PUBLIC UTILTY CASE STUDY

FoxGuard Solutions®

EXECUTIVE SUMMARY

FoxGuard worked with a small public energy utility to successfully design and deploy an automated patching and configuration management solution within a highly segmented and restricted network. According to the organization's IT staff the "PAR contains what we need for patch discovery" and the platform provides "easy to deploy patches." After a year of service they are "very pleased with the solution" and are "expanding the scope of what [they] have FoxGuard monitor."

INTRODUCTION

This organization, like many organizations, is faced with a new set of compliance requirements which mandate increased efforts for patch availability monitoring and mitigation. FoxGuard was asked to evaluate their hardware and software assets and recommend services to address compliance needs. This case study will outline some of the key issues and criteria and discuss the solution.

THE PROBLEM

The organization struggled with monitoring the availability of patches and updates outside of Microsoft. This is a common problem in organizations that lack automated patching solutions beyond OS native services. They needed all non-security and security related patches, updates and firmware. One of the goals for the project was to address patch and update availability monitoring beyond automated tools; as near to 100% coverage as possible. They struggled with the acquisition and deployment of required patches and updates. This was partly due to the lack of a central patch repository and further hampered by the lack of a vendor agnostic patch distribution service.

The IT staff had experience in the manual patching and updating process but did not have experience with the automation side of things. A second goal for the project was to provide a platform for centralized patch provision and scanning which allowed for custom content. They utilized a variety of network devices which makes central management of configurations and device firmware difficult. A third goal for the project was to provide a platform for centralized configuration management and firmware version monitoring.

DECISION CRITERIA

The solution considered the following:

- The organization operates predominantly Microsoft Windows based systems
- Additional patch monitoring is limited to a defined list of third-party applications
- There is a large variety of network appliances running proprietary or Linux operating systems.
- Their network makes heavy use of firewalls for segmentation and access control
- The automated system should utilize a staging server for updates (no Internet access)
- The automated system should include disaster recovery and failover capabilities
- Other security assets are newly deployed across the network including asset management, IPS, and password management
- Small IT staff (2-4 people)
- No experience with automated patching solutions

PUBLIC UTILTY CASE STUDY

THE SOLUTION

Patch and configuration management are not one-size-fits-all solutions. FoxGuard worked with the organization to determine the most appropriate tools for the job.

The organization subscribed to FoxGuard's Patch Availability Reports (PAR) to receive monthly notices on all third-party software assets, as well as, all device and appliance updates. FoxGuard is considered their one source for all patch and update information for the organization.

FoxGuard provided the organization a low-cost Microsoft Hyper-V platform which hosted an automated patching solution (Shavlik Protect) and a network configuration manager (Solarwinds NCM). FoxGuard also provided hands-on training for the platform. The platform was deployed on both the primary and backup networks and replicated to maintain continuity between the two halves of the system. A staging server was also setup to allow required patches to be downloaded from vendor websites without exposing the internal network directly to the Internet. Patches were then replicated to the patching server.

FoxGuard worked with the organization to open communication channels between the staging server and patching server and from the patching server to all applicable endpoints. Additional communication channels were opened between the NCM server and all network devices and appliances. We also aided in troubleshooting firewall and IPS rules across the network to allow full system functionality in accordance with the organizations network segmentation strategy. FoxGuard also assisted in on-boarding all endpoints into the patching server and NCM server configurations.

HOW WE EXCEEDED EXPECTATIONS

FoxGuard worked with the organization to establish expectations prior to arriving on-site. The following items were beyond the scope of effort but provided additional value to the organization:

- FoxGuard identified issues and tailored the system design on-site
- FoxGuard worked with the organization to expedite validation of the platform
- FoxGuard aided in correcting configuration issues with organization equipment
- FoxGuard tailored training to organization personnel
- FoxGuard provided recommendations to enhance security and automation
- FoxGuard worked around on-site delays and delivered on time

For more information, contact FoxGuard:

requestinfo@foxguardsolutions.com @FoxGuardInc company/717871