

Lincoln County, Montana

Application Whitelisting Reduces the Cost to Secure Systems

Lincoln County covers over 3,600 square miles in northwest Montana; an area twice the size of the State of Rhode Island. With a staff of two in information technology, it is simply not possible to be on-site each time a workstation or server exhibits problems or new software needs to be installed.

When looking for a way to provide better services to its users and improve security, Lincoln County turned to Savant Protection. Savant's application whitelisting solution helped the County save funds compared to the expense of antivirus, eliminate system rebuilds and improve endpoint security



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.

"Our environment presents a unique challenge – we have a small staff attempting to maintain control and security over a geographically enormous network, on a limited budget." Ric Kesling, Director of Information Technology

Requirements

Lincoln County faced the same security compliance obligations of larger organizations, but without the critical mass of staff and budget. There were four major issues:

- Stop Malware and Prevent Computer Attacks – The County was concerned with the growing number of attacks by increasingly sophisticated hackers. Antivirus could stop malware that was previously identified by antivirus vendors, but was unable to stop unknown, new and targeted attacks. The County needed a more effective solution than traditional antivirus to protect its information.
- Block Unauthorized Software – Kesling knew that users were adding unauthorized software to workstations and laptops and wanted to regain control over what applications users could run on County’ computers. Shareware, add-on applications, Facebook, LimeWire and other social networking sites were easily accessed or installed. Some of these programs were known to include spyware and even malware. Much of this violated the County’s appropriate use policies, increased the chances of compromise and the potential to lose critical data.
- Compliance Reporting – Lincoln County, like other local governments, faces an array of ever-changing reporting requirements ranging from local and federal mandates to HIPPA and Sarbanes-Oxley. Compliance is critical getting reimbursements, especially federal funds.
- Conserve IT Resources – Time spent on system rebuilds due to infections and unauthorized software installations was a growing problem for Lincoln County. With Kesling and a part-time assistant as the County’s only IT resources, a solution was needed that would conserve management time.

“So many new attacks are devised every day that the idea of maintaining an effective and properly updated antivirus blacklist seems remarkably inefficient and outdated.”

Choosing the Right Solution

Kesling sought a simple solution that could satisfy the County’s needs for better control, increased security, and simplified compliance, all without burdening limited resources. He chose Savant Protection’s Endpoint Security Solution and Enterprise Management System for its ability to meet his needs.



Savant Stops Malware

Lincoln County had used antivirus software for years. Traditional antivirus can stop known malware, but only after an attack has been identified and a “signature file” distributed. Kesling understood that antivirus would not stop targeted attacks that did not match previously identified malware.

Savant’s whitelisting solution stops all unwanted software, even that which has not been previously identified as a threat by antivirus. Savant treats each computer as a unique device with its own whitelist, automatically learning those applications to create an implicit whitelist, while denying all others from executing. Unlike antivirus, Savant does not require

daily updates of “known bad” or “known good” signatures, greatly reducing management overhead.

“By eliminating antivirus software, Savant saved the County money while providing a higher level of protection and control.”



Savant Blocks Unauthorized Software, Allows Trusted Updates

Before Savant, users in Lincoln County could easily download and install unauthorized software. With Savant running in “Lockdown Mode”, authorized applications run normally and no new software can install or run. Savant’s local whitelist is created automatically on installation, making deployment fast and simple.

“Once you know what is there, Savant allows us to remove authorization of unwanted applications, immediately removing the ability of those applications to run.”

Lincoln County 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 that update through the internet such as Windows Updates to update without user or administrator action. Trusted agents also allow organizations that manage endpoints using Altiris or SMS and similar solutions to automatically whitelist applications deployed through those systems while blocking all other software.

“Savant’s effectiveness has eliminated system rebuilds, and its ease of management allowed us to divert personnel into other, more pressing technology projects.”

Savant Simplifies Compliance Reporting

Listing the applications running in an organization is critical to compliance with internal and regulatory standards. Savant simplifies reporting, providing a single view of all software installed by user, group or enterprise wide. Unwanted software can be disabled with the click of a mouse.

Savant is Efficient and Easy to Deploy – Kesling looked at centralized and policy-based solutions and knew the cost and difficulty of deploying and managing these would not work for him. Savant Protection solved this problem through its self-learning approach to deploying and managing whitelisting. Instead of building complex policies, restricting administrative rights and spending months planning a deployment, Savant installs in minutes on each device and automatically “learns” the files that require CPU access. Once installed, Savant will ensure that no additional software can be installed or executed. In addition Savant’ lockdown option ensures that no existing programs can be changed, added or deleted.

Conclusion

In a matter of hours Lincoln County was able to deploy Savant Protection’s whitelisting technology on its workstations and servers, preventing malware from executing, increasing productivity and centralizing control of the network, all while maximizing the limited personnel and financial resources of the County.

“Since deploying Savant there has been no downtime or intrusion of any kind.”



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

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
- Windows Server 2003

