RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: STR-T09R

Adjusting Your Security Controls: It’s The New Normal

Jim Routh

CSO
Aetna
@jimrouth1

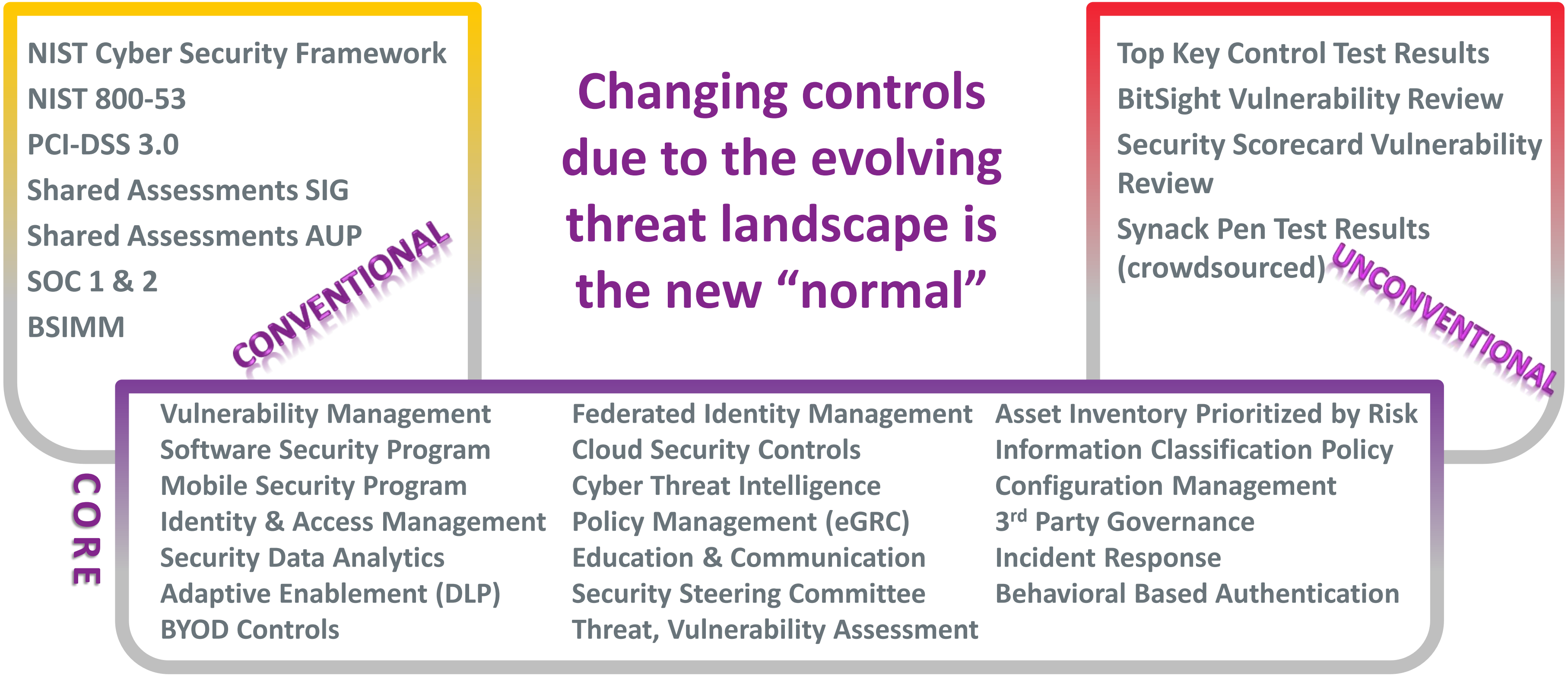
#RSAC

We Were Taught to Adopt a Framework of Controls

Security 101

1. Adopt a framework for controls
2. Document control objectives
3. Document control procedures
4. Implement control standards
5. Measure practices aligned with control procedures

Control Frameworks Implemented



NIST Cyber Security Framework
NIST 800-53
PCI-DSS 3.0
Shared Assessments SIG
Shared Assessments AUP
SOC 1 & 2
BSIMM

Changing controls due to the evolving threat landscape is the new "normal"

Top Key Control Test Results
BitSight Vulnerability Review
Security Scorecard Vulnerability Review
Synack Pen Test Results (crowdsourced)

Vulnerability Management
Software Security Program
Mobile Security Program
Identity & Access Management
Security Data Analytics
Adaptive Enablement (DLP)
BYOD Controls

Federated Identity Management
Cloud Security Controls
Cyber Threat Intelligence
Policy Management (eGRC)
Education & Communication
Security Steering Committee
Threat, Vulnerability Assessment

Asset Inventory Prioritized by Risk
Information Classification Policy
Configuration Management
3rd Party Governance
Incident Response
Behavioral Based Authentication

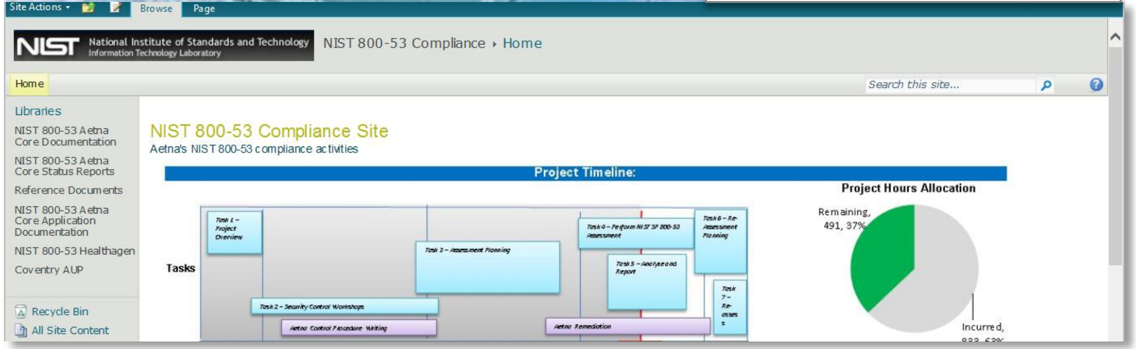
Control Compliance is Easily Measured

NIST Special Publication 800-53
Revision 4

Security and Privacy Controls for Federal Information Systems and Organizations

JOINT TASK FORCE TRANSFORMATION INITIATIVE

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-53r4



Site Actions
Browse
Page
NIST National Institute of Standards and Technology
Information Technology Laboratory
NIST 800-53 Compliance ▸ Home
Home
Search this site...
Libraries
NIST 800-53 Aetna Core Documentation
NIST 800-53 Aetna Core Status Reports
Reference Documents
NIST 800-53 Aetna Core Application Documentation
NIST 800-53 Healthagen
Coventry AUP
Recycle Bin
All Site Content

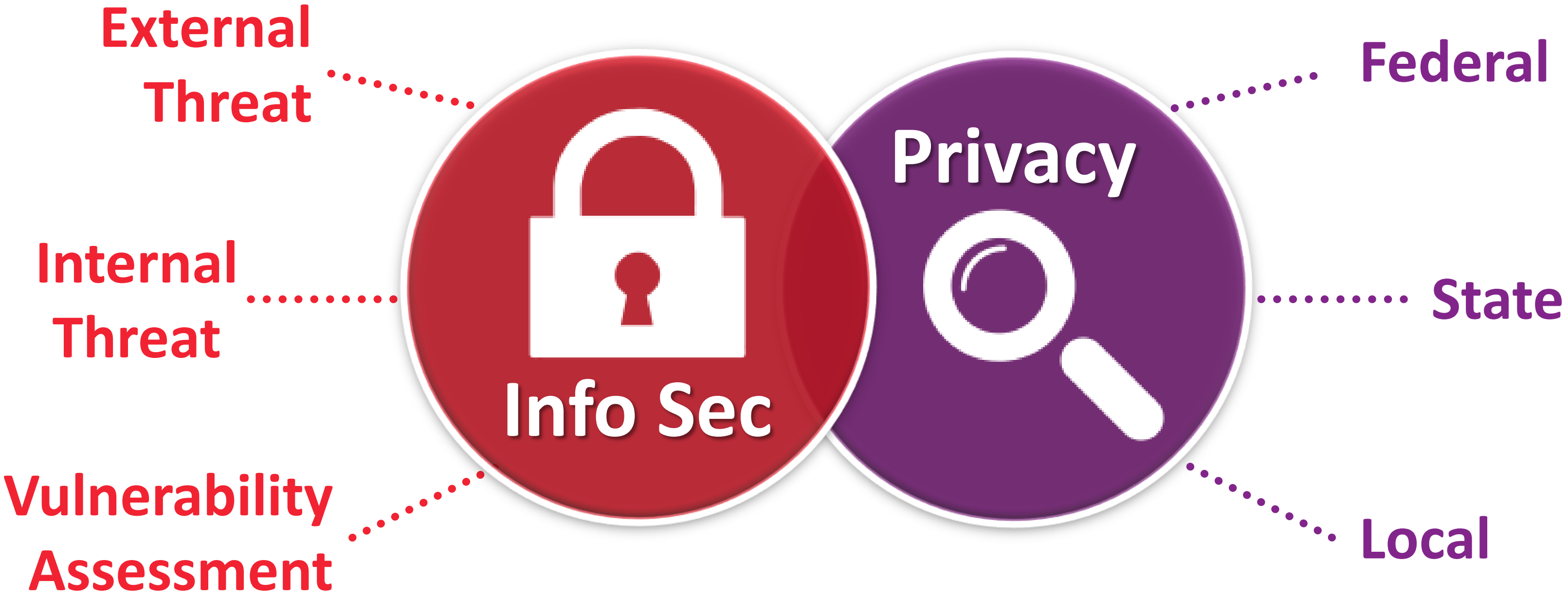
NIST 800-53 Compliance Site

Aetna's NIST 800-53 compliance activities

Project Timeline:
Tasks
Task 1 – Project Overview
Task 2 – Security Control Workshops
Aetna Control Procedure Writing
Task 3 – Assessment Planning
Task 4 – Perform NIST SP 800-53 Assessment
Task 5 – Analyze and Report
Aetna Remediation
Task 6 – Re-Assessment Planning
Task 7 – Re-asses s
Project Hours Allocation
Remaining, 491, 37%
Incurred, 833, 63%

Self Assessment
or
3rd Party Assessment

Privacy Relationship to Information Security


External Threat

Internal Threat

Vulnerability Assessment

Info Sec

Privacy

Federal

State

Local

Compliance-Driven Info Sec

Event

Awareness

Committee

-- Regulatory --

Legislative

Law

Rules Enforcement

Frameworks Are Good…and Not Sufficient

NIST
National Institute of Standards and Technology
U.S. Department of Commerce
800-53

NIST
National Institute of Standards and Technology
U.S. Department of Commerce
Cyber Security Framework

HITRUST
Health Information Trust Alliance

Information Security Management System
ISO 27001
Certified

SANS
Critical Security Controls for Effective Cyber Defense

PCI Security Standards Council™
PARTICIPATING ORGANIZATION

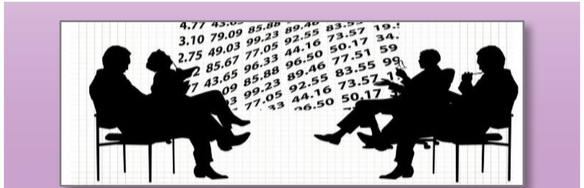
Encryption is Good…and Not Sufficient

In cryptography, **encryption** is the process of encoding messages or information in such a way that only authorized parties can read it.

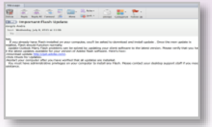
+/w%K4)*}/Z@9s$v#H~=\{^0q<

Dynamic Diversity of Threats

1. Customer Service Rep uses a web-based translation service
2. Site vulnerability is exploited and malware loaded into the browser
3. New session opens and sophisticated malware is installed- interrogates the workstation
4. Attempts to capture claim information to use for phishing attacks on aerospace companies



1. Spanish company selling hacking tools is hacked releasing source code identifying 4 exploits of Adobe Flash
2. Adobe releases patches
3. Threat actor based in China sends phishing emails to senior executives encouraging them to click to install the Adobe patch



Important Flash Update

[illegible]

1. Large cache of stolen credentials released publicly via Pastebin
2. Some of the released credentials used for 3rd party sites and enterprise log ins
3. A few of the credentials are from privilege users

The cyber threat landscape is changing too quickly for frameworks to respond to

The Cyber Threat Landscape Changes Quickly

CHS Community Health Systems

CareFirst

Anthem

United States Office of Personnel Management

PREMERA BLUE CROSS

Excellus

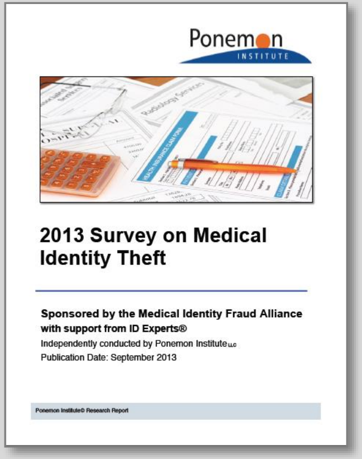
SONY PICTURES

CACI

EVER VIGILANT

Macro Economic Analysis Applied to Cyber

2013



Ponemon INSTITUTE

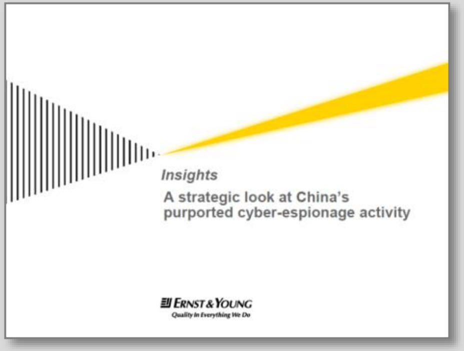
2013 Survey on Medical Identity Theft

Sponsored by the Medical Identity Fraud Alliance with support from ID Experts®

Independently conducted by Ponemon Institute LLC

Publication Date: September 2013

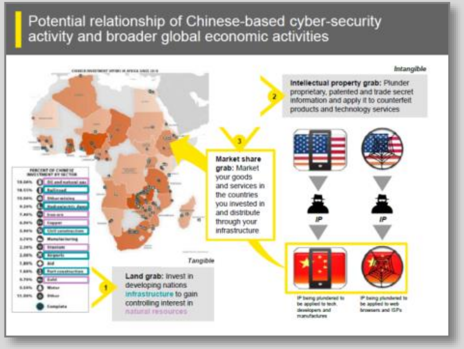
Ponemon Institute© Research Report



Insights

A strategic look at China's purported cyber-espionage activity

Ernst & Young
Quality In Everything We Do



Potential relationship of Chinese-based cyber-security activity and broader global economic activities

Intellectual property grab: Plunder proprietary, patented and trade secret information and apply it to counterfeit products and technology services

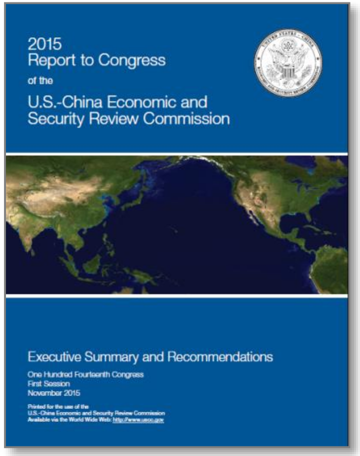
Market share grab: Market your goods and services in the countries you invested in and distribute through your infrastructure

Land grab: Invest in developing nations infrastructure to gain controlling interest in natural resources

IP being plundered to be applied to tech developers and manufactures

IP being plundered to be applied to web browsers and ISPs

2015



2015
Report to Congress
of the
U.S.-China Economic and Security Review Commission

Executive Summary and Recommendations

One Hundred Fourteenth Congress
First Session
November 2015

Printed for the use of the
U.S.-China Economic and Security Review Commission
Available via the World Wide Web: http://www.uscc.gov

A bull black market

The black market of health care data from a cyber economic perspective

NH-ISAC

EY
Building a better working world

A Bull Black Market

There are two black markets: one for common traders and one for nation states and organized crime syndicates. The two markets rarely interact and have different market dynamics.

Maintaining value

- Health care data has a **long shelf life** on the black market.
- Health care data **provides fuller data set** than the financial sector (e.g., **SSN**, medical history, employee information).

EY Building a better working world

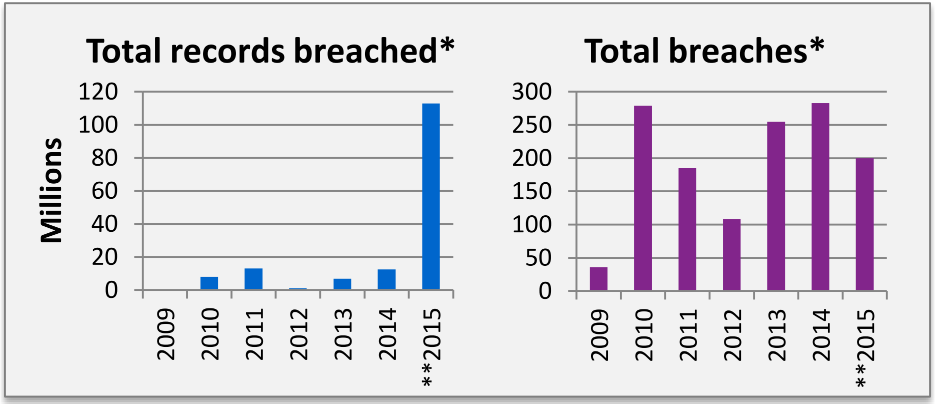
Change in price behavior

- In 2014, PHI sold for **$3-$50** per record. In 2015, **$5-$700**.
- The **most valuable fields** within a data set are SSN, name, and DOB.
- Hackers haven't realized **the real market value** of health care data due to information asymmetries.
- Unlike traditional supply and demand economic model, the price of health care data is dependent on the threat actor's **use of the stolen data, not the volume** of the data stolen.

Increasing supply

- Amount of data stored across the industry.
- Interactions with health care providers.
- Total cybersecurity incidents targeting this industry**.**

The supply of data on the black market is misleading due to dueling black markets



*U.S. Department of Health and Human Services

**2015 data is through October

What Have Nation States Learned?

"It's a walk in the park."

Who is their *customer?*

- Search capability
- Mail account with free storage
- Maps and navigation
- Docs
- And more …

It's ***not*** you!

… One million gigs of data processed each day

Who is their *product?*

You are!

The Mobile Device is Our New Appendage

There are now **more cell phones** on the planet **than there are people**

90% of 19-29 year-olds in the U.S. **sleep with their cell phones**

65% of survey respondents **said mobile phones make them better parents**

75% of survey respondents **bring their phones to the bathroom**

Apple Siri captures everything you say to her for 6 months and aggregates it for 18 months

Source: *Qualcomm, Slick Text Surveys*

What is the most commonly used **mobile app?**

Social media apps have the ability to **use your phone's microphone to listen to your dialog**

Who authorized this potential invasion of privacy?

You did!

Terms of Service - ToS

The average American encounters **1,462** privacy policies a year with an average length of **2,518** words.

☑ I agree with the Terms of Service.

The privacy policy for one of the world's largest online payment systems is **36,275** words … more than Shakespeare's Hamlet!

> "You grant … a nonexclusive, irrevocable, worldwide, perpetual, unlimited, assignable, sublicenseable, fully paid up and royalty-free right to us to copy, prepare derivative works of, improve, distribute, publish, remove, retain, add, process, analyze, use and commercialize, in any way now known or in the future discovered, any information you provide, directly or indirectly to … including, but not limited to, **any user generated content,** ideas, concepts, techniques and/or data to the services, **you submit** to … without any further consent, notice and/or compensation to you or your any third parties. Any information you submit to us is at your own risk of loss." …

Source: *Carnegie Mellon University study*

Walks in the Park Are No Longer Free …

In the U.S., social networks are considered **public spaces** … this means that you should have ***no expectations of privacy*** in the data collected.

- **81% of divorce attorneys** admit to searching social media for evidence
- **70% of HR professionals** have rejected a candidate based on information uncovered in an online search
- **86.1% of police departments** now routinely include social media searches as part of criminal investigations

Your social content from the "Park"

Phishing eMail

Hey John,
It was great seeing you last week at the reunion. I'm sure you didn't recognize me since I lost over 75 pounds from our college days. BTW- you look great and I enjoyed meeting your wife. Here is a picture from the reunion that you'll get a kick out of!
All the best, Jane

Credentials to Employer site

1. John Doe, IluvWk2ay
2. John deColleague Sysadmin 1

Sources: *IACP Center for Social Media survey and Microsoft*

The Most Popular Threat Vector is…

According to the 2015 Verizon Data Breach Investigations Report (VDBIR):

"One of the most effective ways you can minimize the phishing threat is through ***awareness and training."***
—Lance Spitzner, Training Director, SANS Securing The Human

- Phishing was associated with **95% of incidents** attributed to state-sponsored threat actors
- Over 100 million phishing messages arrive in our inboxes every day
- The median time-to-first-click came in at one minute and **22 seconds** across all campaigns

23% of recipients now open phishing messages and **11%** click on attachments

Nearly 50% open emails and click on phishing links within the first hour

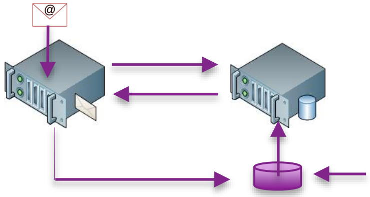
What can we do?

- Improve education/awareness
- Consider *unconventional* controls →

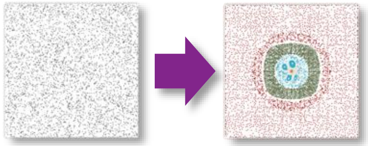
1. New email gateway payload inspection and filters
2. Sinkhole all new domains for 48 hours
3. Enforce inbound filtering (DMARC)

Apply Unconventional Controls

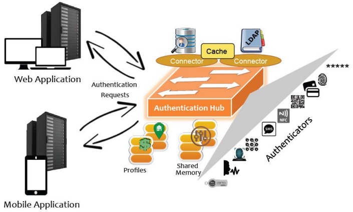
1. **Sinkhole new domains**



2. **Heuristic filtering on in-bound using DMARC**

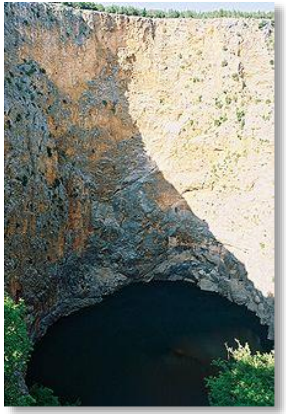


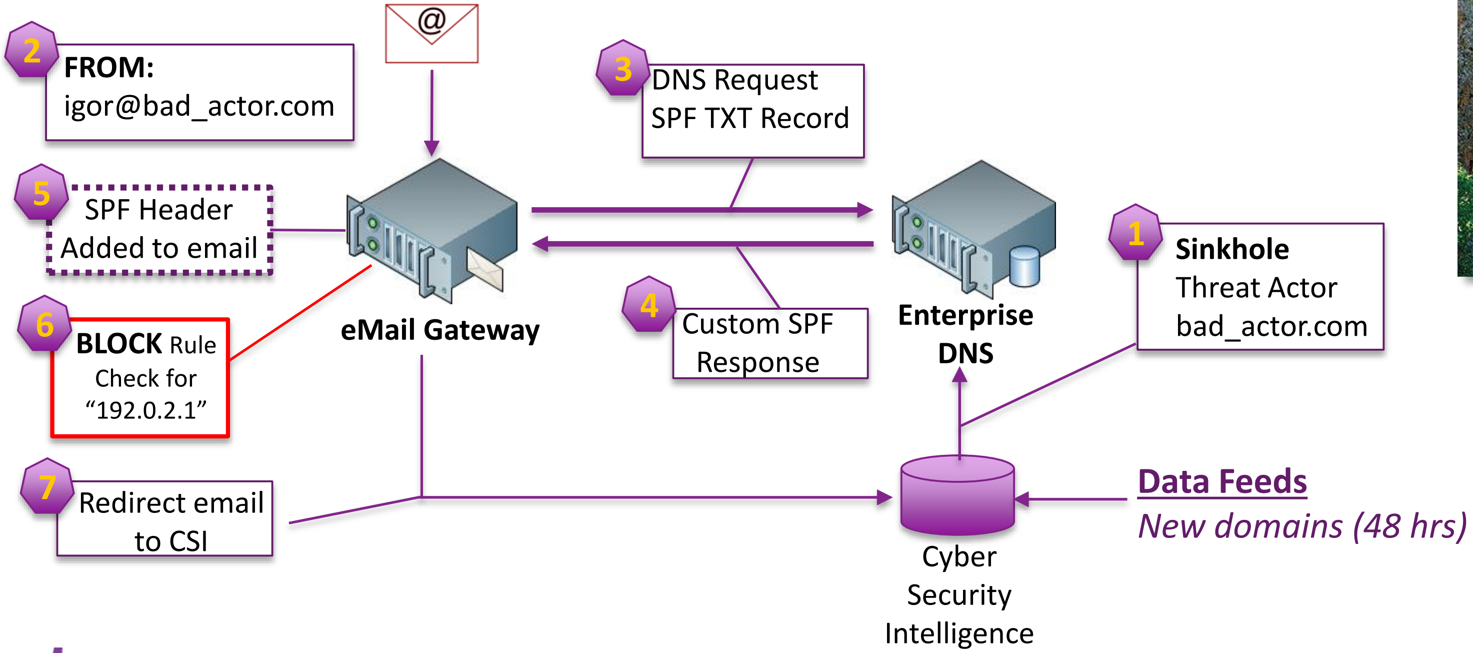
3. **Next Generation Authentication**



Sinkhole Newly Established Domains

A **sinkhole**, also known as a **cenote**, **sink**, **sink-hole**,[1] **shakehole**,[2] **swallet**, **swallow hole**, or **doline** (the different terms for sinkholes are often used interchangeably[3]), is a depression or hole in the ground caused by some form of collapse of the surface layer

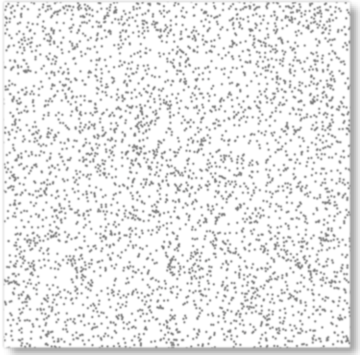


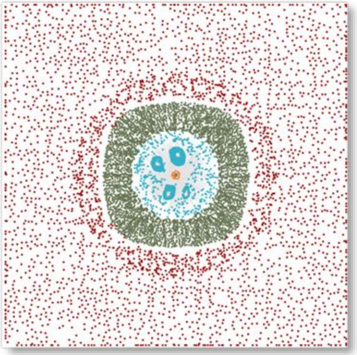


Protect In-Bound Email with Domain Protection

Using email traffic data, the system learns the **unique fingerprint** of all email senders into your enterprise

This durable **identity trust model** is used to stop all messages that do not prove they should be trusted



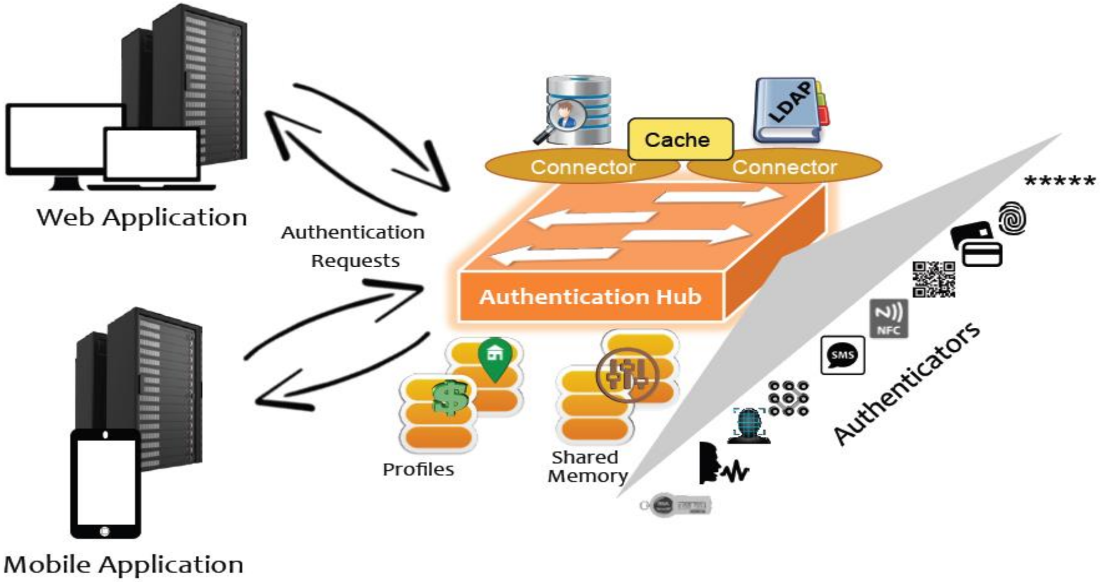


29,231 servers sent email for an enterprise on a single day

312 servers for the enterprise
4,641 servers owned by service providers
9,732 benign email forwarders
14,526 malicious senders

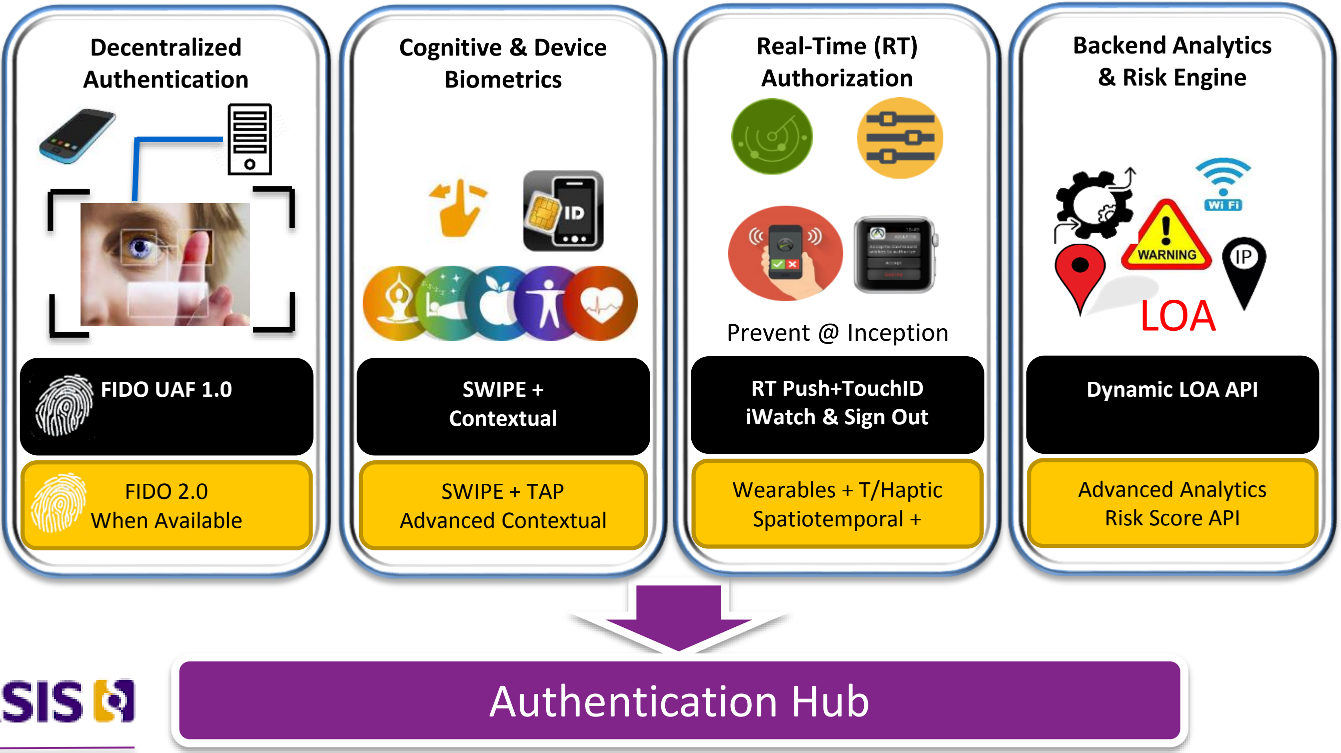
Design an Authentication Hub

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



Next Generation Authentication

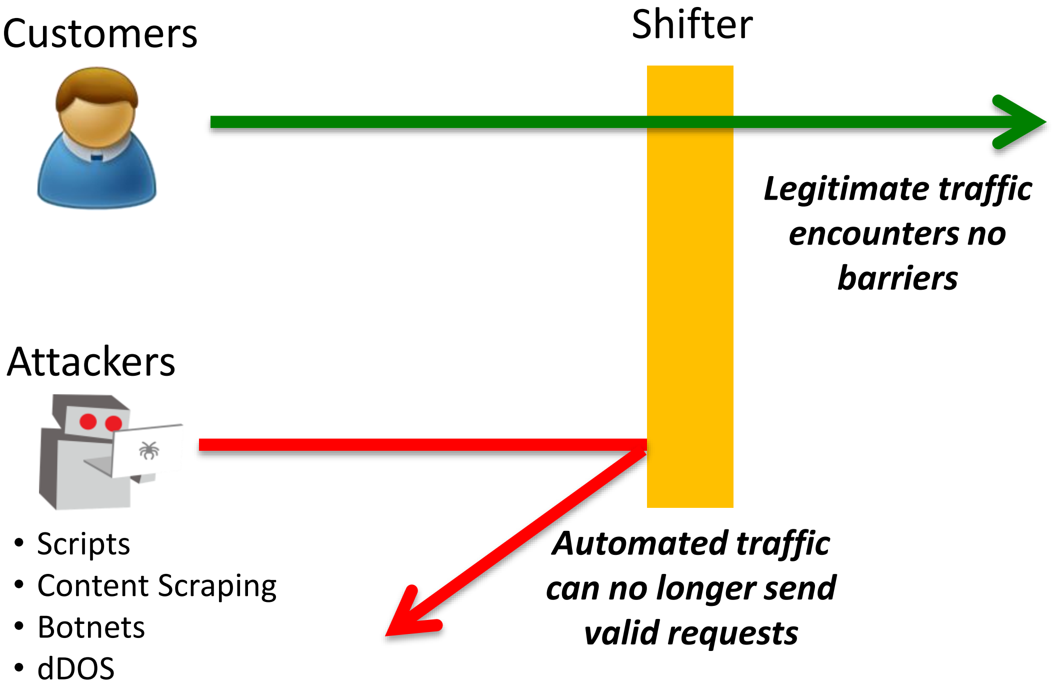
- Binary authentication is obsolete
- Behavioral-based model is key
- Innovation applied to the interface



Decentralized Authentication
FIDO UAF 1.0
FIDO 2.0 When Available
Cognitive & Device Biometrics
ID
SWIPE + Contextual
SWIPE + TAP Advanced Contextual
Real-Time (RT) Authorization
Prevent @ Inception
RT Push+TouchID iWatch & Sign Out
Wearables + T/Haptic Spatiotemporal +
Backend Analytics & Risk Engine
Wi Fi
WARNING
IP
LOA
Dynamic LOA API
Advanced Analytics Risk Score API
Authentication Hub

fido alliance OASIS

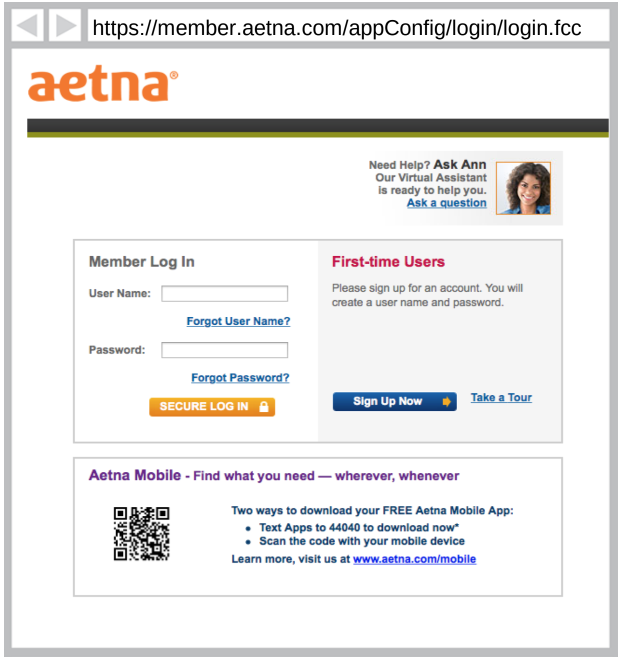
Automated vs. Normal Behavior



Legitimate traffic encounters no barriers

- Scripts
- Content Scraping
- Botnets
- dDOS

Automated traffic can no longer send valid requests


https://member.aetna.com/appConfig/login/login.fcc

aetna

Need Help? **Ask Ann**
Our Virtual Assistant
is ready to help you.
Ask a question

Member Log In

User Name:

Forgot User Name?

Password:

Forgot Password?

SECURE LOG IN

First-time Users

Please sign up for an account. You will create a user name and password.

Sign Up Now

Take a Tour

Aetna Mobile - Find what you need — wherever, whenever

Two ways to download your FREE Aetna Mobile App:

- Text Apps to 44040 to download now*
- Scan the code with your mobile device

Learn more, visit us at www.aetna.com/mobile

Recommendations

- **Adopt and implement** practices aligned with regulatory framework of choice
- **Measure** the effectiveness of the controls aligned with the framework
- **Identify** the enterprise's top threats/risks
- **Apply** control design skills to top threats/risks and consider innovation opportunities

Which Statement Gives You More Assurance?

1. Aetna conforms to the NIST Cyber Security Framework and 800-53

OR

2. Aetna makes 30 changes to controls each month

✓ ***Adjusting Controls … it's the New Normal!***

routhj@aetna.com

860 273-7488

Chairman National Health Information Sharing & Analysis Center
Board member FS-ISAC
ISE Award winner 2014 Healthcare

NH-ISAC

FINANCIAL SERVICES | Information Sharing and Analysis Center