

The background of the top half of the page is a dark, abstract graphic. It features a glowing red and orange circular pattern on the right side, resembling a stylized globe or a data visualization. The background is filled with faint, glowing letters and symbols, suggesting a digital or network environment.

# ACTIONABLE INSIGHTS WITH UNPARALLELED FIM VISIBILITY

**Tripwire** invented File Integrity Monitoring, however that's only one reason why so many consider "Tripwire" synonymous with this critical security control. Tripwire® Enterprise has taken FIM far beyond basic change auditing. It not only collects highly detailed change data in real time, it also adds change intelligence and automated remediation and then integrates this data with the other critical security controls found in Tripwire's integrated solutions.

Tripwire's industry leading FIM solution not only detects changes to files, but helps IT remediate unauthorized changes, reduce risk and maximize uptime.

**LinkShadow®** Cyber Security Analytics Platform is designed to manage threat in real-time utilizing Artificial Intelligence-based Machine Learning to analyze events, perform UEBA, cutting-edge threat hunting & provides threat anticipation.

LinkShadow® provides unparalleled detection of the most sophisticated threats which enhances an organization's defense against advanced cyber-attacks, zero-day malware and ransomware. The chance of an attacker passing through your network is virtually nonexistent.

## INTEGRATION STORY: LINKSHADOW - TRIPWIRE

**LinkShadow®** integrates with Tripwire to complete the full cycle of User and Entity Behavioral Analytics and threat hunting to get the optimum benefit of Tripwire Enterprise technology along with proactive threat detection.

LinkShadow gets full visibility from Tripwire Enterprise around system change activities. LinkShadow injects this intelligence into the advanced machine learning algorithms to identify suspicious and anomalous activities based on the behavioral analysis. LinkShadow act proactively to system change activities that might indicate an early stage of an attack for faster resolution and forensic value.

The image displays two screenshots of the Tripwire Enterprise interface. The top screenshot shows the 'Compliance' section with a table of detected changes. The bottom screenshot shows the 'File Integrity' section with a table of detected file modifications.

TimeDetected	ElementName	RuleName	Severity	ChangeType	TimeReceived
2020-12-21 13:08:01-04:00	C:\User\Administrator\Desktop\testfile.exe	testfile	0	MODIFIED	2020-12-21 05:01:46-04:00
2020-12-21 13:14:05-04:00	C:\User\Administrator\Desktop\testfile.exe	testfile	8000	MODIFIED	2020-12-21 05:09:52-04:00

  

ElementName	PolicyTestName	State	SummaryState
-jy2qj2Dch6n-7jy2qj2Dch6n	Security Group Management: Success and Failure	FAILED	FAILED
-jy2qj2Dch6n-7jy2qj2Dch6n	Security State Change: Success	FAILED	FAILED
-jy2qj2Dch6n-7jy2qj2Dch6n	Security System Event: Success and Failure	FAILED	FAILED
-jy2qj2Dch6n-7jy2qj2Dch6n	Manage Auditing and Security Log: Administrators	FAILED	FAILED
-jy2qj2Dch6n-7jy2qj2Dch6n	Sensitive Privilege User: Success and Failure	FAILED	FAILED
-jy2qj2Dch6n-7jy2qj2Dch6n	Shut down the System: Administrators	FAILED	FAILED
-jy2qj2Dch6n-7jy2qj2Dch6n	System Shutdown without Logout: Disabled	PASSED	PASSED
-jy2qj2Dch6n-7jy2qj2Dch6n	Digitally Sign Secure Channel Data: Enabled	PASSED	PASSED
-jy2qj2Dch6n-7jy2qj2Dch6n	Workstation When SmartCard Removed: Lock Workstation or Higher	FAILED	FAILED
-jy2qj2Dch6n-7jy2qj2Dch6n	Special Login: Success	PASSED	PASSED

## HIGHLIGHTS:

- » Detecting early stages of threats for faster MTTR
- » Gaining visibility on the remote workers
- » Detecting malicious file hashes with intelligence feeds
- » Correlating unusual file modifications on multiple systems simultaneously