FEATURE BRIEF

FILE INTEGRITY MONITORING
with Dome9 SecOps

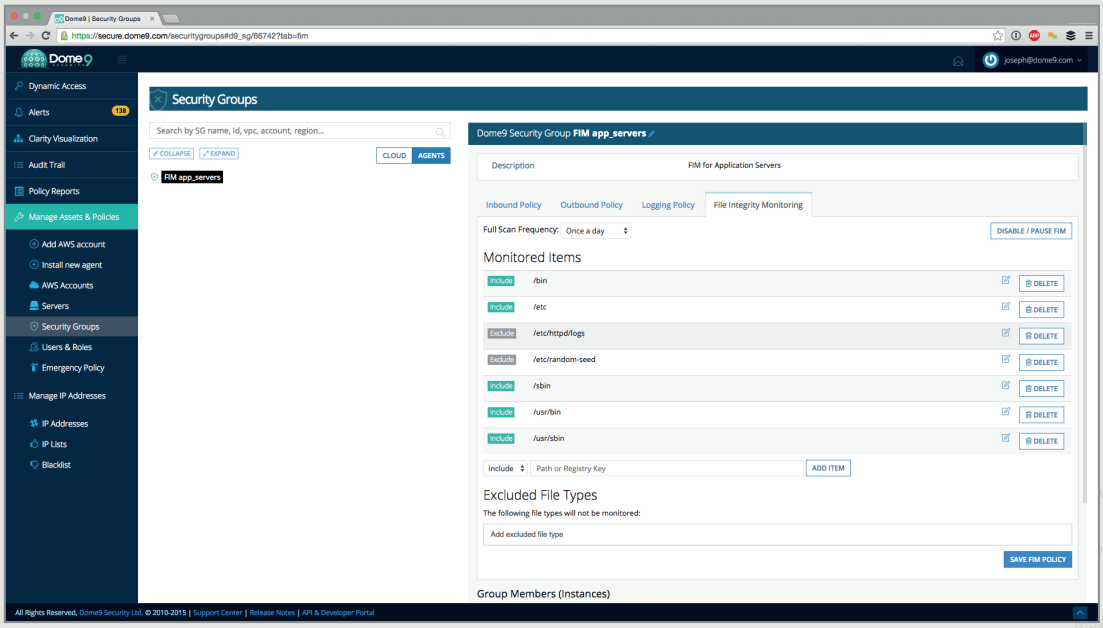
Trap Malicious Activity Across your Cloud Infrastructure

The purpose of most cyber criminals today is gaining secure information in order to gain financial profit. With an endless selection of free open source hacking tools, anyone in the world with an internet connection may be a potential hacker.

Malware is the favorite tool for hackers, and most commonly used. Once a malware is installed on a server, all of the information on the system is compromised for long periods of time until the malware is finally detected. Hackers may use many different approaches in order to get the malware in: social engineering, phishing, software vulnerabilities, etc., but the end goal is the same — install and run the malicious software.

That's where Dome9 SecOps and its File Integrity Monitoring capability comes into play. Dome9's FIM implementation is based on the OSSEC open source package and allows automated and simplified tracking of modification, deletion and creation of selected files and directories on Windows and Linux.

Any attempts to install software, or create or delete files in the system will be detected and reported by Dome9's FIM agent; even rootkits, registry key changes and zero-day attacks. This enables protection for the operating system files, sensitive information and application resources.



Benefits of Using FIM

1. Protection from zero-day and advanced persistent threat attacks
2. Protection of sensitive information and software in the cloud
3. Detection of data loss and data corruption
4. Fulfill compliance regulation and requirements (PCI, HIPAA, SOX and more)

File Integrity Monitoring is a mandatory requirement for complying with the following

- PCI-DSS (Payment Card Industry Data Security Standard, Requirement 11.5)
- HIPAA (Health Insurance Portability and Accountability Act)
- SOX (Sarbanes-Oxley Act)
- NERC-SIP (Nerc Standard SIP)

amazon web services | Partner Network
ADVANCED TECHNOLOGY PARTNER

FILE INTEGRITY MONITORING
with Dome9 SecOps

- SIMPLER SECURITY OPERATIONS
- REDUCED ATTACK SURFACE
- FASTER COMPLIANCE

Key Aspects of Dome9 FIM

Broad Coverage

Dome9 SecOps offers a security layer which tracks and monitors every file system modification, creation and deletion

Advanced Security

Dome9 SecOps offers a security layer that is practically impossible to trick by guaranteeing that any malicious code would be identified once it tries to make persistent or temporary changes to the Operating Sytem file system.

Total Compliance

Dome9 SecOps answers mandatory compliance functionality demands that are required in order to obtain PCI DSS, SOX, or HIPAA certification.

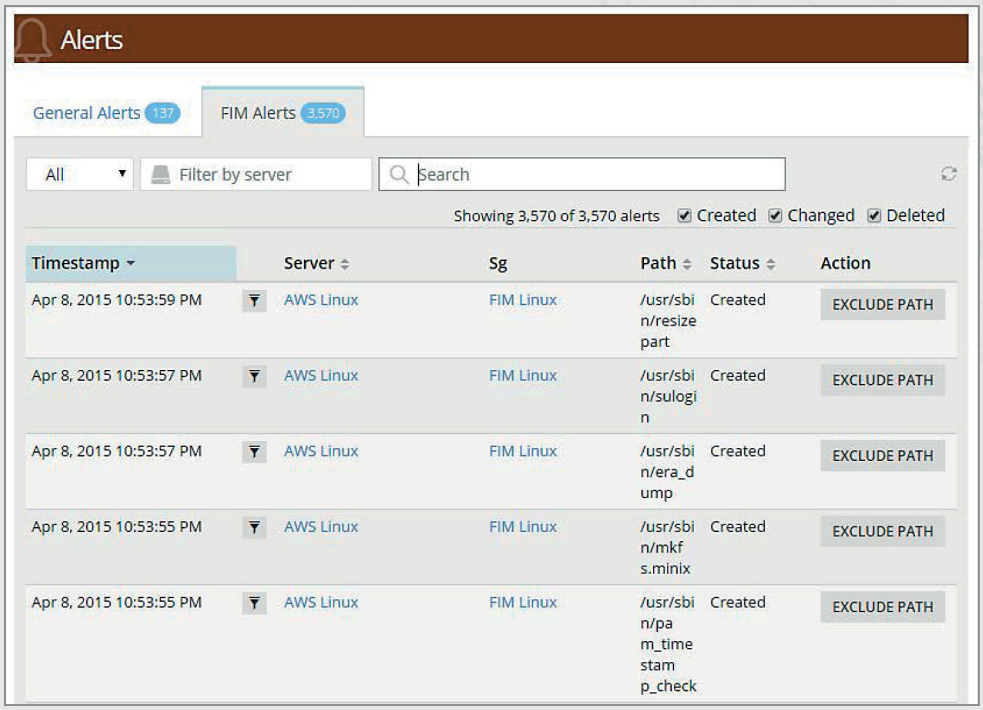
Large Scale

Dome9 SecOps leverages our powerful security policy engine that lets you manage thousands of protected servers under a single Dome9 account

orbograph

"Orbograph's healthcare revenue management solutions meet the strictest HIPAA regulations and security standards. The Dome9 SecOps platform helps us continuously secure our growing AWS cloud infrastructure, and advanced controls such as the embedded file integrity monitoring capability enables us to meet and exceed our auditor's requirements."

Ran Rothschild
Director of Operations
Orbograph



How it Works:

Upon installation of a Dome9 agent and its attachment to a FIM-enabled policy group, an intial scan is performed and a baseline is created. The baseline holds the list of directories, files and their cryptographic checksums and serves as a reference for subsequent scans and real-time protection.

Selected files and directories are then scanned on a periodic basis where the creation of new files is detected. Real-time notification is supported to detect deletion and modification. Changes detected during scheduled scans or upon real-time detection generate alerts that may be handled by different methods. An alert can simply be acknowledged, or the relevant file can be selected to be ignored in subsequent scans by adding it as an exception to the security group FIM policy.

Dome9 is an innovative SaaS-based solution purpose-built to provide security and compliance across Amazon AWS and other public and hybrid cloud infrastructure environments.
Over a thousand organizations, including the world's leading service providers and enterprises, actively secure hundreds of thousands of cloud servers today using Dome9's platform.
The company is headquartered in Menlo Park, CA with an R&D center in Tel-Aviv.

Start your free trial today or schedule a demo with one of our security architects at http://www.dome9.com

info@dome9.com
+1-877-959-6889