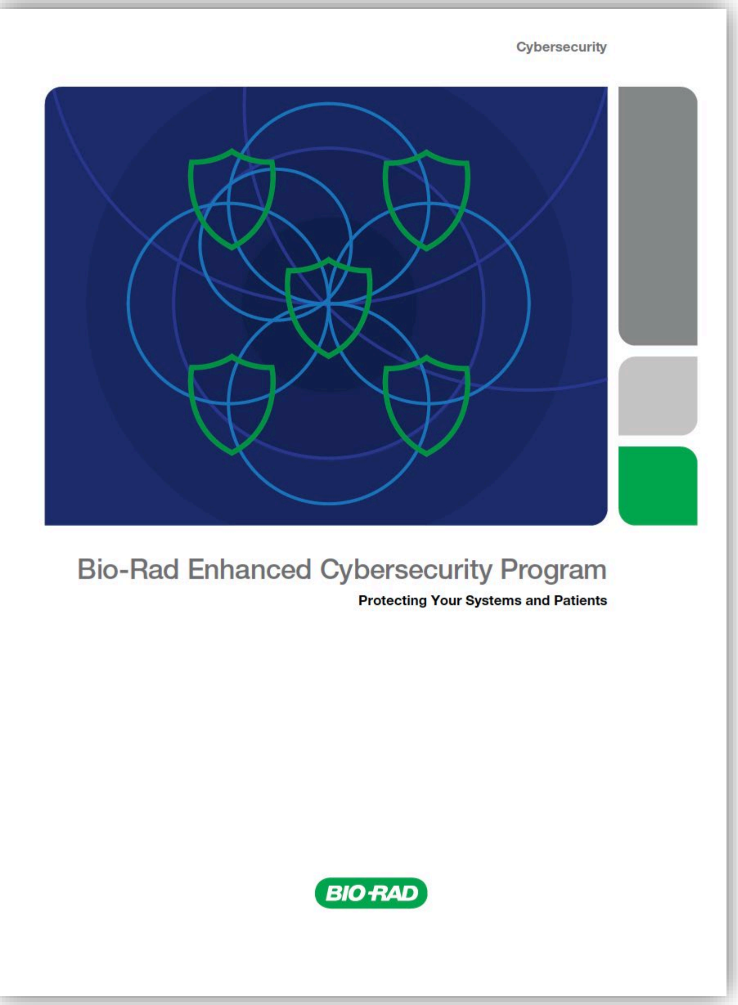
Bio-Rad ECP Publication Guide

December, 2020

Bio-Rad ECP Publication Guide



Cybersecurity

Bio-Rad Enhanced Cybersecurity Program

Protecting Your Systems and Patients

BIO-RAD

Publication Guide

Bio-Rad Enhanced Cybersecurity Program

REF: DG20-1296 Z-1014

For internal Use Only – Not for distribution

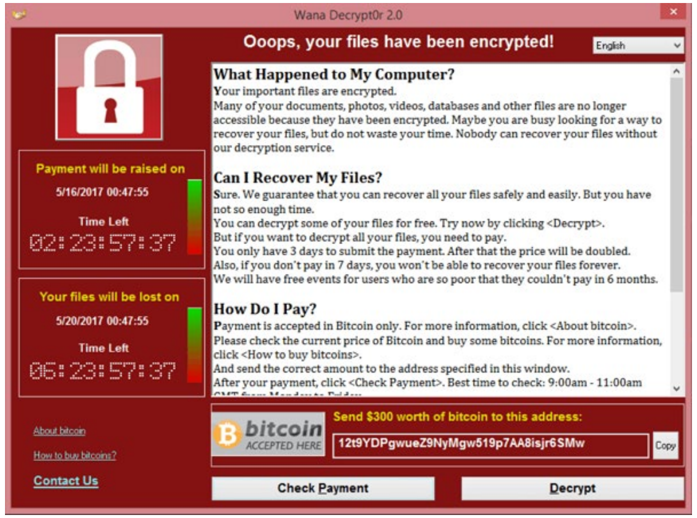
Use this publication to:

- Highlight the importance of cybersecurity in clinical diagnostics
- Discuss the cybersecurity solutions that Bio-Rad has implemented
- Demonstrate how Bio-Rad is protecting systems and patients
- Reassure the benefits of connectivity despite cybersecurity threats
- Support tender/RFP submissions

“Prevention is better than cure”

Global Costs $8 Billion

NHS (UK) – The WannaCry ransomware cyber attack in 2017 cost the National Health Service almost £100m and led to the cancellation of 19,000 appointments



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

“Prevention is better than cure”

- A cyber incident can have a financial impact
- Patient outcomes can be influenced by malicious attacks
- Preventing against cyber attacks allows critical services to be maintained
- Bio-Rad is implementing measures to protect services and patients

Inside left

2. Cybersecurity by Design

The Bio-Rad Cybersecurity Program has adopted a “Cybersecurity by Design” approach to ensure that security measures are being integrated into each stage of our product lifecycle management. We know that clinical diagnostic systems, routinely connected with hospital networks, other medical devices, and the internet, are fundamental in improving laboratory workflow and supporting better patient care.

With more connectivity there is an increasing vulnerability to cybersecurity breaches which can potentially disrupt the delivery of critical services. As a trusted manufacturer and supplier of medical devices and services, Bio-Rad is committed to working together with you and your lab to mitigate against potential cybersecurity risks.

FOCUS POINTS

- New product design / software updates now involves the introduction of features/functions related specifically to cybersecurity e.g. user level access, anonymisation of sensitive patient data, password complexity
- International standards have been introduced specific to information security management (ISO 27001) and cybersecurity protection methods (IEC 62443)
- The benefits of connectivity need to be protected
- This is not a one sided approach – it requires a hand in hand partnership for success

- THE FDA’S ROLE IN MEDICAL DEVICE CYBERSECURITY

An Enhanced Approach to Product Cybersecurity

Bio-Rad is committed to working with hospitals and laboratories to protect your systems and mitigate potential security risks to patients and operators

Digital threats, including viruses, malware, and malicious code can be a threat to the integrity of patient results, treatment, and privacy. As online attacks grow, it becomes more important than ever for Bio-Rad to proactively defend your systems. Bio-Rad’s approach to cybersecurity utilizes the latest thinking in diagnostic system defenses to create a digital barricade against online threats.

Cybersecurity by Design

The Bio-Rad Cybersecurity Program has adopted a “Cybersecurity by Design” approach to ensure that security measures are being integrated into each stage of our product lifecycle management. We know that clinical diagnostic systems, routinely connected with hospital networks, other medical devices, and the internet, are fundamental in improving laboratory workflow and supporting better patient care.

With more connectivity there is an increasing vulnerability to cybersecurity breaches which can potentially disrupt the delivery of critical services. As a trusted manufacturer and supplier of medical devices and services, Bio-Rad is committed to working together with you and your lab to mitigate against potential cybersecurity risks.

More than ever we need vigilance

The healthcare industry is a prime target for cybercriminals looking to exploit vulnerabilities in systems and devices. Sophisticated measures are being employed to prevent data breaches and malicious attacks. Rest assured, we’ve placed cybersecurity at the forefront of our efforts to maintain critical services and protect patients. Our Product Cybersecurity Center of Excellence helps manage and lead all aspects of the Cybersecurity Program.

1. Digital threats, including viruses, malware, and malicious code can be a threat to the integrity of patient results, treatment, and privacy. As online attacks grow, it becomes more important than ever for Bio-Rad to proactively defend your systems. Bio-Rad’s approach to cybersecurity utilizes the latest thinking in diagnostic system defenses to create a digital barricade against online threats.

FOCUS POINTS

- Cyber attacks are on the increase
- Bio-Rad is taking a proactive approach

3. More than ever we need vigilance

The healthcare industry is a prime target for cybercriminals looking to exploit vulnerabilities in systems and devices. Sophisticated measures are being employed to prevent data breaches and malicious attacks. Rest assured, we’ve placed cybersecurity at the forefront of our efforts to maintain critical services and protect patients. Our Product Cybersecurity Center of Excellence helps manage and lead all aspects of the Cybersecurity Program.

FOCUS POINTS

- Bio-Rad have firsthand experience in dealing with cybersecurity incidents
- Bio-Rad have established a team of experts (PCCoE) to coordinate a global approach against an evolving threat

Inside right (1)

1. Bio-Rad utilizes an interconnected approach to maximize the protection of your diagnostic systems

FOCUS POINTS

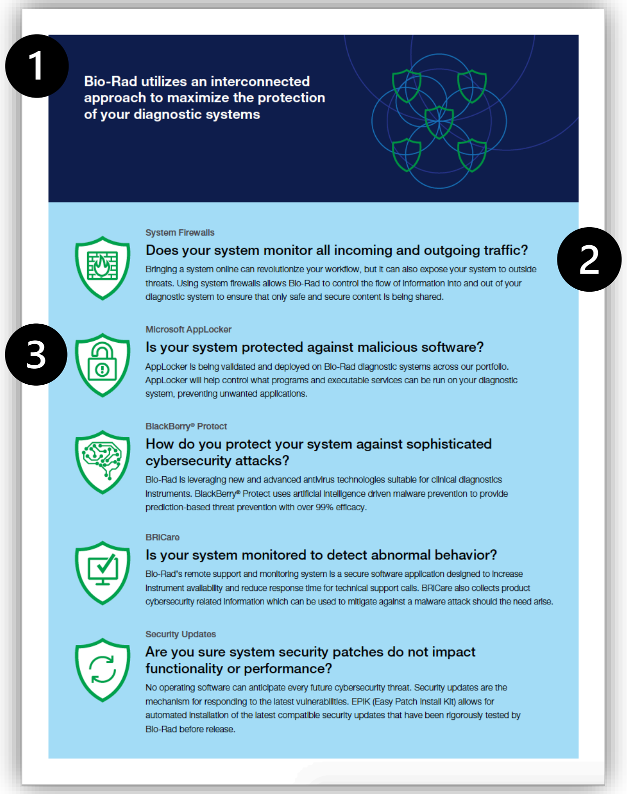
- There is not a single product which can be used to protect against all malicious threats
- The five shields are Bio-Rad’s interconnected defense working together to provide an enhanced approach

3. Microsoft AppLocker

Is your system protected against malicious software? AppLocker is being validated and deployed on Bio-Rad diagnostic systems across our portfolio. AppLocker will help control what programs and executable services can be run on your diagnostic system, preventing unwanted applications.

FOCUS POINTS

- AppLocker allows only the applications approved by Bio-Rad to be run on our systems
- If an application is not on a “whitelist” - it cannot be executed
- AppLocker is validated for use on Bio-Rad systems and is free of charge for our customers



Bio-Rad utilizes an interconnected approach to maximize the protection of your diagnostic systems

System Firewalls

Does your system monitor all incoming and outgoing traffic?

Bringing a system online can revolutionize your workflow, but it can also expose your system to outside threats. Using system firewalls allows Bio-Rad to control the flow of information into and out of your diagnostic system to ensure that only safe and secure content is being shared.

Microsoft AppLocker

Is your system protected against malicious software?

AppLocker is being validated and deployed on Bio-Rad diagnostic systems across our portfolio. AppLocker will help control what programs and executable services can be run on your diagnostic system, preventing unwanted applications.

BlackBerry® Protect

How do you protect your system against sophisticated cybersecurity attacks?

Bio-Rad is leveraging new and advanced antivirus technologies suitable for clinical diagnostics instruments. BlackBerry® Protect uses artificial intelligence driven malware prevention to provide prediction-based threat prevention with over 99% efficacy.

BRiCare

Is your system monitored to detect abnormal behavior?

Bio-Rad’s remote support and monitoring system is a secure software application designed to increase instrument availability and reduce response time for technical support calls. BRiCare also collects product cybersecurity related information which can be used to mitigate against a malware attack should the need arise.

Security Updates

Are you sure system security patches do not impact functionality or performance?

No operating software can anticipate every future cybersecurity threat. Security updates are the mechanism for responding to the latest vulnerabilities. EPIK (Easy Patch Install Kit) allows for automated installation of the latest compatible security updates that have been rigorously tested by Bio-Rad before release.

2. System Firewalls

Does your system monitor all incoming and outgoing traffic? Bringing a system online can revolutionize your workflow, but it can also expose your system to outside threats. Using system firewalls allows Bio-Rad to control the flow of information into and out of your diagnostic system to ensure that only safe and secure content is being shared.

FOCUS POINTS

- Firewalls are the first shield – rules are configured by Bio-Rad during manufacturing to ensure the safe operation of systems when they are connected to the laboratory network

Inside right (2)

4. BlackBerry® Protect

How do you protect your system against sophisticated cybersecurity attacks?

Bio-Rad is leveraging new and advanced antivirus technologies suitable for clinical diagnostics instruments. BlackBerry® Protect uses artificial intelligence driven malware prevention to provide prediction-based threat prevention with over 99% efficacy.

FOCUS POINTS

- BlackBerry® Protect is an **optional** anti-malware solution
- BlackBerry® Protect is a licensed (invoiced) product
- It is validated for use with Bio-Rad Systems
- No other third party anti-malware is approved for use on Bio-Rad systems
- It does not require an internet connection to function
- BlackBerry® Protect allows the routine processing of patient samples without impacting system performance

- Bio-Rad Premium Cybersecurity Offering
- Secure IoT in Healthcare

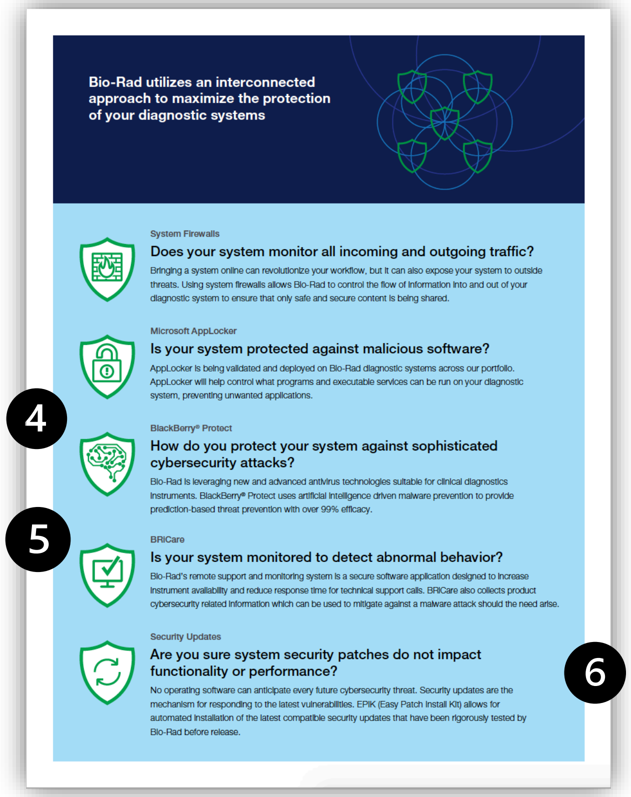
5. BRiCare

Is your system monitored to detect abnormal behavior?

Bio-Rad's remote support and monitoring system is a secure software application designed to increase instrument availability and reduce response time for technical support calls. BRiCare also collects product cybersecurity related information which can be used to mitigate against a malware attack should the need arise.

FOCUS POINTS

- BRiCare functionality has been extended to collect data related to cybersecurity e.g. latest security updates installed
- Patient data is not collected
- In case of a cybersecurity incident, BRiCare could be used to help recover the system to operation
- BRiCare is secure and free of charge for Bio-Rad customers



Bio-Rad utilizes an interconnected approach to maximize the protection of your diagnostic systems

System Firewalls

Does your system monitor all incoming and outgoing traffic?

Bringing a system online can revolutionize your workflow, but it can also expose your system to outside threats. Using system firewalls allows Bio-Rad to control the flow of information into and out of your diagnostic system to ensure that only safe and secure content is being shared.

Microsoft AppLocker

Is your system protected against malicious software?

AppLocker is being validated and deployed on Bio-Rad diagnostic systems across our portfolio. AppLocker will help control what programs and executable services can be run on your diagnostic system, preventing unwanted applications.

BlackBerry® Protect

How do you protect your system against sophisticated cybersecurity attacks?

Bio-Rad is leveraging new and advanced antivirus technologies suitable for clinical diagnostics instruments. BlackBerry® Protect uses artificial intelligence driven malware prevention to provide prediction-based threat prevention with over 99% efficacy.

BRiCare

Is your system monitored to detect abnormal behavior?

Bio-Rad's remote support and monitoring system is a secure software application designed to increase instrument availability and reduce response time for technical support calls. BRiCare also collects product cybersecurity related information which can be used to mitigate against a malware attack should the need arise.

Security Updates

Are you sure system security patches do not impact functionality or performance?

No operating software can anticipate every future cybersecurity threat. Security updates are the mechanism for responding to the latest vulnerabilities. EPIK (Easy Patch Install Kit) allows for automated installation of the latest compatible security updates that have been rigorously tested by Bio-Rad before release.

6. Security Updates

Are you sure system security patches do not impact functionality or performance?

No operating software can anticipate every future cybersecurity threat. Security updates are the mechanism for responding to the latest vulnerabilities. EPIK (Easy Patch Install Kit) allows for automated installation of the latest compatible security updates that have been rigorously tested by Bio-Rad before release.

FOCUS POINTS

- Bio-Rad does not recommend automatic updates to be enabled
- Operating System updates can affect instrument functionality and performance
- By validating security updates before release, Bio-Rad can ensure that instrument operation is not negatively impacted after installation
- EPIK is a tool developed by the Bio-Rad PCCoE that automates the process of Microsoft security updates relevant for Bio-Rad systems

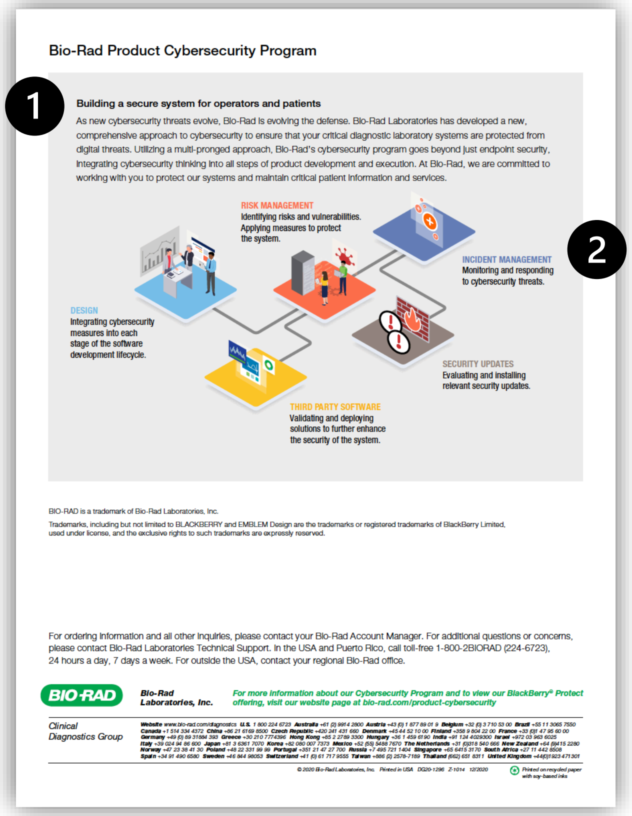
Reverse

1. Building a secure system for operators and patients

As new cybersecurity threats evolve, Bio-Rad is evolving the defense. Bio-Rad Laboratories has developed a new, comprehensive approach to cybersecurity to ensure that your critical diagnostic laboratory systems are protected from digital threats. Utilizing a multi-pronged approach, Bio-Rad's cybersecurity program goes beyond just endpoint security, integrating cybersecurity thinking into all steps of product development and execution. At Bio-Rad, we are committed to
working with you to protect our systems and maintain critical patient information and services.

FOCUS POINTS

- Cybersecurity thinking – this is a dynamic and changing threat which requires the matching of best practices and products
- Bio-Rad is innovating not only in providing the best products for clinical laboratories but also in protecting these critical services
- This is and will remain a partnership with our customers against a common threat.



Bio-Rad Product Cybersecurity Program

1

Building a secure system for operators and patients

As new cybersecurity threats evolve, Bio-Rad is evolving the defense. Bio-Rad Laboratories has developed a new, comprehensive approach to cybersecurity to ensure that your critical diagnostic laboratory systems are protected from digital threats. Utilizing a multi-pronged approach, Bio-Rad's cybersecurity program goes beyond just endpoint security, integrating cybersecurity thinking into all steps of product development and execution. At Bio-Rad, we are committed to working with you to protect our systems and maintain critical patient information and services.

2

RISK MANAGEMENT
Identifying risks and vulnerabilities. Applying measures to protect the system.

INCIDENT MANAGEMENT
Monitoring and responding to cybersecurity threats.

DESIGN
Integrating cybersecurity measures into each stage of the software development lifecycle.

SECURITY UPDATES
Evaluating and installing relevant security updates.

THIRD PARTY SOFTWARE
Validating and deploying solutions to further enhance the security of the system.

BIO-RAD is a trademark of Bio-Rad Laboratories, Inc.

Trademarks, including but not limited to BLACKBERRY and EMBLEM Design are the trademarks or registered trademarks of BlackBerry Limited, used under license, and the exclusive rights to such trademarks are expressly reserved.

For ordering information and all other inquiries, please contact your Bio-Rad Account Manager. For additional questions or concerns, please contact Bio-Rad Laboratories Technical Support. In the USA and Puerto Rico, call toll-free 1-800-2BIORAD (224-6723), 24 hours a day, 7 days a week. For outside the USA, contact your regional Bio-Rad office.

Bio-Rad Laboratories, Inc.

For more information about our Cybersecurity Program and to view our BlackBerry® Protect offering, visit our website page at bio-rad.com/product-cybersecurity

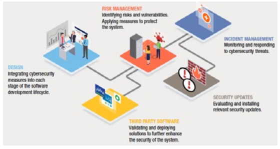
Clinical Diagnostics Group

Website www.bio-rad.com/diagnostics **U.S.** 1 800 224 6723 **Australia** +61 (2) 9914 2800 **Austria** +43 (0) 1 877 89 01 9 **Belgium** +32 (0) 3 710 53 00 **Brazil** +55 11 3065 7550 **Canada** +1 514 334 4372 **China** +86 21 6169 8500 **Czech Republic** +420 241 431 660 **Denmark** +45 44 52 10 00 **Finland** +358 9 804 22 00 **France** +33 (0)1 47 95 60 00 **Germany** +49 (0) 89 31884 393 **Greece** +30 210 7774396 **Hong Kong** +85 2 2789 3300 **Hungary** +36 1 459 6190 **India** +91 124 4029300 **Israel** +972 03 963 6025 **Italy** +39 024 94 86 600 **Japan** +81 3 6361 7070 **Korea** +82 080 007 7373 **Mexico** +52 (55) 5488 7670 **The Netherlands** +31 (0)318 540 666 **New Zealand** +64 (9)415 2280 **Norway** +47 23 38 41 30 **Poland** +48 22 331 99 99 **Portugal** +351 21 47 27 700 **Russia** +7 495 721 1404 **Singapore** +65 6415 3170 **South Africa** +27 11 442 8508 **Spain** +34 91 490 6580 **Sweden** +46 844 98053 **Switzerland** +41 (0) 61 717 9555 **Taiwan** +886 (2) 2578-7189 **Thailand** (662) 651 8311 **United Kingdom** +44(0)1923 471301

© 2020 Bio-Rad Laboratories, Inc. Printed in USA DG20-1296 Z-1014 12/2020

Printed on recycled paper with soy-based inks

2. Infographic



FOCUS POINTS

- Represents the pillars of Bio-Rad's Cybersecurity Program
- These are based upon recommendations and regulations for manufacturers of medical devices
- The shields are the defense in the battle, the program is the strategy in the war against Cybersecurity threats

- Product Cybersecurity Position Paper