



Noise Cancelling FIM



Lavish Jhamb

Senior Product Manager, Compliance Solutions



How many of you use Qualys Cloud Agents?



How many of you know that existing these existing agents can do File Integrity Monitoring (FIM) and File Access Monitoring(FAM)?

Success Formula

For Your File Integrity Monitoring Program

01

Experience seamless onboarding with ready-to-use set up for PCI 4.0

02

Fine-tuned FIM solution with automated noise cancellation

03

Most comprehensive FIM coverage for servers, endpoints, network devices and containers

Outcomes

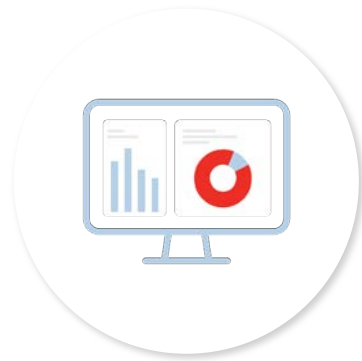


Significant reduction in operational costs for managing FIM



Zero issues in meeting PCI 4.0 FIM Requirements

Why FIM is a Must-have?



File Integrity
Monitoring

45%

Ransomware attacks involve **changes to user files**

60%

Advanced Persistent Threats (APT) **use registry changes for persistence**

35%

Rootkits modify **registry keys to evade detection**

Security Agencies Recommend FIM



"Implement a configuration change control process to detect unauthorized modifications"



"Compare against expected configuration changes and patching plans to verify that the changes are authorized"

The image shows a tablet displaying the CSF Tools interface. At the top is the "CSF Tools" logo. Below it is a breadcrumb trail: "CIS Critical Security Controls > Critical Security Controls v8 > 3: Data Protection". The main heading is "3.14: Log Sensitive Data Access". Under "Threats Addressed:", there are two tags: "Repudiation" (green) and "Information Disclosure" (blue). Under "Group:", there is a link "IG3". Under "Previous Version:", it says "Critical Security Controls Version 7.1:" followed by a link "14.9: Enforce Detail Logging for Access or Changes to Sensitive Data". The "Control Statement" section contains the text "Log sensitive data access, including modification and disposal." and a note: "[csf.tools Note: For more information on the Critical Security Controls, visit the [Center for Internet Security.](#)]". The "Related Controls" section lists "NIST Special Publication 800-53 Revision 5" with three bullet points: "AC-6(9): Log Use of Privileged Functions", "AU-2: Event Logging", and "AU-12: Audit Record Generation".



Verizon 2024 Payment Security Report marks FIM as one of The 20 Biggest Control Gaps

Cost of non-compliance - Business comes to a halt

Source: [Verizon 2024 Payment Security Report -Bottom-20 lists](#)

Challenges with FIM Deployments



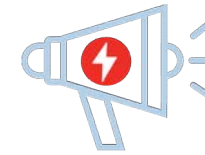
Not the Right Sensor

Sensors responsible for FIM are found using **self-signed certificates**



Fail to Cover Blind Spots

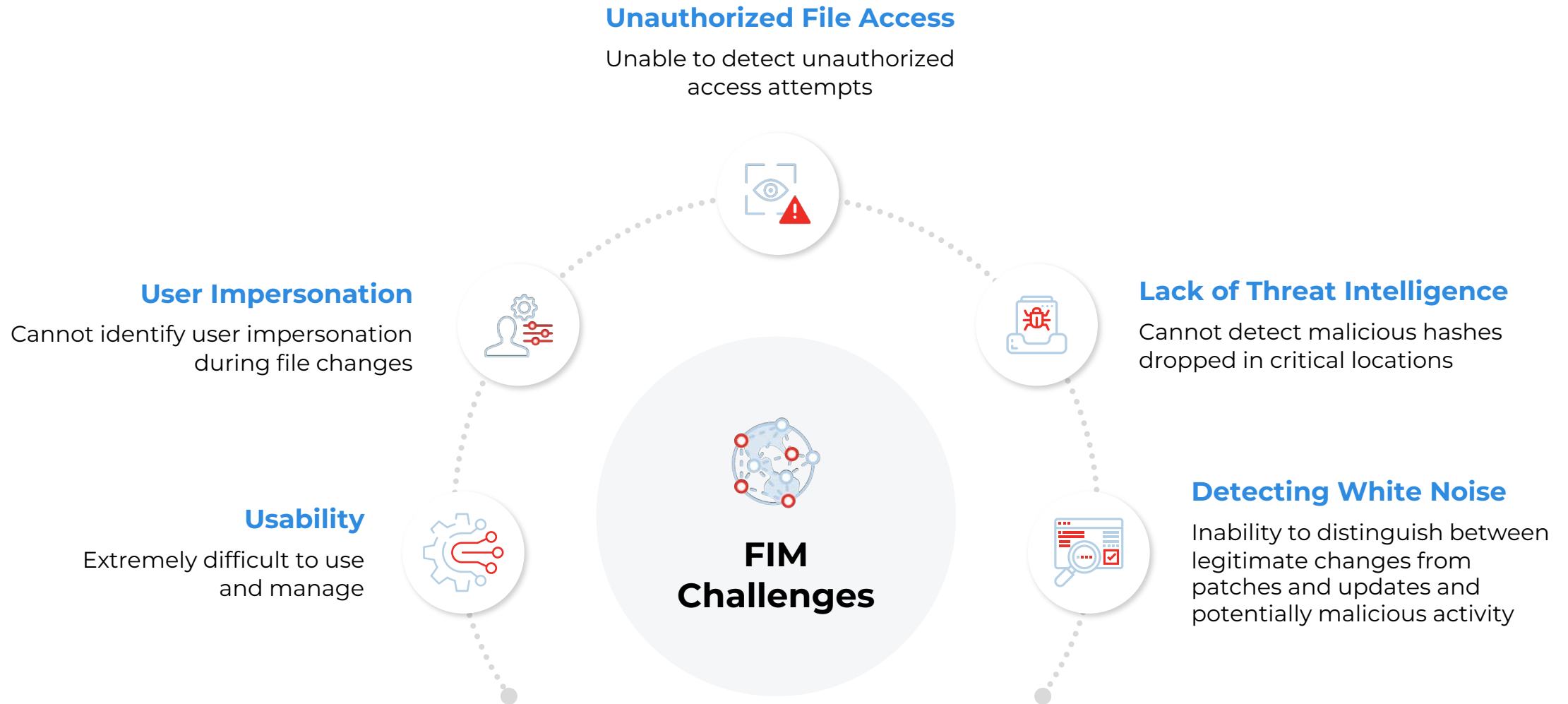
FIM on Network Devices, Container-based FIM, File Access Monitoring (FAM)



Alert Fatigue

Inability to distinguish between legitimate changes from patches and updates and potentially malicious activity

Challenges with Traditional FIM Solutions



The Solution and Its Capabilities



Qualys®

One Platform for Most Comprehensive FIM Coverage

Scanner Appliance

Agentless FIM

Scan-based FIM on network devices

Detect configuration changes in network devices such as routers, switches, and firewalls.



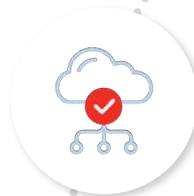
Cloud Agent

Agent-based FIM

Real time monitoring for servers and endpoints

Real time File Access Monitoring (FAM)

Threat detection



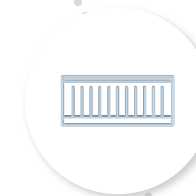
Qualys FIM

Container Sensor

Container Runtime Security

Real time FIM on containers

Track unauthorized access to critical files on containers



DE-RISK YOUR BUSINESS



Noise Cancellation



Trust Status - Automated reconciliation of change events from known vendor updates and patches



User and Process based event suppression:
Eliminate 90%+ of false positives by excluding FIM events generated by known good users and processes

Qualys Cloud Platform

← Event Details : auth.log

File Create : auth.log
Created On : A day ago, Aug 04, 2024 at 12:00:19 AM | Severity: ■■■■

auth.log was created by user root

Basic Details Associated Incident

Event Activity

File Path
/var/log/auth.log

File Reputation Status
Known

Success Status
Yes

File Trust Status
Trusted

Command Executed
/usr/sbin/logrotate/etc/logrotate.conf

Who-Data

Effective User : root (0)

Actual User : tom (1012)

By Process
/usr/sbin/logrotate

File Hash
e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b78526855

Triggers

MONITORING PROFILE	RULE	CATEGORY
Linux Monitoring Profile for PCI DSS - DO NOT DELETE	Rule-11	PCI

File Access Monitoring (FAM)

15%

Of unauthorized access attempts targeted **highly sensitive**.



13.1M

Total Unauthorized
Access Attempts



2.22M

Highly Sensitive Files



14.6M

Total Unauthorized
Access Attempts



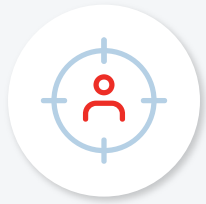
2M

Highly Sensitive Files

DE-RISK YOUR BUSINESS



Identify User Impersonation



Detects when a user impersonates another to gain unauthorized access

Qualys Cloud Platform

← Event Details : hosts

File Content : hosts
Changed On : 3 days ago, Aug 04, 2023 at 01:26 AM | Severity ■■■■■ Actions

Host was changed by user CARFIM\James Show Difference

Basic Details Associated Incident

Event Activity

File Path	Success Status
C:\Windows\System32\drivers\etc\hosts	Yes

Who-Data

- Effective User : **CARFIM\James**
S-1-5-21-4189715595-3213726884-4212328133-1132
- Actual User : **CARFIM\Alex**
S-1-5-21-657214820-925904655-3777385490-1002
- By Process
C:\Windows\system32\cmd.exe

Triggers

MONITORING PROFILE	RULE	CATEGORY
Windows Monitoring Profile for PCI DSS	Rule 5	PCI

Detect High Risk Activities on Your Network Devices

- ✓ Modification of [access restrictions](#)
- ✓ Modification of authentication or [authorization mechanisms](#)
- ✓ Modification of **logging procedures**
- ✓ Modification of the [boot process](#)
- ✓ [Creation of new VLANs, tunnels or virtual interfaces](#)
- ✓ Allowing outbound [connections from a network device](#)
- ✓ Enabling [shell access](#)

Content Change Difference

Difference Removed Word Removed Difference Added Word Added

Cisco Network Configuration Drift

Baseline File

```
144 address-family ipv4 unicast
145 vrf-management
146
147
148
149 Logging console: enabled (Severity: critical)
150 Logging monitor: enabled (Severity: notifications)
151 Logging linecard: enabled (Severity: notifications)
152
153 Logging server: enabled
154
155 Facility      Default Severity  Current Session Severity
156 -----
157 aaa          3                  3
158 aclog        2                  2
159 aclmgr       3                  3
160 afm          3                  3
161
```

Event File

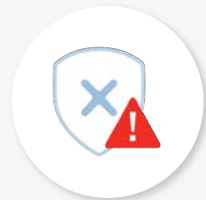
```
144 address-family ipv4 unicast
145 vrf-management
146
147
148
149 Logging console: disabled (Severity: critical)
150 Logging monitor: disabled (Severity: notifications)
151 Logging linecard: disabled (Severity: notifications)
152
153 Logging server: disabled
154
155 Facility      Default Severity  Current Session Severity
156 -----
157 aaa          3                  3
158 aclog        2                  2
159 aclmgr       3                  3
160 afm          3                  3
161
```

Close

Integrated Threat Intelligence



Built-in threat intelligence enriches file reputation status for binaries and portable executable files



Quickly identify malicious or suspicious hashes in monitored locations

Qualys Cloud Platform

← Event Details : 4de0c431cb9805cb419d42e5f3630a74393ed10409bf0e6d3d65c7b95e380aa5.exe

File Create : 4de0c431cb9805cb419d42e5f3630a74393ed10409bf0e6d3d65c7b95e380aa5.exe
Created On : 6 min ago, Aug 04, 2024 at 1:26 AM | Severity ■■■■■ Actions

4de0c431cb9805cb419d42e5f3630a74393ed10409bf0e6d3d65c7b95e380aa5.exe was created by user CARFIM\James

Basic Details Associated Incident

Event Activity

File Path
C:\Financial_Statements\4de0c431cb9805cb419d42e5f3630a74393ed10409bf0e6d3d65c7b95e380aa5.exe

File Reputation Status: Malicious File Trust Status: Untrusted

Success Status
Yes

Who-Data

Effective User : CARFIM\James
S-1-5-21-4189715595-3213726884-4212328133-1132

Actual User : CARFIM\Alex
S-1-5-21-657214820-925904655-3777385490-1002

By Process
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

File Hash
4de0c431cb9805cb419d42e5f3630a74393ed10409bf0e6d3d65c7b95e380aa5

Triggers

MONITORING PROFILE	RULE	CATEGORY
Windows Monitoring Profile for PCI DSS	Emulating Ransomware	PCI



What You'll See in the Demo

- Easy onboarding
- Real-time alerts for Sensitive data access on containers
- User impersonation detection
- FIM on network devices
- Malicious hash detection
- Automated noise cancellation
- Automated FIM Report for PCI 4.0

Demo

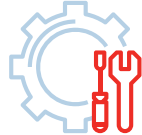


Key Takeaways

Qualys FIM Highlights



No more
manual
reports



No more
siloed tools



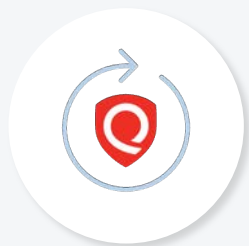
No more fire
drills during
Audits



**No more being
in Continuous
Audit mode**



PCI DSS
4.0 Ready



Latest Updates and Roadmap

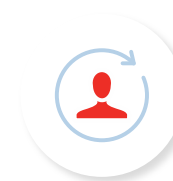
Latest Updates



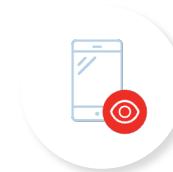
File Access Monitoring (FAM) to detect unauthorized access to sensitive data



FIM on containers



User impersonation detection



FIM on network devices

Roadmap

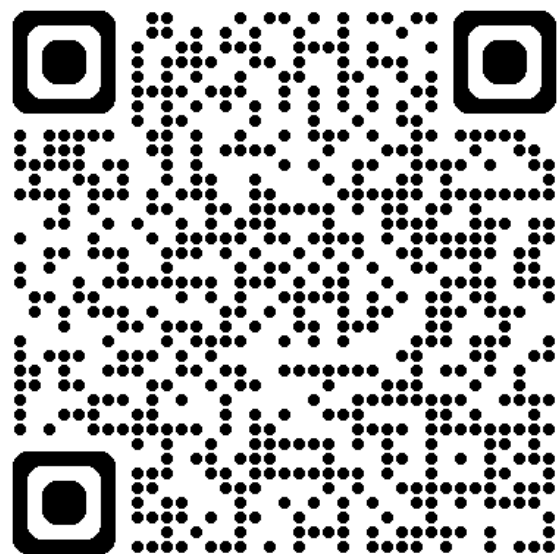
- Fully automated workflow for on-boarding FIM
- Automated noise cancellation
- Response capabilities in FIM – ability to execute commands or scripts on associated hosts in response to FIM events, enabling immediate action and remediation.
- Audit Trails in FIM to track FIM Profile modifications
- FIM Executive Summary Report



 Transurban

Simon Gaiser – CISSP

Cyber Threat & Vulnerability
Specialist, Transurban



Start Your 30-Day
Free Trial of **Qualys FIM**
and get executive FIM
report for PCI 4.0

