OVERVIEW

Contending with the Challenges of Patch Management

For operators and owners of power generation systems, ensuring compliance and guarding against evolving cyber security threats represent critical, continuous imperatives. Toward that end, it’s vital to quickly apply patches and fixes when vulnerabilities are identified. However, for resource-constrained operations teams, these patch validation, testing, and deployment efforts can present a number of challenges:

• **Risk.** Patches can address vulnerabilities but they can also introduce performance and availability issues when they are deployed in production environments—jeopardizing critical power systems and services.
• **Complexity.** Staying on top of vulnerabilities and patches available can be difficult. For internal teams, it can be hard to verify which vulnerabilities affect specific environments and how interdependent systems may be affected.
• **Administrative overhead.** Applying patches can be very labor intensive. Teams need to dedicate significant time and effort to stay abreast of vulnerabilities and patches; download, install, and test patches; and deploy new code into production.

BUSINESS CHALLENGES

$243 billion – $1 trillion: Impact to the US economy of an electricity blackout across 15 US states affecting 93 million people.¹

64% of power and utilities believe that their security strategy is not aligned with today’s risk environment.²

$3.86 million: Average total cost of a data breach.³

SIMPLIFY OT MAINTENANCE AND IMPROVE SECURITY

How can you stay on top of all the patches available and deploy them fast—without breaking your operations or budget? With the Patch Validation Program from GE’s Digital Energy, you can harness comprehensive patch management services that fuel optimized security, reliability, and operational efficiency.

digital.energy

ge.com/power/digitalenergy

©2019 General Electric Company. All rights reserved.
### Solution Introduction
Now, your organization can gain the security and compliance benefits of optimized patch management capabilities, while offloading a lot of the effort and risk associated with handling these efforts internally—with the Patch Validation Program. This program offers comprehensive patch management services that promote the availability, integrity, and confidentiality of your critical controls and related networks.

Through this service, we'll deliver the patches you need—in validated, tested, and easy-to-deploy packages. We further support your patch management efforts through cumulative updates, deployment automation, and useful, easily accessible documentation. By employing this service, your organization can mitigate its exposure to cyber risk, maximize the availability of your critical systems, and boost operational efficiency.

### Key Features

#### Testing and Validation
As part of the program, GE will test and validate antivirus (AV) and host intrusion detection (HID) signature updates as well as operating system (OS) patches. First, we'll verify whether these new releases apply to your environment, and based on that, we'll establish a list of candidates for testing.

GE's staff then test applicable updates in controlled, representative lab environments that offer safeguards against intrusion and tampering. Through this testing, we determine whether updates adversely affect the functional operation of the control system, related interfaces, or system communications. Based on our findings, we can exclude any updates that may introduce performance or availability issues. Further, if a given patch is excluded, we provide documentation to support this exclusion.

#### Patch Packaging and Delivery
Once patches have been tested and validated, we make them available to customers via a secure web portal. We provide cumulative updates so that your organization can stay completely up to date with the latest releases, even if an earlier update wasn't applied. By delivering these complete, scripted packages, we make it easy for your team to incorporate updates into your transfer and change management processes.

#### Host-Based and Central, Network-Based Deployment Options
The Patch Validation Program is available as a stand-alone offering. Through the program, we deliver scripted files that automate the deployment of patches and antivirus updates. In addition, your organization can deploy these patches using Baseline Security Center. Baseline Security Center brings centralized management to the deployment process, reducing the need to run patch deployment tools locally on each system being patched. By harnessing these combined offerings, your team can enjoy even greater speed and efficiency gains.

#### Backed by a Commitment to Quality
We employ Six Sigma tools and we empower team members to make customer-focused quality the highest priority. Further, our team participates in a number of external quality certification programs, including ISO-9001:2015 and ISO-27001:2013.
Service Specifics

Environment Support
- GE’s turbine, generator, and plant controls and associated networks
- GE’s HMI and Historian hosts, GE’s Thin Client HMI / Control Server environments

Onsite Training
- GE offers up to eight hours of onsite patch deployment training during the initial implementation period

Patch Validation Program Support
- GE’s Product Security Incident Response Team (PSIRT) is responsible for monitoring for cyber-security issues that affect products and coordinating responses. You can report an issue through the PSIRT website at the following URL: www.ge.com/security.

How to Get Started
To learn more and sign up, please contact your local GE’s Digital Energy or GE’s Power Services Account Executive or call 770-722-2552.

Sources

Contact Us
www.gepower.com/contact