BOUNCER by CoreTrace™

Secure, Flexible Application Whitelisting

In today's world of ever-increasing, rapid change in the quantity and variety of malicious code attacks, securing and managing endpoint computers has become overwhelming and costly:

- Blacklist-based anti-malware software cannot keep pace with the speed of new malware development.
- Frequent patching, image management, and change management overload help desk resources.
- Industry-related compliance regulations continue to tighten requirements on security and the protection of sensitive information under pain of legal and financial penalties.
- Users' productivity and morale suffer under rigid security and privilege-management systems, unable to easily load necessary applications and updates.
- Tightening budgets restrict operational resources, controlling decisions and limiting the options and opportunities companies need to grow their business.

A new approach is needed — one that reduces risk, lowers endpoint total cost-of-ownership (TCO), and improves productivity in a single, secure solution. That solution is BOUNCER by CoreTrace.

The Design Philosophy of BOUNCER

CoreTrace® designed BOUNCER around three fundamental tenets of endpoint control:

	Tenets of Endpoint Control	BOUNCER Implementation
1	**Control what you know.** A security solution that bases control on what is 'known' about a system is more effective than one that bases control on reacting to 'unknown' attacks.	Application whitelisting
2	**Control at the lowest possible level.** Only a security solution that functions in the kernel can securely deliver the control IT requires.	Kernel-level enforcement
3	**Control transparently.** A security solution should not get in the way of end-users or create additional administrative burden.	Trusted Change

Features Offered in BOUNCER

Kernel-level enforcement and tamper-resistance

BOUNCER's whitelist enforcement mechanism resides in the operating system kernel and only allows approved applications and their files to execute. All other files are denied system resources, thus preventing malware and unauthorized applications from running. For approved applications, BOUNCER creates a unique fingerprint by combining key attributes into a highly tamper-resistant "triple play" definition, including the file path, file size, and a digital digest from the SHA1 algorithm. Using these three parameters, BOUNCER evaluates files as they load into memory to determine whether or not they have been modified.

Automatic whitelist generation for each computer

BOUNCER auto-generates custom-tailored whitelists for each protected endpoint quickly and efficiently, accounting for the fact that different computers may have different applications and processes installed. This capability facilitates automated implementation across any number of computers in matter of minutes.

Minimal impact on system performance

BOUNCER's impact on system resources is so minimal that it usually does not even appear in the Task Manager, ensuring optimum system performance and availability. For platforms where performance and availability are mission-critical operational factors — for example process control systems, ATMs, or POS terminals — BOUNCER represents the first truly viable security solution.

Support for multiple operating systems

Enterprise networks are heterogeneous combinations of different operating systems. The BOUNCER client installs on laptops, desktops and servers across a multitude of platforms, including Windows NT 4/2000/XP/Server 2003/Server 2008/Vista/7 and Solaris 7/8/9/10. BOUNCER will soon support MacOS and Linux systems too.

Advanced protection beyond simple whitelisting

BOUNCER prevents unauthorized applications from executing, stopping all malware payloads cold. BOUNCER's architecture and kernel-level position enable it to extend beyond simple whitelisting to provide additional security like memory protection and script control. In order to prevent exploits such as DLL injections or attempts to write to kernel memory, BOUNCER extends the whitelisting model into memory, preventing execution of processes originating from unauthorized files.

Remediation/removal of unauthorized applications

Even though unauthorized applications cannot execute on BOUNCER-protected systems, you may wish to remove them anyway. BOUNCER is one of the only whitelisting solutions that provide an integrated mechanism for cleanly targeting and removing these unwanted applications and files.

Hardened, self-defending solution

BOUNCER employs the most secure, self-defending architecture available on the market. BOUNCER is a kernel module that has sophisticated defenses that prevent alteration or termination, even by local administrators. BOUNCER has multiple processes that monitor themselves and ensure uninterrupted protection at all times. All communications are fully encrypted and authenticated from the management console to the endpoint.

Intelligence about installed/requested applications

BOUNCER provides valuable intelligence about all installed and requested applications in your environment. In the BOUNCER Control Center, you can quickly view information such as how prevalent applications are, which machines they are on, and how often they are used. Optionally, you can subscribe to the CoreTrace Software Intelligence (CSI) service to receive additional "application assurance" intelligence about applications' risk including information on both "known good" and "known bad" (malware) applications.

Automatic updating for new/upgraded applications

BOUNCER allows modification to custom endpoint whitelists through its patent-pending Trusted Change capabilities — an absolutely essential feature in any application whitelisting solution. Once trust models have been established (e.g., trusted updaters, trusted paths, trusted digital signatures, trusted users), users and automated application-delivery mechanisms such as patch management systems can add or update applications without requiring further IT approval.

To further reduce operational effort, BOUNCER easily matches your approach to each set of users, including two new user privilege modes called AllowQ™ and BlockQ™. BOUNCER's completely unique AllowQ mode enables designated users to temporarily run an application until IT can approve or deny adding it to the whitelist. Under the BlockQ mode, users receive a notification that prompts them to provide a simple business justification for the application. These two flexible user models facilitate easy installations and requests that drop right into a "queue" for administrators to approve or reject. Combined with application intelligence, administrators can make more informed decisions and more easily manage the constantly-changing application needs of your endpoints.

Enterprise-level deployment and scalability

BOUNCER is designed to meet enterprise-level deployment and scalability requirements. BOUNCER is easy to adopt because it utilizes industry-standard architectural and open source components such as SSL, Tomcat, Apache and PostgreSQL. If you desire, BOUNCER can leverage your Active Directory investment to further facilitate your deployment. The BOUNCER management server ships as a virtual appliance, with all of the performance, reliability, fail-over and scalability benefits that virtual appliances deliver. These improvements not only expand the flexibility of options for solution deployment, but enhance scalability as well.

Benefits Gained with BOUNCER

- Stop and remove even sophisticated, targeted, zero-day threats
- Security patches occur on your own terms, not in reactive, unplanned fire drills
- Enforce approved configurations
- Meet critical compliance mandates
- Understand the prevalence, location and usage of applications
- Higher end-user productivity and satisfaction, by allowing users to install the applications they need
- Reduce unnecessary Help Desk requests and reimaging efforts
- Lower the total TCO of each protected system

About CoreTrace

CoreTrace is the leading provider of secure and flexible application whitelisting solutions. The company's award-winning and patented BOUNCER solution is at the forefront of the movement to next-generation endpoint control and security solutions. Unlike other application whitelisting solutions that are simply lockdown technologies, BOUNCER's Trusted Change capability enables IT professionals to predefine multiple sources from which users can safely install applications and have them automatically added to the whitelist — all with minimal IT involvement. The result: full prevention of unauthorized applications, improved overall security, and lower total cost of ownership. CoreTrace's customers include organizations in a wide variety of industries, such as energy, oil and gas, retail, financial services, telecommunications, as well as government agencies. For more information, please visit: www.coretrace.com and follow the conversation at www.coretraceblogs.com.

About GlobalSCAPE®

GlobalSCAPE, Inc. (NYSE Amex: GSB), headquartered in San Antonio, TX, is a global provider of managed file transfer (MFT) and wide area file services (WAFS) solutions for securely exchanging critical information over the Internet, within an enterprise, and with business partners. GlobalSCAPE is a worldwide reseller of BOUNCER by CoreTrace™, the most tamper-proof and scalable application whitelisting solution in the industry. Since the release of CuteFTP in 1996, GlobalSCAPE's solutions have continued to evolve to meet the business and technology needs of an increasingly interconnected global marketplace.

globalSCAPE®

4500 Lockhill-Selma Road, Suite 150; San Antonio TX 78249
1-800-290-5054 (USA & Canada); 1-210-308-8267 (Worldwide)
For more information about GlobalSCAPE, visit **globalscape.com**.