPS)
- Audit: SIEM + native event logs: Win/Unix
- Competitive session-level audit (DirectAudit)
- Window, possible Avecto/BeyondTrust at desktop, GP’s on servers, admins with too broad access

Typical

- Personal A/C’s and Sudo in use: A/C’s local, in NIS?, LDAP, AD?
- Non-human priv. A/C’s: Larger companies possibly vault, smaller, probably manual
- Audit: Keylogger on UX, event logs SIEM on Win
- “I can do everything with GP’s” attitude on Win

Laggards (need to do something ASAP)

- Privileged A/C’s are shared
- No personal A/C’s on Nix, no Sudo
- No competitive products
- Audit: probably reactive, sys logs
- “I can do everything with GP’s” attitude on Win

Maturity Level – End Users, some Privileged

Increase in Shadow IT

- Here lies problems and opportunity
- No real idea what's going on
- Maybe looking at CASB

Multiple SaaS Apps in Use (Sanctioned or not)

- Multiple identities
    - Password issues – reused, weak, bad hygiene
    - Stale identities (leavers, dormant A/C's)

On Premises Apps

- Enterprise SSO in place?
- Multiple identity stores
- Traditional old style IAM solution syncing identities

Definition of Privileged User has Changed

Infrastructure Privileged User

- Traditional privileged IT user, can screw up infrastructure if breached
- Employee or external

Business Privileged User

- Access to sensitive data
- Originally in on-prem apps, now SaaS > risk
- Employee

Ad-hoc workstation Privileged User

- Needs privileges to add printers
- All local machine
- Majority Win, Mac
- Anyone who has a device supplied by IT
- “Everyone needs privilege some time”

Remote Access, non-IT supplied device

- BYOD for mobile, laptops etc.

According to SANS…

SANS CSC 5-1 - Minimize administrative privileges and **only use administrative accounts when they are required.** Implement focused auditing on the use of administrative privileged functions and **monitor for anomalous behavior**.

SANS CSC 5-6 Use **multifactor authentication** for all administrative access, including domain administrative access. Multi-factor authentication can include a variety of techniques, to include the use of smart cards with certificates, One Time Password (OTP) tokens, and biometrics.

SANS CSC 5-8 Administrators should be required to access a system using a fully logged and non-administrative account. Then, once logged on to the machine without administrative privileges, **the administrator should transition to administrative privileges using tools** such as Sudo on Linux/UNIX, RunAs on Windows, and other similar facilities for other types of systems.

SANS CSC 11-4 Manage network devices using **two-factor authentication** and encrypted sessions.

SANS CSC 12-6 Require all **remote login** access to use **two-factor authentication**.

SANS CSC 14-6 Enforce **detailed audit logging** for access to nonpublic data and special authentication for sensitive data

SANS CSC 16-11 Require **multi-factor authentication** for all user accounts that have access to sensitive data or systems.

Addressing SANS Critical Security Controls

SANS CSC	Centrify Identity Platform
SANS CSC 5-1 - Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.	• Restricts access methods and privileges based on job role • Enforces least-privilege rights management by limiting admins to a specific set of tools and commands • Captures complete admin session details: who accessed the system, what commands they entered, and the system output • Enables both real-time and historical monitoring of user sessions, and features robust search and reporting capabilities
SANS CSC 5-6 Use multifactor authentication for all administrative access, including domain administrative access. SANS CSC 12-6 Require all remote login access to use two-factor authentication. SANS CSC 16-11 Require multi-factor authentication for all user accounts that have access to sensitive data or systems.	• Allows for smart card logins on Macs and Linux desktops • Cloud login supports many types of multifactor authentication, including smart cards • Provides Role Based Access Controls so only approved personnel have the ability to access certain applications or raise their privileges for specific tasks
SANS CSC 5-8 Administrators should be required to access a system using a fully logged and non-administrative account. Then, once logged on to the machine without administrative privileges, the administrator should transition to administrative privileges using tools	• Links all entitlements and actions to a single, definitive and centrally managed user identity in Active Directory, allowing users to log in as themselves • Provides Role Based Access Controls so only approved personnel have the ability to access certain applications or raise their privileges for specific tasks
SANS CSC 11-4 Manage network devices using two-factor authentication and encrypted sessions	• Allows the management of network devices only after the successful multifactor authentication of an individual • Provides encrypted sessions to network devices without a VPN
SANS CSC 14-6 Enforce detailed audit logging for access to nonpublic data and special authentication for sensitive data	• Captures complete user session details: who accessed the system, what commands they entered, and the system output • Provides Role Based Access Controls so only approved personnel have the ability to view sensitive audit data

PCI DSS 3.1 Items to know

- Version 3.1 specs must be adhered to by the of June 2016
- Acronyms:
  - PCI – Payment Card Industry
  - DSS – Data Security Standard
  - ROC – Report On Compliance
- The monitoring of compliance is called an assessment and not an audit. Use of the wrong term can result in loss of credibility
- There are 12 requirements across 6 domains to PCI DSS 3.1 Specs
- The ROC is the summary of the assessment activities that verify the entity's compliance status.
- For use with customers there is a short and long version whitepaper of the details to share with customers of specific regulations and the product details

Addressing the PCI DSS 3.1 requirements

PCI Domain	Requirement	Addressed by CSS & CPS
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use the vendor-supplied defaults for system passwords and other security parameters	**Yes** **Yes**
Protect Cardholder Data	1. Protect stored cardholder data 2. Encrypt transmission of cardholder data across open and public networks	**Yes** **Yes**
Maintain a Vulnerability Management Program	1. Use and regularly update anti-virus software or programs 2. Develop and maintain secure systems and applications	**N/A** **Yes**
Implement Strong Access Control Measures	1. Restrict access to cardholder data by business need to know 2. Assign a unique ID to each person with computer access 3. Restrict physical access to cardholder data	**Yes** **Yes** **N/A**
Regularly Monitor and Test Networks	1. Track and monitor all access to network resources and cardholder data 2. Regularly test security systems and processes	**Yes** **Yes**
Maintain an Information Security Policy	1. Maintain a policy that addresses information security for all personnel	**Yes**

Notes

Notes