Sophos Advisement

For the past several years AgriLife IT has been aggressively testing additional control features offered by the Sophos product for workstations in which AgriLife IT supports directly. This has been primarily tested in over 1500 workstations across the state in the Extension Agency.

Below is a brief accounting of those control features that have been tested and the positive results they have provided in order to better protect systems.

Upon your review if you are interested in deploying such controls for your unit I would recommend contacting Philip Hurley, Sophos Administrator, to discuss implementation or any questions you may have. We HIGHLY recommend not implementing these types of controls on your own unless you have fully researched and tested.

NOTE for Clarity: AIT has NOT deployed these control on ANY College, or AgriLife Research systems. The trials have been strictly focused on AgriLife Extension systems. AIT does not manipulate any unit’s individual Sophos Policies or controls. However, AIT does review and communicate with units whose policies which may have consequences of a negative nature or have deviated to far from best practices or TAMUS policy.

Overview of Findings

On-Access Write Scanning
Approximately 1500 workstations in the Sophos Enterprise Console are currently being managed under an On-Write policy. This management was initiated almost 3 years ago.

This policy checks for malicious activity when a file is written to the hard drive. Sophos scans files as they are read, by default. In the past three years, there is no evidence that On-Write, real-time scanning interferes with normal computer operation.

Since being implemented, Sophos On-Write scanning has automatically detected and cleaned infected files without involving the user. Often no other intervention was required by the IT manager.

Blocking Third-party Security Products
Approximately 1500 workstations are also operating under an application control policy that blocks third-party security software, such as MalwareBytes Anti-Malware or McAfee Security Scan. This implementation began in February 2013. This application control does not remove these products—it blocks them from being installed or accessed. The benefit to this control is to avoid having a user install multiple anti-virus and scanning products on a system which will create system performance issues.
However, it can also prevent them from being removed once the policy is in place. The Sophos Enterprise Console records and can report specific workstations that contain blocked applications. The machines with blocked software can easily be identified and the IT manager can respond appropriately.

**Blocking Toolbars**
Approximately 200 computers now have Conduit Internet toolbars blocked. The Conduit products have been problematic because they change default search providers and home pages. In the first few weeks of implementation, Sophos identified 11 workstations on which Conduit products were previously installed.

Conduit products, such as SearchProtect install invasive services, TSR processes, registry entries, browser helper objects and browser add-ons, all of which make it more difficult for workstation managers to remove the toolbar product. Using Sophos to prevent such products from installing in the first place allows IT Support to focus on other issues.

---

**Alan Kurk**
Director/CIO
Texas A&M AgriLife Communications & Information Technology
Phone: 979.845.9343 Email: akurk@tamu.edu