

## CSI Group of Companies

### Application Whitelisting Improves Security, Reduces Costs and Improves Productivity

CSI Group is a diversified concrete products company based in New Hampshire. Its core business includes a number of concrete companies including precast concrete products, shelter systems, fuel vaults, and tunnel systems. CSI delivers a range of concrete and prefabricated systems that reduce the cost of delivering new infrastructure to local government and commercial businesses. In addition CSI has diversified into a retail automobile dealership and a boat manufacturing business.

A unique challenge for CSI's IT team is to centrally control, maintain and secure a range of systems across 7 companies in 5 locations. Chris West, IT Manager for the CSI Group, turned to Savant Protection as he sought to improve his control over varied and relatively remote workstations and servers.



#### Challenge

Control the software applications running on workstations and servers spread over a variety of businesses to stop the misuse of computers causing constant system rebuilds.

The situation was complicated by the fact that different software was required for each company, so it was not a once size fits all problem for administering software. The different businesses and locations made it far too easy for systems to become cluttered and inefficient.

Since users could add whatever they wanted to the systems, West found himself regularly rebuilding systems. West had the responsibility for systems, but no control over them. He also knew this lack of control was a security risk and that it was only a matter of time before the user behavior caused a major security breach. West sought a solution that would not only ensure control but improve security. He wanted to "set it and forget it" allowing him to focus on managing rather than babysitting end user computers.

*"Given the range of companies Savant's software became invaluable by allowing me to lockdown servers and workstations across the board, ensuring that only what needs to run, will be run by our users." - Chris West, IT Manager CSI*

## Requirements

The CSI Group established a simple list of requirements.

- Security – While the Group had never had a major security breach, protecting the design of new product and the bidding process information in a highly competitive space was paramount. West was concerned over what he viewed as the inability of traditional antivirus to stop or contain a targeted or unknown attack.
- Efficiency / User Productivity – The CSI group was concerned over the growing number of the unauthorized download of unapproved applications that sapped the productivity of users, along with the processing overhead associated with traditional antivirus that slowed system performance.
- IT Control and Costs – With the number of companies spread across five locations, the Group was concerned about the ability of users to make undetected changes to programs and files on their workstations, impacting productivity and opening potential attack vectors.

## Choosing the Right Solution

West sought an answer that would not only satisfy his concerns about his company's IT environment, but would also present a cost effective resolution. He examined traditional antivirus and Savant Protection's application whitelisting solution.

*"Savant has enabled my users to utilize the full processing power of their machines while simultaneously blocking unauthorized and potentially dangerous applications from being deployed on their workstations." -West*

CSI Group's antivirus was stopping *known malware*, based on "signature files" that were distributed from the vendor. West saw the shortcomings of antivirus - it would not stop targeted attacks that did not happen to match previously identified malware.

- Savant's whitelisting solution stopped all unwanted software including unknown threats. Savant did not require daily updates of "known bad" or "known good" signatures, dramatically reducing system overhead.
- Savant allowed the IT staff to block unwanted applications that users attempt to install through downloads or via USB ports. This eliminated the threat of contracting spyware and malware by way of careless installations or software from questionable web sites. Before Savant, system rebuilds that took 10% of staff time were virtually eliminated, since users cannot change systems unless authorized.
- With Savant, West was able to lockdown workstations and servers, ensuring that the only programs running on these systems would be ones that were required for the jobs that ranged from accounting, to engineering, design and sales.



Prior to Savant, users had been free to download or install whatever they wished. After installing Savant West discovered with Savant's system intelligence that instant messaging and social networking applications were rampant on his users' workstations. Not only do these types of programs impact productivity, but they are also a known attack vectors for increasingly sophisticated hackers.



Before Savant, users at CSI Group could easily download and install unauthorized software, including toolbars, entertainment, file sharing and other non-business applications. With Savant running in “Lockdown Mode”, authorized applications run normally and no new software can install or run on a protected device, even by users with Windows Administrator rights. Savant’s local whitelist is created automatically on installation, making deployment fast and simple.

CSI Group needed to allow software upgrades and patches for specific applications, without managing these individually. Savant addressed this requirement through “trusted agents”; approved executables designated to make changes to a protected system, and have those changes automatically whitelisted by Savant. Trusted agents allow applications such as antivirus or Microsoft Windows to update through the internet without user or administrator action.

*“By utilizing the lockdown features of Savant, I am able to “set it and forget it” on all of my systems, offering me a peace of mind that traditional antivirus simply can’t compete with.” - West*

**Conclusion**

The CSI Group was able to install Savant’s application whitelisting technology effortlessly across all of the companies that fall under its control. The utilization of the software has increased production, eliminated system rebuilds, and improved the information security of the Group, all while maximizing the limited manpower and financial resources of the IT department.

*“If I had to quantify, I would estimate that less than 1% of my time on a weekly basis is spent managing Savant, giving me the opportunity to devote more of my time to more pressing issues.” - West*

<b>CSI Requirement</b>	<b>Savant Protection Solution</b>
Security - Stop Malware and Prevent Computer Attacks	<ul style="list-style-type: none"> <li>• Blocks known and unknown malware</li> <li>• Protects remote and disconnected users</li> <li>• Protects laptops, workstations, servers</li> </ul>
Efficiency / User Productivity	<ul style="list-style-type: none"> <li>• Blocks installation of unauthorized software (including by Windows Administrators)</li> <li>• Simple to disable unwanted software through centralized management console</li> <li>• Control read/write access to USB, Firewire, CD/DVD, and Network Drives</li> </ul>
IT Control and Costs	<ul style="list-style-type: none"> <li>• Centralized report of application inventory by user, group and enterprise</li> <li>• Logging and alerting of software changes by privileged users</li> <li>• Installs in minutes</li> <li>• Maintains unique whitelist on each device</li> <li>• Self managing clients block all changes</li> <li>• Minimizes system rebuilds</li> </ul>



## Savant Protection

---

### Technical Highlights

- Self-managing endpoints do not require connections to centralized servers
- No centralized database to maintain and administer
- Patent-pending technology for key creation
- Operates independently of local administrative privileges
- Consumes less than 30MB memory
- Runs in Active Protection and Interactive Mode

### Desktop Management Integration

- Symantec Altiris
- Microsoft SMS/SCCM

### Platforms Supported

- Windows 2000
- Windows XP
- Windows XP Embedded
- Windows WEPOS
- Windows Server 2000

