### $\texttt{FFBlackBerry}_{\bullet} \mid \Box \land \Box \Box \Box \Box \bullet$

# What's New in CylancePROTECT® and CylanceOPTICS®

February 2020 Release

SOLUTION BRIEF

### What's New in CylancePROTECT

BlackBerry Cylance's February 2020 release includes a modernization of the user interface (UI), an expansion of role-based access controls (RBAC), and the release of the single agent.

#### **UI Modernization**

Driven by customer demand, CylancePROTECT includes an updated look and feel for the UI. These updates include new colors, fonts, an updated login page, and a new leftside navigation bar.



8	Threat Prot	ection					
	Threats Scrip	t Control	External	Device:			
€	* Threat Filters		0				
t <sub>o</sub> r	Priority: Unsafe		Dri	ag a colun	nn header here to gro	oup by that colu	imn.
Q	High	0		ICON	NAME		PRIORITY
-	Medium	0				V	•
0	Low	16			davin6331d1de.e Search Google   Cher	xe k VirusTotal	Low
44	Status: Last 24 H	lours					
	Ouaraptiped	0			davin1ecc0d2b.ex Search Google   Ches	ke k VirusTotal	Low



#### **Role-Based Access Controls (RBAC)**

RBAC is an approach to restricting system access based on the roles of individual users within an enterprise. RBAC enables restriction of access rights to the information needed for product administrators/users to do their jobs and prevents them from accessing information that doesn't pertain to them. BlackBerry Cylance has made significant strides in the CylancePROTECT RBAC capabilities.

Go to the Navigation toolbar on the left side of the page and select the Settings gear icon.

ЦŞI	Setting	5					
80	Application	User Management	Device Policy	Global List	Update	Certificates	Integ
3		Company: _	Uloh				
to		Installation Token:					
모		Installer:	LINES OF DIVERSION COMP. IN	ote: Arter taking the acti	IN, the current toker	s wa no longer be valo.	
0		CylancePROTECT:	🗱 Windows 🔹 🤹	macOS 🔹 🛕 Lin	- ×		
let.		CylanceOPTICS:	🗃 Windows 🧯 ma	eus •			

Then, go to the toolbar across the top of the page and select User Management.

8	Settings					
	Application	User Management	Device Policy	Global List	Update	Certificates
3 1 1	Users Rol	es				
E @ 1	Cick Cick • A	t User Permissions con a user's name to edit perm idministrator • Zone Mar	nissions. Hover over each nager • <u>User</u> •	role to view permissio Read-only • C	ons. Custom	

To add a new role, select Roles.

NMM +         VENESOS         Voltages +           V         V         V         V         V           King howana         East Reagener         10-2019         V					4 800 NEW ROLE
Not-         Parallolini         Parallolini         Parallolini           Interpretation         Unit Recognized         11/30/31           Interpretation         Unit Recognized         11/30/31           Interpretation         Enterpretation         11/30/31           Interpretation         Enterpre					
Image: set of the second		MODIFIED *		PERMISSIONS	NAME &
Nat Ngen Neumann         Line Neugement         11:52/13           Ng and 13         Pear an Wall         Pear an Wall         11:42/13           One of 13         Line Neugement         11:52/13         11:52/13           Pear and 13         Deals Pelag         Pear Announce         11:52/13           Pears, No Deals         Deals Pelag         Pear Announce         11:52/13           Pears, No Deals         Odd 11:51, None Neutrition         11:52/13         11:52/13           Pears, Pears, No Deals         Odd 11:51, None Neutrition, Neutrition	11 V		T		
Not 01/3         Note Names, Jone         014809           Line Ngr.         Line Nagement         013009           Trans, Name         Dear Anligo, Name Annotes, Jone         013009           Trans, Name         Dear Anligo, Trans, March Institution         013009           Trans, Name, Data in Lorenza         Dear Anligo, Trans, March Institution         013009           Trans, Name, Data in Lorenza         Dear Anligo, Trans, Transmiss, Angeleine, Schwart, Jone         013009           Transmission         Schwart Hamiltonic Contract, Line in Anternature, Supramor, Supra		11/18/2019		User Management	Rule Mgnt Permann
Note Nations, No Jowe         Decess Mails Queens, Thread Pressions         1132019           These, Share, No Jowe         Decess Mails Queens, Thread Pressions         1132019           These, Share, Share (Share) (Share)         Share) (Share)         1132019           These, Share, Share (Share) (Share)         Share)         Share)           Rest and advances tool         Share)         Share)           Rest and advances tool         Share)         Share)           Waregement (Statement - Share)         Share)         Share)           Manual Advances tool         Share)         Share)         Share)		11/14/2019		Trougt Protection, Zones	My test role 123
Natur, Natur, Na Juni         Data Pulay, Sear, Bruer, Marchinekton         113/2019           Natur, Natur, Kaler, Kar, Kaler, Kal		11/14/2019		User Management	User Mgr
New, Store, Data (as or beam         Gink (as, how, how, box         113209           Protect codescent for         Applications (come howership), applications (come howers		11/13/2019		Device Pulicy, Devices, Threat Protection	Threads, Devices, No Zones
splanar Control American April 2014 (2014) Marganese April 2014 (2014) Tread-multimetric approximation (2014) Applanese Approximation (2014) Present Handling Dense, Dath List, Sheat Privation, Sam Marganese Anny Marganese Anny		11/13/2019		Global List, Threat Protection, Jones	Threads, Jones, Global Lin, not Devices
		11/13/2016	stafation Token sation - Invitation URL, R. Application - Univital III, Thread Protection, User	Application - Custom Authentication, Application Management, Application - Installer Download, A Application - Support Lagin, Application - Spring Pateoneri Management, Audit Log, Dentes, Got Management, Zones	Press and benefit test
Device, Joint, no Twents or gold fait Device, Zones 10/13/2019		11/13/2019		Devices, Zones	Devices, Dones, no Torests or global list
Threats, Zones, Descen Descen, Threat-Protection, Zones 11/0/2019		11/1/2010		Devices, Threat Protection, Zones	Presets, Zarres, Devenue
Application - Syring/SDM, Aude Log, Certificates, CylanceCPTICS, Device Paley,			anceOPTICS, Device Palicy,	Application - Sysleg/SIDM, Audit Log. Certificates.	

The easy-to-use Add New Role template allows administrators to give a new employee page access and settings access. The example below illustrates how to add a new role with full access. Full access would include Page Access to:

- 1. Threat Protection
- 2. Zones
- 3. Devices
- 4. CylanceOPTICS
- 5. Reports
- 6. Audit Logs

In the Settings Access section on the right-hand side of the page, select the functions the employee will be allowed to use:

- 1. Application
- 2. User Management
- 3. Device Policy
- 4. Global List
- 5. Update
- 6. Certificate
- 7. Integrations

Role Name	Full Access Example						
	236 characters remaining						
Page Access		Allow	Settings Access	Allow			
Threat Protection		~	Application				
Zones		<b>~</b>	Installation Token Management	~			
Devices		<b>~</b>	Installer Download	~			
CylanceOPTICS		<ul> <li>Image: A set of the set of the</li></ul>	Invitation URL	<b>~</b>			
Reports		<ul> <li>Image: A set of the set of the</li></ul>	Uninstall Password Management	~			
Audit Log		<b>~</b>	Support Login	<b>~</b>			
			Syslog/SIEM	<b>~</b>			
			Custom Authentication	~			
			User Management	<b>~</b>			
			Device Policy	<b>~</b>			
			Global List				
			Update	~			
			Certificates	<b>~</b>			
			Integrations				

RBAC allows administrators to quickly add a new role and limit access to what employees need to access to do their jobs. The example below illustrates the hiring of a new CylanceOPTICS administrator. Go to Add New Role and only allow that employee to access CylanceOPTICS.

Role Name	Optics Only Example			
	236 characters remaining			
Page Access		Allow	Settings Access	Allow
Threat Protection			Application	
Zones			User Management	
Devices			Device Policy	
CylanceOPTICS		<ul> <li>Image: A set of the set of the</li></ul>	Global List	
Reports			Update	
Audit Log			Certificates	
			Integrations	

#### **The Single Agent**

The February 2020 release also includes the unified agent that brings together a single agent and a single installer that is all managed in a single pane for both CylancePROTECT and CylanceOPTICS.

### What's New in CylanceOPTICS

CylanceOPTICS is an endpoint detection and response (EDR) solution that extends the threat prevention delivered by CylancePROTECT by using artificial intelligence (AI) to identify and prevent security incidents. CylanceOPTICS provides true AI incident prevention, root cause analysis, smart threat hunting, and automated detection and response capabilities.

CylanceOPTICS offers:

- AI-driven incident prevention
- Machine-learning-assisted threat detection
- On-demand root cause analysis
- Smart threat hunting
- Remote investigation capabilities

#### CylanceOPTICS 2.4

The 2.4 release of CylanceOPTICS offers several enhancements to the InstaQuery, FocusView, and Context Analysis Engine (CAE) to provide greater visibility capabilities. These enhancement vectors include:

- Registry introspection enhancements
- DNS visibility
- Windows<sup>®</sup> logon event visibility
- RFC 1918 address space visibility
- Enhanced WMI introspection via Windows API
- Enhanced PowerShell introspection via Windows API

The 2.4 release of CylanceOPTICS brings several product enhancements to aid in both the breadth and depth of EDR search parameters. These enhancements are built on a foundation of AI and ML protection. Locally stored intelligence offers real-time confidence to investigate, triage, and remediate when a CAE rule trigger occurs. This gives EDR practitioners the ability to search and remediate at the speed of the threat landscape, and not be delayed by cloud query, protracted forensic analysis, and other time-wasting processes. The EDR team can understand all the artifacts that have occurred before and after the triggering event.

The results are:

- Increased search parameter flexibility within InstaQuery, FocusView, and CAE rules
- Faster incident response
- Alignment with the MITRE ATT&CK framework
- Expanded automated response via CAE rules

Identifying a potential security issue in any environment is important, however, to protect from the fallout of a widespread incident, businesses need the ability and agility to investigate and respond to an attack with speed and certainty. With CylanceOPTICS 2.4, businesses get several new product enhancements to accelerate incident investigation and response options that enable them to gather relevant information about an incident and act fast, either in automated or manual fashion.

### CylanceOPTICS 2.4 Feature/Benefit Matrix

Registry Introspection Enhancements — Provides increased visibility into common Windows Registry persistence points, including manage operating systems and processes) via Focus View, InstaQuery, or CAE detection logic.Enables the endpoint agent to sense, analyze, and processes) via Focus View, InstaQuery, or CAE detection logic.DNS fueltility — Enables the endpoint agent to sense and record what has instigated a DNS query, by which IP address and domain it was initiated, and artifacts of the initiation via Focus View, InstaQuery, or CAEGives standard names to latereation logic.Windows Logon Event Visibility — Enables the endpoint agent to sense and record what has instigated ad Windows Logon event, the user that logged on, by which IP address and ommor insex, roque DNS servers, DNS-based data exfiltration, and connections focus View, InstaQuery, or CAEWindows Logon Event Visibility — Enables the endpoint agent to sense and record what has instigated ad Windows Logon event, the user that logged on, by which IP address and of mean initiated, and artifacts of the initiation via Focus View, InstaQuery, or CAE detection logic.Enables monitoring of a specific user if they access multiple systems and is hase instigated ad Windows Logon event, the user that logged on year visibility to beserve when to beserve when and it seases, analyze, and record an and through the network.Private Address (RFC 1918 / To sense, analyze, and record an avent originating from a private internet address on a private internet address on a to sense, analyze, and record an went origination event via beserve, network via Focus View, InstaQuery, or CAE detection logic.Seful in monitoring for fileless attacks s	Feature	Benefit
DNS Visibility — Enables the endpoint agent to sense and record what has instigated a DNS query, by which IP address and domain it was initiated, and artifacts of the initiation via Focus View, InstaQuery, or CAEGives standard names to internet connections (if available). Providing visibility into DNS cache compromises, rogue DNS servers, DNS-based data exfiltration, and connections to web addresses rather than just IP addresses.Windows Logon Event Visibility — Enables the endpoint agent to sense and record what has instigated a Windows Logon event, the user that logged oon, by which IP address and domain it was initiated, when it was initiated, and artifacts of the initiation via Focus View, InstaQuery, or CAE detection logic.Enables monitoring of a specific user if they access multiple systems and is helpful in detecting and metrast. Further, provides visibility to observe where the attacker went and did when moving laterally through the network.Private Address (RFC 1918 / RFC 4193) Space Visibility — Enables the endpoint agent to sense, analyze, and record a nevent originating from a private internet address on a TCP/IP network via Focus View, InstaQuery, or CAE detection logic.Extremely valuable when looking for lateral movement attacks. Previous versions could only view movement through a private network space.Enhanced WMI Introspection — Instrumentation event via Focus View, InstaQuery, or CAE detection logic.Sieves powerful granular insight into what scripts are launched and what insight into what scripts are launched and what sense, analyze, and record a PowerShell Introspection — Enables the endpoint agent to sense, analyze, and record a PowerShell levent (commonly u	Registry Introspection Enhancements — Provides increased visibility into common Windows Registry persistence points, including memory attacks via Focus View, InstaQuery, or CAE detection logic.	Enables the endpoint agent to sense, analyze, and record a PowerShell event (commonly used to rapidly automate tasks that manage operating systems and processes) via Focus View, InstaQuery, or CAE detection logic.
Windows Logon Event Visibility — Enables the endpoint agent to sense and record what has instigated a Windows Logon event, the user that logged on, by which IP address and domain it was initiated, when it was initiated, and artifacts of the initiation via Focus View, InstaQuery, or CAE detection logic.Enables monitoring of a specific user if they access multiple systems and is helpful in detecting and mitigating potential insider threats. Further, provides visibility to observe where the attacker went and did when moving laterally through the network.Private Address (RFC 1918 / RFC 4193) Space Visibility — Enables the endpoint agent to sense, analyze, and record an event originating from a private internet address on a TCP/IP network via Focus View, InstaQuery, or CAE detection logic.Extremely valuable when looking for lateral movement attacks. Previous versions could only view movement through a private network space.Enhanced WMI Introspection — Enables the endpoint agent to sense, analyze, and record a MS Windows Management Instrumentation event via Focus View, InstaQuery, or CAE detection logic.Useful in monitoring for fileless attacks and lateral movement, living-off-the- land attacks, etc.Enhanced PowerShell werShell event (commonly used to rapidly automate tasks that manage operating systems and processes) via Focus View, 	DNS Visibility — Enables the endpoint agent to sense and record what has instigated a DNS query, by which IP address and domain it was initiated, when it was initiated, and artifacts of the initiation via Focus View, InstaQuery, or CAE detection logic.	Gives standard names to Internet connections (if available). Providing visibility into DNS cache compromises, rogue DNS servers, DNS-based data exfiltration, and connections to web addresses rather than just IP addresses.
Private Address (RFC 1918 / RFC 4193) Space Visibility — Enables the endpoint agent to sense, analyze, and record an event originating from a private internet address on a TCP/IP network via Focus View, InstaQuery, or CAE detection logic.Extremely valuable when looking for lateral movement attacks. Previous versions could only view movement through a private network space.Enhanced WMI Introspection — Enables the endpoint agent to sense, analyze, and record a MS Windows Management Instrumentation event via Focus View, InstaQuery, or CAEUseful in monitoring for fileless attacks and lateral movement, living-off-the- land attacks, etc.Enhanced PowerShell Introspection — Enables the endpoint agent to sense, analyze, and record a PowerShell event (commonly used to rapidly automate tasks that manage operating systems and processes) via Focus View, InstaQuery, or CAE detection logic.Gives powerful granular individual commands were executed out of those scripts. This is useful in monitoring for fileless attacks, lateral movement, living-off-the-land attacks, etc.	Windows Logon Event Visibility — Enables the endpoint agent to sense and record what has instigated a Windows Logon event, the user that logged on, by which IP address and domain it was initiated, when it was initiated, and artifacts of the initiation via Focus View, InstaQuery, or CAE detection logic.	Enables monitoring of a specific user if they access multiple systems and is helpful in detecting and mitigating potential insider threats. Further, provides visibility to observe where the attacker went and did when moving laterally through the network.
Enhanced WMI Introspection — Enables the endpoint agent to sense, analyze, and record a MS Windows Management Instrumentation event via Focus View, InstaQuery, or CAEUseful in monitoring for fileless attacks and lateral movement, living-off-the- land attacks, etc.Enhanced PowerShell Introspection — Enables the endpoint agent to sense, analyze, and record a PowerShell event (commonly used to rapidly automate tasks that manage operating systems and processes) via Focus View, InstaQuery, or CAE detectionGives powerful granular individual commands were executed out of those scripts. This is useful in monitoring for fileless attacks, lateral movement, living-off-the-land attacks, etc.	Private Address (RFC 1918 / RFC 4193) Space Visibility — Enables the endpoint agent to sense, analyze, and record an event originating from a private internet address on a TCP/IP network via Focus View, InstaQuery, or CAE detection logic.	Extremely valuable when looking for lateral movement attacks. Previous versions could only view movement through a private network space.
Enhanced PowerShellGives powerful granularIntrospection — Enablesinsight into what scriptsthe endpoint agent toare launched and whatsense, analyze, and record aindividual commands werePowerShell event (commonlyexecuted out of thoseused to rapidly automate tasksscripts. This is useful inthat manage operating systemsmonitoring for filelessand processes) via Focus View,attacks, lateral movement,InstaQuery, or CAE detectionliving-off-the-land attacks,logic.etc.	Enhanced WMI Introspection — Enables the endpoint agent to sense, analyze, and record a MS Windows Management Instrumentation event via Focus View, InstaQuery, or CAE detection logic.	Useful in monitoring for fileless attacks and lateral movement, living-off-the- land attacks, etc.
	Enhanced PowerShell Introspection — Enables the endpoint agent to sense, analyze, and record a PowerShell event (commonly used to rapidly automate tasks that manage operating systems and processes) via Focus View, InstaQuery, or CAE detection logic.	Gives powerful granular insight into what scripts are launched and what individual commands were executed out of those scripts. This is useful in monitoring for fileless attacks, lateral movement, living-off-the-land attacks, etc.

## What's Forthcoming in CylanceOPTICS?

#### CylanceOPTICS for Linux

CylanceOPTICS will introduce enhanced functionality optimized for several popular Linux<sup>\*</sup> operating system versions Including RHEL, Ubuntu, CentOS, and SUSE. With this entry into the Linux computing environment, CylanceOPTICS has extended the reach of AI-based EDR technology to cover a broader set of threats in both data centers and industrial environments.

### CylanceOPTICS for Linux Feature/Benefit Matrix

Feature	Benefit
Feature Parity with Windows and Mac	Employ superior EDR across the entire environment
Driverless	No kernel level dependencies for enhanced security
CAE Rules for Linux	Automatedly detect malicious events on Linux-based machines
Refract for Linux	Automatedly remediate malicious events on Linux- based machines
Device Lockdown	Isolate infected Linux-based endpoints to stop malware infections

#### **Typical Use Cases**

Examples of this extended footprint include servers, point of sale (POS), automated teller machine (ATM) terminals, and Linux-based fixed-function devices. Use cases for each of these are described below.

#### **Linux Servers**

In enterprise data centers utilizing X86-based servers, Linux is a widely utilized operating system for both baremetal machines and virtual machines within hypervisors. This growth is being further accelerated by the movement within data centers to containers. While endpoints are often the initial target of malware attacks, the primary target is the data on the servers, whether in financial services, e-commerce, or other enterprise applications. There is a mindset within the IT community that if the operating system isn't Windows, malware is not a meaningful threat. An article by Alex Campbell in *PCWorld* dispels this notion and highlights the risks that malware poses for Linux-based systems<sup>1</sup>. Web servers running Linux are a particular target, given their direct presence on the Internet. Mumblehard is one example of a malware package that has been used to target Linux-based web servers. Ransomware such as KillDisk has been used to attack Linux-based servers and systems. Rootkits are also a significant concern, as their installation can provide full access to a Linux server and all of the storage to which the server has access.

#### **POS/ATM Terminals**

Like many embedded systems, POS and ATM terminals generally utilize the Linux operating system. The attractiveness of these devices as malware targets would seem obvious, yet these systems (particularly POS terminals) have often not had robust protection against cyber attacks. Because of this, POS and ATM terminals have been used as conduits for attacks against both retail and financial services companies, resulting in the compromise of identity data for millions of consumers and significant liability events for the organizations. An article in CSO Online described how POS malware attacks are becoming more aggressive. The actual theft of customer data is usually the final act of an attack that has been built up over the years and often starts with the infiltration of the POS system by malware. New attacks are also targeting POS terminals at smaller retailers, which often do not

have the SEIM tools utilized by large enterprises. Similar attacks are occurring against ATM machines (known as jackpotting) in a variety of geographies; a malware package known as Ploutus-D is just the latest example of these malware-based attacks on ATMs. The best strategy to stop these attacks is to understand the likely vulnerabilities of POS and ATM systems and ensure that malware doesn't use these vulnerabilities to penetrate these systems.

#### **Fixed-Function Devices**

PC-based fixed-function devices are growing exponentially, with use cases as diverse as industrial automation systems, Internet of things (IoT) devices, medical equipment, facility management systems, and vending machines. These devices, which are often mission-critical assets in industries such as healthcare, manufacturing, utilities, and gaming, overwhelmingly run the Linux operating system. Fixed-function devices have historically been easy targets for cyber criminals to attack and penetrate, as they may not receive updated patches on a regular basis, and their default credentials are often not modified after these devices are installed. These vulnerabilities have been demonstrated in a DDOS attack which utilized Merai botnets executing on unprotected IoT devices. Preventing malware from being installed on these devices would have mitigated this attack.



#### **Partial Device Lockdown**

Identifying a potential security issue in any environment is important, however, enterprises need to balance data and systems availability with the ability to respond to an attack. With CylanceOPTICS, businesses will get several built-in incident investigation and response options that enable fast remediation of an incident, either in automated or manual fashion, while maximizing user connectivity and uptime. Flexibility is of critical importance when taking action against a threat. CylanceOPTICS will offer the choice of either full lockdown or partial lockdown to suit the needs of the remediation team.

#### **Selective Device Communication**

Partial device lockdown for CylanceOPTICS will allow users to quickly and easily limit a host's network connections to a set of trusted IP addresses or subnets. Partial device lockdown will allow the CylancePROTECT and CylanceOPTICS agents to communicate with BlackBerry Cylance's cloud services by default. By maintaining communication between BlackBerry Cylance's cloud services and endpoint agents, users can continue to use the products to their full potential. For example, a device's policy configuration can be changed to force a more strict set of controls from CylancePROTECT, or a user can initiate an InstaQuery or Focus View to interrogate a device and conduct an in-depth analysis without needing to worry about an infection spreading to other systems or an attacker moving laterally to other systems of interest. When an investigation has concluded or a threat has been eradicated, users can also issue an unlock command directly from BlackBerry Cylance's cloud services to restore previously configured network permissions.

#### **Lockdown Exceptions**

When initiating a partial device lockdown, users will also be able to provide a list of IP addresses and subnets (internal RFC1918 addresses as well as publicly accessible external addresses) that they wish to allow communications to and from. These lockdown exceptions allow users to continue to utilize other tools in their environment to manage their endpoints, conduct additional remediation steps, or introduce new configurations to impacted systems. For example, the IP address of an IT administrator's system could be added as an exception to allow that administrator to remotely log in to the locked down system to conduct actions. Similarly, an incident response subnet could be added to the exception list to allow the system of interest to communicate with storage servers or other analysis tools. This would allow a user to interact with the package deploy or package playbooks features to execute a set of packages on a system and allow the data to be transmitted to a remote system for analysis, all without needing to remove the system from a locked-down state.

#### Total Endpoint Lockdown

If an endpoint is determined to be the source of an outbreak or has been identified as harmful to the environment for some reason, aggressive containment will be able to be taken to move and lock down the endpoint, eliminating its ability to connect to the network. With this flexibility, potential security issues can be remediated quickly and the necessary steps can be taken to stem the attack, protect sensitive data, and keep the business secure.

#### **Technical Details**

With CylanceOPTICS, administrators will be able to quickly isolate an infected or potentially infected device to stop command and control (C2) activity, exfiltration of data, or lateral movement of malware. The lockdown feature will give administrators time to investigate the device or physically remove the device from the network. This action will only be available to administrators in the BlackBerry Cylance Console. Lockdown will disable the network capabilities of the device (LAN and Wi-Fi) for a period of time, from five minutes to 96 hours. If desired, the device can be unlocked prior to the selected lockdown end-time using the unlock key.



#### **Additional Details**

- When an endpoint lockdown time has expired, it can take up to two minutes for that device to appear as connected on the Devices page in CylanceOPTICS.
- CylancePROTECT Agent 1440 and above will display a message on the endpoint (via a notification) when it has been placed into a lockdown
- Once a device has been locked down, the status column will show a red icon in the CylanceOPTICS column to indicate a device is in lockdown

A lockdown will also be able to be initiated from any InstaQuery result, which will re-direct to the devices page filtered to the device associated with the artifact.

#### **Remote Response**

CylanceOPTICS Remote Response streamlines all available system information from within the BlackBerry Cylance Console. By providing an interface for users to intuitively and interactively execute scripts and run traditional or native commands on systems, users will be able to quickly triage a system and see the results of those commands in near-real-time in the BlackBerry Cylance Console without ever needing to navigate away to view returned data. The objectives of remote response and packages are similar in that the workflows offer a mechanism for users to collect information about a system, run scripts, execute applications, or otherwise investigate a system of interest, however, the experience between remote response and packages is the primary difference.

Feature	Benefit
Terminal Interface	Easily investigate and manage remotely
Command Line Access	Execute scripts, commands, and applications within the system with future-enhanced functionality accommodation
Logging Capability	Benefit from a complete audit trail for review

1 https://www.scribd.com/article/372099367/Why-Linux-Users-Should-Worry-About-Malware-And-What-They-Can-Do-About-It

#### About BlackBerry Cylance

BlackBerry Cylance develops artificial intelligence to deliver prevention-first, predictive security products and smart, simple, secure solutions that change how organizations approach endpoint security. BlackBerry Cylance provides full-spectrum predictive threat prevention and visibility across the enterprise to combat the most notorious and advanced cybersecurity attacks, fortifying endpoints to promote security hygiene in the security operations center, throughout global networks, and even on employees' home networks. With Al-based malware prevention, threat hunting, automated detection and response, and expert security services, BlackBerry Cylance protects the endpoint without increasing staff workload or costs.





#### +1-844-CYLANCE

sales@cylance.com www.cylance.com



<sup>©</sup>2020 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY, EMBLEM Design and CYLANCE are trademarks or registered trademarks of BlackBerry Limited, its subsidiaries and/or affiliates, used under license, and the exclusive rights to such trademarks are expressly reserved.