

CYBERSECURITY ASSURANCE PROGRAM CERTIFICATE

Certificate

ULCAP_1066

Issue date

2025-09-26

Expiration date

2026-09-26

Test Report Number

4791834115-001

This is to acknowledge that

Becton, Dickinson and Company

1 Bexton Dr,
Franklin Lakes, NJ, 07417-1815, USA

has had

BD Synapsys v6.11

Synapsys
Software Version: v6.11
Hardware Version: N/A

evaluated and meets the requirements of the standard

UL 2900-2-1: 2023A

Software Cybersecurity for Network-Connectable Products, Part 2-1:
Particular Requirements for Network Connectable Components of
Healthcare and Wellness Systems, First Edition September 1, 2017
including revisions through September 21, 2023

Program owner:

Dean Zwarts

Dean Zwarts, Senior Business Manager

This is to certify that representative sample(s) of the Product described herein have been investigated and as of the date of testing, found in compliance with the Standard(s) indicated on this Certificate. UL Solutions does not provide any representation or guarantee that all security vulnerabilities or weaknesses will be found or that the product will not be vulnerable, susceptible to exploitation, or eventually breached. The designated Certificate Holder is entitled to market the Product in accordance with the Service Agreement and Cybersecurity Assurance Program Service Terms. This Certificate shall remain valid until the indicated Expiration Date unless terminated earlier in accordance with the Service Agreement or if the referenced Standard is amended or withdrawn. This Certificate in and of itself does not authorize the Certificate Holder to use any UL Solutions trademarks on the Certified Product. UL Solutions trademarks may only be used if the Certified Product is also covered under the applicable UL Solutions mark program(s).



Conditions of Certificate

The following conditions must be met for the product to continue to be in compliance with this certificate:

1. Software updates are to be performed in accordance with Synapsys Service Manual (Document “BDDSSGFS7406 - Rev 10_CC-2023-852.pdf”).
2. Only the locally hosted HTTPS server is in scope of this certificate.
3. The server is to be housed in a physically access controlled environment and maintained under facility security policies. BD recommended security configurations are expected to be followed post installation.
4. This certificate does not include Remote Support Services such as remote communication and features enabled for the support engagements.