

Automated Security Configuration and Compliance Management

Discover, diagnose, and repair unwanted changes and unexpected conditions

Triumphant detects and analyzes changes and unexpected conditions on endpoints to determine if those changes are problematic to the security, configuration, or performance of assets managed by McAfee® ePolicy Orchestrator® (ePO™). When a problem is detected, Triumphant Resolution Manager synthesizes a situational remediation that automatically returns the machine to a secure and compliant state. ePO administrators have complete visibility and control of these processes, and event data is directly integrated into the ePO event database.

The endpoint computer population of any organization is undergoing constant change and evolution. The challenge is determining which of these changes represent a potential problem with the security, configuration, or performance of the affected machine. Triumphant leverages patented analytics to detect changes at the most granular level in endpoint computers and servers, analyze the impact of those changes, and synthesize a situational remediation that addresses unwanted changes and unexpected conditions. This capability helps organizations detect previously unidentified malicious attacks, perform security configuration management, and enforce organizational and mandated security policies. The result is greater protection, reduced risk, and increased compliance delivered with greatly reduced labor costs.

McAfee Compatible Solution

Triumphant Resolution Manager v4.3
and McAfee ePO 4.0

Granular Change Detection and Unique Analytics

Triumphant Resolution Manager continually monitors over 200,000 elemental attributes on every endpoint machine, and uses changes to those attributes as the trigger for applying analytic methods to detect potential problems. Triumphant checks these attributes against user defined configurations and policies, against regulatory standards such as PCI or Federal Desktop Core Configuration (FDCC), or against a normative baseline of the organization's endpoint population automatically created by Triumphant's patented analytics. When a machine is found to be out of compliance or a problem is detected, Triumphant synthesizes a situational remediation to return the machine to the desired state. The automated enforcement of configurations and policies ensures that the machine is at a state of continuous security readiness with a minimal amount of human interaction. This, in turn, reduces the attack surface and lowers risk.

Close Integration With ePO

McAfee ePO administrators can take advantage of extensive integration between Triumphant and ePO for visibility and control of Triumphant processes. Triumphant can send alerts to the ePO dashboard to proactively warn of detected problems. Data from Triumphant is integrated into the ePO dashboard in the form of a dashboard summary of the conditions detected by Triumphant Resolution Manager, with the ability to further drill down for more detail. This integration also allows for drill downs from ePO screens into actionable information regarding machine status, configuration, change history, incident history, and performance. Diagnosis summaries provide the ability to move from the ePO view into the Triumphant environment to review, remediate, and perform other related tasks. Incident data from Triumphant is directly transferred into the ePO incident database using the Common Event Format, to ensure that information about the incidents detected and remediated by Triumphant are seamlessly integrated into the ePO data flow. The integration also includes the ability to distribute the Triumphant agent through ePO.

