White Paper

10 Step FIM Approach for Service Reliability, Data Security and Compliance

The performance and availability of network assets is critical to the delivery of the business services dependent on those assets. Nearly all IT shops have some systematic approach to maintaining the integrity of their network infrastructure to deliver services within acceptable service level agreements (SLAs). Ideally, these systems would have some degree of visibility for the dependencies each asset has for the service being delivered. For instance, an e-mail service dependency map would show the application host location (physical or virtual) and all the connection points (other servers, routers, switches, desktops...) where packets are carried to deliver the e-mail service to the end-users across the enterprise.

Sounds simple on paper but in reality, application dependency and configuration management are fleeting concepts that require a lot of data and human resource to manage. For those of you fortunate to have senior organizational support to drive such an initiative, pat yourselves on the back for a job well done but don't stop here. It is a monumental accomplishment to have business service delivery prioritized in a CMDB or CMS with dependencies mapped out and good visibility to how these services are meeting corporate SLAs.

One area that you shouldn't overlook that can derail your ability to hit those SLAs is file integrity monitoring (FIM). Your inability to uphold file integrity not only compromises your ability to deliver critical applications/ services to both user and customer, but it also puts your organization's security and compliance at risk.

We hear every day of different viruses and attacks almost as if they were coming off an assembly line. They come in all shapes, sizes and forms, and they are becoming more sophisticated and harder to detect. The source of the attacks often comes externally but vulnerability can also be exposed from internal activities, for example a disgruntled employee or batch of stolen passwords. And recently, we are seeing the word "cyberspace" added to U.S. Defense Department documents alongside descriptors normally meant for traditional warfare. Congratulations IT admins, you are now soldiers in fighting the next wave across the terrain of "cyberspace."

In a recent "strategic guidance" paper released by the Obama administration, the DOD states: "Our planning envisages forces that are able to fully deny a capable

state's aggressive objectives in one region by conducting a combined arms campaign across all domains – land, air, maritime, space, and cyberspace."

One of 'a capable state's aggressions': Unprotected file systems

File system attacks are becoming more prevalent and sophisticated. Vulnerability can be at any point in your network, whether it be the weakest or strongest link. One successful intrusion can affect the whole network because the attacking virus tends to have the ability to spread or multiply. And the attack can come at any point within your network where files systems are exposed.

Intrusion happens at any point where critical file systems are not monitored and managed to ensure their integrity. An attack can be pinpointed at a vulnerable spot in your file system and then propagate across your entire network. A prime candidate directory needing dedicated monitoring is the windows "system" directory. Intrusion to this directory and others can lead to a disastrous chain of events.

We tend to think that we have sufficient security and that it just won't happen to us, but the reality is that it can, and it does. Have you ever seen an interview with a security officer of a large company just after an intrusion that wreaked havoc? The response is almost always "I didn't think that we were vulnerable in that area." But, of course, they were.

And we can't forget about compliance, specifically the Payment Card Industry Data Security Standard (PCI DSS), which must also be given strong consideration alongside enterprise security requirements while we are discussing FIM.

So what is File Integrity Monitoring?

A FIM application is a must for any organization that has an anti-threat plan. It ensures file compliance by scanning files in configuration-specified directories on Windows and UNIX systems, periodically checking for unauthorized changes and automatically issuing alerts when files are added, deleted, or modified.

FIM is a hot security topic right now, and without a systematic approach to it, every company is exposed to attack. Consider the recent headline:

"If data loss continues on its current trends, it will cost the U.S. economy $290 billion by 2018. This equates to 1.6% of GDP. Is this year turning out to be even worse for getting hacked than last year?"
–Kevin West, CEO K logix, from National Cyber Security Blog.

What is a good approach?

First off, you should start with the goal to be proactive in understanding attack potential. And for good measure, you should also add a large dosage of checks and balances. In its base form, this is File Integrity Monitoring.

Additionally, file systems that are deemed to be potential targets, need to be monitored CONTINUOSLY. Secondly, we need to ensure that the file system has not been changed. Change is an indication that an attack is underway or has already occurred. We must develop a baseline configuration and ensure ZERO deviation from the baseline. We need to know if there have been any "adds," "changes" or "deletes" whenever possible. If there has been any deviation, we need to have the ability to compare the directory and its contents to the baseline. This can only be accomplished by checking every file in the critical directory specified and, as an added measure of protection, using checksum algorithms on the entire directory. A checksum is a fixed piece of data from an arbitrary block of a larger dataset for the purpose of detecting errors that may have been introduced during transmission or storage. The integrity of data can be checked at any later time by computing the checksum against a stored baseline.

If we monitor using checksum, we'll know if something anomalous has occurred and can enact a proactive response against the proper group or individual to address the attack. Also, it may be equally important to

know when a file has not been altered. An example of this might be a virus definition file that gets updated a couple of times per day. A file of this type updated on a regular basis is normal, and if it hasn't been updated on its periodic schedule, an alert must be sent to the responsible group or individual.

Organizations may also have confidential files that need to be monitored closely, and even if the files are merely opened and not changed, notifications need to be generated in order to alert an administrator that there is potential for a security breach.

The 10 Step Approach

So how do you shore up your files systems to better combat intrusion? The following are 10 steps to ensure greater file integrity and a more secure enterprise:

1. Have a FIM system that can scan files quickly and with high frequency. Many FIM products can scan hundreds of files per second.
2. Have a FIM system that can specify files by directory name, file suffix, file prefix or other keyword qualifier. This will speed up the processing time and help cut down on CPU utilization by removing non-critical files to monitor.
3. Make sure your FIM system has checksum calculation capability so you can check each file to see whether any changes were made down to the single-bit level.
4. Have a FIM system that allows the user to adjust CPU utilization. This "tuning" will allow the FIM system to act non-intrusively during heavily used times of the day while not compromising performance on heavily-loaded systems.
5. Make sure your FIM system supports both 32- and 64-bit operating systems.
6. For complete coverage 24/7/365, allow remote support through a web-based user interface. Make sure that your system allows changes to the FIM program while it is running. You may need to monitor changes and make adjustments on the fly.
7. Ensure that your FIM system can monitor software upgrades and issue alerts when failed updates occur.
8. Have a FIM system that can create an image of specific critical directories as a baseline for comparison in the event a security threat has been detected.
9. Make sure your FIM system satisfies the latest PCI DSS compliance standards to secure customer and corporate financial data.
10. And finally, get the technology and work flows to do this now, and empower your people to lock it down. The time is NOW to slam the door on your file systems being an entry-point for intrusion, period!

Proper File Integrity Monitoring not only ensures network security but it also goes a long way in meeting performance and availability SLAs.

Wrap up

It's blatantly obvious but obviously warrants saying: Cyber-threats don't come in the front door. Oftentimes they take place right under your nose and from an internal threat. File Integrity Monitoring ensures that even the most subtle aggression – opening a file and taking a screenshot – is all it takes to constitute a breach. Could you detect such a breach? Do you know when a file is opened and closed in a critical directory, and by whom? Could you track and spot this activity in a virtual store?

A slight change to a registry file, configuration file, or *.exe file can take down a critical application and cause irreparable damage and compromise compliance. FIM is an imperative in today's highly intrusive IT infrastructure. Intrusion from both internal and external sources predicates the need for a file system baseline and structured, systematic check-and-balance procedure to ensure file integrity. This issue is important enough to the federal government that the term "cyberspace" is being used alongside other domains of protection – land, sea, air, space and now, cyberspace.

Failed business service delivery however is not the only cost of poor file integrity. For any organization that stores credit card data, PCI DSS issues a set of guidelines for compliance that, if not followed, can result in significant fines and revocation of the ability to handle credit card data at all. This happened this past February with the Global Payments Inc. breach that affected up to 1.5 million accounts in North America. In this breach, Visa revoked GPI's seal of approval to handle credit card data and GPI has been reeling ever since.

Clearly the key to FIM has several moving pieces in the form of process, systems, and people, all working together in an integrated approach:

- A practical approach (a process) to manage your file system to a baseline and take action when an exception occurs
- A solution that can snapshot a secure state of your file system and automatically alert your people when an exception has occurred
- The right people to implement the solution and hold watch over the security system with honesty and integrity to ensure business service delivery to SLAs and compliance.

With this approach in place, your cash flow can be allocated to building your business and not reacting to a service outage or compliance penalty.

About CorreLog, Inc.

CorreLog, Inc. delivers security information and event management (SIEM) combined with deep correlation functions. CorreLog's flagship product, the CorreLog Security Correlation Server, combines log management, Syslog, Syslog-NG, SNMP, auto-learning functions, neural network technology, proprietary semantic correlation techniques and highly interoperable ticketing and reporting functions into a unique security solution. CorreLog furnishes an essential viewpoint on the activity of users, devices, and applications to proactively meet regulatory requirements, and provide verifiable information security. CorreLog automatically identifies and responds to network attacks, suspicious behavior and policy violations by collecting, indexing and correlating user activity and event data to pinpoint security threats, allowing organizations to respond quickly to compliance violations, policy breaches, cyber attacks and insider threats. CorreLog provides auditing and forensic capabilities for organizations concerned with meeting SIEM requirements set forth by PCI/DSS, HIPAA, SOX, FISMA, GLBA, NCUA, and others. Maximize the efficiency of existing compliance tools through CorreLog's investigative prowess and detailed, automated compliance reporting. CorreLog markets its solutions directly and through partners.
Visit www.correlog.com for more information.

1004 Collier Center Way, Suite 103 · Naples, Florida 34110 · 1-877-CorreLog · 239-514-3331 · info@correlog.com