A Trend Micro Whitepaper I **May 2016**

Moving Beyond Prevention: Proactive Security with Integrity Monitoring

» Detecting unauthorized changes can be a daunting task—but not doing so may allow a breach to go undetected or you to be out of compliance with key regulations like PCI, HIPAA, and others. With Trend Micro Deep Security's system security capabilities like integrity monitoring, organizations can detect and alert on malicious changes in real-time, giving increased visibility and security.

Version: 1.0

INTRODUCTION

In the face of increasing reports of data losses, intellectual property theft, credit card breaches, and threats to user privacy, organizations today are faced with a great deal of pressure to ensure that their corporate and user data remains secure. Although the traditional preventative controls such as firewalls, intrusion prevention (IPS) and anti-virus are in place and doing their job, the constant stream of vendor patches, zero-days, new attacks like ransomware, and changing security requirements are making it hard for most companies to keep up. This helps to explain why security breaches are happening but also why the average time to identification of a breach is about three months[1]. This has led companies to try and find alternative system security approaches to help address the problem.

One of these approaches requires an understanding of the tactics, techniques, and procedures (TTPs) used by an attacker. These TTPs can vary and do evolve, but they tend to stay around longer than specific hacking tool or exploits. They also generally exploit the same weaknesses, use the same entry points and make similar changes to systems. Monitoring these with integrity monitoring provide a good opportunity to help detect real attacks that can be acted on quickly with a low chance of being a false positive.

98 days

Mean time to identify advanced threats

26 days

Mean time to contain advanced threats

Source: Ponemon Institute Advanced Threats in Financial Services: A Study of North America & EMEA. May 2015

*"In financially motivated **attacks against ecommerce servers**, web shells are used to access the payment application code, which is then **modified with a new feature** that will capture the user input…"*

Source: Verizon 2016 Data Breach Investigations Report

ENHANCED SYSTEM SECURITY: INTEGRITY MONITORING AS A DECTECTIVE CONTROL

File Integrity Monitoring (FIM) is probably best known as a key requirement for PCI-DSS. The intent of that requirement is to ensure that all critical files (both operating system and application) do not change without authorization. Really this is the definition of FIM but the concept of detecting unauthorized changes—even beyond files—can be useful way beyond just helping with PCI compliance.

Beyond just monitoring files, detecting changes to the service state, ports listening, and other configurations are also important, making the right integrity monitoring solution very useful as a detective control. These sort of changes can also be very strong indicators of compromise (IOC), and knowing about them in real-time can allow an organization to act quickly in dealing with a breach.

[1] Ponemon Institute Advance Threats in Financial Services: A Study of North America & EMEA. May 2015

HOW TREND MICRO DEEP SECURITY CAN HELP?

Trend Micro Deep Security's system security package includes Integrity Monitoring, which enables organizations to be alerted in real time to any unexpected changes to Linux or Windows workloads. Addressing the need for monitoring beyond only files, Deep Security can monitor the following for changes:

- Directories
- Files
- Groups
- Installed Software
- Registry Keys
- Registry Values
- Services
- Users
- Ports
- Processes
- Results of WQL Quer

In addition, for virtualized deployments on VMware, the solution uses Intel TPM/TXT technology to perform hypervisor integrity monitoring for any unauthorized changes to the hypervisor, extending security and compliance to the hypervisor layer.

Figure 1: Deep Security dashboard view of integrity monitoring events

HOW DOES DEEP SECURITY HELP TO DEAL WITH NOISE?

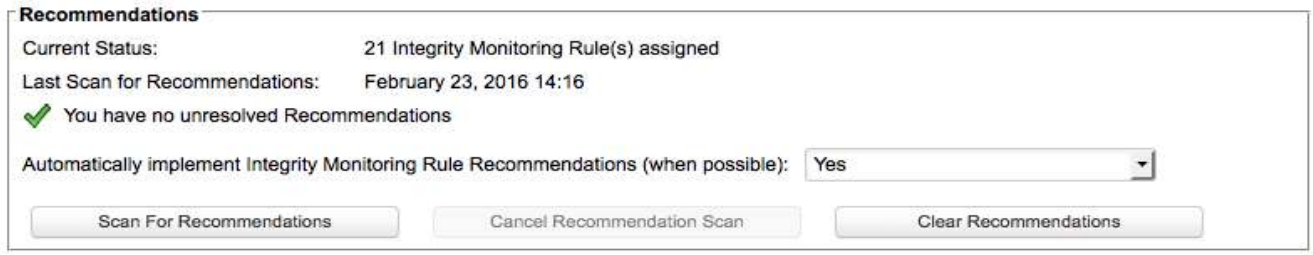
Integrity monitoring can generate a lot of events or noise if not implemented correctly. This could end up being like searching for a needle in a haystack, causing delays and increasing workload in an already over-taxed environment. So knowing which items to monitor is very important. That's why Deep Security provides a number of features to help make this easier.

Trend Micro Threat Research Rules (TMTR)

One of these features is a set of specific rules developed by Trend Micro's Threat Research team to look for highly specific changes to the system that are known to be associated with malicious activities. These rules use multiple sources of change to to reduce the likelihood of a false positive.

Recommendation Scan

A Recommendation Scan is a unique Deep Security feature that can also determine a base set a rules that should be applied to a system. It does this by scanning the system (initially and on an ongoing scheduled basis) to determine the operating system and installed software and then based on what is detected, it recommends rules that should be applied. These rules can also be automatically applied if an organization desires.



Trusted Source Tagging

Trusted Source Event Tagging is designed to reduce the number of events that need to be analyzed by automatically identifying events associated with authorized changes.

A Trusted Source can be either:

1. A Local Trusted Computer,
2. The Trend Micro Certified Safe Software Service, or
3. A Trusted Common Baseline, which is a set of file states collected from a group of computers.

Each option is designed to ease the burden of event management by allowing an administrator to focus on the most important events.

Advanced Monitoring

Deep Security is also highly flexible, providing the ability to create custom rules. There are three templates built-in to the product to help organizations create new rules specific to their needs:

- Registry Value – Monitor changes to registry values
- File – Monitor changes to files
- Custom (XML) - Monitor directories, registry values, registry keys, services, processes, installed software, ports, (and files)

With these customizable templates, administrators can build integrity monitoring rules to best fit the need of the organization.

WHAT KIND OF MALICOUS ACTIVITY CAN DEEP SECURITY DETECT?

There are many TTPs that have been identified and, depending on the system, may be important to monitor. That's why Deep Security's Integrity Monitoring rules can be used to monitor for a wide range of things, including:

- Autorun programs being installed
- Shrinking of log files
- Host file being modified
- Stopping of Anti-Malware
- Installing services
- Network drivers being installed
- Dropping files in the Windows & Win\System32 directory
- Tampering with Web server files and/or directories
- Exfil data
- File permission change (but no file change)

With such broad coverage, it is an ideal solution for proactive security requirements, including those highlighted in sections 6, 10, 11, & 12 of PCI-DSS 3.2.

Below are some examples of how Integrity Monitoring, as a part of Deep Security's system security package, can help monitor and alert on important changes in your environment that may be indicators of compromise (IOCs).

Detecting a Website Defacement

Keeping an eye on changes to files such as the index.html or index.php is a very good way to quickly figure out you've been hacked, and if monitoring for it, can enable a rapid reaction to fix the problem and reduce exposure time.

Depending of the version of Web server, monitoring changes to the .htaccess file is also important. A .htaccess (hypertext access) file is the common name of a directory-level configuration file which allows decentralized management of Web server configuration. Attackers use the .htaccess file to hide malware, backdoors, injecting content and for many other purposes.

Detecting Web Shells

A Web shell is a script/code that runs on a system and can give an attacker remote access to functions on that server. Web shells can be written in any language that a server supports, with the the most common being PHP and .NET languages. These shells can be extremely small, needing only a single line of code or can be full featured with thousands of lines.

Web shells can be installed on a Web server through a compromise such as SQL injection, Remote File Inclusion (RFI), an un-validated file upload feature, or through a valid user's stolen credentials. Once that happens they can gain shell-level access to the host operating system.

To avoid detection by firewalls or antivirus technologies, the attacker may employ evasion techniques such as code obfuscation and encryption. This is where Integrity Monitoring can be extremely useful, as it will notify of all changes to the system and therefore these evasion techniques will not be successful.

Detecting Log File Shrinkage

The expectation that a log file will only grow in size and not shrink is considered to be normal. So detecting such a change is important, as it is a potential IOC. This event may be an attacker trying to cover his\her tracks. Removing log entries related to the attack will make it harder for system admins or forensic investigators track down how the breach happened. It may even help to hide further penetration into the organization reducing the likelihood of being found.

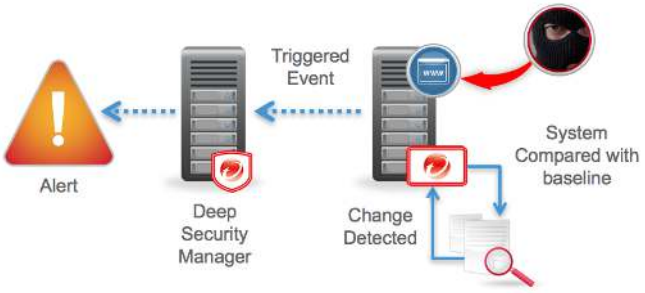
Detecting Lateral Movement

Lateral movement—such as pivoting on the compromised internal network— is an important technique for attackers. A compromised system may be the only entry point to the network. Pivoting allows the attacker to move around unobstructed, bridging the network through this intermediate system. This allows them to gain access to systems they may not otherwise be able to reach.

Pivoting requires ports to be open and certain services to be running. Integrity Monitoring can be configured to alert if any of these are newly added to a system. For example, a Meterpreter session listening on port 4444 will trigger an alert. Invoking NetCat as a listener will do the same.

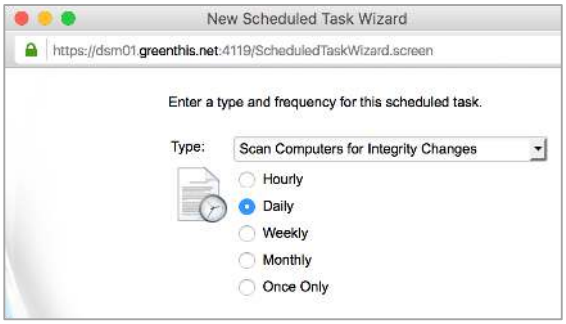
HOW IT WORKS?

Deep Security Integrity Monitoring is a feature that detects changes to select system areas by comparing the current condition of these areas with a hash-based baseline.



These hash-based baselines are created by performing a baseline scan of the areas on the computer specified in the assigned rule. Periodic rescanning of those areas then looks for changes.

This comparison can be triggered using the follow methods:

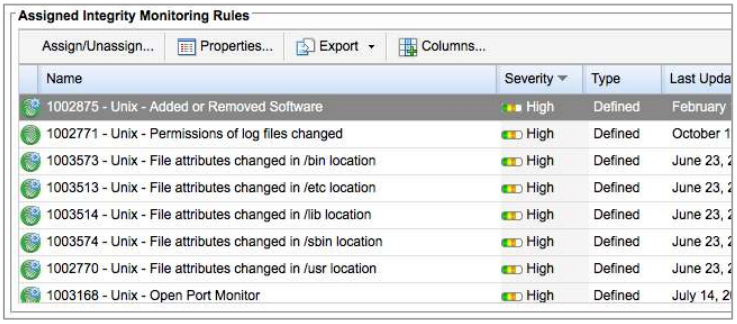


- **Manually** using On-Demand scan trigger - With this option an administrator can initiate a scan by manually clicking the "Scan for Integrity" button or by scheduling a scan in the Deep Security Manager console.
- **Automatically** using the Real-Time trigger - This will be triggered with a change is detected on the monitored entity.

Integrity Monitoring Rules

Integrity Monitoring rules allow the Deep Security Agents to scan for and detect changes. These changes are logged as events in the Deep Security Manager and can be configured to generate alerts. Integrity Monitoring rules can be assigned directly to systems or can be made part of a policy, which can then be applied to multiple systems.

Integrity Monitoring rules specify which entities (files, registry keys, services, etc) to monitor for changes. Deep Security scans all the entities specified by the rules assigned to a system and creates a baseline against which to compare future scans of the system. If future scans do not match the baseline, the Deep Security Manager will log an Integrity Monitoring event and trigger an alert (if so configured).



INTERGRITY MONITORING DEEP DIVE – WEB SHELLS

As was stated previously, a Web shell is a script/code that runs on a system and gives an attacker remote access to functions of the server. They can be installed on a server through a number of methods using techniques like SQL injection, Remote File Inclusion, an unrestricted file upload feature or through a valid user's stolen credentials.

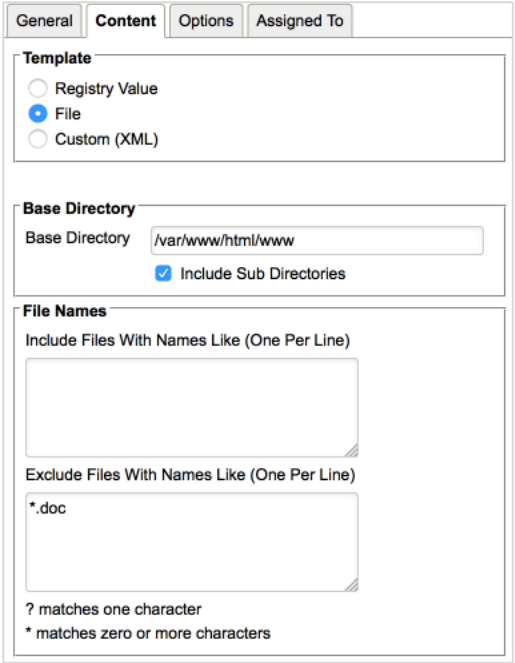
In this Deep Dive we will configure Deep Security's Integrity Monitoring to alert if a specific change is made to a folder on our Web server. In this scenario the business logic of our application only allows for the Microsoft Word file type only. If any other file type exists in the uploads folder, it is a strong indicator of an attack which could be a Web shell. We will also monitor for changes to the listening ports on the server, as this another strong indicator.

Note: In this Deep Dive, rules are being configured on an individual system. Multiple systems can be configured by first configuring a policy, and then applying that policy to each system.

Configuring Deep Security

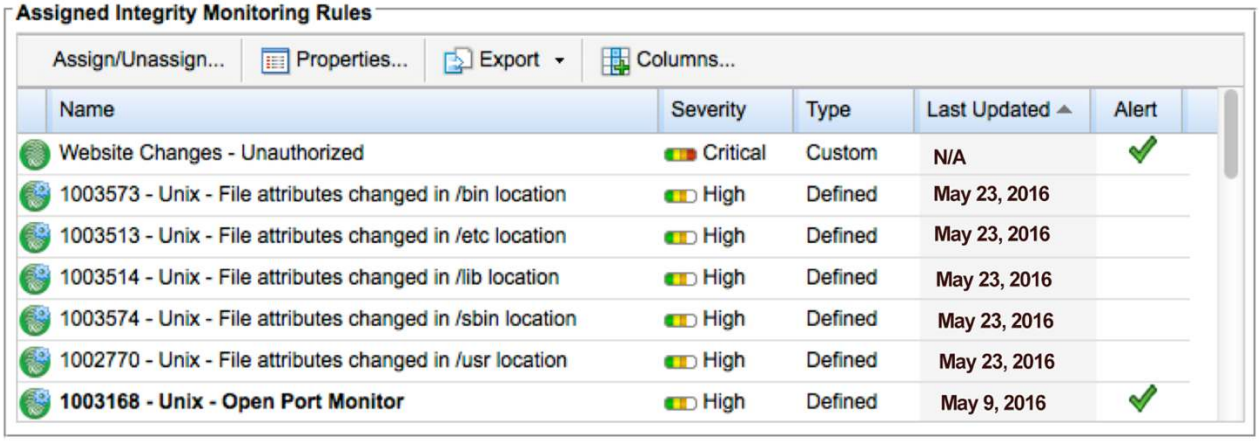
We first configure and install the Deep Security Agent (DSA) and enable Integrity Monitoring. We then "Scan for Recommendations" and choose the option to automatically apply recommended rules.

At this point a base set of Integrity Monitoring rules have been applied to the Web server. These recommended rules have already been configured to notify if changes are detected. Additional customization of the rules can still be performed and in some cases may be required because of specific server and/or application requirements. In our scenario, a new rule is required to monitor the uploads folder on our Web server. We also modified an existing rule (Unix – Open Port Monitor) to send real time alerts if a change is made to the listening ports on the server.



To create a new rule, we open the Integrity Monitoring tab in the Deep Security Manager interface, click Assign/Unassign, then click New and then New Integrity Monitoring Rule. On the General tab we can set the name and choose the Severity. On the Content tab we need to choose a template. In our example we select File and then set the Base Directory we want monitor. We can also include and exclude files to monitor. In our example the business logic of our application only allows for Microsoft Word format only. Therefore, we add *.doc to the "Exclude Files with Names Like" box. This rule will then trigger for any file added to the uploads folder that is not a Microsoft Word document. We then click the options tab and enable alerting and real-time monitoring. We click ok and assign the rule to the server.

We then find and highlight the "Unix – Open Port Monitor" rule and click properties. On the options tab we enable alerting.



Now that we have all the rules created and modified we need to build a baseline. To do that we click on Rebuild Baseline on the Integrity Monitoring tab. Once the task is finished, our system is ready to monitor any changes to the folder.

We also need to configure an On-Demand integrity scan to check the server for changes. We do this in the Deep Security Manager console under Schedule Tasks. We schedule the task to run daily at 12:20 pm. An On-Demand scan is not required for listening ports as events are captured in real time.

Note: Trend Micro Deep Security Integrity Monitoring provides real time integrity monitoring for all Windows systems Entities. For Linux, real time monitoring is only available for identifying changes to running services, processes and listening ports.

Exploiting the system

In our scenario, an attacker exploits a new discovered file upload vulnerability which allows unrestricted uploads to the server. The attacker uploads a file that contains only a few lines of code which allow direct access to the server using a command summited through the URL. This is also known as a Web shell. See Figure 2 for for further details.

The attacker returns later to execute a specially crafted URL that gives command line access to the server. They then start executing commands against the server as part of the reconnaissance phase of the attack.

In Deep Security, the addition of the file to the Web server triggers our Integrity Monitoring rule, and an alert is displayed after our daily scan has completed. At this point, an organization would be able to take action to stop the attack and hopefully stop it from spreading. If the attack includes changes to running ports, Deep Security's real-time Integrity Monitoring picks up this change, and alerts administrators stop the attack. They can then fix the vulnerability on the server, which prevents the attack from happening again.

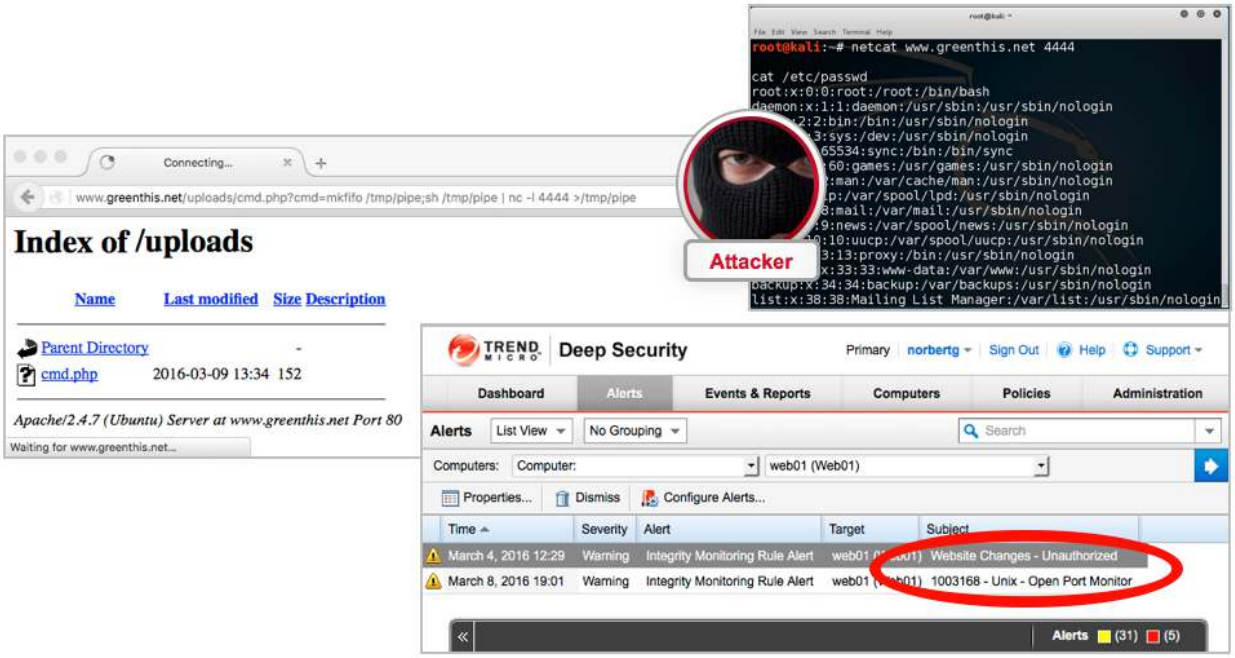


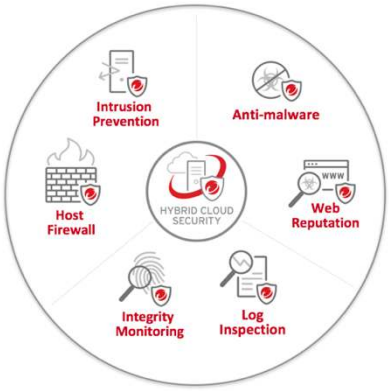
Figure 2: Details of the Web Shell attack

Note: In our Deep Dive example, the only control that we are illustrating is Integrity Monitoring. We are not using any other Deep Security capabilities, which could be used to provide real-time protection for the servers. These include additional capabilities from the Anti-malware, Network, and System Security packages.

CONCLUSION

As organizations search for better ways to protect their environments, Trend Micro Deep Security can play a significant role in addressing many server security requirements. Delivered from the market leader in server security[2], Deep Security can address server security across physical, virtual, cloud & hybrid environments. Available as software, service, or via the AWS and Azure marketplaces, it can help organizations streamline the purchasing and implementation of essential security elements required to protect their environment.

Deep Security includes a comprehensive set of host-based security controls, including:



- **Network security** enabling virtual patching through *Intrusion Detection & Prevention (IDS/IPS)* and a *host-based firewall*
- **Anti-malware** with Web reputation to protect vulnerable systems from the latest in threats
- **System security** through *integrity monitoring* & *log inspection*, enabling the discovery of unplanned or malicious changes to registry and key system files, as well as discovering anomalies in critical log files.

As discussed in this paper, as a part of the system security package, Deep Security's Integrity Monitoring goes beyond typical file integrity monitoring, enabling organizations to:

- Identify suspicious changes on servers, including flagging things like registry settings, system folders, and application files that shouldn't change—when they do. This includes examples like detecting Web site defacement, Web shells, log file shrinkage, and lateral movement.
- Accelerate compliance with key frameworks like the SANS/CIS Critical Security Controls, as well as key regulations like PCI-DSS and HIPAA. For example, PCI-DSS 3.2 specifically calls out file integrity monitoring in sections 6, 10, 11, and 12. Beyond integrity monitoring, Deep Security also helps by delivering multiple security controls, central control, and easy reporting in a single product.

Find out more about Deep Security on our Web site: www.trendmicro.com/hybridcloud.

Securing Your Journey to the Cloud

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.

[2] IDC, Worldwide Endpoint Security Market Shares: Success of Midsize Vendors, #US40546915, Figure 5, Dec 2015