



BOUNCER by CoreTrace™

Lower TCO with more secure, more available endpoints

Managing endpoints is a serious drain on enterprise IT budgets. Between constant patching, help desk calls, unregulated change and rampant malware, you spend a substantial percentage of time and money keeping your endpoints functioning.

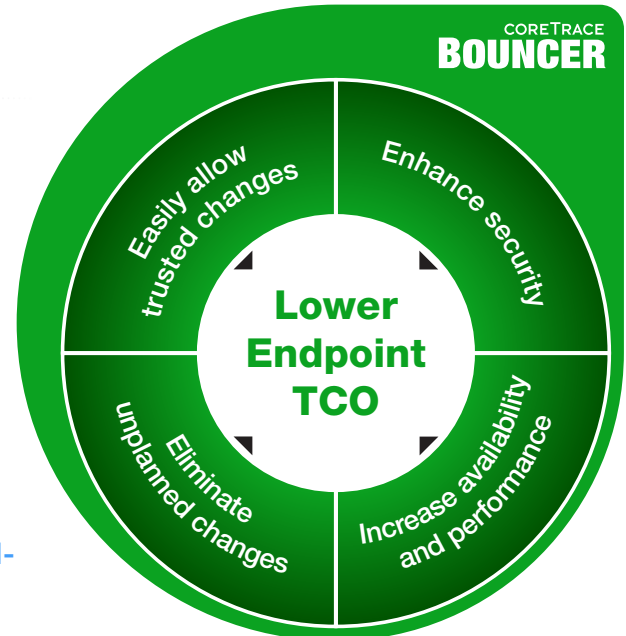
BOUNCER™, the world's only high-security and easy-change application whitelisting solution, lowers endpoint cost of ownership by improving availability and performance, enhancing security, and boosting user productivity.

Create a more secure, more available, and lower cost endpoint infrastructure by employing:

- ✔ Unmatched application whitelist enforcement, not only preventing the execution of unauthorized or malicious applications (even zero-day exploits and rootkits) but also memory-based attacks within whitelisted applications (e.g., DLL injection attacks).
- ✔ Auto-generation of custom-tailored application whitelists, enabling automatic implementations across thousands of computers — in only a matter of minutes.
- ✔ Patent-pending “Trusted Change”, allowing users to install, upgrade, and download approved applications from trusted sources without involving IT staff.
- ✔ Turnkey and patented infrastructure, providing a complete, more secure solution that operates at the lowest levels of the operating system.
- ✔ Administrative and reporting capabilities, enhancing control and providing the visibility needed for compliance requirements.

Fundamentals

BOUNCER generates a list of approved applications on a given computer (laptop, desktop, server), then quickly and seamlessly compares each launched application against that list. If it's not on the list, it doesn't run, period. The BOUNCER client operates at the deepest levels of the operating system, and BOUNCER's application whitelisting extends all the way into the memory.



How does BOUNCER lower endpoint TCO:

- ✔ No malware running rampant compromising security and performance
- ✔ Fewer security patches to take up all of your IT staff's time
- ✔ No unmanaged or unauthorized configuration changes
- ✔ Improved regulatory compliance through increased security and documented, controlled change
- ✔ Higher end-user productivity by allowing users to install needed applications
- ✔ Fewer help desk calls



What happens if malware turns a whitelisted application such as Microsoft Word® into an insidious memory exploit? BOUNCER still stops it, even though it's not launching a new executable, because BOUNCER monitors the application memory.

What happens when users need to add new applications or update existing ones? BOUNCER has the application whitelisting market's best solution — simple, effective, and patent-pending “Trusted Change” — that enables user-driven application modification without involving your IT staff each time.

Change-ready whitelisting

Change is the only constant, so what happens when you restrict applications severely? Do you have IT approve every single change from every user? Not with BOUNCER!

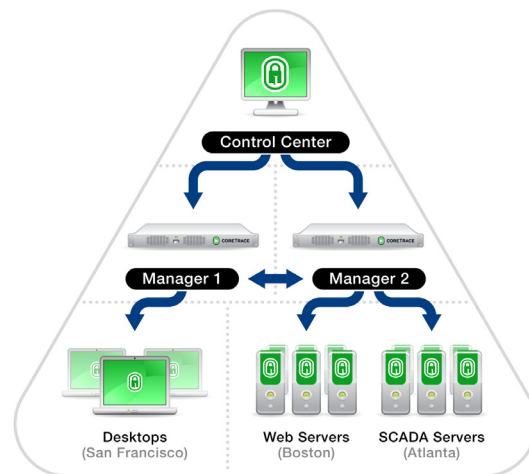
BOUNCER's patent pending Trusted Change lets you set up a “circle of trust” to lower the costs associated with other, lockdown-oriented whitelisting solutions. Your IT department selects one or more “trust sources” (e.g., trusted applications, trusted paths [e.g., share drives], trusted updaters, trusted digital signatures, and even trusted users) from which users can install or upgrade applications.

As long as users operate within the “circle”, they get their applications as usual — and you get all the security with none of the administrative overhead.

About CoreTrace

CoreTrace® is the pioneer of client-based application whitelisting. The company's award-winning and patented high-security, easy-change BOUNCER solution is at the forefront of the movement in 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.

For more information about CoreTrace or BOUNCER, please visit www.coretrace.com.



How does BOUNCER work:

- ✓ The **BOUNCER Client** is a lightweight agent that resides at the lowest level of the operating system
- ✓ The **BOUNCER Manager** is a hardened device that sits between the endpoints and the Control Center
- ✓ The **BOUNCER Control Center** is the secure, simple administrative interface
- ✓ The **BOUNCER Network** is the fully encrypted, two-factor authenticated network that unites all components

BOUNCER stopped 100% of computer viruses during Defcon 16's “Race to Zero” competition, outshining traditional blacklisting antivirus applications. No matter the threat, BOUNCER stopped it 100% of the time. Blacklist-based products averaged a success rate of only 60%.