

INTRODUCTION TO TRIUMFANT



What We Do

Triumphant offers unique software that automatically discovers, analyzes and remediates unexpected changes and conditions on endpoint computers and servers, assuring that these computers are compliant, properly configured and secure so they are ready for business. We deeply scan every computer, every day, analyze that information to detect problems, diagnose those detected problems, synthesize a remediation, and automatically apply that remediation.

In short, we assure organizations that their endpoint computers are business ready, which has the resulting benefits of minimizing security risks, reducing IT support costs, ensuring compliance and increasing quality of service. More specifically, we apply our solution to the following:

- [Security](#). Triumphant first ensures that all security policies and controls are enforced across the organization and that endpoint security software is properly installed, is properly configured and is operational. Triumphant then closes a critical gap in the perimeter by detecting the threats that evade traditional signature based security software. Triumphant will analyze such an attack, assess the threat it represents, and synthesize a remediation to remove the malicious software. The unique capabilities of the Triumphant platform make it a critical last line of defense.
- [Compliance and Configuration Management](#). Triumphant ensures that endpoint computers and servers are compliant and properly configured for business by eliminating the problems caused by a complex and constantly evolving operating and technical environment. Machines can be checked against organization specific policies and configurations, or pre-defined policies for federal or industry specific mandates.
- [Incident and Problem Management](#). Triumphant reduces service desk calls and reported incidents by proactively identifying and resolving known errors on endpoint computers and servers, and by detecting, analyzing, and remediating previously unidentified problems. This eliminates user downtime and reduces the time service desks spend on resolving software and hardware issues by up to 50%.

Security

The evolving nature of malicious attacks coupled with the complexity of dealing with the rapid change and increasing complexity of endpoint computer environments has made securing endpoint computers an enormous challenge. Random hacking for disruption and recognition has evolved to targeted attacks for financial gain by organized groups of cyber criminals. New attacks are being constantly created that evade traditional signature based defensive software, and even when an attack has a known signature it can still slip through the perimeter. Compounding the problem is the fact that far too often defensive software is improperly installed or improperly configured, preventing this software from doing its job. A recent study by Verizon Business showed that a vast majority – 94% - of security incidents can be traced to software that is either missing or mis-configured. ¹

The first way Triumphant helps secure endpoint computers is to make sure that all elements of security readiness – software, policies, and controls – are in place for every computer, every day. This is accomplished by deeply scanning each computer and using Triumphant’s patent

pending analytics to assess the following critical elements of endpoint security:

- Triumfant checks to see that the organization's standard portfolio of endpoint security software is deployed, properly configured, and operating as expected, thereby maximizing the effectiveness of these tools.
- Triumfant checks each machine to ensure that it starts the day in compliance with security policies and controls. This includes hundreds of settings in the operating system and various applications.
- Triumfant checks each computer for known software vulnerabilities, identifying situations where missing patches are creating a security exposure.

When Triumfant detects an unexpected change or condition, it analyzes the incident, synthesizes the appropriate remediation and applies that remediation, eliminating the need for human diagnosis and intervention. The idea is painfully simple: all of the protections deployed by an organization are only effective if enforced and in working order.

The second way Triumfant helps secure endpoint computers is by detecting the zero-day attacks and the other malicious activity that traditional signature based tools often miss. A recent Gartner study stated: "Even the best signature databases can miss the wild threats 2% to 10% of the time, and most have less than a 50% chance of catching completely new threats. Signatures are extremely ineffective against targeted threats and zero day threats." ² Triumfant's analytical engine contains anomaly based detection that can identify unusual changes in sensitive areas of the software that are consistent with the behaviors and structures of malicious applications. When such an attack is discovered, Triumfant determines the components of the suspected malware, the threat level it represents and synthesizes a remediation to remove the malicious code. And Triumfant does not stop at removing the offending program; it also cleans up artifacts associated with the attack.

The end result is that the security risk to endpoint machines is minimized and critical gaps in endpoint security are closed. Triumfant ensures that the steps already in place to protect endpoint computers are doing their job, and then steps in to identify attacks that these protections do not see, making Triumfant the last line of defense. Other offerings can perform configuration management, but they do not deliver the daily frequency or the diagnostic range and accuracy of Triumfant. Furthermore, Triumfant's ability to use anomaly based detection to identify attacks not covered by signature based tools is completely unique to the industry. The story is completed with a reporting capability that provides unmatched visibility into the organization's security readiness.

Compliance and Configuration Management

Triumfant ensures that endpoint computers and servers are compliant and properly configured for business, effectively eliminating the problems caused by a complex and constantly evolving operating and technical environment. In the past, compliance implied passing an audit once per quarter or once per year. With Triumfant, every machine is effectively audited every day, and if a non-compliant condition is detected, the problem is analyzed, an appropriate remediation is synthesized, and the machine is automatically remediated to restore it to compliance.

Triumphant Resolution Manager checks over 200,000 attributes per computer that results in a quantum leap of diagnostic range and accuracy over other compliance and configuration management tools. The patent pending analytical engine eliminates the need for human intervention and dramatically reduces the time required to remediate problems by automating the process of analyzing the root cause of the problem, determining the proper remediation, and performing the remediation. The result is near continuous level of compliance with significantly reduced support costs, coupled with unparalleled visibility into the audit readiness of endpoint computers.

Triumphant takes configuration management a step farther than traditional tools that perform this function. Triumphant uniquely combines in unparalleled scan scope and patent pending analytics to do comparative analysis against endpoint computer populations to determine if there is a normal configuration value for literally thousands of attributes. Constructing and maintaining policies used by traditional configuration management systems (and Triumphant) requires human effort and therefore there exists a practical limit as to the how many policies can ultimately be created. Automating the determination of normal configurations for those attributes not addressed by policies enables Triumphant to detect abnormal configurations across the entire range of configurations items. As a result, Triumphant greatly extends the reach and range, and ultimately the benefit, of the configuration management process.

Triumphant is also extremely flexible, enabling users to check machines against organization specific policies and configurations, or pre-defined policies for federal (i.e. FDCC) or industry specific mandates (i.e. PCI). A few specific examples:

Federal Desktop Core Configuration (FDCC)

Triumphant Resolution Manager is one of a very few products validated by the National Institute of Standards and Technology (NIST) as conforming to the Security Content Automation Protocol (SCAP) and its component standards. SCAP validation assures that a solution meets the NIST standards for validating the linkage between computer security configurations and the NIST controls framework, and is a required component of FDCC compliance.

Triumphant provides FDCC policy templates that supplement the official FDCC SCAP content to provide the information needed to not only assess FDCC compliance but also perform the necessary remediations when non-compliant conditions are detected. FDCC specific reports provide ongoing visibility into FDCC readiness and generate the machine readable FDCC report format that can be submitted directly to the OMB.

Green IT Power Management

Triumphant Resolution Manager is the perfect solution for enforcing the power management policies for endpoint computers, effectively reducing power consumption when these computers are not in use. For environments containing more than 10,000 computers, the savings can easily amount to more than a million dollars per year. More importantly, Triumphant delivers this capability in an intelligent, highly automated, and flexible way that

maximizes impact without interfering with usability or with system management and administration processes.

Triumphant provides policy driven management of Windows XP and Windows Vista power configuration settings enabling IT administrators to easily establish and maintain a desired power scheme across a distributed computing environment. A Wake-on-LAN capability is included so computers that have been shut down can be automatically returned to a ready state (including sub-nets) for scheduled maintenance activities.

Incident and Problem Management

The environments in which endpoint computers operate evolve daily and are rapidly growing in complexity. Triumphant Resolution Manager empowers organizations to address this complexity and deliver high availability and quality of service in a very cost effective fashion without locking down the environment and stifling end user productivity. Triumphant helps businesses and government agencies address interruptions in service by proactively identifying and resolving known errors on endpoint computers and servers (Incident Management) and by providing insights to problems where the root cause has yet to be determined (Problem Management). The net effect is to reduce or eliminate user downtime and to reduce the labor costs of diagnosing and remediating these problems.

When an IT service disruption occurs, Triumphant automates the process of detecting, identifying, categorizing, prioritizing, diagnosing, and remediating the incident – tasks normally performed by human beings. Triumphant Resolution Manager uses its patent pending analysis engine to diagnose the problem and synthesize a discrete (and reversible) remediation to address the issue and restore the machine to working order. The Triumphant platform also learns and adapts based on prior incidents by collecting data about these incidents in the incident knowledge base. This information can be easily augmented by the service management team to address customer specific incident types, further adapting the platform to maximize incident management coverage.

In the case of known problems, Triumphant may be able to detect and remediate the problems before it causes a service disruption. If the service interruption has already occurred, Triumphant can accelerate diagnosis and remediation and reduce the scope of the interruption and save the labor costs associated with the diagnosis and remediation. In the case of errors where the root cause is unknown, Resolution Manager greatly accelerates problem management by identifying anomalies, automatically correlating related anomalies, performing an automatic threat analysis, and storing the resulting knowledge so that recurrences of the same incident can be quickly and efficiently addressed. Triumphant also excels at surgically and automatically removing unauthorized applications, eliminating a major issue that erodes resources and generates unnecessary support costs.

Triumphant can significantly reduce user downtime and reduces the time the services desk spends on resolving software configuration errors such as undesirable or unauthorized software, application and operating system corruption, and abnormal application and operating system settings. This can directly affect end user satisfaction and help service providers to improve their performance against related service level agreements. Since the types of incidents automated

by Resolution Manager tend to require the greatest amount of human time and expertise, the savings can be substantial, enabling payback in less than one year.

Summary

The nature of Triumfant Resolution Manager leads to equally unique and compelling solutions for security, compliance and configuration management and incident and problem management. The advantages are numerous, and are entirely distinctive to Triumfant. End users realize maximum utility from their machines while interruptions to service are reduced, as is the human costs of addressing those interruptions. Compliance to internal and external policies are checked and enforced daily, keeping the environment in a constant state of audit readiness. Endpoint machines are more secure against the evolving nature of today's attacks. And actionable reports provide unparalleled visibility into the computing environment.

Regardless of the application, the benefit comes down to the knowledge that every computer is checked every day, and the process of detecting, diagnosing and remediating problems is fully automated. The result is that our customers start each day knowing that their endpoint machines are secure, configured, and compliant - and therefore ready for business.

1 – “2008 Data Breach Investigations Report”; Baker, Hylender, Valentine, et al; Verizon Business, Inc.

2 – “Magic Quadrant for Endpoint Protection Platforms, 2007”; Firstbrook, Hallawell, et al; Gartner, Inc.

About Triumfant

Triumfant offers unique analysis software that automatically discovers, diagnoses and remediates unexpected changes and conditions on endpoint computers and servers, ensuring that these computers are secure, compliant, audit ready, properly configured and ready for business. Triumfant scans every computer every day, helping organizations to minimize security risks, reduce IT support costs, ensure compliance and increase quality of service. To learn more about how Triumfant can help your organization, please call us at 800.267.2190 or visit us at www.triumfant.com.