



For Immediate Release

U.S. Army Adds Triumfant to Information Assurance Approved Products List

Triumfant Resolution Manager Approved for Anomaly Detection on Endpoint Computers and Servers

Rockville, MD – April 6, 2009 -- [Triumfant](#)®, creator of patent-pending software that automatically discovers, analyzes and remediates unexpected changes and conditions at the endpoint, today announced that Triumfant Resolution Manager has been approved for the U.S. Army Information Assurance Approved Products List (AIAPL). Selection of Resolution Manager for Anomaly Detection on laptop computers, desktop computers and servers was based upon receipt of a favorable Lab report of the stringent Army's IA tools evaluation process by the U.S. Army Technical Integration Center for the U.S. Army Office of Information Assurance and Compliance (OIA&C).

"Triumfant is extremely pleased and proud to be added to the Army's Approved Product List," said John Prisco, president and CEO of Triumfant, Inc. "Our addition to this list demonstrates the ability of Triumfant Resolution Manager to meet the Army's high standards for security and operability under rigorous testing. Our inclusion as the only approved vendor for anomaly detection is further validation of the uniqueness of our product and; therefore, the unique value it can deliver for our DoD customers. Triumfant is dedicated to ensuring that DoD customers can use our products with confidence knowing that we have passed the testing by the Army Technology Integration Center (TIC)."

Triumfant Resolution Manager uses its patent-pending analytics to identify and remediate anomalies - unexpected changes and conditions - in endpoint computers and servers. Triumfant uses this ability to:

- See the malicious code that other signature based endpoint security products miss, by detecting anomalies that are indicators of malicious activity such as suspicious auto-start methods, unusual firewall exceptions, and anomalous modifications to the TCP/IP stack. Triumfant requires no prior knowledge or signature to detect an attack, and the remediation process addresses all collateral damage to the machine eliminating the need to re-image infected computers.
- Ensure that every machine starts every day compliant and audit ready to any number of policies and controls, including FDCC compliance. For example, Triumfant has expressed the Army Golden Master into a set of policies and can detect and remediate non-compliance automatically.
- Reduce the number of trouble tickets by a 20 percent to 40 percent by proactively spotting and fixing problems before they interrupt service. This includes the removal of unauthorized software.

Because Triumfant scans machines to the most granular level, it can readily spot anomalies and then perform in-depth analysis of the detected change to assess the threat it represents and synthesize a surgical remediation for that specific problem on that specific machine. Patent-pending analytics assure that the detected condition is truly anomalous by comparative analysis to other machines in the endpoint population; thereby eliminating the false positives that have been problematic for previous attempts at anomaly detection.

About Triumfant

Triumfant® leverages a one-of-a-kind ability to discover, diagnose and repair unwanted changes to endpoint computers and servers to create compelling solutions for endpoint security, compliance and configuration management, and incident and problem management. These solutions, powered by the Triumfant Resolution Manager™ platform, enable businesses and government agencies to reduce IT support costs, minimize security risks, enforce continuous compliance and increase quality of service. For more information, visit www.triumfant.com.

Triumfant, Triumfant Resolution Manager and the Triumfant logo are the exclusive properties of Triumfant, Inc. and are registered with the U.S. Patent and Trademark Office.

Triumfant Press Contact:

Nicole Nolte
Welz & Weisel Communications
(703) 218-3555
Nicole@w2comm.com