

SENTINEL

REAL TIME FILE MONITORING

WHAT IS SENTINEL?

AND WHAT CAN IT DO FOR YOUR BUSINESS?

SENTINEL is a web application file system and integrity monitor that alerts you in real time if any files, websites, or applications on your server have been compromised. Imagine catching a hacker before they are able to infect the application. Your website is safe and secure with SENTINEL.

About **SENTINEL**

Most Security is Reactionary. Not **SENTINEL**.



What if you could catch hackers in real time before they accessed your data? **SENTINEL** makes that possible.

Increasingly websites and web applications are being attacked and compromised by hackers all around the world. **If you think they target just high profile companies, you'd be wrong.**

What if you could protect your server from these threats before they happen? What if you could be alerted in real time that hackers were trying to compromise your website? With **SENTINEL**, you can catch and eliminate threats before any permanent damage can be done.

1

Real Time Detection

Identify, track and alert on attacks in real time. Determine which modifications are real and which ones are malicious

2

Easy Setup

No coding necessary. Simply install **SENTINEL** on your server, and be instantly monitored.

3

Easy Configuration

Once Installed **SENTINEL** takes care of everything including Anti-Virus checks.

SENTINEL Features

EASILY DETERMINE WHICH FILES WERE UPLOADED, MODIFIED, DELETED, AND INFECTED ON YOUR WEBSITE.



24/7 365 SECURITY MONITORING

Constant Security Monitoring and Protection across all your web applications and domains for total visibility, anytime, anywhere.



WEB APPLICATION FILE INTEGRITY MONITOR

All web application assets are monitored in real time, 24/7, for both file creation and file modification events.



ANTI-VIRUS CHECKS INCLUDED

As soon as a file is uploaded or modified it gets checked against a constantly updated set of Anti-Virus rules.



FULLY AUTOMATED & CUSTOMIZED REPORTING

Generate Daily, Weekly, Monthly, and/or Domain specific reports for total visibility across all your web applications and domains.

Detailed Threat Information

Full scope details on every recorded attack

Detailed File Access Timeline

Complete timeline of file activity across your web application

Detailed Anti-Virus Scans

See if any modified files are actually viruses or malware

Full File Access Type Tracking

Easily determine how and when a file was accessed

The screenshot displays the Phirewall web interface. At the top, there is a navigation bar with tabs for Dashboard, Attacks, Sentinel, Rules, Whitelist, Banned, Users, Reports, and Help. On the right side of the navigation bar, there are links for My Account and Logout. Below the navigation bar, the main content area is titled "Detailed Sentinel Log". It includes a "View the Last:" dropdown menu with options for Year, Month, Week, Day, and All. Below this, it states "Currently showing all entries (1914 Total Entries):" and a page number "196" with a right arrow. There is a search filter section with a "Select Filter" dropdown, a "Select Filter" dropdown, and an "AND" dropdown. Below the search section are three buttons: "Search", "Add Filter", and "Clear Filter". The main part of the interface is a table with the following columns: Domain, File, Action, Status, and Detected Time. The table contains 20 rows of data, showing various file access events for the domain "example.com".

Domain	File	Action	Status	Detected Time
example.com	/home/bluemoun/public_html/wp-content/plugins/gotmls/safe-load/_SESSION/GOTMLS.d81cce6e948117a42c8:832	Added	Clean	Tue, 12-22-2015 3:06:42 AM
example.com	/home/bluemoun/public_html/wp-content/plugins/gotmls/safe-load/_SESSION/GOTMLS.f0363b877684be9a91861cc	Added	Clean	Tue, 12-22-2015 3:06:42 AM
example.com	/home/bluemoun/public_html/wp-content/themes/s5_spectrum/cache/v2update	Modified	Win.Trojan.Cqpass-1714	Tue, 12-22-2015 3:06:42 AM
example.com	/home/bluemoun/public_html/wp-content/plugins/gotmls/safe-load/_SESSION/GOTMLS.7ee8f5081bbb485be5307a	Added	Clean	Sun, 12-20-2015 5:49:03 PM
example.com	/home/bluemoun/public_html/wp-content/plugins/gotmls/safe-load/_SESSION/GOTMLS.53fbbd11609364ba44e51cf	Added	Clean	Sun, 12-20-2015 5:49:03 PM
example.com	/home/bluemoun/public_html/wp-content/plugins/gotmls/safe-load/_SESSION/GOTMLS.00f1c46a3c7b59e9c775446	Added	Clean	Sun, 12-20-2015 5:49:03 PM
example.com	/home/bluemoun/public_html/wp-content/themes/s5_spectrum/cache/v2update	Modified	Clean	Sun, 12-20-2015 5:49:03 PM
example.com	/home/bluemoun/public_html/wp-content/themes/s5_spectrum/cache/v2update	Modified	Clean	Sun, 12-20-2015 5:07:06 PM
example.com	/home/bluemoun/public_html/wp-content/plugins/gotmls/safe-load/_SESSION/GOTMLS.3e9c98961846c940d667a7	Added	Clean	Sun, 12-20-2015 5:05:43 PM
example.com	/home/bluemoun/public_html/wp-content/plugins/gotmls/safe-load/_SESSION/GOTMLS.069e10541973aee920d9bf	Added	Clean	Sun, 12-20-2015 5:05:43 PM
example.com	/home/bluemoun/public_html/wp-content/themes/s5_spectrum/cache/v2update	Modified	Clean	Sun, 12-20-2015 5:05:43 PM
example.com	/home/bluemoun/public_html/test.txt	Removed	Clean	Sun, 12-20-2015 3:37:51 AM
example.com	/home/bluemoun/public_html/test2.txt	Removed	Clean	Sun, 12-20-2015 3:37:51 AM
example.com	/home/bluemoun/public_html/wp-content/themes/s5_spectrum/cache/v2update	Modified	Clean	Sun, 12-20-2015 3:37:51 AM
example.com	/home/bluemoun/public_html/wp-content/themes/s5_spectrum/cache/v2update	Modified	Clean	Sun, 12-20-2015 3:34:06 AM
example.com	/home/bluemoun/public_html/test.txt	Removed	Clean	Sun, 12-20-2015 3:19:20 AM
example.com	/home/bluemoun/public_html/test.txt	Added	Clean	Sun, 12-20-2015 3:18:29 AM
example.com	/home/bluemoun/public_html/test2.txt	Added	Clean	Sun, 12-20-2015 3:18:29 AM
example.com	/home/bluemoun/public_html/wp-content/themes/s5_spectrum/cache/v2update	Modified	Clean	Sun, 12-20-2015 3:18:29 AM
example.com	/home/bluemoun/public_html/wp-content/themes/s5_spectrum/cache/v2update	Modified	Clean	Sun, 12-20-2015 3:17:20 AM

Detailed Custom Reports

Generate custom server, or domain reports daily, weekly, monthly, or yearly



FULL SERVER
SENTINEL FULL REPORT
04-11-2016

SENTINEL.SPECTANT.IO

SENTINEL FULL SERVER REPORT
04/11/2016

Table Of Contents

Executive Summary 3
Detailed Sentinel Log 4

SENTINEL SPECTANT.IO 2/81

SENTINEL FULL SERVER REPORT
04/11/2016

Since 11-19-2015, 1915 file changes have been identified. Of these 1915 file changes, 1 file(s) have been identified as malware.

The following table represents a brief view of the files, their changes, and their changes:

File(s) by Name			
File Name	Change	Malware	Comment
...\\...\\...\\...	ADD	NO	
...\\...\\...\\...	MOD	NO	
...\\...\\...\\...	DEL	NO	
...\\...\\...\\...	ADD	NO	

The PCI standard states that any file identified as malware be removed in order for that system to pass the PCI certification process. Currently 1 file would FAIL a PCI inspection and 1913 files would PASS a PCI inspection.

Following the PCI standard is a great baseline to use in determining which issues to tackle first, but it is important to track ALL file changes that have been identified within your site(s) to fully understand the real cause for why these files were modified and how any identified malware was placed on the system. The following charts represent the number of malware identified as well as the total file activity.

By understanding the real cause for why the files have been added or modified within your site(s) you can begin to understand the underlying application functionality of your site(s) and make appropriate changes to prevent unnecessary file system activity.

SENTINEL SPECTANT.IO 2/81

SENTINEL FULL SERVER REPORT
04/11/2016

Since 11-19-2015, 1915 file changes have been identified. Of these 1915 file changes, 1 file(s) have been identified as malware.

The following table represents a brief view of the files, their changes, whether or not the files contained malware, as well as when the file was added, removed, or modified. The table is organized by date with the most recent change being listed first.

ID	File Name	Change	Malware	ModifiedDate
1915	...\\...\\...\\...	ADD	NO	04/11/2016 10:00:00
1914	...\\...\\...\\...	MOD	NO	04/11/2016 09:55:00
1913	...\\...\\...\\...	DEL	NO	04/11/2016 09:50:00
1912	...\\...\\...\\...	ADD	NO	04/11/2016 09:45:00
1911	...\\...\\...\\...	MOD	NO	04/11/2016 09:40:00
1910	...\\...\\...\\...	DEL	NO	04/11/2016 09:35:00
1909	...\\...\\...\\...	ADD	NO	04/11/2016 09:30:00
1908	...\\...\\...\\...	MOD	NO	04/11/2016 09:25:00
1907	...\\...\\...\\...	DEL	NO	04/11/2016 09:20:00
1906	...\\...\\...\\...	ADD	NO	04/11/2016 09:15:00
1905	...\\...\\...\\...	MOD	NO	04/11/2016 09:10:00
1904	...\\...\\...\\...	DEL	NO	04/11/2016 09:05:00
1903	...\\...\\...\\...	ADD	NO	04/11/2016 09:00:00
1902	...\\...\\...\\...	MOD	NO	04/11/2016 08:55:00
1901	...\\...\\...\\...	DEL	NO	04/11/2016 08:50:00
1900	...\\...\\...\\...	ADD	NO	04/11/2016 08:45:00
1899	...\\...\\...\\...	MOD	NO	04/11/2016 08:40:00
1898	...\\...\\...\\...	DEL	NO	04/11/2016 08:35:00
1897	...\\...\\...\\...	ADD	NO	04/11/2016 08:30:00
1896	...\\...\\...\\...	MOD	NO	04/11/2016 08:25:00
1895	...\\...\\...\\...	DEL	NO	04/11/2016 08:20:00
1894	...\\...\\...\\...	ADD	NO	04/11/2016 08:15:00
1893	...\\...\\...\\...	MOD	NO	04/11/2016 08:10:00
1892	...\\...\\...\\...	DEL	NO	04/11/2016 08:05:00
1891	...\\...\\...\\...	ADD	NO	04/11/2016 08:00:00
1890	...\\...\\...\\...	MOD	NO	04/11/2016 07:55:00
1889	...\\...\\...\\...	DEL	NO	04/11/2016 07:50:00
1888	...\\...\\...\\...	ADD	NO	04/11/2016 07:45:00
1887	...\\...\\...\\...	MOD	NO	04/11/2016 07:40:00
1886	...\\...\\...\\...	DEL	NO	04/11/2016 07:35:00
1885	...\\...\\...\\...	ADD	NO	04/11/2016 07:30:00
1884	...\\...\\...\\...	MOD	NO	04/11/2016 07:25:00
1883	...\\...\\...\\...	DEL	NO	04/11/2016 07:20:00
1882	...\\...\\...\\...	ADD	NO	04/11/2016 07:15:00
1881	...\\...\\...\\...	MOD	NO	04/11/2016 07:10:00
1880	...\\...\\...\\...	DEL	NO	04/11/2016 07:05:00
1879	...\\...\\...\\...	ADD	NO	04/11/2016 07:00:00
1878	...\\...\\...\\...	MOD	NO	04/11/2016 06:55:00
1877	...\\...\\...\\...	DEL	NO	04/11/2016 06:50:00
1876	...\\...\\...\\...	ADD	NO	04/11/2016 06:45:00
1875	...\\...\\...\\...	MOD	NO	04/11/2016 06:40:00
1874	...\\...\\...\\...	DEL	NO	04/11/2016 06:35:00
1873	...\\...\\...\\...	ADD	NO	04/11/2016 06:30:00
1872	...\\...\\...\\...	MOD	NO	04/11/2016 06:25:00
1871	...\\...\\...\\...	DEL	NO	04/11/2016 06:20:00
1870	...\\...\\...\\...	ADD	NO	04/11/2016 06:15:00
1869	...\\...\\...\\...	MOD	NO	04/11/2016 06:10:00
1868	...\\...\\...\\...	DEL	NO	04/11/2016 06:05:00
1867	...\\...\\...\\...	ADD	NO	04/11/2016 06:00:00
1866	...\\...\\...\\...	MOD	NO	04/11/2016 05:55:00
1865	...\\...\\...\\...	DEL	NO	04/11/2016 05:50:00
1864	...\\...\\...\\...	ADD	NO	04/11/2016 05:45:00
1863	...\\...\\...\\...	MOD	NO	04/11/2016 05:40:00
1862	...\\...\\...\\...	DEL	NO	04/11/2016 05:35:00
1861	...\\...\\...\\...	ADD	NO	04/11/2016 05:30:00
1860	...\\...\\...\\...	MOD	NO	04/11/2016 05:25:00
1859	...\\...\\...\\...	DEL	NO	04/11/2016 05:20:00
1858	...\\...\\...\\...	ADD	NO	04/11/2016 05:15:00
1857	...\\...\\...\\...	MOD	NO	04/11/2016 05:10:00
1856	...\\...\\...\\...	DEL	NO	04/11/2016 05:05:00
1855	...\\...\\...\\...	ADD	NO	04/11/2016 05:00:00
1854	...\\...\\...\\...	MOD	NO	04/11/2016 04:55:00
1853	...\\...\\...\\...	DEL	NO	04/11/2016 04:50:00
1852	...\\...\\...\\...	ADD	NO	04/11/2016 04:45:00
1851	...\\...\\...\\...	MOD	NO	04/11/2016 04:40:00
1850	...\\...\\...\\...	DEL	NO	04/11/2016 04:35:00
1849	...\\...\\...\\...	ADD	NO	04/11/2016 04:30:00
1848	...\\...\\...\\...	MOD	NO	04/11/2016 04:25:00
1847	...\\...\\...\\...	DEL	NO	04/11/2016 04:20:00
1846	...\\...\\...\\...	ADD	NO	04/11/2016 04:15:00
1845	...\\...\\...\\...	MOD	NO	04/11/2016 04:10:00
1844	...\\...\\...\\...	DEL	NO	04/11/2016 04:05:00
1843	...\\...\\...\\...	ADD	NO	04/11/2016 04:00:00
1842	...\\...\\...\\...	MOD	NO	04/11/2016 03:55:00
1841	...\\...\\...\\...	DEL	NO	04/11/2016 03:50:00
1840	...\\...\\...\\...	ADD	NO	04/11/2016 03:45:00
1839	...\\...\\...\\...	MOD	NO	04/11/2016 03:40:00
1838	...\\...\\...\\...	DEL	NO	04/11/2016 03:35:00
1837	...\\...\\...\\...	ADD	NO	04/11/2016 03:30:00
1836	...\\...\\...\\...	MOD	NO	04/11/2016 03:25:00
1835	...\\...\\...\\...	DEL	NO	04/11/2016 03:20:00
1834	...\\...\\...\\...	ADD	NO	04/11/2016 03:15:00
1833	...\\...\\...\\...	MOD	NO	04/11/2016 03:10:00
1832	...\\...\\...\\...	DEL	NO	04/11/2016 03:05:00
1831	...\\...\\...\\...	ADD	NO	04/11/2016 03:00:00
1830	...\\...\\...\\...	MOD	NO	04/11/2016 02:55:00
1829	...\\...\\...\\...	DEL	NO	04/11/2016 02:50:00
1828	...\\...\\...\\...	ADD	NO	04/11/2016 02:45:00
1827	...\\...\\...\\...	MOD	NO	04/11/2016 02:40:00
1826	...\\...\\...\\...	DEL	NO	04/11/2016 02:35:00
1825	...\\...\\...\\...	ADD	NO	04/11/2016 02:30:00
1824	...\\...\\...\\...	MOD	NO	04/11/2016 02:25:00
1823	...\\...\\...\\...	DEL	NO	04/11/2016 02:20:00
1822	...\\...\\...\\...	ADD	NO	04/11/2016 02:15:00
1821	...\\...\\...\\...	MOD	NO	04/11/2016 02:10:00
1820	...\\...\\...\\...	DEL	NO	04/11/2016 02:05:00
1819	...\\...\\...\\...	ADD	NO	04/11/2016 02:00:00
1818	...\\...\\...\\...	MOD	NO	04/11/2016 01:55:00
1817	...\\...\\...\\...	DEL	NO	04/11/2016 01:50:00
1816	...\\...\\...\\...	ADD	NO	04/11/2016 01:45:00
1815	...\\...\\...\\...	MOD	NO	04/11/2016 01:40:00
1814	...\\...\\...\\...	DEL	NO	04/11/2016 01:35:00
1813	...\\...\\...\\...	ADD	NO	04/11/2016 01:30:00
1812	...\\...\\...\\...	MOD	NO	04/11/2016 01:25:00
1811	...\\...\\...\\...	DEL	NO	04/11/2016 01:20:00
1810	...\\...\\...\\...	ADD	NO	04/11/2016 01:15:00
1809	...\\...\\...\\...	MOD	NO	04/11/2016 01:10:00
1808	...\\...\\...\\...	DEL	NO	04/11/2016 01:05:00
1807	...\\...\\...\\...	ADD	NO	04/11/2016 01:00:00
1806	...\\...\\...\\...	MOD	NO	04/11/2016 12:55:00
1805	...\\...\\...\\...	DEL	NO	04/11/2016 12:50:00
1804	...\\...\\...\\...	ADD	NO	04/11/2016 12:45:00
1803	...\\...\\...\\...	MOD	NO	04/11/2016 12:40:00
1802	...\\...\\...\\...	DEL	NO	04/11/2016 12:35:00
1801	...\\...\\...\\...	ADD	NO	04/11/2016 12:30:00
1800	...\\...\\...\\...	MOD	NO	04/11/2016 12:25:00
1799	...\\...\\...\\...	DEL	NO	04/11/2016 12:20:00
1798	...\\...\\...\\...	ADD	NO	04/11/2016 12:15:00
1797	...\\...\\...\\...	MOD	NO	04/11/2016 12:10:00
1796	...\\...\\...\\...	DEL	NO	04/11/2016 12:05:00
1795	...\\...\\...\\...	ADD	NO	04/11/2016 12:00:00
1794	...\\...\\...\\...	MOD	NO	04/11/2016 11:55:00
1793	...\\...\\...\\...	DEL	NO	04/11/2016 11:50:00
1792	...\\...\\...\\...	ADD	NO	04/11/2016 11:45:00
1791	...\\...\\...\\...	MOD	NO	04/11/2016 11:40:00
1790	...\\...\\...\\...	DEL	NO	04/11/2016 11:35:00
1789	...\\...\\...\\...	ADD	NO	04/11/2016 11:30:00
1788	...\\...\\...\\...	MOD	NO	04/11/2016 11:25:00
1787	...\\...\\...\\...	DEL	NO	04/11/2016 11:20:00
1786	...\\...\\...\\...	ADD	NO	04/11/2016 11:15:00
1785	...\\...\\...\\...	MOD	NO	04/11/2016 11:10:00
1784	...\\...\\...\\...	DEL	NO	04/11/2016 11:05:00
1783	...\\...\\...\\...	ADD	NO	04/11/2016 11:00:00
1782	...\\...\\...\\...	MOD	NO	04/11/2016 10:55:00
1781	...\\...\\...\\...	DEL	NO	04/11/2016 10:50:00
1780	...\\...\\...\\...	ADD	NO	04/11/2016 10:45:00
1779	...\\...\\...\\...	MOD	NO	04/11/2016 10:40:00
1778	...\\...\\...\\...	DEL	NO	04/11/2016 10:35:00
1777	...\\...\\...\\...	ADD	NO	04/11/2016 10:30:00
1776	...\\...\\...\\...	MOD	NO	04/11/2016 10:25:00
1775	...\\...\\...\\...	DEL	NO	04/11/2016 10:20:00
1774	...\\...\\...\\...	ADD	NO	04/11/2016 10:15:00
1773	...\\...\\...\\...	MOD	NO	04/11/2016 10:10:00
1772	...\\...\\...\\...	DEL	NO	04/11/2016 10:05:00
1771	...\\...\\...\\...	ADD	NO	04/11/2016 10:00:00
1770	...\\...\\...\\...	MOD	NO	04/11/2016 09:55:00
1769	...\\...\\...\\...	DEL	NO	04/11/2016 09:50:00
1768	...\\...\\...\\...	ADD	NO	04/11/2016 09:45:00
1767	...\\...\\...\\...	MOD	NO	04/11/2016 09:40:00
1766	...\\...\\...\\...	DEL	NO	04/11/2016 09:35:00
1765	...\\...\\...\\...	ADD	NO	04/11/2016 09:30:00
1764	...\\...\\...\\...	MOD	NO	04/11/2016 09:25:00
1763	...\\...\\...\\...	DEL	NO	04/11/2016 09:20:00
1762	...\\...\\...\\...	ADD	NO	04/11/2016 09:15:00
1761	...\\...\\...\\...	MOD	NO	04/11/2016 09:10:00
1760	...\\...\\...\\...	DEL	NO	04/11/2016 09:05:00
1759	...\\...\\...\\...	ADD	NO	04/11/2016 09:00:00
1758	...\\...\\...\\...	MOD	NO	04/11/2016 08:55:00
1757	...\\...\\...\\...	DEL	NO	04/11/2016 08:50:00
1756	...\\...\\...\\...	ADD	NO	04/11/