Grid Cyber Security

Third Party Security Patch Management Services Fact Sheet

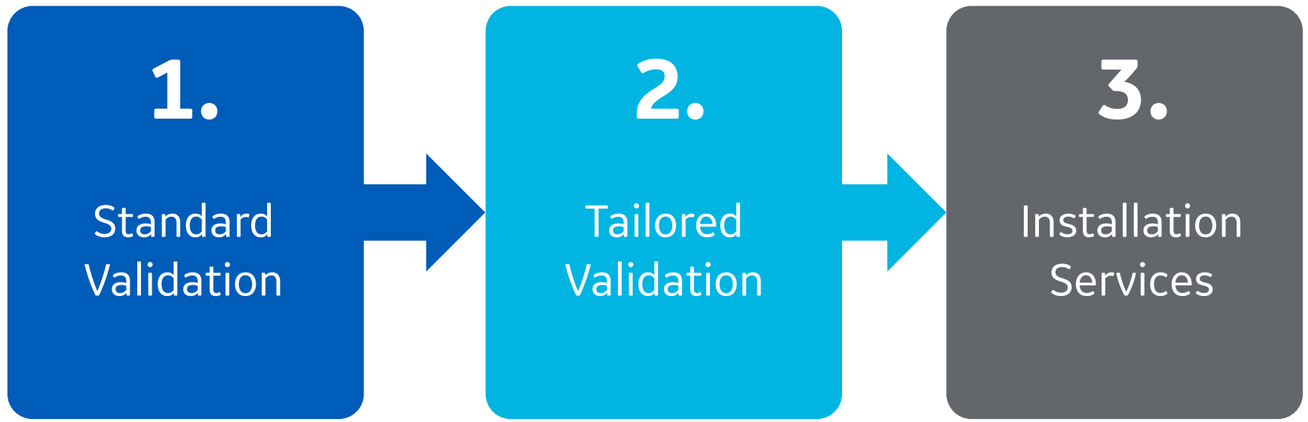
Maintaining appropriate levels of security patches is a key aspect of any good cyber defense strategy, and is a specific requirement for compliance with a number of security standards and regulations, such as NERC CIP and EU's NIS Directive.
For systems that must be operationally available 24/7, the patching strategy is significantly different than the traditional IT approach, where some degree of planned downtime is tolerable. In these mission-critical environments, security patches must be analyzed, assessed and tested much more thoroughly to ensure there is no impact to the functioning of the system, and must be applied in a highly controlled manner.

GE Digital Grid's Third Party Security Patch Management Services help maintain an effective level of cyber security without compromising product functions or operations. Security Patch Management is a tiered service for customers using supported versions of GE Digital Grid's products and associated third party software to help them stay up-to-date with vital security patches. Security Patch Management is a collaboration between GE and the customer in which GE performs applicability assessment and patch testing to provide a level of confidence before security patches are applied by GE or the customer on QAS/support systems and then on live systems.

Key Benefits

- Maintain compliance with NERC CIP and cyber security best practices
- Reduce patch identification efforts with pre-identified third-party patches applicable to the product
- Reduce operational risk by deploying patches tested by GE
- Easily view and manage patch planning through the 24/7 portal
- Where GE manages the 3rd party licenses on behalf of the customer, reduce time and errors with automated, synchronized patch delivery
- Access experienced GE engineers for testing and deployment help
- Improve accuracy with patch deployment documentation
- Alleviate resource constraints with flexile service levels

GE offers several incremental levels of service to assist customers, who can choose their degree of involvement depending on their technical capability and availability of resources.



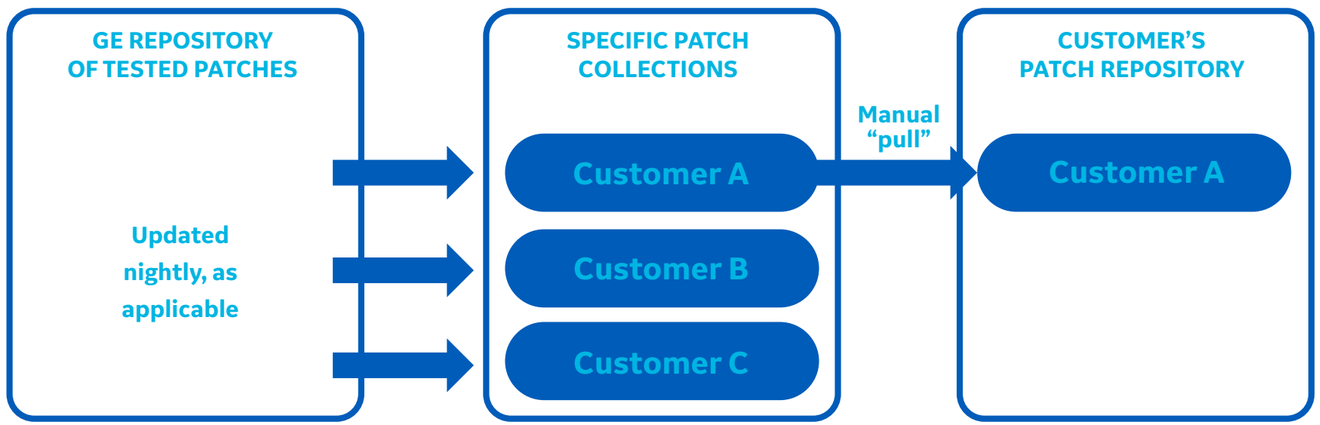
1. Third-party Security Patch Standard Validation

Third-party Security Patch Standard Validation is the foundation service from GE. It comprises a rigorous process of assessing and certifying select, covered third party software security patches that are notified by US-CERT, ICS-CERT, third-party vendors, and other sources, and released by third-party vendors to address cyber security issues. GE aims to test and validate third party security patches within 30 days of the patch's release by the vendor. Validation testing is performed in a standardized security-testing environment, using the latest supported version of the product.

Subscribers to this service have 24/7 access to the Security Patch Management portal, which includes a live patch management report showing the current status of all patches and provides advanced notification of future planned version changes. The portal also includes installation instructions, links to other security sites, and technical support for patch-related questions.

Additional Service – Automated Patch Delivery

This simplifies the delivery of relevant patches where GE manages the third party license, by creating an area for each customer on a secure GE server where applicable, validated patches are collected and can then be pulled as required for installation. For some operating systems, such as Linux, it may be possible to offer an automated, synchronized delivery service to streamline the process still further.



2. Third-party Security Patch Tailored Validation

Tailored Validation goes a step beyond the Standard Validation service that tests on a standard product environment, and provides engineering services to gather, install and test the available third-party security patches on the customer's representative, non-production system. This representative system includes customer-specific product versions, any custom-developed software and customer-specific configurations that would not be present in the standard product environment. GE's installation and targeted testing in this environment provides the customer additional confidence that the third party security patches should not cause issues when deployed in the field. This service is generally performed on an agreed-upon frequency and includes a report documenting the results.

3. Third-Party Security Patch Installation

Third-Party Security Patch Installation provides planning and remote or on-site engineering services to install the validated third-party security patches on the customer's fielded systems, including a report documenting the results. This is performed on an agreed-upon frequency and will require support from customer personnel to bring nodes in/out of the system during the installation program. The customer is responsible for field-testing.

	*GE responsibility		*Customer responsibility
1. Third-party Security Patch Standard Validation			
2. Third-party Security Patch Tailored Validation			
3. Third-party Security Patch Installation			
	• Identify relevant vendors/ products • Assess patches for applicability • Test patches against standard system • Review results • Approve results • Communicate status (via portal) • Customize patch deployment (RPMs) • Document instructions	• Implementation planning • Collect patches • Assess for applicable patch levels • Deploy applicable patches to customer's representative, non-production system(s) • Test patches on representative system(s) • Record all results	• Implementation planning • Logistics for deployment (release of nodes, etc) • Deploy patches to each applicable node • Test each node – roll back if any problems • Record all results	• Formulate patching policy – frequency, conditions, exceptions, etc. • Decide whether to apply each available patch (risk-based) • Provide connectivity/ access to GE, to pull patches • Make nodes available for patching • Provide access to GE to work on system (if necessary)

Contact Us
ge.com/digital/sales-contact-me