



# Cyber Asset Protection (CAP)



**2nd**

Energy is a top target for cyber attacks, the second most targeted industry worldwide<sup>1</sup>



**22%**

Outdated and unpatched software constitutes 22% of security issues<sup>2</sup>



**29%**

Patch management can reduce your attack surface up to 29%<sup>3</sup>

**Bentley Nevada's Cyber Asset Protection (CAP) Subscription solution is a key part of a layered strategy for industrial Operational Technology (OT) process control network environments. The subscription service includes both operating system and anti-virus/intrusion detection signatures to cover updates for System 1 servers. Monthly updates can be applied to individual Servers or to multiple Servers via the SecurityST centralized management platform saving time and providing additional cyber security threat management capabilities.**

## Why Patching is Critical

Patching your systems is one of the best things you can do to protect your assets and ensure the operating systems and programs running are updated to provide the latest security protection without risking your operation. 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. Our testing process ensures the software, which is the best method to guarantee Bentley Nevada Condition Monitoring Systems receive tailored patches and an applicability report on a monthly basis.

## What it is

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

- Windows Patch Updates (2012–2019) – Server OS, Microsoft Excel (2013–2016 – 32-bit), Microsoft SQL (2014–2016)
- Antivirus Updates (Symantec, McAfee)
- Monitoring System Firmware Updates (when required by security vulnerability)
- Work Instructions for issues found during validation (new deployment scripts, modification instructions)
- Technical Support through Bently Nevada (Technical Information Letter/Technical Information Notice; direct communication)

## How it helps

### Protects

- 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
- Accelerates your change management approval process

### Supports reporting requirements

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

## Cyber Asset Protection (CAP) software subscription scope

### Validation covers:

- Latest two versions of System 1 v6.9x
- Latest two versions of System 1 v18.x or newer
- Windows® Operating Systems (2008R2–2016)
- Microsoft Excel® (2013–2016 – 32-bit)
- Microsoft SQL® Server (2014–2016)

### How it is delivered:

- Bently Nevada Flexera CAP Secure Portal (download approved ISO's)
- Offline Secure Delivery (Hash comparison tool)

## The validation and testing process

### Interrogation testing criteria:

- Each update baseline is defined
- Each update follows the same testing process (not a fast fail test)
- Representative software environment
- Communication testing (intra/inter-system/network)

### Benefits of validation:

- Patch files are tested to ensure system integrity
- Bently Nevada works directly with vendor to resolve patch issues
- Technical Information Letter (TIL) for any unresolved patch issues
- System reliability peace of mind

### What's Included with your subscription

- **Cap program documents:** contains important information about the components of CAP software update subscription as well as process instructions and reports.
- **Compliance/documentation:** assists with compliance (NERC CIP, NEI, etc), system design, reliability, and configuration baseline documentation; ports, services and hardening documentation. Monthly updates are documented and scripted for operating system, applications and antivirus signatures.
- **Support:** Access to Bently Nevada Technical support team for CAP-related questions which will be addressed by the cyber security support team.

## 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

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

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

<sup>3</sup> [https://ics-cert.us-cert.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems\\_S508C.pdf](https://ics-cert.us-cert.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S508C.pdf)