PATCH MANAGEMENT SOLUTIONS

FoxGuard Solutions®

WHY PATCH CONTROL SYSTEMS

Industrial control systems (ICS) in critical infrastructure (CIKR) are high-risk attack and exploitation targets. Patches and updates are required to help resolve security vulnerabilities, functional issues and meet compliance requirements.

COMPLIANCE BURDEN

NERC CIP compliance regulations state that registered entities are required to have a patch management process for tracking, evaluating and installing cyber security patches for their identified cyber assets of applicable systems

TIME & RESOURCE BURDEN

Patch management can be time consuming and very labor intensive. Most entities operate highly heterogeneous systems, often requiring multiple technical resources just to support continuous monitoring of hundreds of third party software and vendor websites for newly released patches. Utilities can spend over $500,000 per year, simply to monitor as many as 800 vendor sites for patch releases.

SCOPE BURDEN

As the complexity of industrial control systems evolves, so does the number of devices and applications that need to be patched for both security and compliance reasons.

DEVICES & APPLICATIONS SUPPORTED

OPERATING SYSTEMS	3RD PARTY APPLICATIONS	NETWORK DEVICES	FIELD DEVICES

PUMP

PATCH & UPDATE MANAGEMENT PROGRAM

WHY FOXGUARD?

FoxGuard has proven excellence in not only meeting compliance requirements but also solving functional issues and security vulnerabilities. We have successfully deployed patching solutions in over 150 sites, in 15 countries in the past 10 years.

For a fraction of the price and the time it takes to continuously monitor hundreds of vendor websites and review patches, FoxGuard can deliver the convenience of an automated patch management solution specifically customized for your operation.

Our field-experienced security experts have over a decade of patch delivery experience in IT and OT space. We understand the complexities of the control systems in CIKR environments. Thus we can efficiently alleviate the never-ending burden of managing patches.

FoxGuard has relationship with the U.S. Department of Energy (DOE) and many leading industrial control system vendors. We leverage our relationship to develop a robust patch management solution for the energy industry.

FoxGuard can centralize your patch management burden, help you meet the NERC CIP compliance requirements in a simplified, cost-effective and timely fashion and facilitate a more secure environment by being up-to-date with critical updates & patches.

PATCH MANAGEMENT SOLUTIONS

COMPREHENSIVE SOLUTION

A robust patching program requires a cyclical and consistently monitored solution to ensures a secure and healthy system. To ensure a successful patch management program we provide the following services:

ASSET IDENTIFICATION & BASELINE

Prior to monitoring patch data, it is critical for the utility to properly document all of their critical assets from which to build a baseline. This process can be time consuming, and in many cases requires a certain level of technical talent to accurately complete this process. FoxGuard provides this service in order to build a proper patch management program. This is the foundation for all other steps in the process.

AVAILABILITY REPORTING

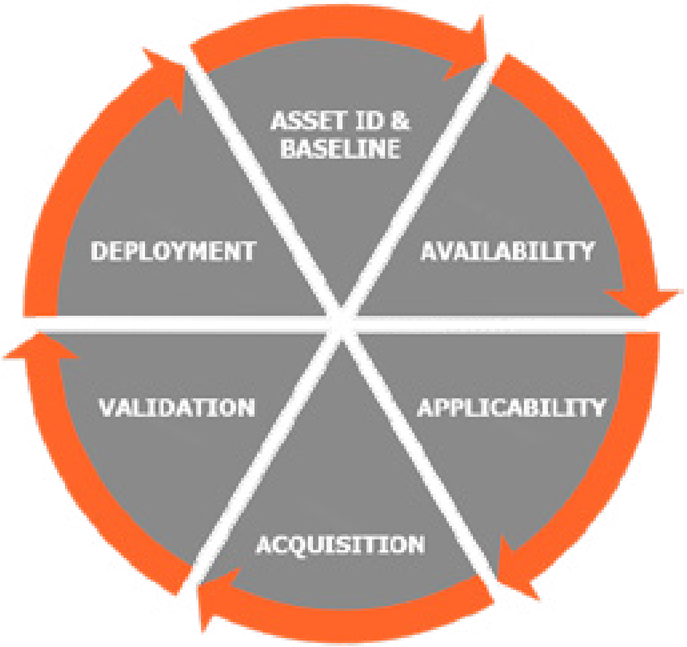
FoxGuard monitors operating systems, 3rd party software applications, network devices and field devices to provide monthly intelligence reports that track the release of cyber security patches specific to your environment.

APPLICABILITY REPORTING

FoxGuard evaluates released security patches for applicability of devices and software used in your environment. Reports are provided for further review with in-house analysis and sign-off to support compliance requests.

PATCH ACQUISITION

FoxGuard can acquire and authenticate applicable patches for delivery in a single, comprehensive deliverable. We support multiple delivery methods, including secure electronic download and tamper-resistant physical distribution via physical media. All deliverables are digitally signed using public-private key technologies.



PATCH VALIDATION

FoxGuard develops and implements a representative patch validation environment (at your facility or in our lab), to test applicable patches for use with your software applications and equipment. Test plans are highly customized and may address a variety of scenarios such as:

- Basic functional testing
- System performance comparisons
- Discovery and documentation of logical network port changes

PATCH DEVELOPMENT

FoxGuard designs a comprehensive, easy-to-use patch management and deployment solution that best fits the needs of your specific environment. We offer a variety of field services to support acceptance testing, implementation and training as part of our turnkey platform.