promisec
Actionable Endpoint Intelligence

>> Capabilities Overview:
File Integrity Monitoring (FIM) and
File Reputation Service

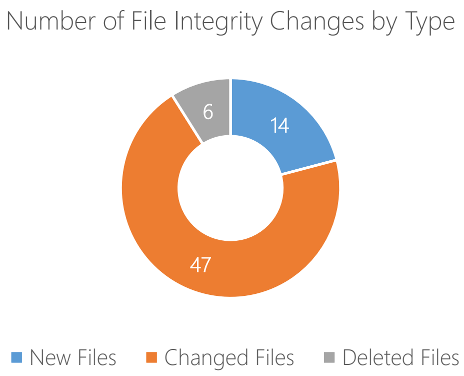
File Integrity Monitoring with Integrated File Reputation

Stop Threats Before They Have a Chance to Start

Despite every effort to maintain good access control, critical static files will change on endpoints in your environment. While some files will change simply as a part of using a desktop, laptop or server, core operating system and application files should *never* change unless they're being patched or upgraded. If those files are compromised by malware or are replaced with older, deprecated versions, new threats and vulnerabilities can make their way onto your technology assets, and the results can be devastating. You need to know when files change, the contextual information to understand why, and most of all, the assurance that files are not compromised by rootkits, trojans or other malware.

Full-Context File Changes with Integrated File Reputation

File integrity monitoring (FIM) and file reputation monitoring are fully-integrated features of the Promisec Enterprise Manager (PEM) platform. FIM allows system administrators and managers as well as security professionals to gain immediate insight into critical files and directories that have changed over time. File reputation compares new and modified files to a globally-sourced database of known bad actors, and allows organizations to identify files that represent an immediate threat. PEM delivers true, hash-based FIM capabilities, allowing security and IT operations professionals to quickly identify changes that are suspect, and integration with file reputation allows security personnel to rapidly identify suspect files and quickly take action. PEM users can automatically correlate this information with other intelligence data from the PEM platform to determine whether file changes are legitimate, or whether they point to operational or security problems within the environment.

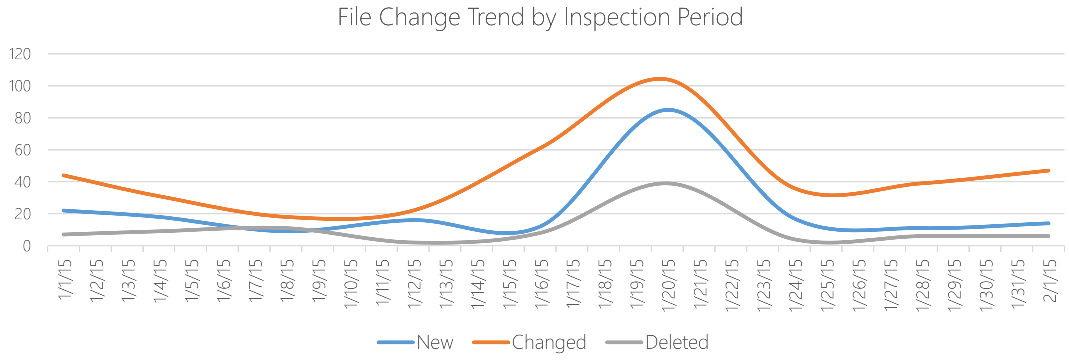


Promisec delivers file integrity metrics through clear, unambiguous visualizations and reports

Fully Integrated, Fully Agentless

Unlike other endpoint detection and response (EDR) products that either have no native FIM capability or file reputation, or charge separately for these capabilities as "modules", Promisec Enterprise Manager provides FIM and file reputation as out-of-box capabilities that provide seamless integration with other data collected within the PEM intelligence engine, allowing security and IT operations personnel to gain a deeper understanding of what is really affecting and influencing their end points.

And of course, like all other components of the PEM platform, our file integrity monitoring is 100% agentless with a zero footprint on your endpoints, ensuring no unwanted performance impacts and eliminating complex distribution and management scenarios.



Promisec demonstrates file integrity patterns and trends over time, so security personnel can identify anomalies that occur outside of change control.

Contact Promisec today, and see how unified endpoint security and IT operations can reduce the risks to your enterprise, without the added complexity of a heavy, agent-based solution.

>> Contact Us: +1.781.453.1105 | sales@promisec.com | www.promisec.com