MAIN EGRITY

New Ways to Maintain Integrity

FIM+ System Integrity

Partners:

PCI Security Standards Council

IBM Registered Business Partner

splunk>

Presented By: Al Saurette (403) 818-8625 Al@maintegrity.com

Agenda

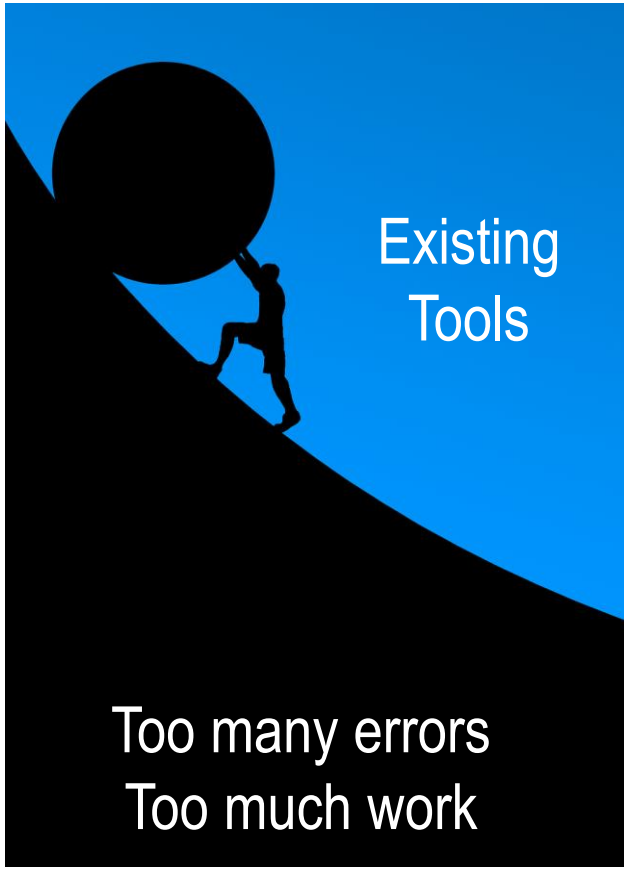
- Need for better security
- Perimeter vs internal security
- What is FIM and how does it help
- Fixing knowledge gaps
- Understanding the FIM process
- Automating breach detection and response
- Compliance
- System & application integrity
- Wrap-up and questions

Background

- Principals involved in Enterprise Software since the late 1980's
  - Products launched - Harbor, HCD, Stand Alone Environment, ISPW
- 2014, FIM+ concept started as a verification tool for application rollouts
- 2017, notice FIM technology would be PCI/DSS requirement in Jan 2018
- No mainframe FIM solution existed
  - Form a company (MainTegrity),
  - Develop improved mainframe security using FIM - highly automated, feature rich
- Initially detection only – now gather forensics / assist with recovery
- Financing completed in August of 2018

Imagine a mainframe software start up in 2017… who would of thought?

Challenges



Do you need to?

- Manage multiple LPARs, systems, customers securely
- Ensure integrity – z/OS, key sub-systems, applications, config members
- Make insider threat detection, response and recovery faster and easier
- Audit / certify system integrity of z/OS, sub-systems, apps, configs
- Integrate relevant info from FIM, SMF, change control, SIEM, SMP/e, etc.
- Save time and effort expert tools that learn – auto-discovery, zero admin
- Modernize, make new and existing staff more efficient
- Improve internal security and compliance (PCI/DSS, GDPR, NIST)

InSecurity

2019 IBM / Ponemon report

- +500 organizations surveyed
- Detection – **206 days**
- Respond & Recover – **+73 days**

Why you should care

- Average breach cost: $4.3 Million
- Brand / reputation impact
- You may lose your job

Root Cause

Malicious Attack - 51%	Outsider breaking in
Human Errors - 25%	Insiders making errors
System Glitches - 24%	Corrupt files, bad configs

Errors not resulting in data breaches not reported

Mainframes matter

- $7.7 trillion credit card payments (annual)
- 29 billion ATM transactions (annual)
- 87% of credit card transactions

IBM sponsored 2019 Ponemon *Cost of Data Breach Study*

Better detection, Faster response

Why 206 days? Existing tools subject to:

- Stolen credentials mask malicious actions
- Flawed data - Faulty rules, Recording gaps, Config changes
- One time events can be missed
- False alarms

Identify attacks that bypass other tools

- Bit by bit comparison – is it 100% correct or not?
- Reports altered components - not just suspicious events
- Errors are reported until fixed – hard to overlook
- Retroactive – identifies existing errors
- Audit key apps and systems on demand

No amount of AI can fix flawed data

An FIM approach

File Integrity Monitoring (FIM)

Take a snapshot of your files at a trusted level – Baseline
Saves version keys in an encrypted vault
Later take another snapshot and compare

FIM Design Criteria

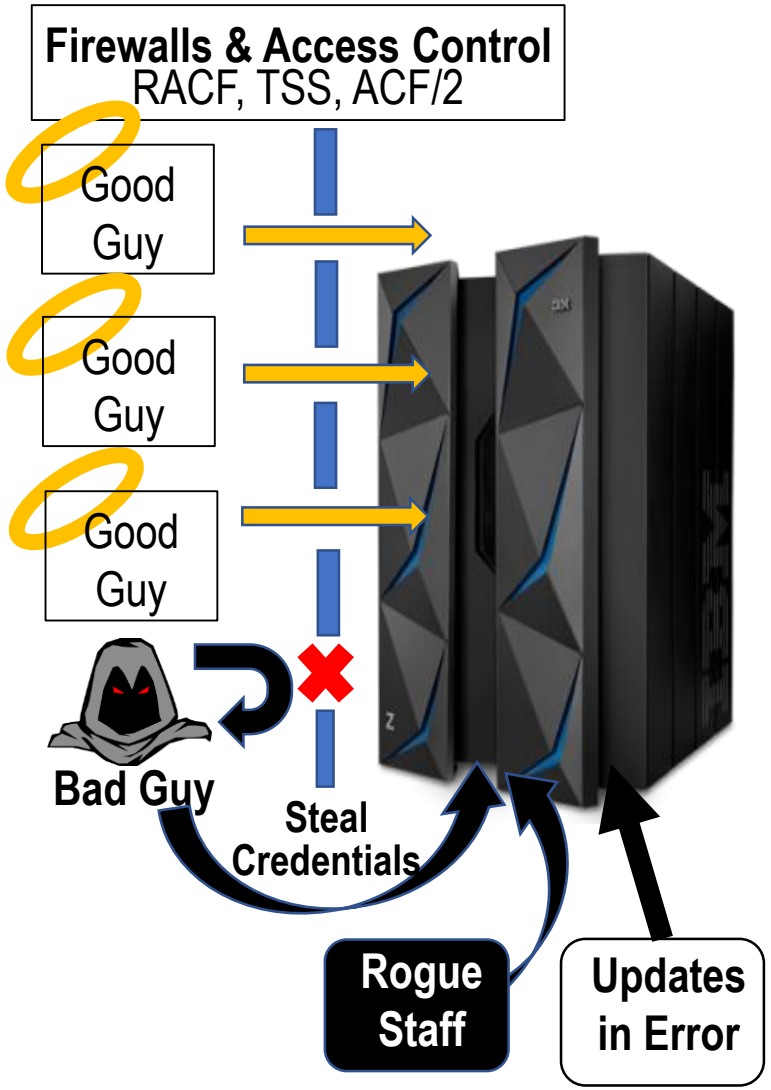
Systems, Apps, Subsystems (CICS, IMS, TCP/IP …)
Executables, JCL, Configs, Scripts, Logs, Encrypted, USS
High Performance - negligible CPU - offload to crypto card
Email & text alerts, integrates with SIEMs (Splunk, QRadar, etc)

Active content comparison

Conclusive evidence that whole systems match desired state

Existing tools HOPE changes are correct. FIM proves it.

What is an insider?



Conventional Security – Guard the perimeter

- Insiders are past Firewall / Access Control
  1. Bad Guys Steal Credentials
  2. Trusted employees go rogue (addiction, financial, health)

Well meaning staff make mistakes (deploy, update)

- Were the changes correct?
- Are all the LPARS the same? Exceptions?
- Traditional monitoring is manual (Labor intensive)
- Requires lots of z/OS specific skills

Bridge the Knowledge Gap

Issues

Skill sets differ between mainframe and other systems
In-depth knowledge takes years to develop
Mainframes are not inherently more secure

Give staff the right tools

- Control / View from 3270, GUI, integrate your SIEM
- Click alert to initiate FIM+ forensics
- Get Who, What, When, Where, Why data in seconds
- Know components / systems affected – Scope of attack

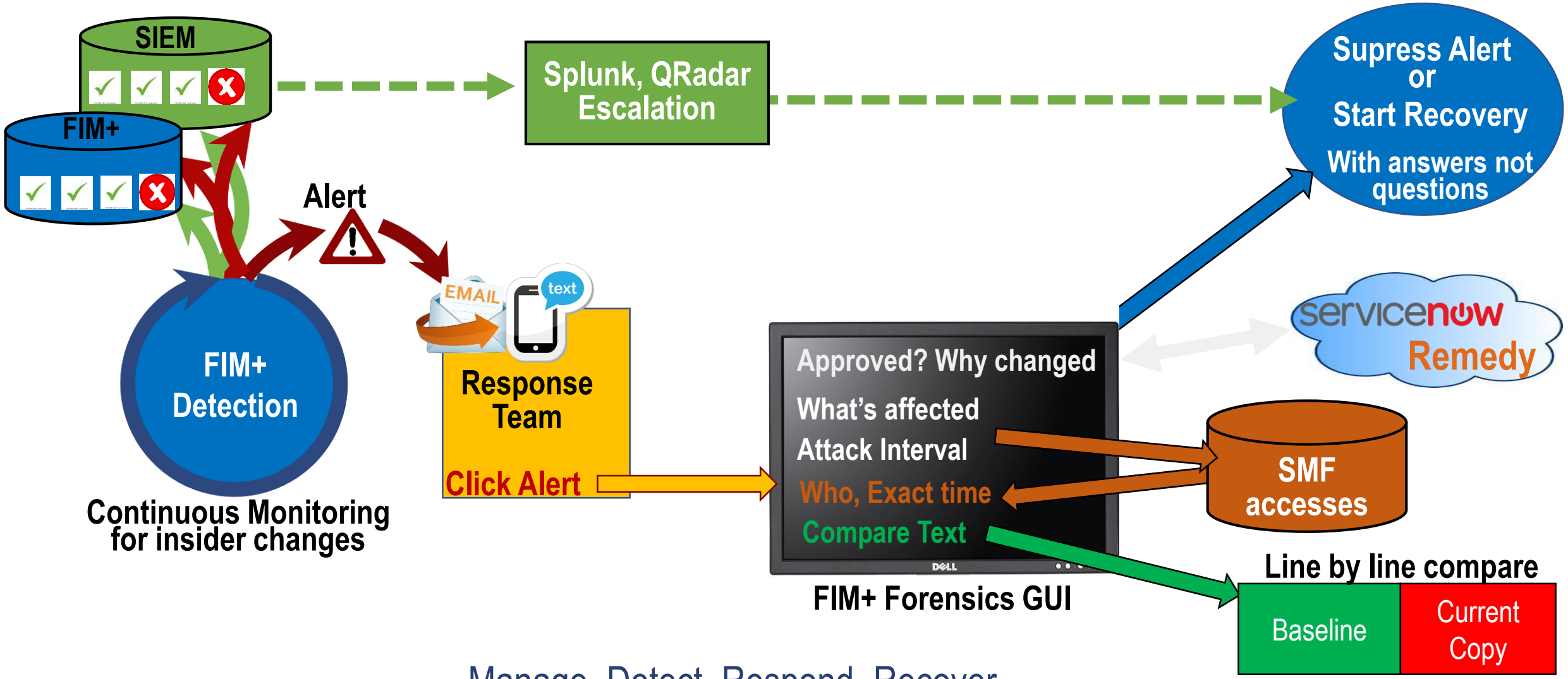
Zero-admin Initiative

- On-going auto-discovery of components in use (APF, configs …)

Lost in a sea of info

Know what's going on BEFORE the phone rings

Logical FIM process



Manage, Detect, Respond, Recover

Advanced Forensics

Eliminate false alarms

- Did it really change or just look suspicious?
- Was it authorized? Instream query of ServiceNow, Remedy, etc.

One click compare to baseline

- Finds the line that changed

Audit application and system deployments

- Detect wrong versions, forgotten changes, and backout errors

Log success and failure

- Know last good date – defines attack & restore intervals
- Fetch only relevant SMF accesses (in attack interval)

Answers instead of questions at a crucial time

2 Click - Fornesics

FIM+ send text or email alert

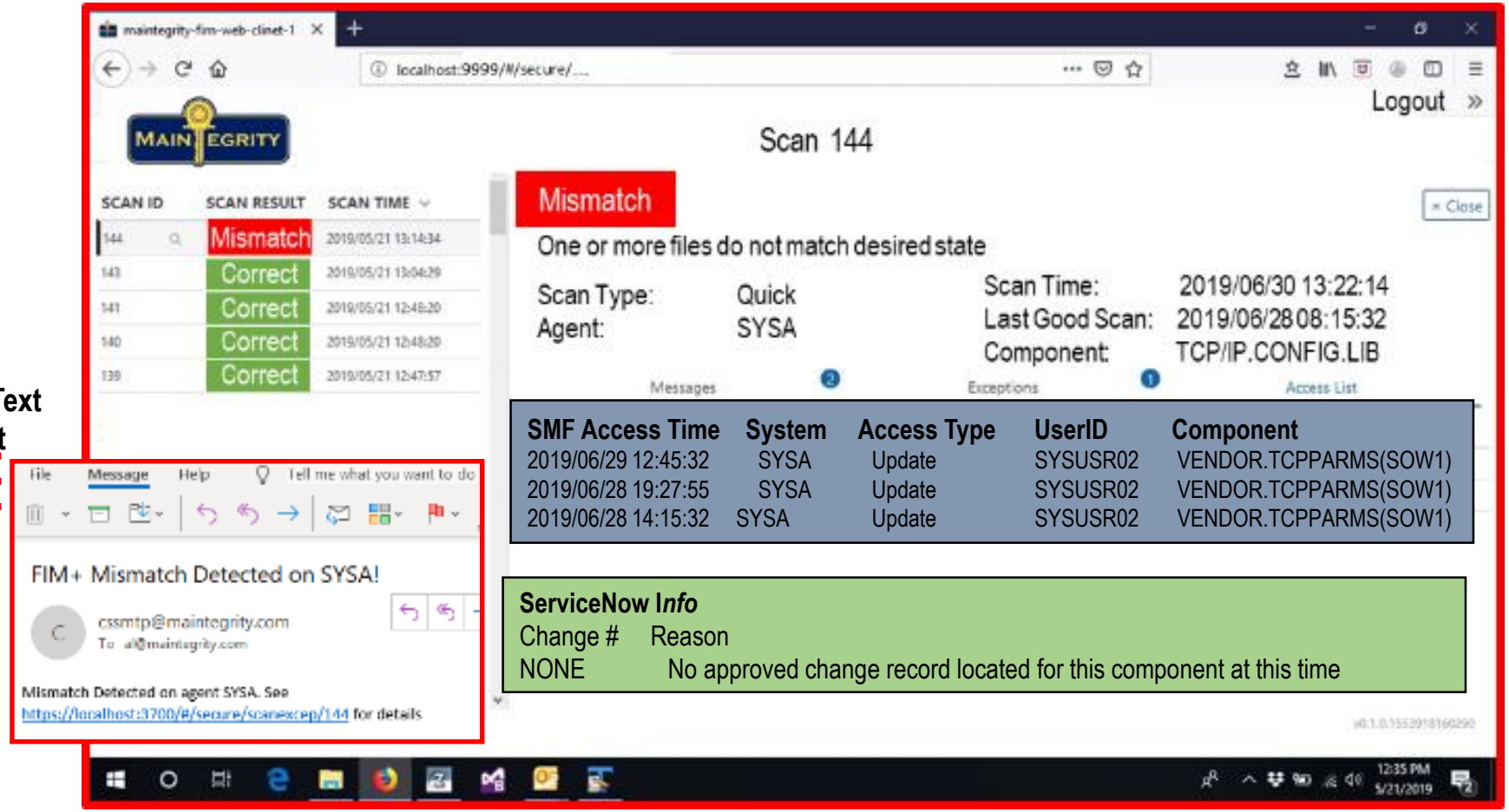
Click 1

When an alert is received one click opens the GUI in any browser and displays detailed info including SMF access data

Click 2

Another click fetches change control info from ServiceNow or Remedy dynamically, without needing mainframe skills.

Email,Text Alert



2 more clicks – to respond

MAINTEGRITY

Click 3

Click 3 can invoke instream file compare to show exactly what line changed.

Trusted Component

Incident: **SN 2349** *Last good:* **2019/05/22 09:39:28**

```
# Shell script to assign TCP/IP port.
if test -t 1; then
    TCP/IP Port 2645    161.185.160.93
    exit
```

New York

Suspect Component

Incident: **SN 2349** Error time**: 2019/05/22 18:49:03**

```
# Shell script to assign TCP/IP port.
if test -t 1; then
    TCP/IP Port 2645    95.31.18.119
    exit
```

Russia

Click 4

Complete restore can be accomplished by clicking the FIM+ Recovery Assistant to select and verify all files required

FIM-based Recovery Assistant

H-Recover	File #1	2019/05/22 09:39:28
H-Recover	File #2	2019/05/22 09:39:28
	⋮	
H-Recover	File #99	2019/05/22 09:39:28

Power of Automation

Provides quick answers instead of questions, when time is critical

	FIM & Access Data*			Classic Response
Detect	Advanced Detection			Basic detection
Respond	Alarm verified Know WHY Know Scope Know Attack Interval Review accesses (dozens) Know Who did it Show changed lines			Is it a false alarm? Why was it done? What was affected? When did it start? Review accesses (thousands) Who did it? What did they do?
Recover	Corrective action Verified correct	**Minutes**	**Weeks**	Corrective action Hope its correct

* Automate forensics / recovery with change info, SMF and FIM data at your fingertips

NIST Cyber Security Framework V1.1

Source: NormShield - MainTegrity Inc. April 2019

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning *	Recovery Planning *
Business Environment	Awareness and Training	Security Continuous Monitoring *	Communications *	Select Restore Files *
Governance *	Data Security	Detection Processes *	Analysis *	Improvements *
Risk Assessment	Info Protection Processes and Procedures		Contents Comparison *	Communication *
Risk Management Strategy	Maintenance		Mitigate / Improve *	Verify Restore *
	Protective Technology			

* New, stronger controls with FIM

FIM

Compliance – PCI V3.2.1 / V4

Harden security then prove compliance:

- Continuous monitoring, FIM corroborating evidence
- Specific PCI controls and best practices strengthened
- On–demand audit provides conclusive proof

FIM helps you:

- Finish audit and get back to real work faster
- Save real time / $$$ on next audit
- Your CIO can sign off compliance with confidence

Specific PCI controls

☑	1.1.1
☑	6.4
☑	10.5
☑	11.5
⋮	
☑	Sec 12

Part 3b. PCI Compliance Attestation
Signature of Executive Officer _____
Executive Officer Name: _____ *Title:* _CIO, CFO, CEO …_

Know you're secure, Know you comply

System / App Integrity

What FIM data allows:

- Verify systems and apps remain correct over multiple LPARS
- Manage versions and specific deviations
- Detect unauthorized or changes in error, even using legitimate credentials
- Identify code drift across environments before it causes problems
- Retroactive – Can be used to verify / correct existing problems
- Utilize configuration data from ServiceNow / Remedy and SCM tools (Endevor, ChangeMan, ISPW)
- Confirm SMP/E and what's in use match (find alterations, adds, deletes)
- Complete forensic info gathering and presentation

Prove Systems & Apps in use are correct (Scheduled, On Demand)

FIM data can help you

- Discover APF, subsystem and application components
- Detect changes that bypass existing tools (internal threats)
- Respond to incidents faster – automated detection / forensics
- Eliminate false alarms & redundant effort
- Integrate with current software (standard job streams, REST APIs)
- Comply with specific PCI, NIST, GDPR requirements
- Allow staff to make the right decisions, with all the facts in one place
- Run all on mainframe, or feed your enterprise security console

Start preventing problems today

Questions and Wrap-up

Start preventing problems today

- Eliminate false alarms, Automated forensics for the real ones
- Delivers **Zero-Admin** features – like APF scan, Config Scan, Appl versioning, etc
- Give deploy team real validation - within the change window

Save time the first day, and every day

- If a problem occurs - Who gets hung out? Make sure its not you

Find out more:

- Book a deep dive demo or a free trial – with no obligation - today

Mainframes are high value targets – Defend them properly