



Product Fact Sheet

The Bottom Line:

- Detects attacks that evade detection by traditional signature based security tools in real-time
- Synthesizes and applies a remediation to remove the malicious code, ending the attack
- Remediates all collateral damage from an attack to eliminate the need for re-imaging
- Ensures that existing endpoint protections are properly installed and configured
- Enforces security configuration policies at the operating system level and at the application level
- Unmatched visibility into the security readiness of the endpoint computer population

Triumphant, Incorporated
800 King Farm Boulevard
Rockville, MD 20850
301.917.6280
301.917.6299

ENDPOINT SECURITY

Closing Critical Gaps in Endpoint Protection

The vast majority of endpoint security tools rely on prior knowledge of the attack to either detect the attack, remediate the effects of the attack, or both. This approach is simply not sustainable in the face of today's malicious attacks which are growing in volume and complexity at a geometric rate.

Triumphant Resolution Manager can automatically detect and remediate malware without the need for signatures or human intervention. That is because Triumphant uses patent pending granular change detection and analytics to identify malicious attacks, eliminate false positives, analyze the attack, and synthesize a surgical remediation in real-time. Because Triumphant needs no signatures, it can detect highly targeted and zero day attacks that other traditional signature based tool miss at a rate that exceeds 50 percent.

The depth of information collected by Triumphant allows it to build remediations that remove the offending executable as well as repair the collateral damage done by the attack. Open ports are closed, modified configuration settings are restored, and registry entries are repaired, effectively eliminating the costly process of re-imaging the machine. The ability to build these sophisticated remediations eliminates the need for human intervention – and the associated delay – to build scripts to address the problem.

Triumphant performs vulnerability management, security configuration management, compliance management, and whitelist/blacklist operations from a single administrative console. Triumphant ensures the security readiness of every machine by making sure that traditional endpoint security tools are properly deployed, properly configured, and fully operational to effectively perform their role. Triumphant also enforces security configuration settings and policies at the operating system and application level.

Product Advantages:

- Detects indicators of malicious activity in real-time, confirms that there has been an attack, builds a remediation, and stops the attacks in seconds, not hours or days.
- Synthesizes a discrete remediation for detected attack that eliminates the malicious code and addresses all of the collateral damage from the attack including opened ports, altered configuration settings, and deleted or altered executables.
- Utilizes sophisticated remediations to eject rootkits, neutralize watchdog processes, uncloak hidden processes and identify randomly named executables.
- Checks every computer every day to ensure that it conforms to security policies and automatically remediates any machine found to be in non-compliance.
- Enforces security configuration settings at the OS level and at the application level.
- Ensures that all deployed security software is operational and properly configured to maximize its effectiveness and addresses attacks directed at neutralizing such software.
- Removes unauthorized software, thereby eliminating any potential threats associated with software such as peer-to-peer applications.
- Leverages NIST SCAP content to scan for thousands of known vulnerabilities, identifying situations where missing patches are creating a security exposure.
- Delivers extensive reporting to provide critical insight to security activities from the machine level to executive summary views.
- Provides incident response teams with unparalleled visuals into the granular forensic evidence of the changes made to an attacked machine.



Product Fact Sheet

Closing the Gaps in the IT Security Perimeter

- Detects targeted and zero day attacks before they can spread and cause significant damage
- Eliminates gaps caused by missing or improperly configured software
- Ensures that every computer is in compliance with security policies and controls at the start of every business day
- Combines the critical elements of malware detection & remediation, vulnerability management, compliance management, security configuration management and whitelist/blacklist management through one agent and one command and control console

Triumphant, Incorporated
800 King Farm Boulevard
Rockville, MD 20850
301.917.6280
301.917.6299

ENDPOINT SECURITY

Triumphant is the one solution that effectively closes the critical gaps in the IT security perimeter for endpoint computers. Ensuring proper installation and configuration of traditional security defenses means that the organization is more secure with the investments already in place. Enforcing security policies and controls across the organization on a daily basis eliminates human error and removes potential weak points in the perimeter. The ability to scan every computer every day, detect potential threats not seen by signature based tools, analyze the threat and its potential impact, and synthesize a remediation makes Triumphant Resolution Manager uniquely equipped to protect against attacks that evade traditional defensive software or do not have an associated signature.

Product Benefits:

- Sees all of the attacks on a machine, whether from malicious code or a maliciously intended insider by tracking all of the changes to the machine and identifying indicators of malicious activity. Triumphant's patent pending analytics compare these indicators against the broader endpoint population to effectively eliminate false positives.
- Builds surgical remediations on the fly without the need for human intervention or involvement from third party resources. As a result, the remediation is applied to the problem in seconds - not hours or days - stopping the attack before it further infects the machine or spreads to other machines in the endpoint environment.
- Unlike solutions that simply delete the malicious executable, Triumphant remediates all of the collateral damage done by the malicious code even if some other tool detects the attack, eliminating the costs and service interruption associated with re-imaging.
- Once an attack is identified for any given machine, administrators can use the information gained from addressing that machine to scan the endpoint environment for any other instances of the attack and apply the created remediation, effectively ending the threat to the entire organization in minutes.
- Automated remediation of configuration issues, missing defensive software, or violations of security policies reduces the administrative resources and the associated costs of addressing these problems while ensuring that security policies are enforced and defensive software is properly installed and configured.
- Policy-driven implementation increases flexibility and control and provides discrete tuning of policies across the population, to specific groups and to individual machines.
- Administrators can use the included security policy templates, modify these templates or easily create their own using a graphical user interface.
- Effectively combines vulnerability management, security configuration management, compliance management and whitelist/blacklist operations onto a single administrative console through one agent.
- Provides an actionable view into endpoint security readiness that is unprecedented in the industry through a wide range of standard reports, a user interface to create custom reports, the ability to distribute reports to executives and stakeholders and the power to export reports to integrate the information into business documents.

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.