Automated Security Configuration and Compliance Management

Discover, diagnose, and repair unwanted changes and unexpected conditions

Triumfant 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, Triumfant 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. Triumfant 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.

Granular Change Detection and Unique Analytics
Triumfant 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. Triumfant 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 Triumfant's patented analytics. When a machine is found to be out of compliance or a problem is detected, Triumfant 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 Triumfant and ePO for visibility and control of Triumfant processes. Triumfant can send alerts to the ePO dashboard to proactively warn of detected problems. Data from Triumfant is integrated into the ePO dashboard in the form of a dashboard summary of the conditions detected by Triumfant 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 Triumfant environment to review, remediate, and perform other related tasks. Incident data from Triumfant is directly transferred into the ePO incident database using the Common Event Format, to ensure that information about the incidents detected and remediated by Triumfant are seamlessly integrated into the ePO data flow. The integration also includes the ability to distribute the Triumfant agent through ePO.
Context Sets Triumfant Apart
The patented analytics at the foundation of Triumfant Resolution Manager analyze granular changes in the context of the broader endpoint population, not just the affected machine. The analytics use sophisticated correlation and grouping methods to build a detailed, multidimensional representation of the endpoint population called the Adaptive Reference Model. This model contains a normative baseline of configuration settings that is generated automatically and is continuously refreshed to capture the normal evolution of the organization’s endpoints. By combining the granular change detection capabilities of Triumfant with the context of the Adaptive Reference Model, Triumfant can detect problems without the need for prior knowledge of the problem. This context also ensures that the analysis performed by Triumfant is accurate and free from false positives.

The net effect is that Triumfant does not rely on explicit configurations and policies to see compliance and configuration issues in individual machines. Of course, organizations can provide explicit configurations and policies which will be integrated into the Adaptive Reference Model and subsequently continuously enforced. But the unique capabilities of Triumfant extend configuration management to those attributes not addressed by explicit rules by leveraging the baseline.

These same analytics also power the unique capability to synthesize a situational remediation to address detected problems. Continuous monitoring means that Triumfant sees changes to the endpoint machine, and the analytics leverage the available context of the Adaptive Reference Model to correlate the changes and group them into broader incidents. It is this depth of knowledge that allows Triumfant to build a remediation that addresses all facets of the incident, including collateral damage to the machine. The context of the Adaptive Reference Model also powers unique donor technology that will use other machines in the affected machines group to provide replacements for missing or corrupted files and registry keys.

The extent of Triumfant’s analytics provides deep insights into the endpoint population, and Triumfant has built an extensive library of reports that surfaces this information in extremely actionable formats. Much of this unique data is available via simple drill downs from the ePO dashboard, providing easy integration with existing ePO screens.

About Triumfant
Triumfant’s ability to automatically discover, diagnose, and repair unwanted changes and unexpected conditions on endpoint computers ensures that each organization’s machines maintain the highest level of security readiness with minimal human costs. The result is lower risk, reduced labor costs, and increased compliance. Integration with ePO allows visibility and control to the Triumfant capabilities through the ePO dashboard.

About McAfee ePolicy Orchestrator (ePO) software
McAfee ePO software is the industry-leading security and compliance management platform. With its single agent and single console architecture, ePO software provides intelligent protection that is automated and actionable, enabling organizations to reduce costs and improve threat protection and compliance.