

Security Patch Management Services

OSI Professional Services

While patch management is critical to the security of your control system and ultimately your operation, the process of effectively researching, deploying and maintaining patches is an incredibly costly and complicated endeavor.

The validation and deployment of patches is a highly time consuming and complex process. Without a comprehensive strategy to ensure that the accurate patches are deployed quickly and correctly in your environment, you may be exposed to some of the most severe vulnerabilities.

OSI's Patch Management Service ensures that corporate risk tolerance, security vulnerabilities, configuration/change management, IT infrastructure inventory, and functional and business issues affecting your critical cyber assets are addressed in a timely, efficient and cost-effective manner. OSI's Patch Management Service enables our customers to quickly and confidently implement all 3rd party and OEM security patches to maintain a stable and secure control system operation.

OSI is committed to offering the best security products and services to mitigate your organization's ongoing cyber security protection initiatives. The NERC CIP standards, as well as other regulatory cyber security directives, reinforce the need for a formal and comprehensive Patch Management program in support of your mission critical SCADA and control system infrastructure.

To help strengthen your stance on cyber security OSI offers a comprehensive and flexible patch management program to meet your specific needs.

What is Patch Management?

Patch management is a general IT term referring to managing platform and applications software security updates and software patches which are issued by software vendors. NERC CIP standards require you to make sure your control system software includes all applicable latest security patches from all your software suppliers including the platform software such as operating systems, relational databases, etc.



Overview of Software Patch Update Cycle

There are hundreds or even thousands of patches which may be issued by the 3rd party software vendors every year. Managing the applicability of these patches as well as the compatibility of these patches with your control system software could be a daunting task.

OSI's Patch Management Services are intended to facilitate and assist you in certification of 3rd party patches and determination of their applicability to your **monarch**[™] system. Our Patch Management Services will assist you in the following areas:

- **Applicability Determination:** We will determine and evaluate the applicability of the OEM patch to your **monarch** system.
- **Compatibility Evaluation:** We will determine whether the applicable patch will or will not interfere with the functionality of the **monarch** system and that the **monarch** software will run or will not run as before with the OEM patch installed.

Continued...

- **Remedial Strategy:** For offending 3rd party/OEM patches which are critical to your system, we will provide work arounds or an OSI software patch to make sure the operation of your **monarch** system after the patch installation remains unchanged.
- **Help Desk Support:** We will provide a Help desk and support hotline to answer any questions on your patch installation of the OSI patches or general patch management issues.
- **Supplemental Support:** We can provide you with engineering services and labor to install the OEM patch as well as the OSI patch, either through remote support or via on-site filed service calls.

Service Highlights

OSI's Patch Management Service is designed to seamlessly integrate a robust patch management process into your daily control system IT operations. Our security professionals take a comprehensive and top-down approach to patch management, and utilize industry best practices such as ISO 17799. The process is also based on applying business and technical requirements, including those for change management, network infrastructure, security policies, and operating systems and other 3rd party software inventory.

OSI certification methodology is based on the U.S. Department of Homeland Security's Procurement Language for Control Systems and the NERC CIP requirements. All pertinent 3rd party and OEM software patches are continuously monitored and tested by OSI security professionals in a Sandbox environment and their applicability and impact on your simulated control system software are evaluated and are certified for deployment on your target system.

Patch Management Service Levels

In order to offer a cost effective program for various needs and budgets, we offer a multi-level Patch Management Service (PMS) program.

Patch Management service levels available are:

- Silver service
- Gold service
- Platinum service

Based on the service plan that is selected, subscribers will then be notified of certified patches at varying frequencies such as quarterly, monthly, or weekly/immediately upon availability.

Various factors determining the applicability of a particular service plan and its associated cost are:

- **monarch** Software version in use
- Number of OSI products installed on your system
- Operating system(s) version(s) used
- Number of servers, workstations and complexity of operation
- System size in terms of points, RTUs, etc.
- System complexity in terms of backup systems, Training Simulators, Development Systems, etc.
- Existence of a Quality Assurance System or Program Development System for testing purposes (sandbox environment) to facilitate patch management/installations

If you prefer, or if you are unsure of your specific needs and requirements, OSI can perform a Patch Service audit of your current system by dispatching the OSI Cyber Security personnel to visit your site, assess your needs and develop a plan that meets your security requirements while considering your budget constraint.

For more information please contact us at Sales@osii.com.