UTOPIC software

SECURITY

Preserve. Protect. Recover!

IF ANTI-VIRUS IS DEAD, THEN WHAT?

How configuration automation fills the vulnerability gap

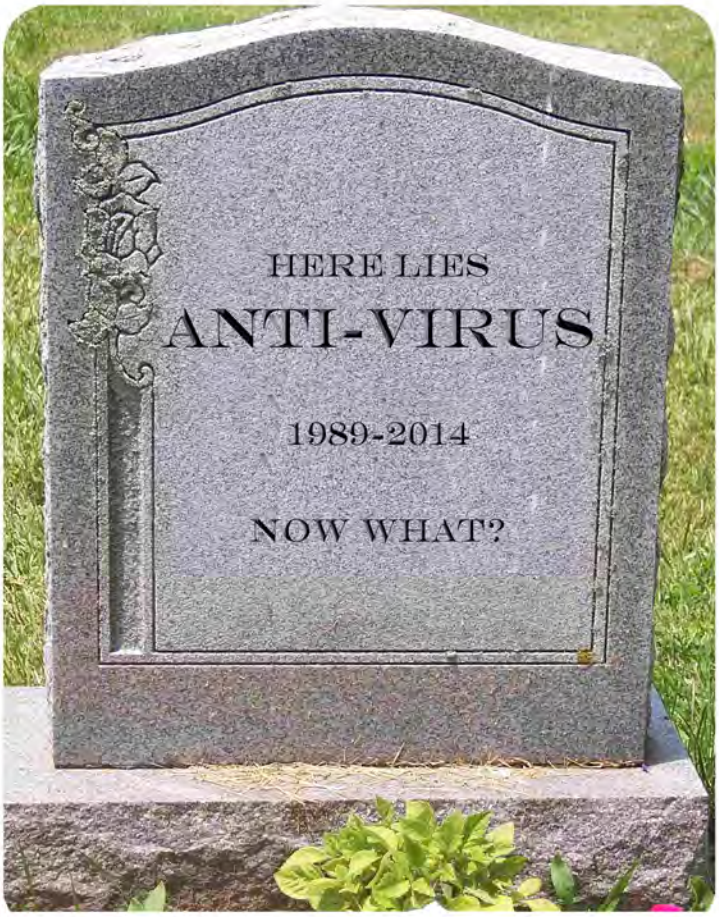
(813) 444-2231
partner@utopicsoftware.com
www.utopicsoftware.com

"Antivirus 'is dead,' says Brian Dye, Symantec's SVP for information security. Dye estimates antivirus now catches just 45% of cyberattacks."

-Wall Street Journal May 4, 2014

Earlier this month, the progenitors of anti-virus software declared that "anti-virus is dead." (Wall Street Journal May 4, 2014) According to Symantec and other industry leading statistics the software designed to prevent malware, spyware and other intrusive tactics are doomed to failure. They say that **anti-virus only catches 45% of the threats.**

The battle is being lost because prevention and protection are always two steps behind. As fast as someone comes up with a preventive signature, six more even nastier bugs are developed and released on unsuspecting networks. It is said that **95% of all networks** (source: FireEye and ThreatSTOP) **have some sort of active infection.**



Configuration tools may not be a traditional security solution, but as an *automated* component in a larger initiative, enables key security features.

IF ANTI-VIRUS IS DEAD, THEN WHAT

To add fuel to the fire, IT security thought guru Eugene Kaspersky recently said: "The single-layer signature-based virus scanning is nowhere near a sufficient degree of protection - not for individuals, not for organizations large or small."

The barbarians may be at the gates, but it's not all doom and gloom. Many IT pros, those associated with mid- and larger tier enterprises recognize that security best practices are not singularly tied into firewall protection, but an interoperable combination of key functions.

The defenses may be in place, but the war is still not being won. An organization may be continuously monitoring, correlating, provisioning, authenticating, blocking, but too many companies are not taking advantage of what makes security more effective; more prolific across a wider enterprise expanse. What is missing is automation.

Let's return to the company that depends heavily on anti-virus to prevent breaches and other negative impact events. If Symantec is a credible source, then this company needs a new and innovative way of maintaining a safe and secure environment. Let's also assume that even with a stack of other security tools, that phishing, botnets, and malware will always find a way to breach the network. If multinationals like Citibank, Target and Sony struggle with breaches, than the likelihood is you do as well (sources say 78% experienced breach in the past 2 years). What needs to happen is to automatically protect.

In the absence, or more likely in support of anti-virus protection, initiating some sort of automated **repair/recovery** program seems to be a progressive alternative growing in acceptance and popularity. It is based on the continuous maintenance of an ideal state. This way, any time an unauthorized outside influence tries to change a registry, attach itself to a file, or embed itself in a supported application, the system rejects these modifications in favor of the ideal state. After every PXE reboot of a workstation, or device, the automated system reapplies the latest approved image.

Within this scenario, any infection introduced after the last boot up is eliminated. Case in point: an inside sales person uses your network and internet connection to reach their independent email account. They see a new email from a friend: "U should see this." Thinking the friend is a trustworthy source, the

email is opened and the link within is clicked. The website redirect seems harmless enough, a picture of puppies or a video of a skateboarder miserably miscalculating an airborne trick. However, on the next click a **Secure Shield dialog box appears** and lets the user know their network is in danger. Believing they are good stewards of the company, click on the link to load the "security update." And as fast as that, the ransom-ware makes their device a paperweight.

Without automation, a help desk tech will probably spend several hours diagnosing and then manually restoring the hacked registry. Even if a fresh image is available, there is still the necessary manual intervention of reapplying specific user settings, applications and privileges based on the business need, corporate policies and organizational role. Then there is a greater time commitment on investigating whether the issue has spread beyond the single device or has evolved into a greater threat. One moment of carelessness creates hours and hours of IT involvement, QA/testing, and re-ensuring compliance requirements. This doesn't include the lost productivity, potential risk and cost this threat poses to the entire network.

The same scenario using repair/recovery automation doesn't prevent the recklessness, but prevents the mistake from spreading further. All the user needs to do is turn the machine off and back on. This applies a fresh ideal state. The ransom-ware and any other unauthorized change are gone… automatically without IT intervention. More importantly, the ideal image is configured for the individual (or their role). The image maintains their applications, settings, latest updates and other unique components so the system lifecycle is perpetuated, uninterrupted and remains firmly under IT's control.

Real time configuration management security also supports compliance considering that several of the SANS critical controls (which serve as the basis for more than 3 dozen regulatory compliance agency mandates) are maintained through proper configuration and demonstrated control. For example, PCI/DSS requires: "*2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards*." SAN simplifies this to mean "*Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers."* The ability to continuously maintain an ideal state for a variety of roles is the key to ensuring assets are only

available to appropriate users. If each device is covered under a Repair/Recovery Reimage configuration protocol, then (as HIPAA 11.0 demands) you are demonstrating control over data. The system cannot accept unauthorized changes (as detailed in your organization's standards and policies) to registry, applications or files. This is not to say an organization can forgo provisioning, log archiving, firewall reinforcement or authentication, but automating configuration puts another proverbial brick in your defense wall.

Security requires attention 24/7…

"If I can cut that in half, we're talking a staggering amount of money," says Bruce Perrin, CIO for Florida-based Phenix Energy Group. "Seventy percent of what security professionals do could be done completely automatically, giving them more time to do things that are more important."

62 percent of respondents in a recent IDG Research survey indicated they automate less than 30 percent of their security functions. For most companies that turns out to be a great deal of manual personnel hours. Hackers don't sleep, so why should your security? Unless an IT department is staffed around the clock, there is a certain amount of time that users are on their own. And the most blatant issues (the ones that gain headlines) don't start as brute force attacks—they are sneaky and insidious that can lay dormant for days or months (like Heartbleed); so that middle of the night emergency call may never come until it's too late. By automating the configuration-break/fix process, organizations remove a significant burden.

For example, a unified school district in Central Florida manages a student computer lab more than 2000 PCs. They conservatively estimated that each PC experiences some sort of break/fix incident every 90 days (and 5% experience a catastrophic failure each year). And each incident required a manual intervention of one hour each. This equated to approximately 7,450 man hours over the course of the year. Also when considering the ROI, the average downtime of each machine was at least 4 hours from report to resolution. When they applied *an automated process*, the **break/fix issues were reduced by 90%.** This saved 9,450 hours and an **annual cost savings of slightly less than 16,000/mo ($191,121/yr)**.

EXAMINING THE ROI

Existing Repair/Recovery/Reimage Process

PC end-points	2,000
Incidents per year (1:90 days/device)	8,100
Cost per incident	$28.50 (based on nt'l salary avg)
Hours for manual intervention	7,450* (> 3.5 FTE system techs)
Existing Costs	**$212,325**

New AUTOMATED Configuration Process

PC end-points	2,000
Incidents per year (1:90 days/device)	810 (90% reduction)
Cost per incident	$28.50
Hours for manual intervention	744* (1/3 FTE system techs)
Adjusted Costs	**$21,204**

Annual Savings: **$191,121 or 6,700 combined personnel to reassign to higher level tasks**

ROI: **After investment (subscription *and* services), ROI was achieved in 97 days.**

Automation also promotes the ability to respond to higher value threats in a shorter amount of time. And if you can reduce the number of security incidents through automation, you reduce the risk of data loss, which again can amount to staggering amounts of money given the potential cost of a single breach.

Repair/Recovery/Reimage **may not be a traditional security solution, but as an automated component in a larger initiative, enables key security features** that are not only compliance requirements, but keep the operating environment running smooth over the course of the lifecycle. And, for that reason alone, should be included as part of any organization's next generation security arsenal.

Let us prove it!

Schedule a demo today