

Solidcore Steps Up with Expanded Change Control Solution

Abstract

Solidcore recently announced the release of its latest version of S3 Control, the company's real time change control software. This new release broadens the product's coverage, adding support for network devices and database platforms in addition to the desktop and server operating systems already supported, while building further upon the product's unique automatic enforcement capabilities. Enterprise Management Associates (EMA) believes that this release increases Solidcore's ability to compete with niche change control vendors, and improves its position as a complement to larger systems management vendors. Enterprises relying on static, reactive change reporting solutions should begin to reevaluate their approach to change control.

Solidcore Introduces Support for Network Devices and Databases

On September 11, 2006 Solidcore, a provider of real-time change control solutions, announced the new release of its S3 Control software product. This release features support for network devices and a variety of database platforms, including offerings from Oracle, IBM, Microsoft, and Sybase. This expands S3 Control significantly, to provide a broad, consolidated view of change and control across the organization, beyond the product's traditional orientation.

Solidcore's offering differs from most other change control solutions on the market in that it is oriented towards real-time, proactive prevention, not after-the-fact reaction to change control issues. Moreover, the product integrates with change management systems like BMC Remedy, linking change management with change control through its unique combination of visibility, accountability, and automatic enforcement capabilities.

Background

Distributed enterprises face significant difficulties managing change. It is often chaotic, unmanaged, and unauthorized, leading to support problems, downtime issues, and customer service failures. Vendors have sought to bring order to this chaos via change control solutions, but the approach is often merely reactive. Many products rely upon periodic polling of system configurations, detecting changes only after they have occurred. Such reactive solutions raise an alert only after an unauthorized change has occurred, so not only has there already been a breakdown in process and policy, but the damage is already done. This failure to control and prevent unauthorized change can be extremely costly, because such

“after-the-fact,” notification-only solutions cannot prevent problems, but effectively serve only as forensic tools. Other solutions might detect problems in the change process, but require manual intervention in order to resolve the problems. This is marginally better, but any manual intervention delays the resolution lifecycle, adds to operational costs, and increases the risk of human error.

Solidcore brings a different approach to this issue, by adding automatic, real-time change tracking and enforcement to change management. S3 Control continuously tracks changes and forwards them to a central aggregation point, with monitoring and enforcement occurring at the kernel level, so files and registries can be protected at the source. S3 Control can ensure changes are made only to specific files, in specific time windows, and by specific tools. This unique capability goes beyond even remediation, and includes real-time, automatic interdiction of unauthorized changes. This ensures that S3 Control can detect and respond to unauthorized change immediately and automatically.

Solidcore complements existing change management processes, especially when used in conjunction with Remedy or other change management systems. For example, when changes cause problems, Solidcore provides visibility with forensic and audit data, which speeds up problem diagnosis and resolution. When authorized changes are made, it provides accountability by auditing and reconciling these changes to assist with compliance and process improvement efforts. When out-of-policy changes are made (e.g. without approval, or outside approved timeframes) it can optionally provide enforcement by automatically preventing unauthorized change, reducing the volume of unwanted change, in turn reducing the number of problems that such change causes. This gradation of change control discipline – from visibility, through accountability, to enforcement – allows enterprises to implement change control discipline at a rate that is appropriate for the environment.

Key Ramifications

The following are the key ramifications of this announcement:

- **Broader Reach** – Solidcore continues to broaden its reach within the enterprise, providing a consolidated view and enforcement of change across not only servers and desktops, but now also network devices and databases. Furthermore, this addition now enables holistic coverage of the entire foundational stack of point solutions within the enterprise.

- **Unique Approach** – Solidcore’s approach, comprised of real-time change control monitoring coupled with automatic interdiction of unauthorized or out-of-policy changes, is unique within the industry and offers clients unmatched opportunity to mitigate risk and prevent damages.

While some competitors in this space offer similar messages, and some provide the ability to remediate unauthorized change after it has occurred, EMA is unaware of any competitor that is able to proactively and automatically prevent change with local, kernel-level interdiction. This proactive approach, which focuses on preventing the risk (and resultant damage), has been strongly validated within the past year by Solidcore customers

For example, WebEx states that by implementing the product over three months on over 2,000 servers, the company reduced service outages by more than 50%. Key to this was the enforcement of a specific policy, one which specified that system changes could not occur outside established maintenance windows. The cost savings have been substantial, both in hard and soft dollars. Not only has this prevented lost business and the negative brand impact that would have resulted from service outages, but WebEx also reportedly reduced the headcount dedicated to supporting their previous reactive audit system by more than 80%, and was able to focus those resources elsewhere. In addition, the dynamics and resultant costs of outages when they do occur has also been reduced. Prior to the implementation of Solidcore, system failure was said to be measured in hours, even days; now, root cause analysis is often obtained within minutes.

EMA’s Perspective

Enterprise Management Associates (EMA) believes that Solidcore provides a very effective solution to detect, report, prevent, and control unauthorized change. With this release, that capability now covers even more of the enterprise. The addition of support for network devices and databases to the support for desktops and particularly servers already available, enables Solidcore to provide a broader, more detailed view within the enterprise. This is particularly the case where point solutions are in play as change can now be effectively controlled across all the lower levels of the application stack.

Solidcore’s automated response directly addresses key issues in server management and availability. Recent EMA research has shown that over 60% of all downtime is the result of faulty configuration changes. Further research has shown that the average problem lifecycle is between one and four hours, in large part because of significantly manual diagnostic and remediation processes. Solidcore will help to prevent this

avoidable downtime by reacting to unauthorized configuration changes immediately and automatically. EMA believes that Solidcore’s capabilities will therefore achieve key data center management and availability goals by addressing the root cause of problems, and by reducing the cost, risk, and delay associated with manual responses to problematic changes.

EMA also believes that this new release, and the broader offering it represents, signals the ongoing acceptance and continued endorsement of S3 Control’s unique automatic enforcement approach by Solidcore’s customers. It also signals a new front in the ability of Solidcore to compete in the marketplace. Solidcore was already competitive with other smaller ISVs. Specialty vendors focused on Change and Configuration Management (CCM), such as Tripwire, Configuresoft, and mValent, should see this release as upping the competitive ante, as Solidcore clearly aims to compete even more strongly with these vendors. Solidcore certainly faces a strident battle with these vendors, each of which has specific competitive advantages. However, EMA believes that S3 Control’s competitive feature set, and the newly expanded coverage, will certainly help Solidcore win some deals from them. For larger systems management vendors that offer CCM solutions, such as BMC Software, CA, and IBM, Solidcore provides a valuable complementary offering, and with the increased breadth of this release, could even be positioned as a viable alternative for some specialized requirements. Solidcore’s ability to automatically prevent unauthorized change, rather than just remediate it, is a gap that these larger vendors should seek to fill.

Accordingly, EMA recommends that enterprises that rely upon vendors with traditional, static change control solutions – especially those that predominantly offer only monitoring and reactive notification – should take stock and begin to reevaluate their approach to change control and configuration management. Outages, particularly within revenue generating systems, simply cost too much to rely upon notification after the fact. Likewise, EMA believes that vendors must work to orientate their solutions towards prevention and enforcement of change control policies, or risk future obsolescence.



ENTERPRISE MANAGEMENT ASSOCIATES®

Phone: 303.543.9500, Fax: 303.543.7687
www.enterprisemanagement.com

1219.110106