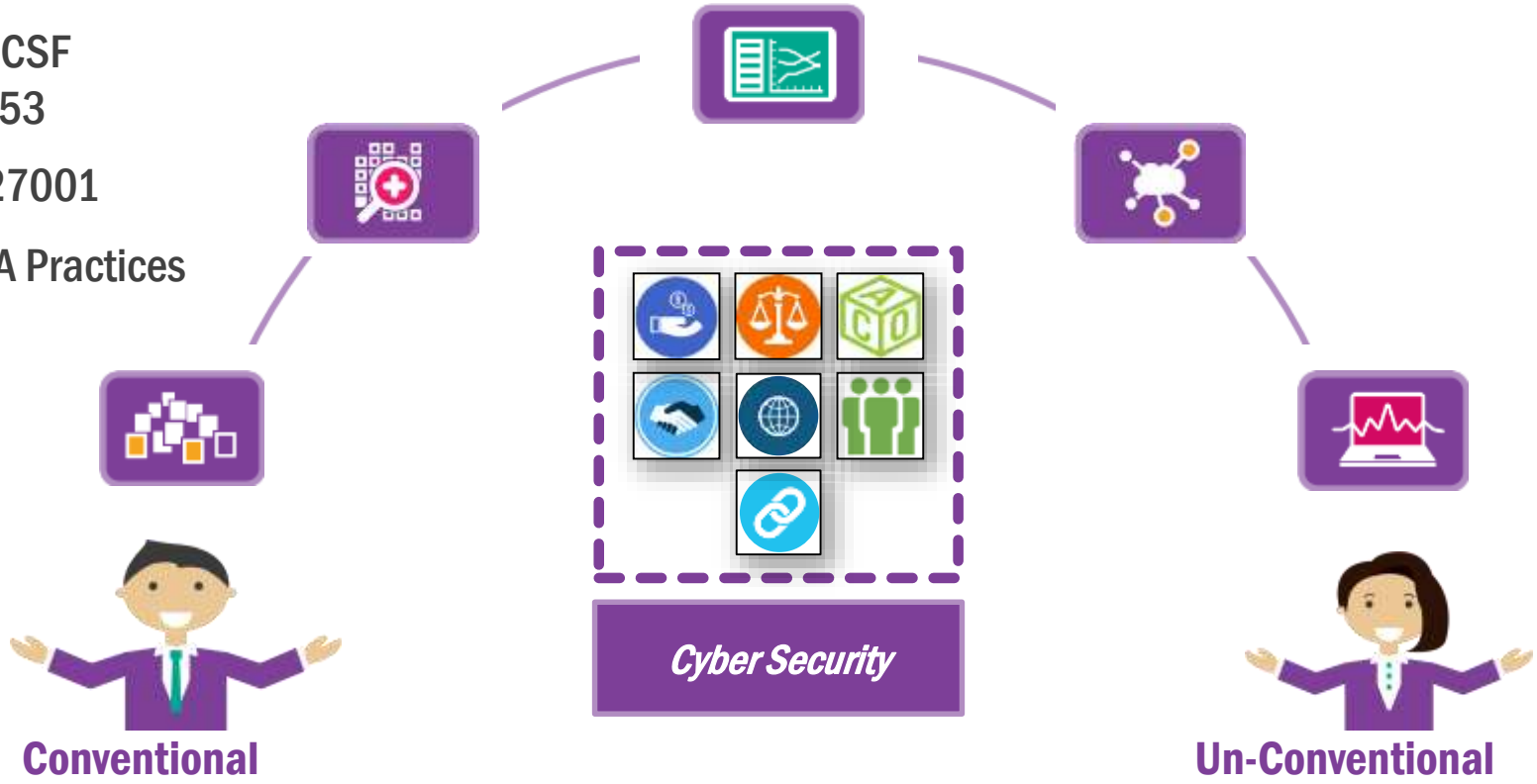
Model-driven security

Kim Kowalewski, Product Mgr. NGA, Aetna | September 2017

aetna

Evolution from conventional to unconventional controls

- NIST CSF 800-53
- ISO 27001
- AICPA Practices



Model Driven Security

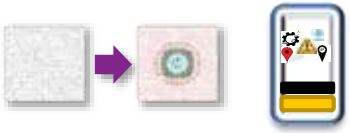
Traditionally, when new controls are written, a Security Professional sits down and manually inputs them into the system.

Using Security Models, the Security Professional defines different models that make dynamic changes to the control points.

Where we are investing today…

Phishing

- Inbound email protection
- Behavioral authentication



Privilege User

- Reduce privilege users
- Provide context
- Behavioral analytics

Exfiltration or Extortion

- Network behavioral analytics
- Adaptive enablement

The trouble with passwords...

Most people use less 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**

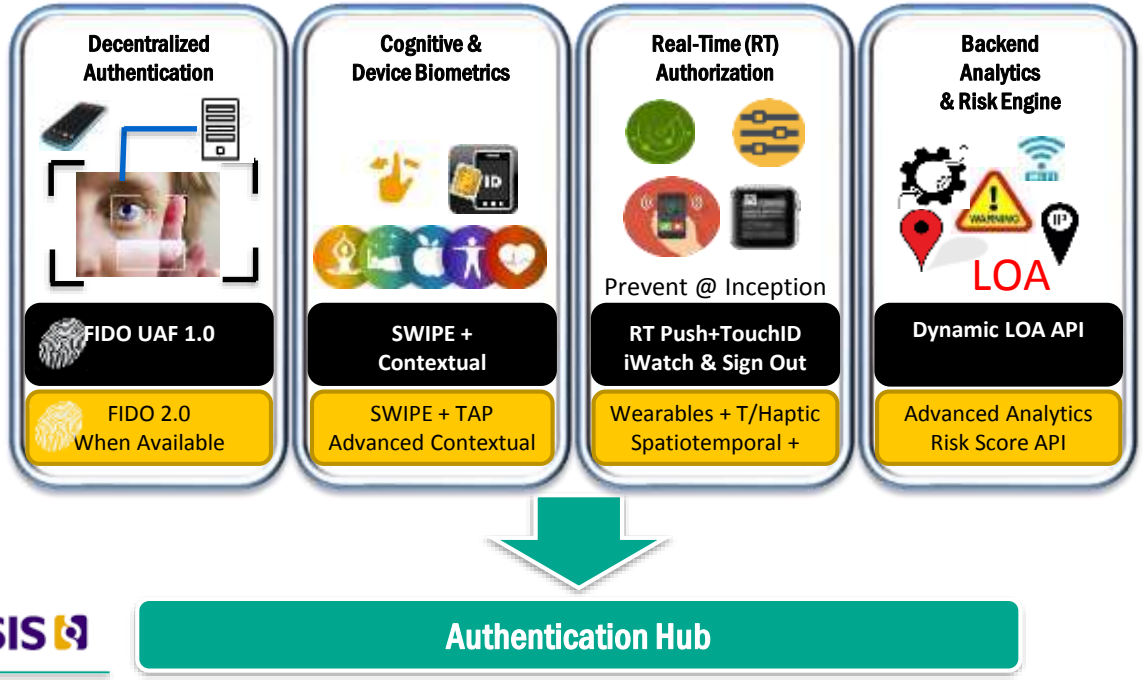
49%

of adults write their passwords down on paper

Sources: Pew research; Telesign research

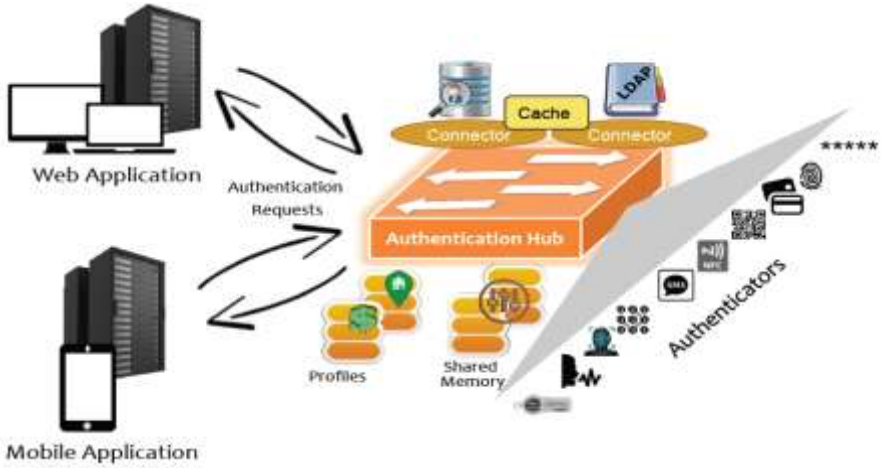
Behavioral based authentication

- Binary authentication is obsolete
- Behavioral-based model is key
- Innovation applied to the interface



Authentication framework for mobile & web

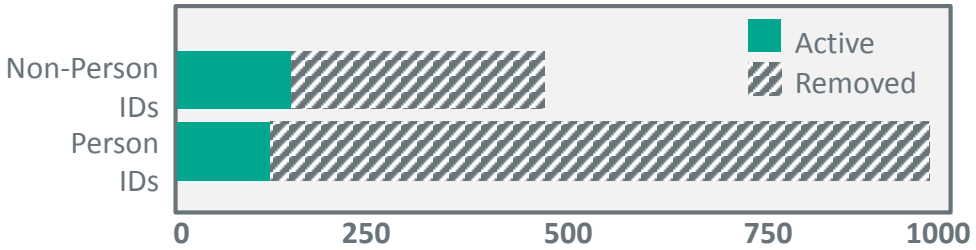
- One framework
- Multiple authentication tools
- Change controls without changing applications
- Across mobile and web
- Policy-driven authentication model



Privilege User

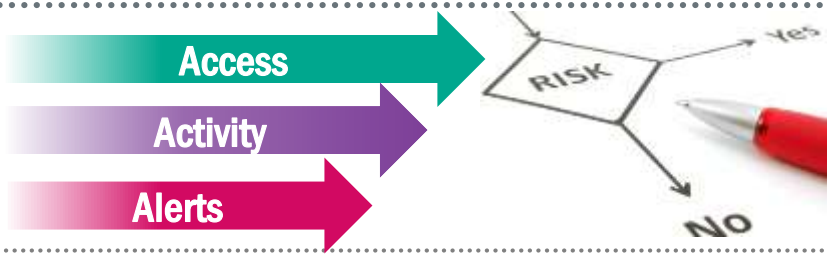
Privilege user & activity management activity

1 Reduce the number of privilege users



2 Provide context to monitoring and change admin tool choice

3 Implement data analytic techniques to determine behavioral patterns

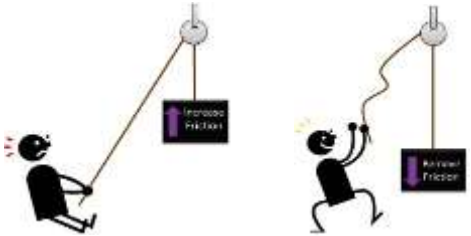


Exfiltration or Extortion

Adaptive enablement

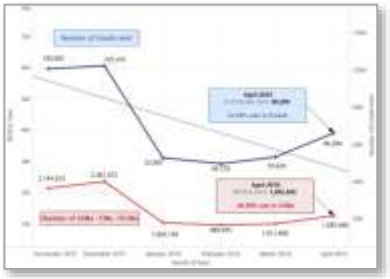
Network Behavioral Analytics:

1. Monitor flow into and out of the network
2. Establish patterns represented in models
3. Alert for anomalies outside of normal patterns



Adaptive Enablement

1. Create friction for high risk behavior in email and web browsing
2. Enable risk managed behavior by removing obstacles
3. Report on the results to three levels in the organization
4. Allow the natural cultural governance to reinforce the right behavior

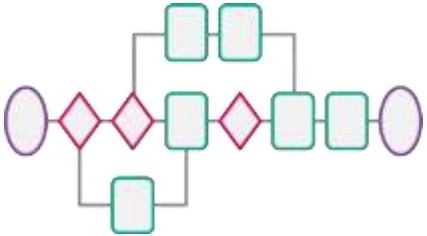


Adaptive Enablement			
Data Loss Prevention	Web Proxy	Entitlements	Physical Access

Model-driven security controls have arrived…

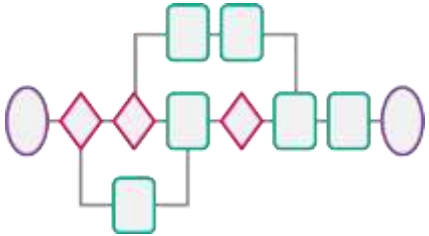
Phishing

- Inbound email protection
- Behavioral authentication



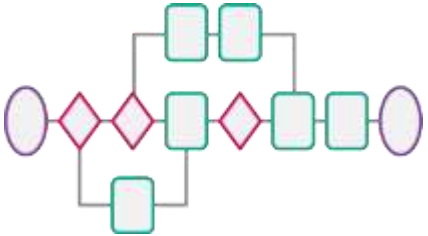
Privilege User

- Reduce privilege users
- Provide context
- Behavioral analytics



Exfiltration or Extortion

- Network behavioral analytics
- Adaptive enablement



Questions?

Kim Kowalewski
Product Mgr., Aetna
kxkowalewski@aetna.com

aetna