Bently Nevada
Cyber Asset Protection (CAP)

2nd

Energy is a top target for cyber attacks, the second most targeted industry worldwide[1]

22%

Outdated and unpatched software constitutes 22% of security issues[2]

29%

Patch management can reduce your attack surface up to 29%[3]

Bently Nevada's Cyber Asset Protection (CAP) subscription for System 1 provides customers with cyber security best practices for patching and defending System 1 Servers and Clients using patch management and antivirus/host intrusion protection. CAP includes tested, documented, scripted and securely delivered Windows® and antivirus patches on a monthly basis for System 1 Servers and Clients saving time and providing additional cyber security threat management capabilities.

Why Patching is Critical

Patching systems is one of the best things to do to protect assets. It ensures the operating systems and programs running are updated to provide the latest security protection. Listed as two of the "First Five Quick Wins" by The SANS Institute, a well-respected authority on information security and cyber security training, patching of application and system software is critical to improving and maintaining a robust security posture.

The Importance of Validation

With validated patch management, the updates are validated in a secure lab that mimics the plant environment in order to identify any incompatibilities that may exist before the patch is applied to a live production system. This allows operators to safely and confidently patch their systems, ensure uptime is not compromised, and protect systems against cyber threats without having to create simulators themselves.

Cyber Asset Protection (CAP)

Validated Cyber Security for System 1 Software that includes the following supported components:

System 1 Validation

Latest two versions of System1 v6.9x
Latest three versions of System 1 20.x or newer

Windows® Validation

Windows® Server Operating Systems (2012 R2-2019)
Windows® 10 Professional 2004 and 20H2 Microsoft Excel® (2016 32-bit)
Microsoft SQL® Server (2016 and 2019)

Antivirus Validation

Antivirus Updates (Symantec, McAfee)
McAfee AV definition will be in both *.Exe and *.DAT formats to support standalone and centralized deployment.

Supporting Documentation

Work Instructions for issues found during validation such as new deployment scripts and modification instructions.

What’s Included

CAP Program Documents

Important information about the components of CAP software updates as well as process instructions and reports.

Compliance/Documentation

Documentation to assist with compliance (NERC CIPs, NEI, etc), system design, reliability, and configuration baseline documentation; ports, services and hardening.

Monthly updates are documented and scripted for operating system, applications and anti-virus signatures.

Support

Access to Bently Nevada Technical support team for CAP-related questions which will be addressed by the cyber security support team.

How It Helps

Products

Validated patching protects System 1 Servers and clients, the most vulnerable point of the system.

Minimizes risk and downtime by ensuring updates are tested in a customer simulated environment with 3rd party validation to correct issues before delivery and accelerate your change management approval process.

Supports Reporting Requirements

Provides an up-to-date and cumulative inventory of applicable updates and their status.

How It Is Delivered

Delivered via the Bently Nevada Software License Portal (download approved ISO’s) and Off-line Secure Delivery (hash validation and digitally signed).

The Validation and Testing Process

Interrogation Testing Criteria

Each update baseline is defined to meet regulations and standards such as NERC CIP, NEI 08-09, and IEC 62443.

The same testing process is followed for all updates involved.

Benefits of Validation

Patch files are tested to ensure system integrity and any unresolved patch issues are communicated via a Technical Information Letter (TIL) prior to being deployed in a production system.

Bently Nevada works directly with vendors, such as Microsoft, Symantec, and McAfee to resolve patch issues with System 1 Software.

Validated patching in a test environment prior to deployment provides system reliability peace of mind.

Baker Hughes Support for Regulations and Standards-A Trusted Partner for Compliance

As a vendor of industrial controls, Bently Nevada embraces its responsibilities to assist critical infrastructure owners to improve their security postures and support adherence to industry standards.

Bently Nevada aligns to multiple best practices frameworks and standards, and helps customers meet regulations such as NERC CIP, NEI 08-09, and IEC 62443.

Sources

1 https://www2.deloitte.com/insights/us/en/industry/oil-and-gas/ cybersecurity-in-oil-and-gas-upstream-sector.html

2 https://www.bulletproof.co.uk/industry-reports/Bulletproof%20-%20Annual%20Cyber%20Security%20Report%202019.pdf

3 https://ics-cert.us-cert.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S508C.pdf