RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **IDY-R09**

Going Beyond the Basics: An Advanced Privileged User Management (PUM) Program

Kurt Lieber

Chief Information Security Officer
Aetna, the Health Care Benefits division of CVS Health

2018 Breach Statistics

Top 3 Breach Types:

- Hacking
- Unauthorized access ↑ **19%**
- Employee error/negligence/ improper disposal/loss

= 377 data breaches. Exposing the highest number of sensitive records at **404 million**

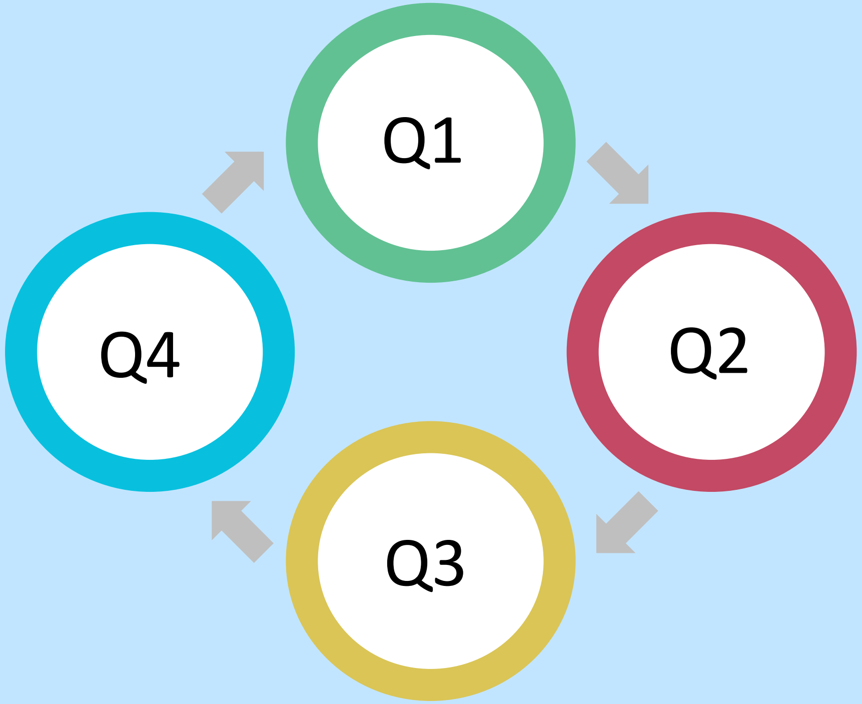
Non-sensitive records (email addresses, passwords, usernames, etc.) exposed = **addt'l 1.68 billion**

Source: Identity Theft Resource Center

Current “best practices” and reality #1

“Best Practice”:

Periodic access reviews



Reality:

“Access recertifications add a tremendous amount of value to my organization.” *-Said no one, ever…*

Top Five Myths of Periodic Access Recertifications

- People diligently review each and every access recertification request they receive.
- People are willing to take time away from their day jobs to perform a quality review.
- Reviewing access once a quarter reduces risk.
- Performing access recertifications based on a periodic schedule is effective.
- Access recertifications do more than just make compliance people happy.

Current “best practices” and reality #2

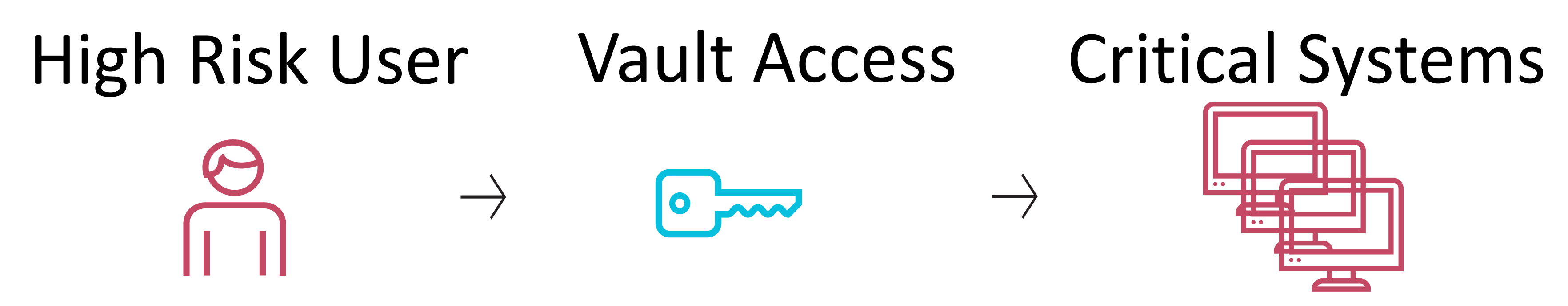
Most breaches involve compromised privileged credentials and bad actors gaining unlimited access to critical systems and data

28% of 2018 cyberattacks involved insiders

“Best Practice”: Use a password vault

Reality:

Password vaults are better than nothing, but account still exists

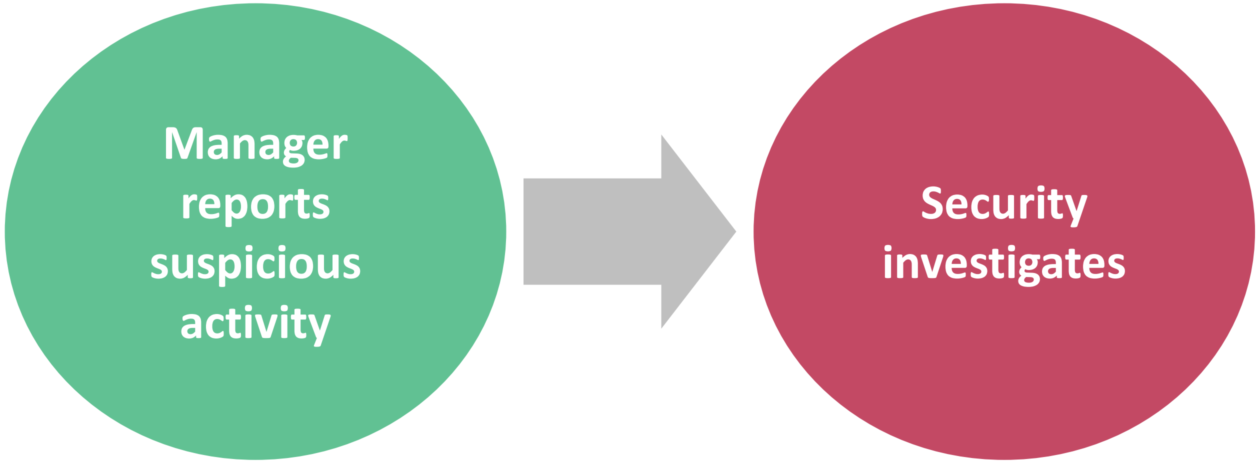


Sources: One Identity; Verizon 2018 Data Breach Investigations Report

Current “best practices” and reality #3

“Best Practice”:

Detective User Behavioral Analytics (UBA)



Manager reports suspicious activity

Security investigates

Reality:

How quickly will it be detected?

Or when the manager is on vacation?

Current “best practices” and reality #4

“Best Practice”:

Multi-Factor Authentication (MFA)

Authentication using two of the following:

- Something you know
- Something you have
- Something you are

Reality:

- MFA only binary. Once you’re in, you’re in
- Susceptible to hijacks
- Tokens can be lost or stolen
- Creates significant user friction

Current “best practices” and reality #5

“Best Practice”:

Change your passwords every 90 days

Reality:

Repeatable patterns:

ComplexPassword#1

ComplexPassword#2, etc.

Easy to guess passwords:

Spring2019!

Summer2019!, etc.

Entire Windows 8-character password space can be brute forced in under 2.5 hours

Source: Slashdot

The trouble with passwords

Most people use fewer than 5 passwords for all accounts

50%

of those haven't changed their password in the last 5 years

Reuse makes them easy to compromise

39%

of adults use the same password for many of their online accounts

They are very difficult to remember

25%

of adults admit to using less secure passwords, because they are easier to remember

There are lots of places to steal them **from**

49%

of adults write their passwords down on paper

Sources: Pew research; Telesign research

The real trouble with passwords

Most people use the minimum required length

63%

of employees had an 8-character length password

People love to use seasonal words in passwords

100%

of CVS Health password audits find seasonal words used in passwords

Domain admin account passwords are not strong enough

100%

of all Domain Admin accounts were cracked

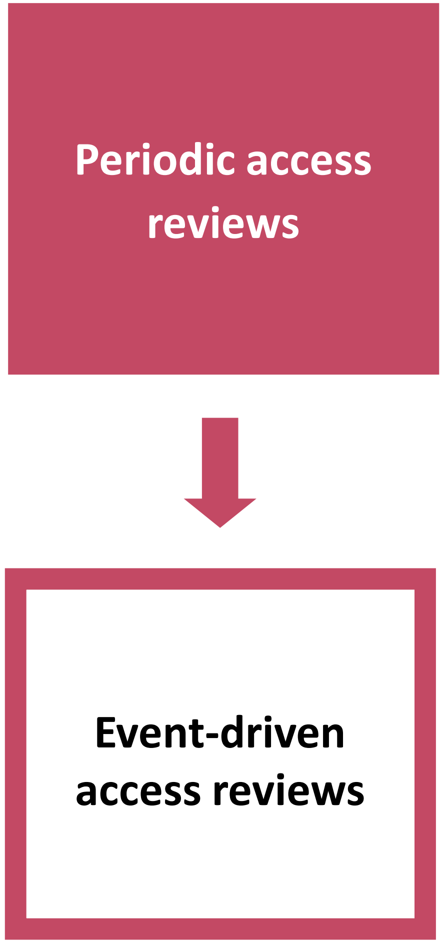
It doesn't take long to crack passwords

55%

of Aetna passwords cracked in under 2 hours

Sources: Aetna password audit

Instead, consider the following



Periodic access reviews

Event-driven access reviews

Event-driven access reviews

Where should you start?

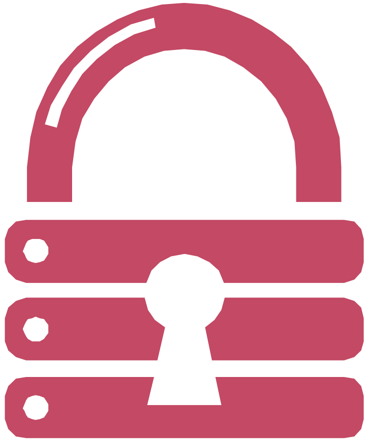
- Identify the areas of risk
- Do you need to review access to all your applications? **Why?**
- Do you need to review read-only access? **Why?**
- If someone is in the same job, year over year, does their access profile really change? **NO**
- If someone transfers to a new job, does their access profile change then? **YES!**

Checklist for a better access recertification program

- Stop reviewing low-risk entitlements

Who cares?

- Start reviewing access based on events, such as job transfer
- If you must maintain PARs, limit them to your highest-risk access, such as Privileged Access



Making it happen

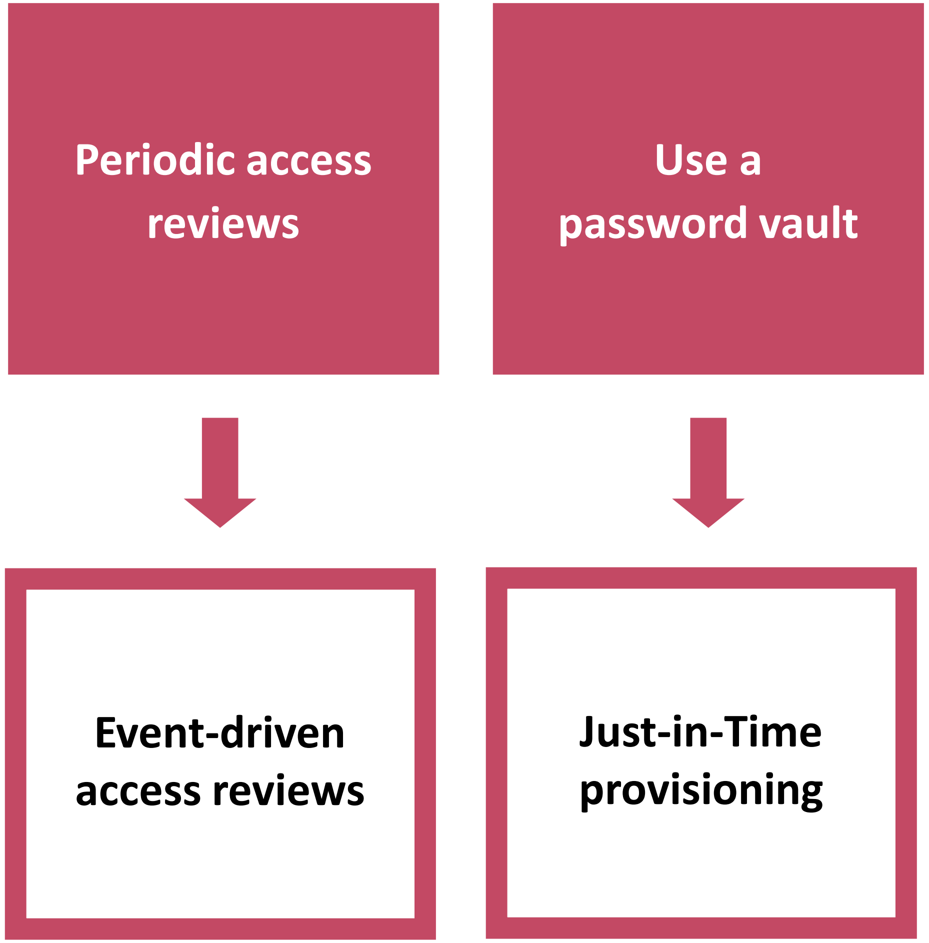
- How the heck do you sell this to the auditors?

  Facts don’t care about opinions. Use the facts.

- Start simple - baby steps.
- Implement the new controls and test them before you retire the old ones.
- Keep your friends close and your auditors closer.

  Over communicate

Instead, consider the following



Periodic access reviews

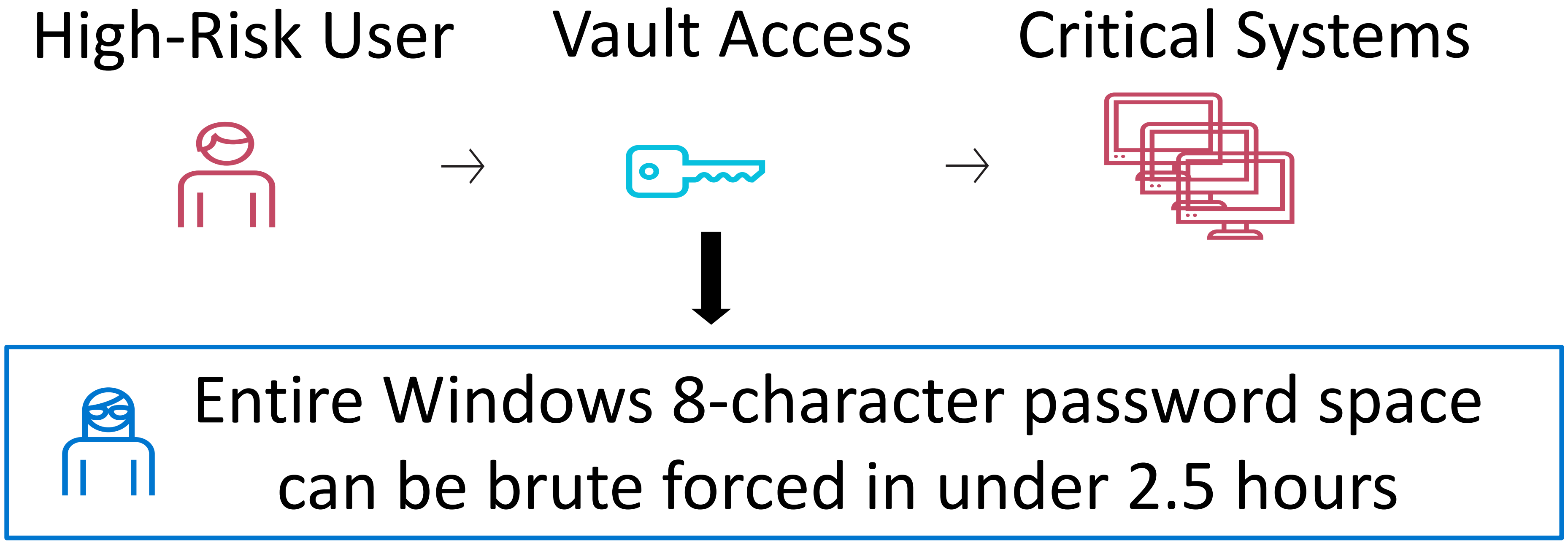
Use a password vault

Event-driven access reviews

Just-in-Time provisioning

Just-in-Time Provisioning

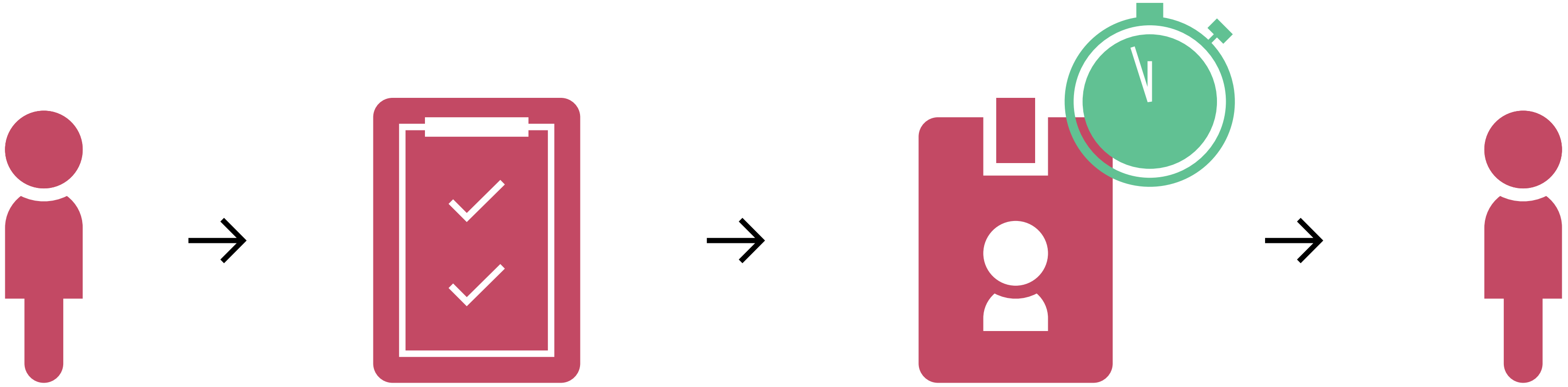
As we've seen…



High-Risk User → Vault Access → Critical Systems

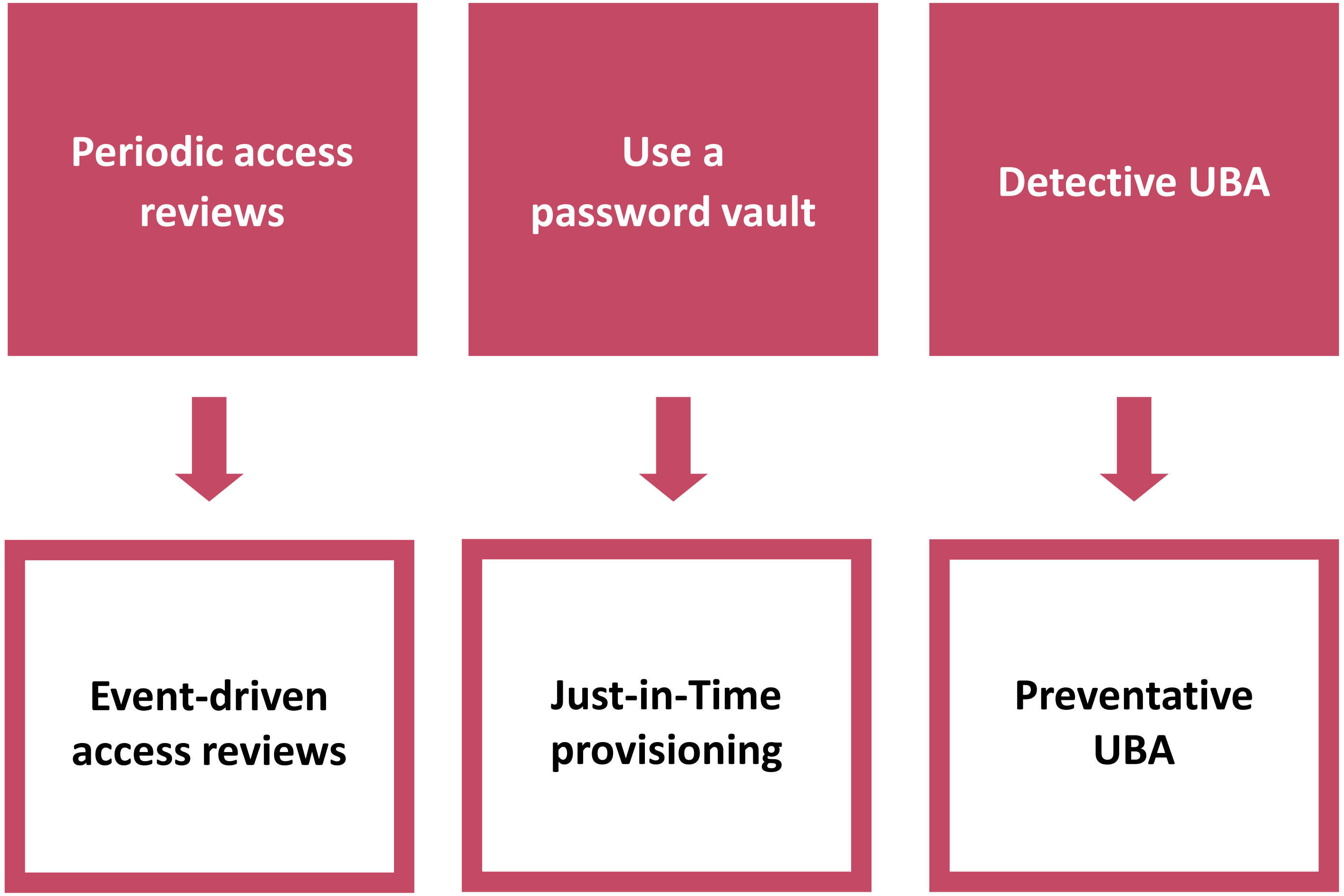
Entire Windows 8-character password space can be brute forced in under 2.5 hours

Instead...



Unlike password vaulting,
the access is not there when not being used

Instead, consider the following



Periodic access reviews

Use a password vault

Detective UBA

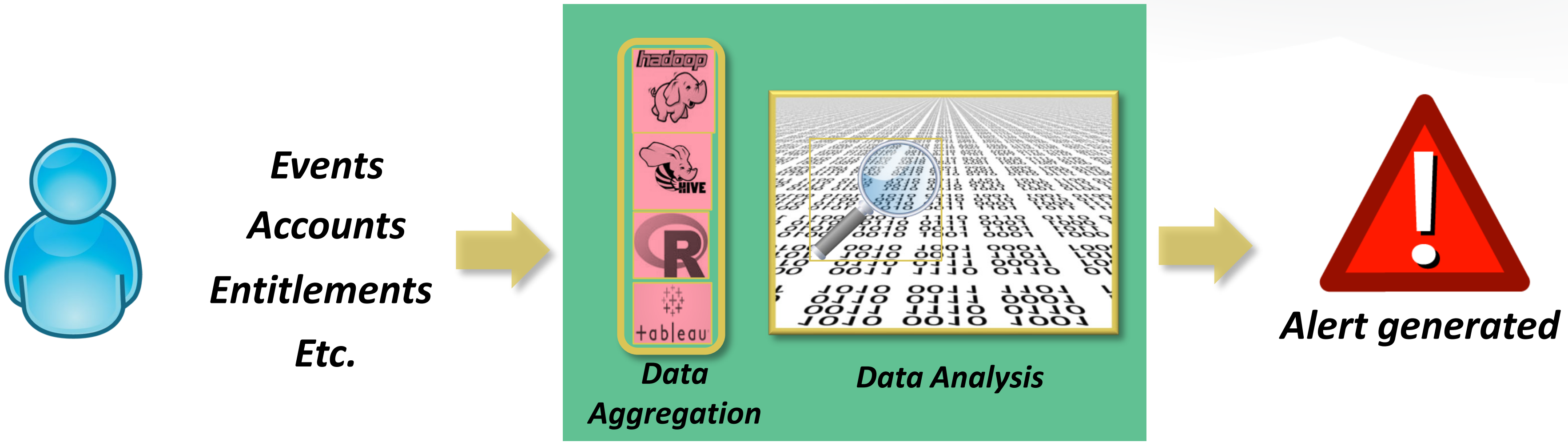
Event-driven access reviews

Just-in-Time provisioning

Preventative UBA

Detective UBA vs. Preventative UBA

Detective UBA



Events

Accounts

Entitlements

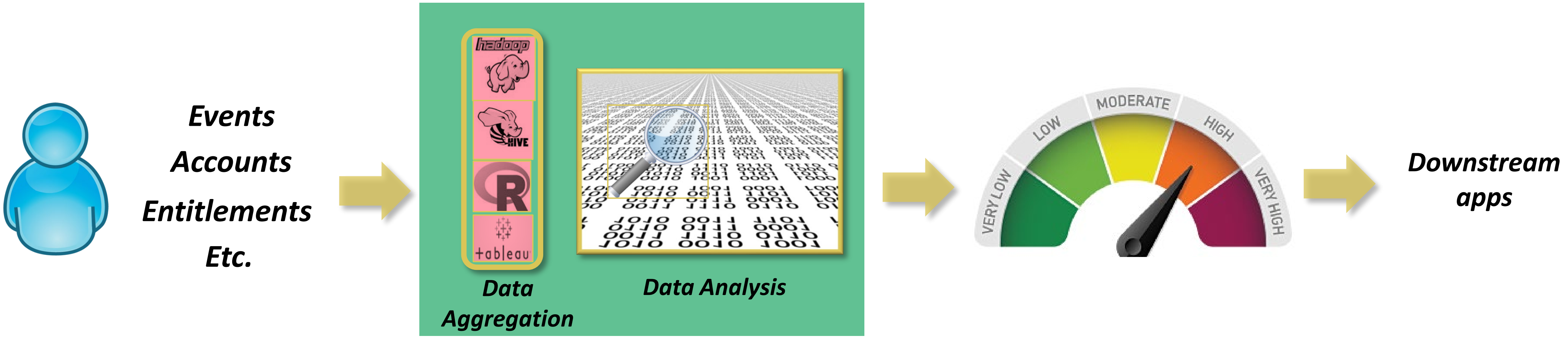
Etc.

Data Aggregation

Data Analysis

Alert generated

Preventative UBA



Events

Accounts

Entitlements

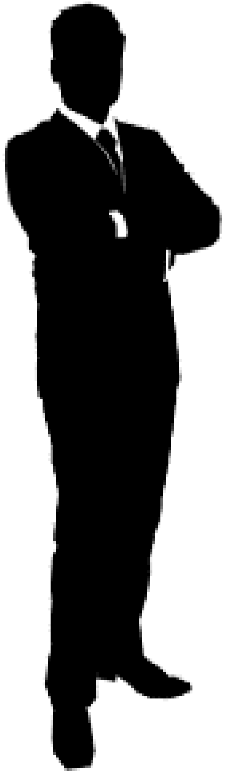
Etc.

Data Aggregation

Data Analysis

Downstream apps

Example: Privileged Password Vaulting



User attempts to check out a vaulted password

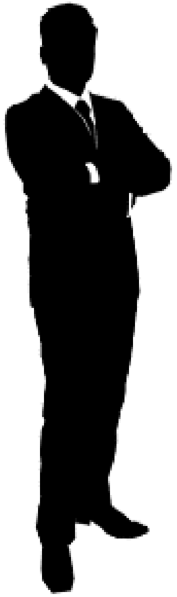
VERY LOW
LOW
MODERATE
HIGH
VERY HIGH

Risk score is evaluated

Denied/Call HelpDesk

Example: Data Loss Prevention

Using Data Loss Prevention (DLP)

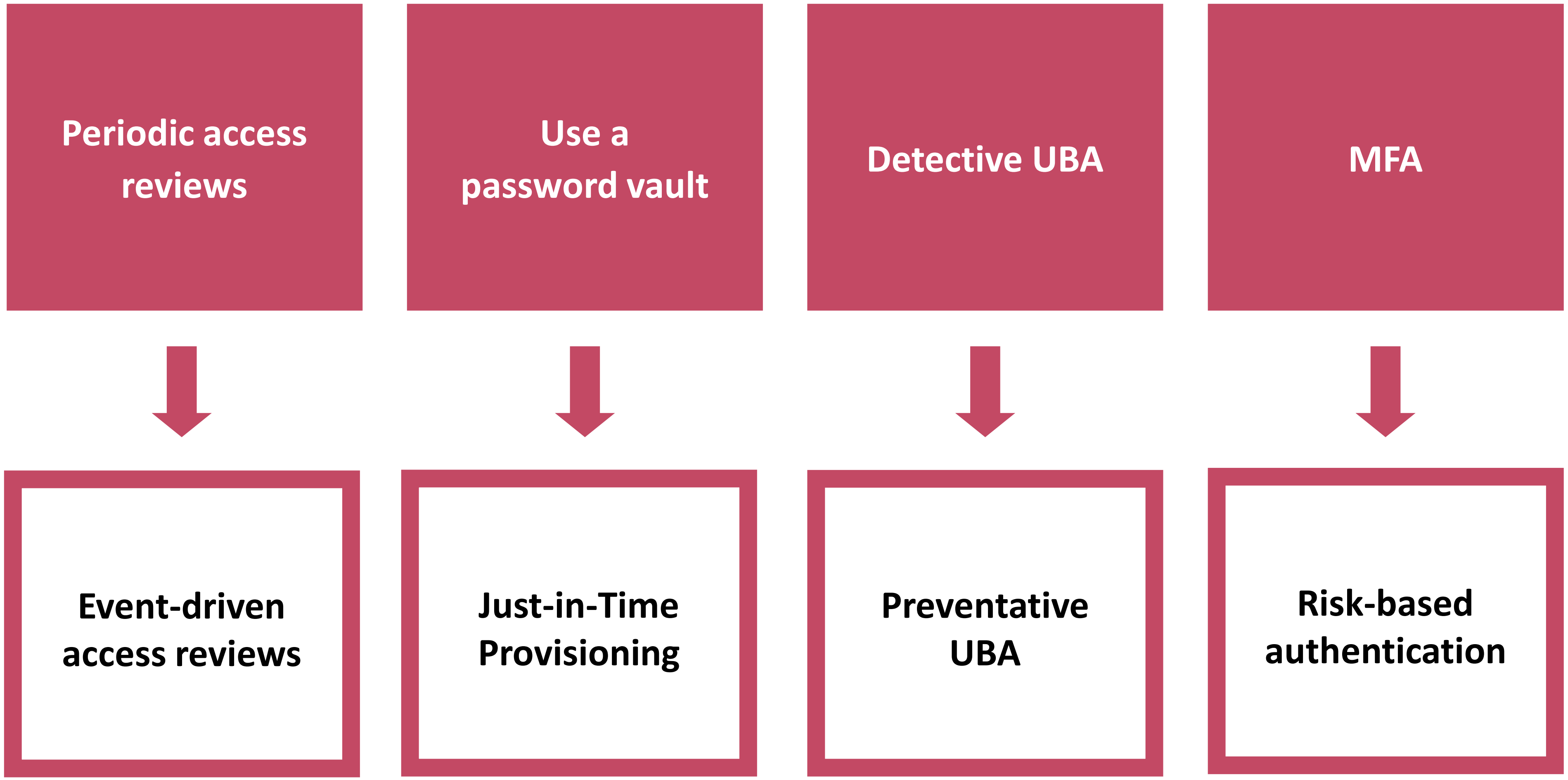


User gives two-week notice

The risk to the enterprise has changed; this user is now considered HIGH risk

Block from sending email that contains high-risk data

Instead, consider the following



Periodic access reviews → Event-driven access reviews

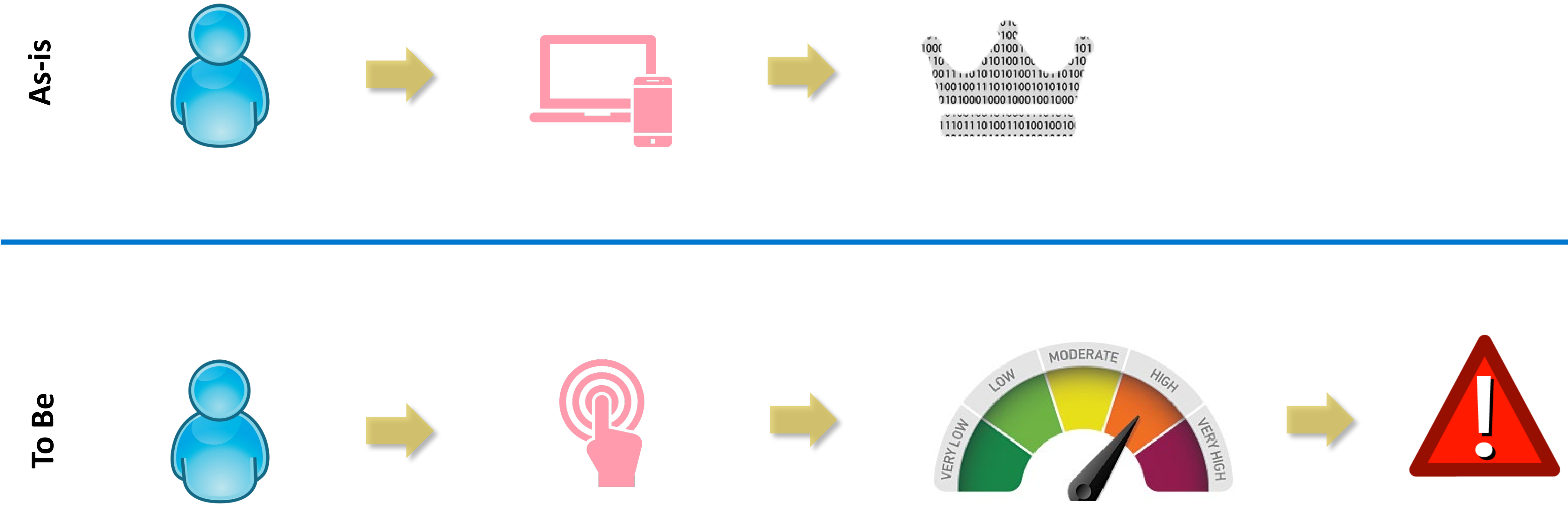
Use a password vault → Just-in-Time Provisioning

Detective UBA → Preventative UBA

MFA → Risk-based authentication

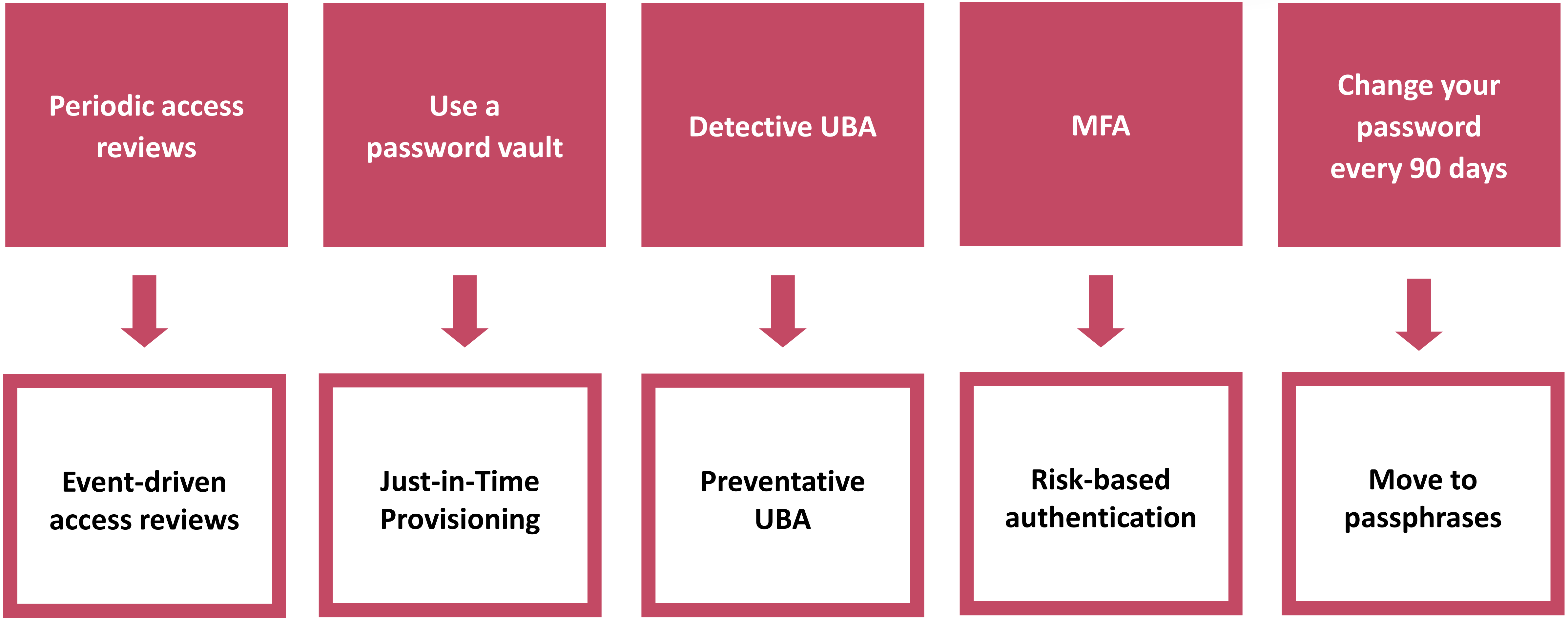
Risk-based authentication

Token can be stolen
SMS code can be hijacked



Preferably biometric

Instead, consider the following



Periodic access reviews → Event-driven access reviews

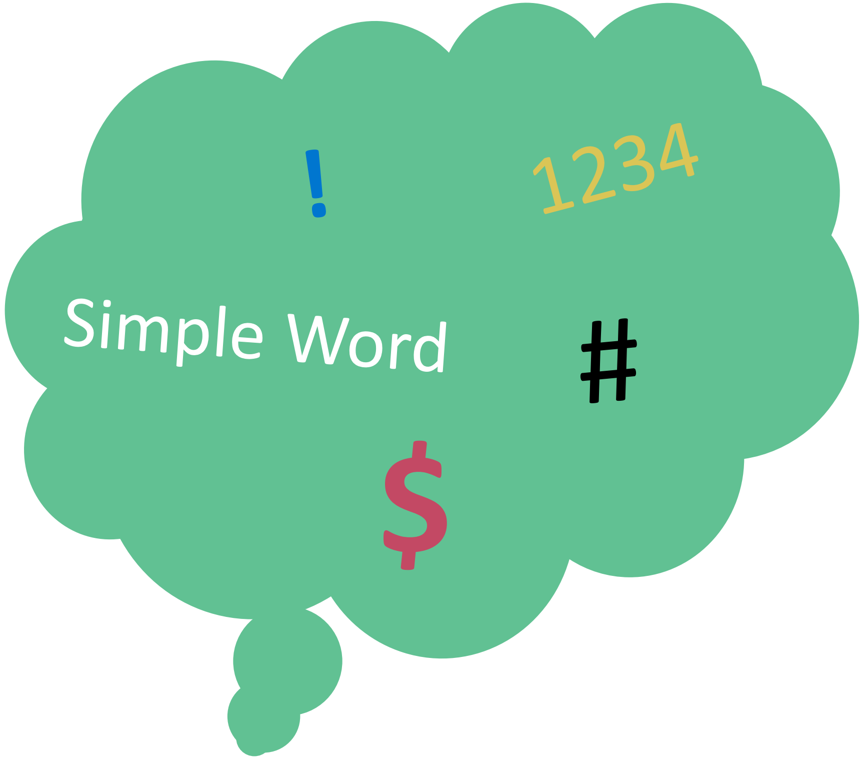
Use a password vault → Just-in-Time Provisioning

Detective UBA → Preventative UBA

MFA → Risk-based authentication

Change your password every 90 days → Move to passphrases

Passwords



!

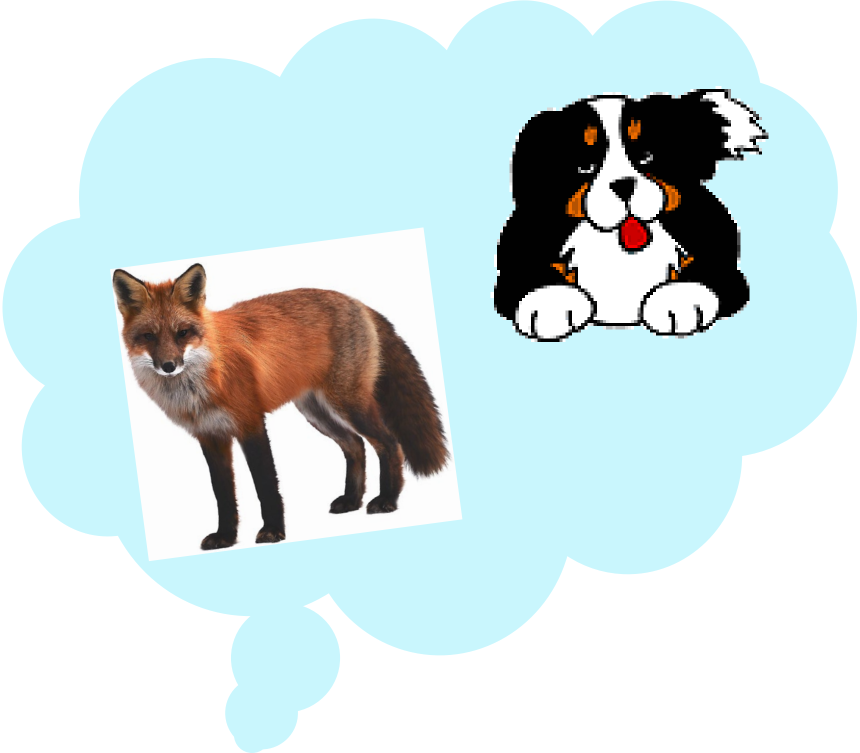
1234

Simple Word

#

$

What people think of



What people should think of

Move to passphrases

- The best solution is going to get rid of passwords all together, but this won’t happen in the near future.
- Instead of passwords use passphrases…

The quick brown fox jumped over the lazy dog.

Tqbfjotld.

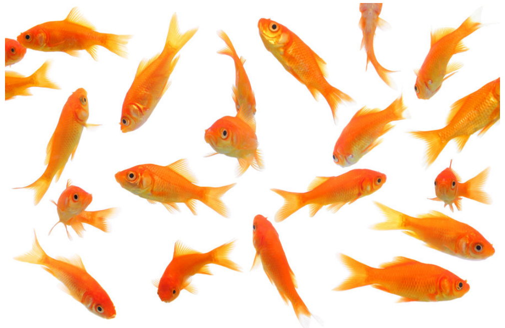
👤 = ☹

But what about privileged service accounts?

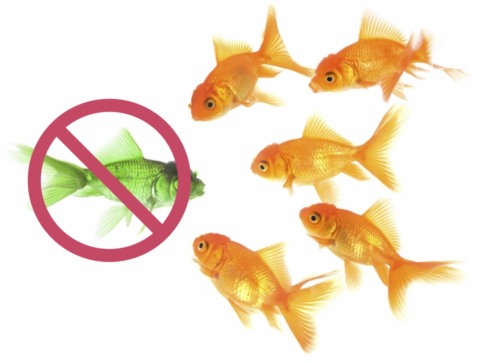
Current State

- Lack purpose and ownership
- Often have non-expiring passwords or infrequent password changes
- Often have more privileges than they need
- But…typically are used to perform the same tasks

Future State: Service Account Profiling

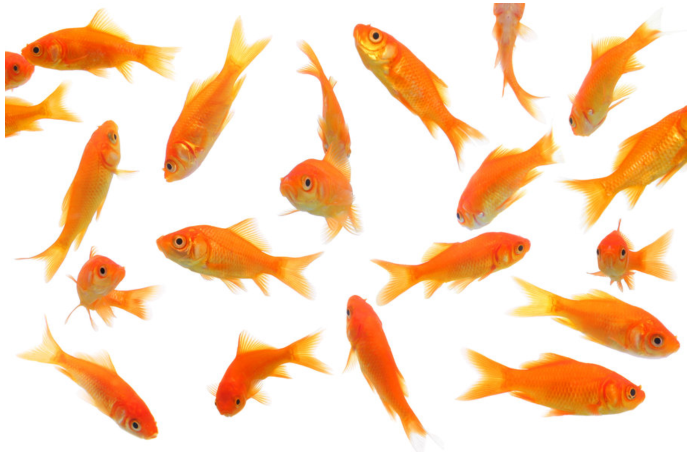


Establish normal profile over a period of time



Detect and block activity that happens outside the profile

But what about privileged service accounts?



Establish normal profile over a period of time

+

Detect and block activity that happens outside the profile

No longer require less effective controls such as periodic password reset and vaulting

Apply What You Have Learned Today

- Next week you should:
  - Identify which of the current “best” practices you follow
- In the first three months following this presentation you should:
  - Socialize an awareness program for why these controls may not be effective
  - Identify which of the suggested methods would work for your organization
- Within six months you should:
  - Obtain executive stakeholder buy in and be working towards implementation