



# INTRODUCTION TO TRIUMFANT

## Innovative Software to Keep Your Endpoints Secure, Configured, and Compliant

Triumfant offers one-of-a-kind software that automatically discovers, analyzes and remediates unexpected changes and conditions on endpoint computers and servers. This unique capability powers innovative solutions in Endpoint Security, specifically real-time malware detection and remediation and continuous enforcement of security configurations and policies. Triumfant deeply scans every computer to identify granular changes, analyzes those changes to detect problems and malicious activity and synthesizes a remediation to surgically repair the machine or return it to compliance. Automating the detection and remediation of problems and non-compliance on endpoint machines empowers Triumfant customers to minimize security risks, reduce IT support costs, ensure compliance and increase quality of service.

Triumfant continually scans over 200,000 attributes on every endpoint computer, creating the unprecedented ability to see changes at the most granular level. This information powers patented analytics that analyze the detected changes in the context of the broader endpoint population, effectively eliminating the false positives that have plagued previous attempts at anomaly detection. By leveraging granular change detection, Triumfant can uniquely identify malicious activity that evades signature based antivirus software, can spot when a machine is non-compliant with organizational policies or regulatory mandates, or can preemptively identify known problems that may interrupt service. The ability to see every change in each machine enables Triumfant to synthesize and execute a situational and contextual remediation to return all changed attributes to their pre-attack condition and eliminate the need to re-image. While other products require human intervention to perform problem analysis and to build a remediation script, Triumfant automates the entire process, eliminating labor costs and significantly reducing the time from infection to remediation.

### Areas of Application:

- **Real-time Malware Detection and Remediation.** The ability to identify changes at the most granular level means that Triumfant is uniquely able to detect, analyze and remediate malicious attacks in real-time without the need prior knowledge of the attack. Triumfant can see the attacks that other defenses miss or the attacks designed specifically to evade those defenses such as zero days, rootkits, and polymorphic attacks. The story does not end at detection as Triumfant synthesizes a remediation to remove the malicious code and all of the associated artifacts, restoring configuration settings and registry attributes to return the machine to its secure condition before the attack. Triumfant's sophisticated remediation capability means that a machine goes from infection to remediation in five minutes: no gaps in detection, no time lost analyzing the attack, no exposure waiting for someone to write and distribute a remediation script, no costly re-imaging.
- **Continuous Enforcement of Security Configurations.** Triumfant continuously enforces security configurations and ensures that the other endpoint protection software for that machine is in place, properly configured, and operational. Triumfant uses unique change detection technology to detect when a machine is non-compliant to configuration settings and policies (organization specific or mandated policies such as FDCC) and automatically remediates the affected machine to return it to compliance. Triumfant also removes unauthorized applications to remove the threat associated with such programs. Triumfant's unique capabilities directly lower risk by maintaining the endpoint population at the highest possible state of security readiness and minimizing the attack surface of each computer. Triumfant makes security automation a reality, providing these benefits with minimal labor costs.

### Unique Software = Unique Benefits

Triumfant customers enjoy benefits that are unique as the Triumfant software. Endpoint machines are secure against the evolving nature of today's complex malicious attacks. End users realize maximum utility from their machines while reducing interruptions to service – along with the human costs of addressing those interruptions. Compliance to configurations and policies – both internal and externally mandated - are checked and enforced daily, keeping the environment in a constant state of audit readiness. Actionable reports provide unparalleled visibility and situational awareness into the computing environment. Triumfant customers start each day with the confidence that their endpoint machines are secure, configured, and compliant and therefore ready for business in an increasingly hostile environment.