sdmsoftware

CASE STUDY

PacStar®

Challenge

No PowerShell tool could automate changes to GPO settings in administrative templates and user containers.

Solution

Group Policy
Automation Engine

Results

- Automates changes to GPO settings easily and efficiently
- Differentiates PacStar from competitors in military sector
- Saves time and money by preventing costly configuration errors

"Administrative templates and user containers affect 75% of GPO settings, and Group Policy Automation Engine is the only solution to support them."

JEFF GROSSMAN
Security Architect
PacStar

Organization

Based in Portland, Oregon, PacStar develops advanced voice, data and video solutions for military, government and commercial organizations. PacStar's principal customer is the U.S. Department of Defense (DoD) for whom it provides tactical and deployable systems for first-in communicators.

THE CHALLENGE

When working on solutions for the DoD, PacStar follows configuration standards in Security Technical Implementation Guides (STIGs). STIGs contain technical guidance to lock down information systems and
software that might be vulnerable to malicious computer attacks.

PacStar has three objectives: Deliver secure systems to the warfighter in the field, reliably replicate secure configurations during manufacturing, and meet or exceed STIG requirements. To meet these objectives, PacStar uses Windows PowerShell to automate the application of STIG requirements relevant to a particular DoD solution.

The challenge was finding a way to fully automate Group Policy Object (GPO) settings that correlate to STIG items in Windows. The GPO editor is an entirely manual solution. Partial automation with other Microsoft Management Console snap-ins was an option, but partial automation makes it difficult to trace a setting back to its STIG requirement, and updating a STIG item requires recreating the security database. Most important: Snap-ins do not support administrative templates or the
entire user container.

Another possibility was direct manipulation of the Windows Registry, but some GPO settings don't have documented registry settings. Plus, it's impossible to set items in the user container. PacStar needed a fully automated solution for its non domain-joined products.

"These challenges led us to search for a PowerShell library that could overcome the shortfalls in native Microsoft tools," said Jeff Grossman, Security Architect, PacStar. "Although there are several GPO manipulation products available—even free ones—most of them focus on tasks related to GPOs in the domain environment, and we needed non-domain features. Only one solution could handle administrative templates and user containers."

The Solution

PacStar chose SDM Software's Group Policy Automation Engine to automate GPO settings in the local security policy of non domain-joined Windows systems during production of communications solutions for the DoD. Group Policy Automation Engine uses PowerShell or .Net to script GPO changes in both domain-joined and non domain-joined environments.

"Administrative templates and user containers affect 75% of GPO settings, and Group Policy Automation Engine is the only solution to support them," Grossman said.

PacStar uses Group Policy Automation Engine to configure DoD products before shipping them. For example, products must include systems that are locked when unattended because unattended systems are susceptible to unauthorized use. The screen saver must be set to a maximum of 15 minutes and password-protected to safeguard critical and sensitive data from exposure to unauthorized personnel with physical access to the computer. The options must be configured in the user container.

"Without Group Policy Automation Engine, our only other option is to introduce manual steps into the STIGing process," Grossman said. "That process is slow and error-prone, no matter how well documented the steps are. This is why Group Policy Automation Engine is so important to our automation strategy. Not only does it help us prevent configuration errors, we save 30 minutes in configuration time per product. No other solution provides the needed functionality like Group Policy Automation Engine."

THE RESULTS

Automates changes to GPO settings easily and efficiently

PacStar develops secure, customized communications solutions for military, government, and commercial entities. For DoD projects, PacStar relies on Group Policy Automation Engine with Windows PowerShell to automate STIG requirements in administrative templates and user containers of non domain-joined Windows systems. Group Policy Engine is the only solution that manipulates administrative templates and user containers.

Differentiates PacStar from competitors in military sector

Group Policy Automation Engine gives PacStar a competitive advantage by helping produce secure systems quickly and accurately. Group Policy Automation Engine makes it easy for PacStar to trace GPO settings back to their STIG requirements.

"We've earned a solid reputation among branches in the military based on our security expertise," Grossman said.

Saves time and money by preventing costly configuration errors

Group Policy management tasks that could take hours take minutes with Group Policy Automation Engine. For example, scripting the changes saves PacStar 30 minutes per system and diminishes the risk of costly human error.

sdmsoftware

SDM Software, Inc. is the leader in providing products for managing Windows Group Policy technology. With extensive real-world knowledge and experience managing Windows environments ranging from 100 to 100,000 systems, we build products that are designed with administrators in mind. For more information, contact us at +1 415 226 1308 or visit www.sdmsoftware.com.

©2015 SDM Software, Inc.