



## SOLUTIONS: IT SECURITY

### Closing Critical Gaps in Endpoint Protection

Organizations face one cold reality: the attacks on their IT systems are constantly evolving, with new vulnerabilities exposed and exploited daily. It is not just that the attacks are growing in volume - of more immediate concern is the progression from random, indiscriminant attacks from rogue hackers to coordinated and targeted attacks for financial gain by well organized cyber criminals. At the same time, computer users within businesses are rapidly adopting social media and other so-called Web 2.0 sites such as blogs, wikis, instant messaging and social networks, creating new pathways for malicious activity.

While the threats have evolved, defensive software is still largely based on the traditional method of signature based recognition that relies on the prior knowledge of vulnerabilities and attacks. This fundamental concept – used by security software such as antivirus, anti-spyware and personal firewalls - creates a real and critical gap in the security perimeter. This gap is significant, as multiple studies indicate that signature based tools can have a 50% or higher failure rate at detecting the attacks where there is no known signature, and may miss 5% of attacks when there is a signature. As a result, organizations are relentlessly subjected to new attacks specifically designed to evade traditional protections.

The threat does not come from worms, trojans and botnets alone. Maliciously intended insiders can evade defensive software to infiltrate a machine and then use a myriad of techniques to cover their work. Users may indirectly endanger a machine by installing unauthorized software or directly cause vulnerabilities by altering critical configuration settings or disabling defensive software. The bottom line is that endpoint computers are under relentless attack on a number of fronts, and the problem will only get worse.

#### **You Don't Know What You Don't Know:**

IT Security experts have long believed that this critical gap in the IT perimeter could be closed by a tool that detects unexpected changes and conditions (anomalies) on endpoint computers to spot previously unidentified threats before they cause significant harm. Triumphant Resolution Manager has made this promise a reality with a platform that uses granular change detection to identify, analyze, and remediate the next wave of cyber threats in real-time while leveraging patent pending technology to eliminate the problem with false positives that plagued previous attempts at anomaly based detection.

Triumphant Resolution Manager continuously scans for unusual changes that are consistent with the behavior and structure of malicious applications. These include unusual auto-start methods, stealth techniques such as those used by root kits, and unusual firewall exceptions. As a result, malicious attacks that are not detected by traditional signature based tools are recognized by Triumphant in real-time, along with all of the changes to the machine associated with the attack. Resolution Manager immediately applies its deep analytics to verify that it is indeed an attack and assesses the full extent of the threat.

Resolution Manager does not stop at detection, using its diagnosis of the problem and knowledge of the changes to the machine to synthesize a surgical remediation. Triumphant is uniquely capable of generating extremely sophisticated remediations that see through stealth techniques, neutralize watchdog processes, eject rootkits, and track down randomly named executables. These remediations do not simply delete the malicious executable; they repair all of the collateral damage from the attack, effectively eliminating the need for costly re-imaging. The entire process from detection to remediation requires no human intervention and takes mere minutes, not hours or days like other tools. The information about the attack and the remediation is captured so that Resolution Manager can scan the entire population for any other occurrences of the attack, and remediate machines where the attack is detected. With Triumphant, a massive attack on your endpoint population can be thwarted in 30 minutes or less.



## SOLUTIONS: IT SECURITY

### Ensuring Security Readiness:

Triumphant is uniquely able to help businesses and government agencies ensure the security readiness of endpoint computers on a daily basis, combining multiple security processes into one efficient agent and centralizing command, visibility and control:

- **Malware detection.** The ability to detect changes at the most granular level allows Triumphant to detect, analyze and remediate malicious attacks in real-time without the need for signatures or any prior knowledge of the attack.
- **Security Configuration Management.** Triumphant verifies that the organization's standard portfolio of endpoint security software is correctly deployed, properly configured, and operating as expected. This maximizes the effectiveness of these tools and eliminates vulnerabilities from missing or mis-configured software. This includes operating system and applications level settings.
- **Compliance Management.** Triumphant checks each machine to ensure that it starts the day audit ready and in compliance with security policies and controls. Triumphant Resolution Manager applies security policies that are customizable from the departmental level down to individual machines. Triumphant also provides policy templates for specific security mandates such as FDCC SCAP compliance and Payment Card Industry (PCI) compliance.
- **Vulnerability Management.** Triumphant uses the NIST SCAP vulnerability database to scan each computer for known software vulnerabilities, identifying where missing patches create a security exposure.
- **Whitelist/Blacklist Management.** Triumphant excels at deleting unauthorized software from endpoint computers, and build custom remediations to ensure that no malicious code is left behind by the deleted application.

To complete the picture, Triumphant provides a comprehensive set of reports that deliver unmatched visibility into the security readiness of the endpoint environment from an executive summary view down to the details of each machine. These reports surface this information in actionable form so these insights can be transformed to practical action.

### The Last Line of Protection for Your Organization:

As the nature of threats against endpoint computers continues to evolve, Triumphant uniquely stands as the last line of protection to defend organizations from the very real costs – and the reputational damage - associated with a successful attack. Triumphant leverages unique anomaly based detection to identify and remediate the threats that evade traditional security software. Triumphant further helps secure end-point computers by ensuring that all aspects of security readiness – endpoint security software and security specific policies, controls and configuration standards - are in place to close gaps in the endpoint perimeter. The automated nature of the product – particularly the automated diagnosis and remediation - reduces the need for administrative support and the associated costs over the life of the product.

### About Triumphant

Triumphant® 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 Triumphant 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.triumphant.com](http://www.triumphant.com).