nCounter® Pro Analysis System Cybersecurity FAQ

*April 2022*

Cybersecurity is an important consideration for research and clinical laboratories. To help answer common questions from customers using nCounter® Pro Analysis System, we have prepared a FAQ intended for lab managers and IT administrators.

The nCounter Pro Analysis System (nCounter Pro) is composed of two instruments: a Prep Station and a Digital Analyzer. The Prep Station is a liquid handling robot that removes excess reagents and binds, immobilizes, and aligns molecules in place on a cartridge, so when it is moved to the Digital Analyzer, the probes can be counted and analyzed.

1. **Does the nCounter Pro need an external network connection to function?**

* **No. Use of the system does not require access to external networks.**
* The system is designed to use only local area networks (LANs) for communication.
* Laboratories that do not want to expose nCounter instruments to external-facing networks have the option of not networking the Digital Analyzer.
* Local networking of the Digital Analyzer is needed to upload CDF and RLF files via the network**.**
* Local networking of both the Prep Station and Digital Analyzer is needed to receive email notifications from the system.

**2. How is network traffic controlled on the nCounter Pro?**

* **Each instrument (Prep Station, Digital Analyzer) has network firewall software enabled to control incoming LAN-based network traffic.**
* The Windows 10 IoT firewall on nCounter instruments blocks all inbound traffic except the following, which the firewall treats as exceptions:

|  |  |  |  |
| --- | --- | --- | --- |
| **Instrument** | **Type** | **Description of Permitted Port** | **Port** |
| **Digital Analyzer** | Port | FTP | TCP 20, TCP 21 |
| Port | HTTPS | TCP 443 |
| Port | SQL Server Default Instance | TCP 1433 |
| Port | nCounter framework lock web service | TCP 8090 |
| Port | nCounter framework service Web app | TCP 4430 |
| Port | nCounter framework WCF service host | TCP 8525 |
| Port | nCounter framework secure file transfer | TCP 22 |
| Port | nCounter framework SQL server connection port | TCP 3306 |
| Port | nCounter Web app port (non-applicable for systems configured with only Life Sciences mode) | TCP 8080 |
| Service | File and Printer Sharing | TCP 139, TCP 445, UDP 137, UDP 138 |
| Service | UPnP framework (subnet scope) | TCP 2869, UDP 1900 |
| **Prep Station** | Service | File and Printer Sharing | TCP 139, TCP 445, UDP 137, UDP 138 |
| Service | UPnP framework (subnet scope) | TCP 2869, UDP 1900 |

* **No communication occurs between the Prep Station and Digital Analyzer when the system is run in Life Sciences mode.**

**3. Is any data communicated between the Prep Station and Digital Analyzer?**

* **No. The nCounter Pro does not support any type of wireless communications.** (WLAN and Bluetooth are not supported).

**4. Does the system support wireless connectivity?**

* Only LAN-based connectivity is supported.
* **Yes. Data stored on the nCounter Pro is encrypted to the AES-256 standard.**

**5. Is the data stored on the system encrypted?**

* Additionally, the hard drive is encrypted to the TPM 2.0 standard.
* Only LAN-based connectivity is supported.

**6. Does the system support cloud storage?**

* **No. The nCounter Pro does not utilize any cloud-based storage or retrieval of data.**
* All data generated by the system is stored locally.
* Customers must download data directly from the system or arrange to copy files from the system’s dedicated export directory to a network folder using SSH/SFTP.

**7. Are anti-virus and anti-malware tools included on the system?**

* **The nCounter Pro uses a more stringent form of data security than anti-virus and anti-malware.**
* Both systems use Windows Defender Application Control (WDAC), which allows **only** NanoString-approved operations and programs to run.
* This prevents all unauthorized executables, scripts, and code from running, providing robust protection from viruses and malware and protects the system from unauthorized software or manipulation from external sources.
* Because this effectively represents a closed environment, standard anti-virus products and anti-virus updates are not needed.

**8. How does NanoString protect the operating system used on the nCounter Pro?**

* **The software architecture of the system prevents all end-users from seeing or accessing the underlying Windows operating system.**
* The system uses a custom shell on both the Prep Station and Digital Analyzer to prevent customer end-users from accessing the Microsoft Windows 10 IoT operating system on the Digital Analyzer and Prep Station instruments.
* The nCounter software application that runs on the Prep Station and Digital Analyzer instruments is the graphical user interface and serve as the custom shell.
* When the Prep Station and Digital Analyzer instruments boot up, this custom shell prevents the user from accessing the Windows operating system.
* The custom shell “locks down” the operating system by altering the interactive logon procedure. For example, if a user attempts to enter CTRL+ALT+DELETE, they would discover that this keystroke combination is disabled.

**9. Does the nCounter Pro include an OS firewall?**

* **Yes. The Windows firewall on Prep Station and Digital Analyzer instruments is configured by NanoString to strictly limit the communication of Windows programs and services on each instrument.**
* All Windows programs and services are blocked from communicating unless they use a port specified as an exception in the firewall (see table under Question 2).

**11. How can I install the latest OS patches on my system?**

* **Since the nCounter Pro uses a custom shell and whitelisting to protect the system from unauthorized modifications, you will not be able to independently install OS patches or any third‑party applications**.
* Users should consult NanoString Technical Services ([support@nanostring.com](mailto:support@nanostring.com)) regarding OS patches for their system.
* **User logins are optional on systems but may be set to required depending on how it is configuration by the customer’s system administrator.**

**12. What type of user authentication is needed to use the system?**

* System administrators may configure their system to require logins, as desired.
* Once a system has been configured to require logins, user logins are necessary to operate instruments, view/download data, and access administrative or maintenance functionality.
* NanoString designed both the Prep Station and Digital Analyzer instruments so runs can be initiated only if the operator is standing in front of the instrument. Remote instrument operation is not supported.
* **Yes, a network security appliance can be used in conjunction with the nCounter Pro. The appliance would be installed between the nCounter Pro and the existing network per the schematic shown below:**

**13. Can I use a network security appliance with the systems?**



For the nCounter Pro to operate correctly in this configuration, the appliance would need to be configured with the following ports accessible:

|  |  |  |  |
| --- | --- | --- | --- |
| **Source** | **Type** | **Description of Permitted Port** | **Port** |
| **Inbound Traffic** | Port | FTP | TCP 20 |
| Port | SSH/SFTP | TCP 21 |
| Port | nCounter framework service Web app | TCP 4430 |
| **Outbound Traffic** | Port | Mail | TCP 25, TCP 587 |
| Port | DNS | TCP 53 |
| **Traffic on the NanoString Instrument Side** | See table in Section 2 above. | | |

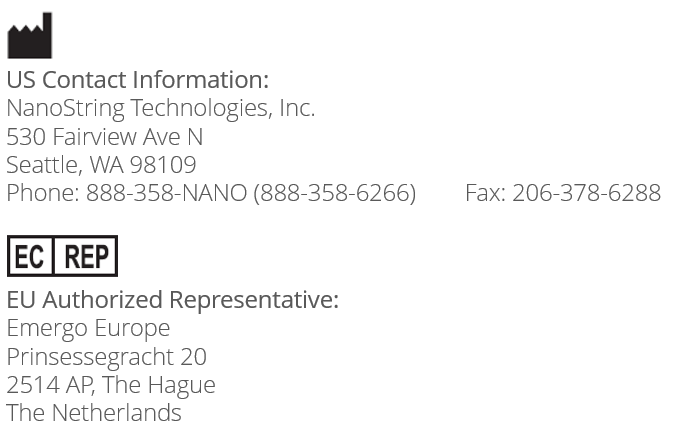
NOTE:

To ensure full functionality, it is recommended that a DNS entry be created that maps the system name, i.e., the serial number of the digital analyzer, to the IP address of the network security appliance.

**How can I get more information?**

* **Contact NanoString at Support@nanostring.com.**



© 2022 NanoString Technologies, Inc. All rights reserved. NanoString, NanoString Technologies, and nCounter are trademarks and/or registered trademarks of NanoString Technologies, Inc. in the United States and/or other countries.