Carbon Black.

Bit9 Security Platform 7.2.3

Release Notes

Product Version *7.2.3.3703*
Patch 6
3 August 2017

Carbon Black, Inc.
1100 Winter Street, Waltham, MA 02451 USA
Tel: 617.393.7400 Fax: 617.393.7499
E-mail: support@carbonblack.com
Web: http://www.carbonblack.com

Introduction

The *Bit9 Security Platform v7.2.3 Release Notes* document provides information for users upgrading from previous versions as well as users new to Bit9 Platform. It consists of the following major sections:

- **Before you Begin**: This section describes preparations you should make before beginning the installation process for Bit9 Server.
- **Bit9 Platform v7.2.3: New and modified features**: This section provides a quick reference to changes in the Bit9 Platform made since Bit9 Platform 7.2.2.
- **Bit9 Platform v7.2.2: New and modified features**: Since version 7.2.2 is also relatively new, we have included a quick reference to feature changes made in that release.
- **Corrective Content**: This section describes issues resolved by this release as well as more general improvements in performance or behavior.
- **Known Issues and Limitations**: This section describes known issues or anomalies in this release of Bit9 Platform v7.2.3 that you should be aware of.
- **Contacting Support**: This section describes ways to contact the Technical Support team for this product, and the information to prepare that will help troubleshoot a problem.

This document is a supplement to the main Bit9 Platform documentation.

About your Bit9 Platform Distribution

Your Bit9 Platform distribution includes the Bit9 Server installation program. Bit9 Server custom-generates agent installation packages at your site for each protection policy you define, so no separate agent installer is needed in the original distribution.

Purpose of This Release

This release contains corrective content that resolves reported issues. Please carefully review the "Corrective Content" section and especially the "Known Issues and Limitations" section.

Documentation

The Bit9 Platform documentation set includes online Help built into the console and PDF files distributed with the product and/or available on the User eXchange. The set includes:

- **Installing the Bit9 Server:** Provides instructions for installing and configuring the Bit9 Server.
- **Using the Bit9 Security Platform:** Describes Bit9 Platform operation, including step-by-step instructions for administration and configuration tasks. Management topics for computer systems, including **agent installation**, are also covered.
- **Bit9 Platform Events Integration Guide** – Describes the events that are generated, tracked, stored, and accessible through the Bit9 Platform system, and the ways you can access Bit9 Platform event data outside of the Bit9 Console user interface.
- **Bit9 API Documentation** – Instructions for configuring the Bit9 API are included in *Using the Bit9 Security Platform.* Up-to-date documentation of the actual API objects and properties, as well as code examples, is available at: https://github.com/carbonblack/bit9platform
- Other documentation, including operating environment requirements, supported agent operating systems, and special-purpose information, is available on the User eXchange.

Before you Begin

This section describes preparations you should make before beginning the installation process for Bit9 Server. These include actions to take before installing Bit9 Server, preparations you should make for configuring the server after installation, and general information you should know about server and agent. It contains information for both upgrades and new installations.

System requirements

The document *Bit9 Security Platform Version 7.2.3 Operating Environment Requirements* describes the hardware and software platform requirements for the Bit9 Server and the SQL Server database that stores Bit9 data. The document *Bit9 Agent Supported Operating Systems v7.2.3* provides the current requirements for systems running the agent. Both are available to customers with login credentials on the User eXchange.

Both upgrade and new customers should be sure to meet the requirements before proceeding.

Additional downloads

This section contains links to download additional software that may be required to install Bit9 Platform version v7.2.3. Consult *Installing the Bit9 Server* for more information.

Windows Installer 4.5:
http://www.microsoft.com/en-us/download/details.aspx?id=8483

SQL Server 2012 Express:
http://www.microsoft.com/en-us/download/details.aspx?id=43351

Bit9 Server upgrades

This section is for upgrades only. If you are not upgrading, see New Bit9 Platform Installations (page 5). For more detailed upgrade instructions, please refer to *Installing the Bit9 Server*. It is available on the User eXchange.

Below is a table explaining the supported upgrade paths for Cb Protection servers

Upgrading from	Upgrading to
v5.1.2	⇨ v6.0.2 latest ⇨ v7.2.1 latest ⇨ v7.2.3
v6.0.0	⇨ v6.0.2 latest ⇨ v7.2.1 latest ⇨ v7.2.3
v6.0.1	⇨ v6.0.2 latest ⇨ v7.2.1 latest ⇨ v7.2.3
v6.0.2	⇨ v7.2.1 latest ⇨ v7.2.3
v7.0.0	⇨ v7.2.3
v7.0.1	⇨ v7.2.3

v7.2.0	⇨ v7.2.3
v7.2.1	⇨ v7.2.3
v7.2.2	⇨ v7.2.3
v7.2.3 previous version	⇨ v7.2.3 current version

Support for the upgrade process

Bit9 Server and Agent update releases are covered under the Customer Bit9 Platform Maintenance Agreement. We recommend reviewing content on the User eXchange prior to performing the upgrade for the latest information that supplements the information contained in this document. Technical Support is available to assist with any issues that may develop during the upgrade process. Our Professional Services organization is available to assist with the upgrade process to ensure a smooth and efficient upgrade installation.

Rescanning of agents after server upgrade

When Bit9 Server is upgraded from one major version to another (such as v7.2.0 to v7.2.3), ongoing enhancements to "interesting" file identification make it necessary to rescan the fixed drives on all Bit9 Platform-managed computers. These upgrades also require a new inventory of files in any trusted directories to determine whether there are previously ignored files that are considered interesting. This involves the same activity as agent initialization, and can cause considerable input/output activity, which can require between minutes and many hours, depending upon the number of agents and the number of files. Gradual upgrade of agents is recommended to avoid an unacceptable impact on network and server performance. See "Enabling Automatic Agent Upgrades" in the *Using the Bit9 Security Platform* guide for details.

Before running the server upgrade

The following tasks should be done *before* you run the Bit9 Server upgrade program:

- **Software update:** When installing on Windows Server 2008 R2, the Microsoft Visual Studio 2010 SP1 (x86) runtimes are a prerequisite. In many cases, these runtimes will already have been installed. This software is available from the following link: https://www.microsoft.com/en-us/download/details.aspx?id=5555
- **Backup Bit9 Server database:** Backup your Bit9 Server database before you begin the upgrade process. You *must* have a recent backup available so that there is a recovery option in case of database update failure during server update.
- **Backup certificates separately:** In v7.2.3, Bit9 Server's Certificates will be backed up in the Database. However, IIS certificates are not backed up automatically. Please do a separate backup of IIS certificates, and if upgrading from 6.0.2, all Bit9 Platform certificates, on a system other than Bit9 Server.
- **Disable distribution systems:** If you use third-party deployment mechanisms (e.g. SCCM), either: disable the distribution of the Bit9 Agent using SCCM, and use Bit9 Server for upgrading agents; or disable Bit9 Server from upgrading agents, and use your third party deployment mechanism to upgrade the agents.

- **Stop SQL background jobs:** Because the Bit9 database is updated during a server upgrade, no other database jobs should be running. This includes background jobs on database maintenance and backups activity. Stop any of these jobs, and confirm that no one else is using database before initiating the Bit9 Server upgrade.

Prepare for post-upgrade tasks

Be prepared to do the following tasks after you run the Bit9 Server upgrade program:

- **Review external event settings:** If you use External Events, review the settings to ensure they are still enabled and correctly functioning. Also, if you are upgrading from a pre-7.0.0 release, note that the external event schema has been changed. Review the upgrade section of *Installing the Bit9 Server* for information on how to upgrade it.
- **Review updaters:** New Updaters have been added. Review the Updaters tab on the Software Rules page to make sure the correct updaters are enabled. See the section "Bit9 Platform v7.2.3: New and modified features" and "Bit9 Platform v7.2.2: New and modified features" for lists of new and improved updaters since v7.2.1.
    - **Update agent distribution points:** If you use 3rd-party deployment mechanisms (e.g. SCCM), re-enable or re-create them using new agent packages from the upgraded Bit9 Server. Beginning with v7.2.3, you use ParityHostAgent.msi for *all* agent upgrades. MSP files are no longer used for patch/hotfix upgrades.
    - **Review the new Bit9 Platform installations section:** Although it is for new installations, this section also includes information of possible interest for upgrades.
    - **Enable System Health indicators:** Bit9 Platform includes a System Health page, which reports on factors that affect the performance of your server, including the compliance of your environment with Operating Environment Requirements. Consider enabling this feature to keep your system healthy.

New Bit9 Platform installations

This section describes preparatory tasks and suggested post-installation tasks for new Bit9 Server installations. Although targeted at new installations, it should be reviewed by new and upgrade customers.

For more detailed instructions about preparations you must make, please refer to the separate document, *Installing the Bit9 Server*.

Prepare for Bit9 Server installation

- **Choose account for Bit9 Server installation:** Use of a Domain Service Account is recommended for Bit9 Server installation. If you plan to use Active Directory services or use an authenticated proxy to access the Internet, a Domain Account is *required* for Bit9 Server Service. This account must have Local Administrator privileges on the Bit9 Server. Do not change the permissions level of the account with which you install Bit9 Platform after installation.
- **Prepare to enable Bit9 Agent management access:** The Bit9 Agent Management screen in the new installation dialog allows you to designate a user or group, or a password usable by anyone, to perform certain agent management activities assisted by a member of the Technical Support team. Especially if you will have client computers that will never be connected to Bit9 Server, it is best to set up a client access option before generating and

distributing agent installation packages. If you are unable to configure access during installation, you can do it later on the Management Configuration page in Bit9 Console. See Using the Bit9 Security Platform (or online help) for more details.

Prepare for post-installation tasks

- **Enable Bit9 Platform CLI management access:** If you did not enable Bit9 Agent Management access during installation, go to the General tab of the System Configuration page in Bit9 Console to enable it, preferably before deploying agents. See "Configuring Agent Management Privileges" in Using the Bit9 Security Platform or online help for details.
- **Confirm agent installation privileges:** The Bit9 Agent installer must be run by a user with the appropriate administrative rights. On Windows, this can either be Local System or a user account that has administrative rights and a loadable user profile. On OS X and Linux, the user must be able to run as root (sudo is one of the techniques that may be used).
- **Consider agent rollout impact:** As soon as the Bit9 Agent is installed, it connects with the server and begins initializing files. Because initialization can involve an increased flow of data between the Bit9 Server and its new client, be sure your agent rollout plans take your network capacity and number of files into account — simultaneous agent installation on all the computers on a large network is not recommended. Deploying agents in disabled mode will avoid this situation.
- Review the **Known Issues and Limitations** section before deploying agents: Certain Known Issues may affect agent deployment and require actions on the server *before* you deploy agents.
- **Review trusted updaters:** Review Trusted Updaters to ensure the correct ones are enabled for your environment before you begin large-scale Bit9 Agent deployment.
- **Review root certificates for trusted publishers:** Trusted Publishers are validated by Windows. For proper validation to occur, the correct, up-to-date root certificates must be installed for these publishers. You should ensure that Microsoft root certificate updates are included in your Windows Updates. If you plan to use in-house certificates, ensure that your in-house root certificates are installed on each endpoint on which you will install Bit9 Agent.
- **Test user-supplied certificates:** Bit9 Server allows use of user-supplied certificates for Bit9 Agent-Server communication. To validate this certificate, each agent system must have up-to-date root certificates. Test your new certificates before large-scale Bit9 Agent deployment begins. See "Securing Agent-Server Communications" in Using the Bit9 Security Platform or online Help for more details.
- **Review content of trusted directories for distribution systems:** If you use Windows Software Update Services (WSUS) or other software distribution mechanisms (e.g. SCCM or Altiris), pre-approving this content with a Trusted Directory before large-scale Bit9 Agent deployment will ensure a more effective transition to High Enforcement Level.
- **Script Files:** It is most efficient to define your script rules before you enable to avoid having to rescan the file system to look for those scripts. Java Tracking is an example. Support for tracking Java class and jar files is not enabled by default. If you plan to track Java applications, please choose Rules->Software Rules from the console menu and enable the rules for Java on the Scripts tab.

- **Exclude Bit9 Agent from AV scanning:** Antivirus products, including Microsoft SCEP, should be configured to exclude Bit9 Agent files from scanning. Please refer to the Using the Bit9 Security Platform guide for details about the files or folders to exclude for each platform.
- **Consider other agent interactions:** Certain other types of software may interact with the Bit9 Agent – contact Technical Support for more information on each of these cases:
    - Disk encryption software may interact with the Bit9 Agent. In general, full disk or partition encryption should minimize the chances of problems. However, some encryption products are compatible with Bit9 Platform with other types of encryption (file or folder) enabled.
    - Ghosting or imaging systems with Bit9 Platform pre-installed requires additional steps on the master system. Please consult the "Managing Virtual Machines" chapter in the Using the Bit9 Security Platform guide for more information.
- **SQL recovery model:** The simple recovery model is recommended. Use of the full recovery model may affect Bit9 Server performance. If you intend to use the full recovery model, please contact Technical Support for more information.
- **Enable System Health indicators:** Bit9 Platform v7.2.3 includes a System Health page, which reports on factors that affect the performance of your server, including the compliance of your environment with operating environment requirements. Consider enabling this feature to keep your system healthy. Software Reputation Service has to be enabled for the health indicators are delivered to your server.

Bit9 Platform v7.2.3: New and modified features

The following sections provide a quick reference to the feature changes made since v7.2.2.

Support for Windows 10 Anniversary Update

This release includes support for Microsoft Windows 10 Anniversary Update, including upgrades to this operating system with the Bit9 agent in place. In previous releases, it was necessary to remove the agent when doing major and minor OS upgrades. Please note these important requirements, recommendations, and open issues:

- OS upgrades with the agent in place will work only when upgrading to Windows 10 Anniversary Update and later. You must enable Trusted Directory approval of WIM files for in-place agent upgrades to succeed, as described in the next section.
- If you do not have another anti-virus product installed, Windows Defender is enabled by default when you install Windows 10. Consider enabling the Windows Defender updater on the Bit9 Console (**Rules > Software Rules > Updaters**) to make sure update files for this application are not blocked.
- If you plan to install Windows 10 Anniversary Update directly from an ISO, you may need to take additional steps. This case is still being addressed by our engineering team. Please monitor the https://community.carbonblack.com/thread/3367 on the Carbon Black User eXchange for any changes to the status of this case and Windows 10 support in general.

Acceptable In-Place OS Upgrades with 7.2.3 Agent Installed

Current OS	Upgrading To OS
Windows 7	Windows 10 Anniversary Update (August 2016)
Windows 8	Windows 10 Anniversary Update (August 2016)
Windows 8.1	Windows 10 Anniversary Update (August 2016)
Windows 10	Windows 10 Anniversary Update (August 2016)

Enabling Trusted Directory Approval of WIM Files

Beginning with Bit9 Security Platform version 7.2.3, you can enable “crawling” and approval of the contents of Windows Image (WIM) files in trusted directories. Addition of WIM crawling increases approval coverage of updates you receive via Windows Server Update Service (WSUS).

One important use of this feature will be to enable Bit9 Platform 7.2.3 to support updates to the upcoming Windows 10 Anniversary Update on your endpoints without removal of the agent. The procedure described below is a prerequisite for these in-place updates. There may be additional requirements. See https://community.carbonblack.com/thread/3367 for the latest information on Windows 10 Anniversary Update support.

See “Approving by Trusted Directory” in *Using the Bit9 Security Platform* or console help if you have not already set up a trusted directory. If you use multiple trusted directories, the procedure must be repeated for each one in which you want WIM files to be approved.

Important: If you perform the following procedure, the console Events page and diagnostics output on the agent itself will show four health check failures: three referencing the **ImageX.exe** file and one noting a discrepancy in the number of files in the agent directory. You may ignore these error messages. See issue 51615 in the Known Issues and Limitations section for details.

To allow trusted directory approval of WIM files:

1. Choose or create the trusted directory in which you want to approve the content of WIM files (including those in ISOs). On the system where the trusted directory is located, download the Microsoft Windows Automated Installation Kit (AIK): https://www.microsoft.com/en-us/download/details.aspx?id=10333

   This includes **imagex.exe,** which is required for WIM approval. The download page also includes information and requirements for installing the AIK. Note that although Windows 7, 8, and 10 are not included in the list of supported operating systems, you should be able to use this kit on systems running those operating systems (and their server equivalents).

2. Disable tamper protection on the agent running on the trusted directory server.
   a. On the console menu, choose **Assets > Computers**.
   b. In the Computers table, find the name of the computer hosting the trusted directory, and click on the name or View Details button.
   c. On the Computer Details page, click on **Disable Tamper Protection** in Advanced section of the right menu bar.
3. From the download location, copy **ImageX.exe** into the agent installation directory (typically C:\Program Files (x86)\Bit9\Parity Agent).
4. In the Bit9 Console, approve the ImageX.exe file on the agent hosting the trusted directory:
   a. On the console menu, choose **Tools > Find Files** and search for **ImageX.exe**
   b. In the Find File results, check the box next to ImageX.exe and choose **Approve Locally** or **Approve Globally** on the Action menu.
5. On the Computer Details page for the agent on which you placed ImageX.exe, re-enable tamper protection.
6. Add WIM files to the file types that Bit9 can “crawl” in a trusted directory:
   a. Navigate to the Support page in the Bit9 Console by manually entering the URL: https://<serveraddress>/support.php

   b. Click on the Advanced Configuration tab, and in the Agent Configuration panel, check the box for **Enable Deep Crawl**.
   c. In the next line, **Deep Crawl Files**, add "*.wim" to the end of the list of file extensions if it is not already there. Use a comma to separate the new extension from the previous one in the list. Click **Update** when you are finished.
7. On the console, choose **Assets > Computers**, and locate the computer that has the trusted directory. You must wait until this computer shows **Up to date** in the Policy Status column of the Computers page before proceeding.
8. Copy or move any ISO files and/or separate WIMs you want approved into the trusted directory. The inventory and approval of the contents of these files begins. Completion of this process could take several hours and consume considerable system resources, depending upon your hardware.

For additional info on ImageX.exe, see:

https://technet.microsoft.com/en-us/library/cc722145(v=ws.10).aspx

For additional info on WIM, see:

https://www.microsoft.com/en-us/download/confirmation.aspx?id=13096

New Custom Rules

New custom rules have been added in v7.2.3. These rules treat *read-only file mappings* of executable files by applications using the .NET runtime as *file executions*. Note that some rules are effective on agents at specific Enforcement Levels. For more details see the following document in the User eXchange: https://community.carbonblack.com/docs/DOC-4913.

The new rules are:

1. Report read-only memory map operations on unapproved executables by .NET applications.
   This is a report only rule that is **enabled** by default.
2. [Sample] Deny read-only memory map operations on unapproved executables by.NET applications in high enforcement.
   This custom rule is **disabled** by default.
3. [Sample] Prompt for read-only memory map operations on unapproved executables by .NET applications in medium enforcement."
   This custom rule is **disabled** by default.
4. Deny read-only memory map operations on banned executables by .NET applications.
   This custom rule is **enabled** by default.

Removal of Windows Installer Patch Program

Beginning with version 7.2.3, you use **ParityHostAgent.msi** for *all* manual Windows agent upgrades. This includes upgrades from agent versions from 6.0.0 through 7.2.2 as well as build-to-build upgrades from previous 7.2.3 releases (for example, from 7.2.3.546 to 7.2.3.760). Prior to 7.2.3, an MSP was used for build-to-build upgrades, but that is no longer necessary or supported. If you are using a software distribution system like SCCM you will need to adjust your command line parameters for upgrading the agent.

New and Improved Updaters

A new updater, Microsoft Office 2016, has been added to v7.2.3. Improvements to the following updaters have been made in previous releases of v7.2.3:

- Carbon Black Tamper Protection
- Google Chrome
- GoToMeeting
- Windows 8, 10, and Server 2012

The following new (Bolded) or improved trusted updaters are included in v7.2.3 Patch 5 and later:

- **Cb Defense sensor for Windows**
- **Cb Defense sensor for Mac**
- SCCM
- Adobe Acrobat for Mac
- Google Chrome for Windows
- Roaming Profiles: Improve performance when roaming profiles are in use by ignoring writes of some files by the Roaming Profiles Service. [51298]

Red Hat / CentOS Agent Support in this Release

Bit9 Platform Linux agents are not included in this release. [44255]

The initial release of v7.2.3 (Build 3106) included an early access version of the Linux agent installer that was not approved for release and should not have been in the distribution. This Linux agent should not be installed.

The Linux agent package is not included in the installer. However, the 7.2.0 Linux agent is compatible with the 7.2.3 Bit9 server. To deploy the 7.2.0 Linux agent, you should download the Linux installer from the Carbon Black User eXchange, and follow instructions listed below:

1. From the latest 7.2.0 agent, copy these files into the c:\Program Files (x86)\Bit9\Parity Server\hostpkg folder on the 7.2.3 server:
    a. b9agent.rpm
    b. b9notifier.rpm
    c. Bit9Redhat6Install.bsx
2. In that directory on the server:
    a. Rename the file b9agent.rpm to b9agentRedhat6.rpm.
    b. Make a copy of the same file and rename the copy to b9agentRedhat7.rpm.
    c. Rename the file b9notifier.rpm to b9notifierRedhat6.rpm.
    d. Make a copy of the same file and rename the copy to b9notifierRedhat7.rpm.
    e. Make a copy of the Bit9Redhat6install.bsx file and rename the copy to Bit9Redhat7install.bsx.
3. On the server, navigate to: https://<myservername.mydomainname>/shepherd_config.php
4. Set the property “GenerateRedhatInstaller” to “true”.
5. Restart the server. The host packages displayed in the server will now include “Redhat”.

Bit9 Platform v7.2.2: New and modified features

The following is a quick reference to the feature changes made in v7.2.2:

- Some threat Indicator Sets have new indicators that will identify new types of threats.

- Display patch number in console [44917]
    - Details: The Bit9 Server console now displays the patch number after the build number in the top navigation pane of every page.
    - Applies to: Server
- Added available fields to API for custom rules. [44626]
    - Details: The following fields have been added in the API for custom rules:
      1. ruleUITemplateId for rule UI Type
      2. ruleAction for the rule action
    - Applies to: Server

  Up-to-date documentation of the API objects and properties, as well as code examples, is available at: https://github.com/carbonblack/bit9platform
- QRadar Certification for new event types [42922]
    - Details: The integration with QRadar has been enhanced to recognize new Bit9 events when using the June 2015 version of QRadar or later. See the *Bit9 Platform Events Integration Guide* for details of the QRadar integration.
    - Applies to: Server
- Set default size limit for logs [46342]
    - Details: Previously, agent log files were allowed to grow without limit. In this release, the default log rotation size is 50 MB; they are rotated out after exceeding the limit. The logs are not compressed. The agent keeps the current "live" log and one old log. If you need to capture larger logs; contact Technical Support for instructions.
    - Applies to: Agent [Windows]
- The following new or improved trusted updaters are included in v7.2.2
    - Adobe Air
    - Apple System Performance
    - Bit9 Agent Tamper Protection
    - Carbon Black Tamper Protection
    - FlowDock (Mac)
    - Google Chrome for Mac
    - Google Chrome for Windows
    - Google Drive for Mac
    - GoToMeeting for Windows
    - GoToMeeting for Mac
    - Linux System Performance
    - Mac System Updates
    - McAfee Viruscan Enterprise 8.5
    - Webex for Chrome
    - Webex for Firefox
    - Webex for Internet Explorer
    - Windows 8, 10, and Server 2012 Updates

Corrective Content

Corrective Content in Bit9 Platform 7.2.3 Patch 6 (Build 3702)

Server and Server Installation

- Improved reporting about the Cb Response sensor on the computer details page. When Bit9 manages a computer on which a Cb Response sensor is installed, the version of the Cb Response sensor now appears on the Computer Details page. [51980]
- Fixed a problem with how lists of policies were handled internally that occasionally prevented upgrades and the creation of new policies. [50489]
- Fixed a problem where failures of file uploads that were part of file analysis could degrade database performance. The underlying table is now pruned as needed. [52735]
- Removed a race condition that could occur in the nightly cleanup job (the Daily Prune Task). This race condition prevented the clean-up job from completing. [52734]
- Improved reporting during installations and upgrades by providing better tracking of index creation. [52740]
- Fixed an integer overflow error that had resulted in large backlogs and failures in background tasks. This issue is only known to occur for deployments of over 50,000 endpoints. [52731]
- Made the timeout for slow synch with SRS configurable with the configuration property ReporterSRSTaskSQLTimeout. Changed the default to 6 minutes (360 seconds). [52493]
- Made 7.2.3 agents compatible with Windows 10 Redstone 10 “Creators update”. Versions of the agent prior to 7.2.3 Patch 6 are not compatible with Windows 10 Redstone 10 “Creators update”. Upgrade to 7.2.3 Patch 6 or higher before installing or upgrading to this version of Windows 10. [52878]
- Provided tracking for file renames and deletions in Windows 10 Creators Update. In this Windows release, Microsoft has introduced new means by which a file can be deleted or renamed. To ensure that your agents are properly tracking deletions and renames, upgrade them to 7.2.3 Patch 6 or later before deploying or upgrading them to Windows 10 Creators Update. [52747]
- Fixed a problem where some intermediate and root certificates that were seen on agents were not being reported to the server and therefore would not appear in the console. This issue should autocorrect itself within a few hours after upgrading the server and agent to 7.2.3 Patch 6 and higher. [52863, 52901]
- Fixed an issue with the daily database maintenance task that had been caused by an arithmetic overflow. [52959]
- Repaired links from the Events page to the Device Details page that had been broken when the name of a device given in an event included a plus sign. [52990]
- Removed a cross-site scripting vulnerability on the Computers page, hosts.php. [53065]
- Restored file instances that had been erroneously excluded from the fileinstance API because they did not belong to a file instance group. [2052]
- Fixed an issue with event rules that prevented the 'move computer' action from working in certain scenarios. [1834]

Agent

- Made user-specific CSIDL or Path macros refer to the user-set location rather than the user's default location. [52564]
- Improved the performance of per-user macros on multi-user systems (such as Terminal Server) by preventing the rule's expansion to one rule per user and by instead relying on a wildcard in the path. [52657]
- Updated the Cb Defense Updater to avoid blocks on updates of Cb Defense. [51367, 50598]
- Extended tamper protection to cover the registry keys the agent uses to start up in safe mode. Agent start up in safe mode is turned off by default and must be configured by policy. This change prevents tampering with this setting. [52640]
- Made it possible to upgrade agents from 7.2.2 to 7.2.3 without using the Bit9 Server. To do this, one must set the agent config property "allow_upgrades=1". As this workaround will not be required in future upgrades, you can remove the allow_upgrades property after the upgrade completes. [52707]
- Fixed a problem that prevented agents on Macs from reading config properties when using strong SSL to communicate with the Bit9 Server. [52243]
- Made agent upgrades more robust by stopping the upgrade when the agent service cannot be stopped successfully. [52708]
- Fixed an anomaly caused by incomplete certificate chains encountered when validating a file signature. That anomaly occurs when a file that was signed by a certificate that lacked a full certificate chain to a trusted route. This occurs because the issuing certificate for the signing certificate was absent from the local machine's certificate store. Under these conditions, the agent would treat the signature as ineligible for approval; it would report a partial chain failure. However, if a separate file came in with the same signing certificate but with the full chain as part of its signature, then the agent could still mistakenly treat the certificate chain as partial even though it could now complete the chain. In this release, the agent will attempt to reconstruct the full chain each time it encounters a signing certificate that is missing its issuing certificate. [52712]
- Made the agent more responsive to updates in certificate status. When a certificate changes validity status from invalid to valid (such as when a partial chain becomes complete after trusted roots are updated), the agent will now properly re-evaluate the file state of all files that have that certificate in either the signing chain or the counter signing chain to see if the file should now be approved. Previously, the agent only handled validity status changes for certificates in the primary signing chain and not the counter-signing chain. In the past, a workaround for this problem was to restart the agent since that forced re-evaluation of all file states. In this release, no reboot is necessary; the file states should be updated as soon as the agent recognizes a change in certificate validity status. [52792]
- Addressed an agent interoperability issue that can, for example, show up as double fault bugchecks when Unidesk and ESET Security are concurrently deployed. [52984]
- Improved the Microsoft Office 2016 updater so that updates to Microsoft Office 2016 no longer cause blocks. [51802]
- Added an Adobe Creative Cloud updater for Windows and Mac systems. [53007, 53015, 1822]

- Provided additional protection to registry keys. Previously, if there were a registry block rule in place for a particular path like HKLM\Software\Foo\Bar and a user attempted to rename HKLM\Software\Foo to HKLM\Software\Foo2 the operation would not be denied since the rule was only setup to block modifications to "Bar" and not to its parent keys. Before the agent allows a key rename to occur, it will now evaluate whether any child key or value of the key being renamed is covered by a block rule. If any subkey or value is covered by a block rule, the entire rename operation will not be allowed. This helps avoid bypasses like the recently disclosed DoubleAgent injection technique. Also note that, as part of this fix, if you have a registry report rule enabled, when a key is renamed you will now see registry modification events for each child subkey or value whose name was affected by the change. [53006, 53024]
- Corrected the GoToMeeting Updater so that it works on Windows XP and Windows 7 32-bit. [1439, 51991]
- Updated the GoToMeeting Updater to reflect GoToMeeting's new certificates. [1693]
- Fixed three separate issues that, under rare conditions, could cause the Bit9 agent to deadlock, which in turn could cause the machine to hang. [52962, 53060, 1330, 52996]
- Made it possible for the Bit9 Agent's command-line tool, dascli, to communicate to the Bit9 service over ports other than the default port (3142). When the default port is in use and the agent config setting random_cli_port is enabled, the agent will use a random port for such communications instead. [53030, 37092, 45634, 1810, 1214]
- Closed a kernel memory leak for Mac agents. [1477]
- Fixed an issue where network paths were not appearing as in the expected format of "\\server\share" but rather with a prefix of either "??\globalroot\device\mup\" or "??\globalroot\device\lanmanredirector" prefix. Note that, if not all agents are upgraded to version 7.2.3 Patch 6 or later, custom rules may still need to account for both name formats. [2039]
- Eliminated unnecessary file analysis operations on unchanged files by correcting a problem whereby some file read operations had been incorrectly classified as write operations. Now these operations are correctly classified as read operations. [1469]
- Fixed a problem introduced with the 7.2.3 Patch 5 Mac agent whereby transitions in and out of sleep could fail in general when the agent was present. Sleep/wake failures caused by the agent have been addressed except for one scenario: When using FileVault with NVRAM FileVault Key destruction on standby (the DestroyFVKeyOnStandby power setting), a sleep/wake failure can still happen. To avoid sleep/wake failures on systems using FileVault, set the DestroyFVKeyOnStandby to 0. If that is not an option, set standby to 0. See the macOS pmset command for more information. [1371]
- Provided a workaround to prevent a kernel panic when doing kernel-tracing with variable length strings on macOS 10.12 when length-formatted strings are not null-terminated. [1320]
- Fixed a problem that caused the b9daemon to crash intermittently on macOS. The cause was an unhandled exception from the Boost library. [1161]
- Removed some unexpected execution blocks on macOS of binaries written by trusted processes. These were due to the b9daemon process not tracking processes that started soon before or soon after the b9daemon itself starts. [1213]

- Prevented blocks that had occurred on updating the Cb Response sensor. [2105, 2211]

Corrective Content in Bit9 Platform 7.2.3 Patch 5 (Build 3471)

Server and Server Installation

- Preserved the policy-specific settings of ATIs updated from the cloud. [51126]
- Provided support for case-sensitive SQL Server instances. [52036]
- Prevented newly received updaters issued from the cloud from getting disabled as a result of a configuration setting left from version 6 of the product. [52123]
- Fixed an issue where the "*Malicious file detected"* alert was configured to ignore already approved or banned files, but triggered for indirectly approved/banned files (e.g., by publisher). [52128]
- On the Computer Details page, prevented users without "Change advanced options" permission from viewing the "Convert to template" command, use of which requires that permission; moved the "Reset CLI Password" command under the Actions header. [52386]
- Eliminated a requirement that users have "Change advanced options" permission to be able to reset a computer's CLI password. [52486]
- Corrected the URL for submitting files for analysis through the Check Point connector, eliminating analysis failures caused by the previous incorrect address. [52451]
- Added support for two file analysis environments for Check Point: Windows 7 - 64bit and Windows 8.1 - 64bit. [52468]
- Added support for connections to external WildFire sites through a proxy. [52490]

Agent

- Corrected a problem that prevented the agent from properly managing script files if the files were discovered (and considered uninteresting) before a script rule affecting them was enabled; setting up script rules before deploying agents is still recommended. [51915]
- Modified the Mac System Updates updater to avoid an issue where minor upgrades OS X with System Integrity Protection (SIP) enabled could result in temporary files being left in the agent's file inventory after they were removed from disk; a cache consistency check is recommended to clean up these files from previous versions. [50477/51492]
- Addressed an issue in which the Mac agent caused sleep/wake failures on some systems. [51263]
- Addressed an issue where the agent was not re-expanding rules after a new product was installed, preventing rules that depended on the new product from taking effect until the next user login, rule change or restart. [51377]
- Made performance improvements to reduce agent CPU usage and improve overall performance, especially in Unidesk, Citrix, or multi-user Terminal Services environments. [52039, 52318, 52355]
- Modified the Cb Response and Cb Protection Tamper Protection updaters to correct a problem in which the agent did not persist a rule element used in these updaters, which could cause unauthorized modification to the Cb Response service keys. [52131]

Corrective Content in Bit9 Platform 7.2.3 Patch 4 (Build 3327)

Server and Server Installation

- Corrected an issue that could cause the console to malfunction when configuration changes were made to the parity.ini file during a server upgrade. [51535]
- The template Tag '{$host_name}' can now be used for Elevated Privilege Alerts. [51618]
- Increased the SQL command timeout from 30 to 60 seconds for fast syncs between the server and SRS, reducing the number of fast sync error reports. [51629]
- It is no longer necessary to activate Basic Authentication and Directory Browsing in IIS when you are installing the Bit9 Server. [51757]

Agent

- Addressed an issue on the Events page in which the Policy field was blank if the page was filtered by Subtype and the subtype chosen was 'Malicious file detected' or 'Potential risk file detected'. [51355]
- Corrected a path problem in the Carbon Black updater for Mac that prevented updates to the Cb Response sensor on systems running the Bit9 Mac agent. [51380]
- Addressed an issue on Windows agents in which rules failed because file hashes from an imported *configlist.xml* file did not have uppercase characters converted to lowercase, resulting in a mismatch; these characters are now converted. [51409]
- Corrected an issue in which an agent health check queried all Windows agent systems for processes that only exist in 32-bit Windows, generating erroneous health check errors similar to the following: *Error[Severity[Low] There have been 4 kernel assertions since the last health check Total[4] LastAssertion[179447 ms ago]]*. [51432]
- Modified the agent to remove the SSLv2 flag in the agent config setting "winhttp_secure_protocol_flags" if there are flags for both SSLv2 and TLS1.2; use of both flags prevents agents from communicating with the server. [51483]
- Added a low-severity health check to report when Windows agents have both SSLv2 and TLS1.2 flags set for "winhttp_secure_protocol_flags"; the SSLv2 flag (hex value 0x8) should be removed to restore agent-server communication if this health check appears. [51483]
- The <ApprovalRequestId> tag is now supported in Approval Request mail templates. [51529]
- Addressed an issue in which files that should have been blocked could sometimes run if they were executed via a local UNC path. [51546]
- Addressed a problem in which a large number of recent file changes could cause the Windows agent to crash. [51602]
- Addressed an issue on Windows agents that caused a spurious, intermittent health check failure for 'notifiermessages.dll'. [51617]
- Fixed a Windows agent problem with parity.sys where buffer allocation failures were not detected, which caused a *SYSTEM_SERVICE_EXCEPTION(3b) BSOD* with an exception code of *C000005*. [51623].
- Updated the Windows agent tamper protection rules to prevent creation of custom application compatibility shims for protected processes. [51728]

- Addressed an issue on Windows agents that could prevent correction of duplicate file hash data and result in loss of local approval. [51797]
- Addressed an issue that could prevent the Windows agent from sending some file reports and events to the server, which caused information displayed in the console to be out of date. [51803]
- Addressed a deadlock condition on Windows agents caused by improper recursive locking activity, usually on systems with a large number of CPUs or cores. [51929]

Corrective Content in Bit9 Platform 7.2.3 Patch 3 (Build 3270)

- Addressed an issue in which an AB exclusion included on the shephard_config properties page caused to exclude *all* agent events that were not tied to a file (including health check events). [50725,51073]
- Resolved a system hang that occurred on Windows systems during login when other file system filter drivers were installed and system volume mounting was in progress during load. [51067]
- Resolved an agent issue in which installing a very large number of Windows Updates (100,000+) overfilled the agent log file and caused a crash. The default number of displayed updates in the log is now limited to 15,000. [51068]
- Addressed an issue in which a large number of logins on 'Terminal Server' style machines (Microsoft, Citrix, and others) caused high CPU usage by the agent. [51070]
- Added logic to handle contentions between the Windows agent and some installation tools, such as SCCM, when those tools rename files after they are copied to the endpoint. [51134]
- Addressed an issue in which incorrect product version information on Windows agents could cause both build-to-build agent updates and operating system updates to fail. The most common case showed an agent health check failure with the message, "Agent health check fails for "Cached MSI File[c:\windows\installer\1dad81.msi] does not exist on disk IEID[3].”" [51226]
- Added the powershell.exe process to the definition of the Powershell Script Rule, which previously only included the file association for .ps1 and .psm1 extensions. [51065]
- Corrected a timeout error that occurred when a user navigated to the Event Rules page, selected checkboxes, and clicked the Re-Apply button at the top of the list. [51069]
- Added a missing Set Computer Tags command on the Action menu of the Computers (table) page in the console. [51160]
- Improved the server installer’s ability to find required registry values, addressing an issue that was causing upgrades from 7.2.3 Patch 0 to fail. [51186]
- Expanded tamper protection rules to protect all Carbon Black executables. More information can be found on Cb User eXchange in the DOC-5360. [51501]
- Improved the interaction between the Windows agent and Unidesk by automatically approving files sourced from Unidesk read-only layers. [51564]
- Corrected an issue in which some local approval events on Windows agents were not sent back to the server. [51567]

Corrective Content in Bit9 Platform 7.2.3 Patch 2 (Build 3204)

- Unable to scan the Windows Defender Advanced Threat Protection folder on Windows 10 AU [50664]
    - Details: In the Windows 10 Anniversary Update official release, Microsoft added new files under the Windows Defender Advanced Protection folder. In previous releases, the Bit9 agent was unable to analyze these files to determine and inventory their contents. In this release, the agent has been modified to allow successful analysis and approval of the contents of Windows 10 Anniversary Update ISOs, if you have configured WIM support as described in the section Enabling Trusted Directory Approval of WIM Files on page 8. You must complete this procedure first if you plan to upgrade to the Anniversary Update while in High or Medium Enforcement.
    - Applies to: Server, Agent [Windows]
- Agent binaries not approved by hash in v7.2.3 Patch 1 [50586]
    - When server version 7.2.3 Patch 1 was installed, its agent binaries were not approved by hash and so would block on systems in High and Medium Enforcement on machines that were missing root certificates. This problem has been corrected in this release.
    - Applies to: Server, Agent [All]

Corrective Content in Bit9 Platform 7.2.3 Patch 1 (Build 3116)

- Enabling rules to address .NET execution resulted in blocking all dlls [50491]
    - Details: In the initial release of v7.2.3, several new rules were added that attempted to address a .NET execution bypass. Enabling the blocking versions of these rules through the console caused the rules to malfunction, and they would block all DLLs on the agent-managed systems. In this release, the console issue has been corrected and the rules should work properly.
      Note: When you upgrade to Patch 1, any edits you may have made to these rules will be lost and the rules will be restored to their default configurations. See New Custom Rules on page 10 for a description of the rules.
    - Applies to: Server, Agent[Windows]

- Upgrading to 7.2.3 server, the health indicator will display an error message “The Bit9 Server is missing an important update.” Stating 7.2.2.1116 P2 is available.
    - A new Health Indicator has been released through our cloud service. If your server is not connected to our cloud service, this issue will continue to show the health alert, which can be ignored.
    - Applies to: Server

Corrective Content in Bit9 Platform 7.2.3 Patch 0 (Build 3106)

In this release, numerous defects were addressed, including security issues. The list below is a high-importance subset of those fixes.

- Server patch upgrades failed when attempting to add files [48750]

  - Details: In previous releases, the Server patch installer was not creating new folders needed before it attempted to add certain new files to the product, which caused the patch upgrade to fail. In this release, the required folders are created prior to addition of the new files.
  - Applies to: Install

- The Server no longer sets BITS and Win Update processes to use separate threads [48132]
  - Details: In prior releases, the Bit9 Platform configured the BITS and Windows Update services to use separate svchost.exe instances instead of a single shared one. This caused a system hang when attempting to run Windows Update on Windows 10 systems. This release does not separate the services and configures existing separated instances into a single shared instance to resolve this issue.
  - Applies to: Install

- Console event rule page object 'EventRulesGUI.php' not updated during upgrade [47851]
  - Details: For some server upgrade paths, the Event Rule page in the console was not correctly patched. In this release, the page is updated as expected during a server upgrade, eliminating related issues on that page.
  - Applies to: Server

- Server upgrade fails if the SQL server is more recent version [47902]
  - Details: The server upgrade fails if the SQL server was upgraded to a more recent version and then the Bit9 server was re-installed or reconnected to the database. This due to the COMPATIBILITYLEVEL of the das database is lower than the rest of the databases. This failure has been corrected in this release.
  - Applies to: Server

- Unable to access Bit9 News feed portlet [48017]
  - Details: On Dashboards using the Bit9 News portlet, the old URL, https://www//bit9.com/feed, was not being redirected correctly to the new URL, https://www.carbonblack.com/feed, preventing access to the feed. The link now redirects properly.
  - Applies to: Server

- Wildfire File Analysis test not working for Bit9 Server integration [48498]
  - Details: Pressing the Test button used to test Bit9 Server connectivity to WildFire cloud did not provide accurate results, for example, reporting failure when there was actually a working connection. The test works properly in this release.
  - Applies to: Server

- Rendering of link in navigation panel now corrected [48538]
  - Details: On Chrome and Firefox, the left-hand “Nav” link was displayed upside down. This has been corrected.
  - Applies to: Server

- SQL Configuration document not current with Operating Requirements document [48908]
    - Details: Previous editions of theBit9 Platform *SQL Server Configuration* document were missing information about memory size and SQL memory cap for deployments of 20001 to 30000 endpoints using SQL Server Standard. That information was added to the RAM Configuration table in the latest version of the document.
    - Applies to: Server

- Need both 'Bit9, Inc' and 'Bit9, Inc.' as approved publishers [48984, 49999]
    - Details: On Windows 10 systems, the Bit9 publisher appears in slightly different formats. One is 'Bit9, Inc' (without a period) and the other is 'Bit9, Inc.' (including the period at the end). In this release, both forms are approved publishers, preventing low-level health check failures and eliminating problems with key files appearing to be unapproved.
    - Applies to: Server

- Network Latency discussion restored to SQL Configuration Guide [49051]
    - Details: The *SQL Server Configuration* guide formerly contained a section discussing network latency. It was inadvertently deleted in some editions. The current version restores this section.
    - Applies to: Server

- Live Inventory public database views missing file instances [49064]
    - Details: Previously, some results were missing from the ExFileInstances view in the Live Inventory SDK "bit9_public" schema. This has been corrected.
    - Applies to: Server

- A reboot during a Mac agent upgrade sometimes uninstalls the agent[47572]
    - Details: Under certain conditions, a reboot during a Mac agent upgrade could completely uninstall the agent instead.In this release, the upgrade process has been changed so that reboot does not impact the upgrade in this way.
    - Applies to: Agent [Mac]

- A Kernel Panic could occur with the presence of other security products [47809]
    - Details: When other security products that use kernel extensions are present, and when accessing other file system types other than HFS, it was possible for the Bit9 agent to use too much stack memory, resulting in a double-fault panic. This has been corrected in this release.
    - Applies to: Agent [Mac]

- Mac System Updates updater not enabled by default [48023]
    - Details: In previous releases, the Mac System Updates updater was not enabled by default. It is enabled for new installations in this release. Upgrades to this release will leave the updater in whatever state you had it on your system before upgrade.
    - Applies to: Agent [Mac]

- When the agent is upgrading, the starting version is hard to discover [48425]
    - Details: When a Mac agent upgrades, information is logged in the /var/log/install.log file. In previous releases, this file did not include the version being upgraded *from*. The starting version is now logged during agent upgrade.
    - Applies to: Agent [Mac]

- Under rare conditions, the daemon could crash on shutdown [48636]
    - Details: Under rare conditions, the Bit9 Mac agent daemon process could crash on shutdown. This was due to an unsynchronized access to shared resources in a few thread terminations. This version synchronizes access on shutdown, resolving the problem.
    - Applies to: Agent [Mac]

- Accessing files on a forcibly removed mount point can cause a kernel panic [49483]
    - Details: When a Mac system accessed files on a mount point that had been forcibly removed, a kernel panic could occur due to a race condition. This version of the agent resolves the problem.
    - Applies to: Agent [Mac]

- Adobe Flash Updater may block [49871]
    - Details: An issue with tracking shortlived processes that write files could lead to unexpected blocks of actions take by the Adobe Flash Updater. In this release, process tracking has been improved and these blocks should not occur.
    - Applies to: Agent [Mac]

- Manual shutdown of the agent daemon taking too long to shutdown [50093]
    - Details: Manual shutdown of the Mac agent daemon using "b9cli –shutdown" was taking longer than expected because of a thread cleanup issue. The relevant thread is now cleaned up from the threadpool and now the shutdown works as expected.
    - Applies to: Agent [Mac]

- Reduced kernel memory footprint [47944]
    - Details: A change was made in this release to reduce the kernel memory footprint of the Bit9 agent. This should improve performance and also might avoid crashes on systems where the available memory is already constrained when the agent is started.
    - Applies to: Agent [Windows, Mac]

- Blocks on Google Chrome software_reporter_tool.exe after update [47455]
    - Details: After updates to Google Chrome on Windows, there would be blocks on the Chrome software reporter tool. Improvements to the Google Chrome updater in this release prevent those blocks.
    - Applies to: Agent [Windows]

- Bit9 agent causing BSOD with 1E stop code [47878, 49186]

  - Details: The parity.sys device driver had a flaw that could cause a NULL address to be dereferenced, causing a BSOD with a 1E and c0000005 exception. In this release, the parity.sys driver has been corrected to check the pointer before use. In one occasion, the risk of the BSOD occurring increases with CPU count.
  - Applies to: Agent [Windows]

- Spread out periodic kernel processing [47907]
  - Details: A periodic task in the kernel scheduled every 15 minutes would consume a CPU core for some seconds. On a system with only 1 or 2 cores, this activity could preempt user-initiated activity and make the machine look frozen. In this release, processing is spread out to be less disruptive to the user.
  - Applies to: Agent [Windows]

- Random BSOD (bugcheck 0x50) during normal operations [48308]
  - Details: In rare cases, the agent kernel driver could reference freed memory, resulting in PAGEFAULTINNONPAGEDAREA 50 bugcheck. In this release, a flaw in memory reference tracking has been corrected, eliminating the crash.
  - Applies to: Agent [Windows]

- Random BSOD with stop code 0x7F [48309]
  - Details: When the agent processed long path names, the system could bugcheck with a doublefault stop code 0x7F. In this release, the parity.sys driver has been corrected to avoid using excessive stack when processing long path names.
  - Applies to: Agent [Windows]

- Files blocking after GotoMeeting update [48367]
  - Details: Some files would block after an update to GotoMeeting. The GoToMeeting updater has been improved in this release to prevent those blocks.
  - Applies to: Agent [Windows]

- Blocks seen sometimes after Windows 10 updates. [48412]
  - Details: System files would sometimes block after Windows 10 system updates. In this release, improvements were made to the “Windows 8, 10 and Server 2012 Updates” updater to prevent those blocks.
  - Applies to: Agent [Windows]

- Automatic purge of uploaded files purges diagnostic files but not interesting files [49384]
  - Details: Previously, the option to automatically purge uploaded files from the server deleted only diagnostic files. In this release, it deletes both uploaded diagnostics and any other files uploaded from the inventory.
  - Applies to: Server

- An updater was added for "Microsoft Office 2016" [49552]
  - Details: This release includes a new updater for updates to Microsoft Office 2016.
  - Applies to: Agent [Windows]

- Some default registry rules not created correctly [49731]
    - Details: Some default Registry Rules were not being created correctly, and this prevented them from being sent to the agent. This included a rule intended to make it possible to use Sysprep without disabling tamper protection. In this release, the default registry rules have been corrected and should be send to the agent.
    - Applies to: Agent [Windows]

- Noisy debug event causes loss of more important events [49854]
    - Details: An internal debug event could be generated at high frequency, causing loss of more important non-debug events. That event has been removed in this release.
    - Applies to: Agent [Windows]

- Agent pruning events too aggressively [49867]
    - Details: The agent event pruning logic could prune events before they were sent to the server, which could lead to lack of visibility into blocks and other activity on the agent. In this release, the pruning issue has been corrected.
    - Applies to: Agent [Windows]

- Windows updates fail with error 80070006 [50106]
    - Details: When they were installed, previous versions of the Bit9 Agent would change the service configuration of Windows BITS and Wuauserv services from the default of ‘shared’ to be 'own process'. This reconfiguration caused Windows update failures with error 80070006. Installing this release will set the service configuration back to the default values of 'shared' for BITS and Wuauserv services.
    - Applies to: Agent [Windows]

Known Issues and Limitations

- If you use email notifications for Alerts and Approval Requests, you might see a server email notifier exception with the following message:
  "4.7.0 Timeout waiting for client input exception."
  This exception is caused by temporary mail server overload, and should resolve itself after a short delay. [CBPTR-31032]
- If you are installing the agent manually or via a third-party distribution system and want to specify a non-default data directory, do not choose a data directory that is underneath the main program installation directory. Putting the data directory under the installation directory will cause the agent to malfunction and disconnect. [CBPTR-31463]
- The section Enabling Trusted Directory Approval of WIM Files describes a procedure that involves copying a tool called **ImageX.exe** from a Microsoft download into the agent installation directory. Enabling WIM file approval can be useful in a variety of situations, and it is *required* if you want to leave the agent installed while upgrading to Windows 10 Anniversary Update (and later).

  If you complete this procedure, four different agent health check failures will be reported, both on the Events page of the console and if you view diagnostics directly on the agent system:

  - "Bit9 Agent detected a problem: Install directory File[imagex.exe] has no expected metadata"
  - "Bit9 Agent detected a problem: File[imagex.exe] has unexpected ApprovalReason[...] in InstallDir[...]"
  - "Bit9 Agent detected a problem: Found unexpected interesting file[imagex.exe] in InstallDir[...]"
  - "Bit9 Agent detected a problem: Number of files found in InstallDir[...] Found[...] Expected[...]"

  These messages can be safely ignored. [CBPTR-3078]
- The agent currently tracks all the extracted content from the Windows 10 WIM image in the temp directory. A rule to ignore these writes to is not yet functioning properly. [CBPTR-29899]
- This version of the server does not support Windows Server 2016 or IIS 10.
- Upgrading from the initial release of v7.2.3 (Build 3106) to later versions of v7.2.3 may require the agent service to be restarted if the agent has not been restarted since installing 7.2.3 (Build 3106). If you attempt to upgrade to a 7.2.3 patch release and see the agent upgrade status change to the following, you will need to restart the agent:
  Agent Upgrade: Failed executing <cmdline>

  To correct this problem, go to the Computer Details page for the agent, select **Other Actions** in the right hand navigation panel, and choose **Restart service**. After a few minutes, the agent should re-attempt upgrade and should succeed.

  Note: This issue only affects upgrades to this release from the first released v7.2.3 build. Upgrades from 7.2.2 and earlier agents are not affected. [CBPTR-30192]

- After agent diagnostic files are generated and then uploaded to the server, they are not deleted from the agent system. This can lead to a significant build-up of large, unnecessary files on the agent if diagnostics are requested repeatedly from the same agent. It may be necessary to manually remove diagnostics zip files from an agent in these cases after the files are successfully uploaded to the server. On the Computer Details page for the agent, go to the Advanced section of the right menu bar, and choose **Other Actions > Delete diagnostic files on computer**. [CBPTR-29121]
- Applying a temporary override can cause an agent to disconnect. A temporary workaround is to request the agent to reconnect by the command “dascli connect” at the agent. [CBPTR-29353]
- When rules targeted to a specific user are exported and then imported, the Bit9 Platform sometimes fails to assign the rule to the user on import. If this happens, assign the rule explicitly to the targeted user *after* import. [CBPTR-28119]
- When you run a Custom Rule to test an execution block on an OS X system, the agent may report that the process for the blocked execution is *xpcproxy*. This is a normal condition based on the implementation of the OS X operating system. When creating a rule that applies to applications invoked from the typical launching mechanisms of Finder and/or launched on OS X, it is best to also include */usr/lib/dyld* as a potential parent for the application. [CBPTR-26838]
- The Bit9 Server requires several C++ runtimes in order to operate properly. If the installer detects that the runtimes are not present on your system, it will present a dialog requesting permission to install the required C++ runtimes on the system. Please click the “Install” button to allow the installation of C++ runtimes required by the Bit9 Server. [CBPTR-26385]
- The Administrator Login Account group can be disabled, and if you have not created another group and account with full administrative privileges, you may not be able to access the Bit9 Console interface to re-enable it. To correct this, enter "ParityServer.exe /adminReset" from the command line. Note that this will also restore all admin permissions and the default admin/admin password. [CBPTR-24804]
- After the server is upgraded from v6.0.2 to v7.2.x, a globally defined password for agent management does not work on the command line interface for new agents. For these upgrades, if you used a global password, it must be reset on the General tab of the System Configuration page. [CBPTR-23544]
- Registry Rules that use a path containing links will not work. For example, if you use a path with *HKLM\SYSTEM\CurrentControlSet*, the rule will not work because CurrentControlSet is a link to the other ControlSet(s). To work around this limitation, consider using wildcards in the path to cover all of the cases to which you need to apply the rule; in the example above, you might use *HKLM\SYSTEM\ControlSet** . [CBPTR-23250]
- On Bit9 Console file pages, an underscore at the end of a file name in a search filter is ignored. [CBPTR-14750]
- In rare cases, agent upgrades may be blocked because older Bit9 MSI or MSP packages referenced during upgrade have no global file state. This can occur after a server upgrade from a release *prior to* 6.0.2.228, 7.0.0.1229, or 7.0.1.1109. If you have upgraded from a version prior to those listed, you may have this problem if:
    - Users report that the Bit9 Platform Notifier shows MSI or MSP blocks after you have enabled agent upgrades.

- On the console Events page, you notice multiple file block events for the same MSI or MSP files.
- Agents have an Upgrade Status of "Upgrade Scheduled" but do not ever change to "Up to Date" and have an Upgrade Error of "Agent Upgrade: Unknown error executing" or "Agent Upgrade: Failed executing".

If this situation occurs, do the following:

1. **Turn off automatic agent upgrades:** In the Bit9 Console, go to the **Administration > System Configuration** page and click on **Advanced Options**. On the Advanced Options tab click the **Edit** button at the bottom of the page, in the Bit9 Agent panel, choose **Disabled** on the menu, and then click **Update** at the bottom of the page.
2. **Locally or globally approve the Bit9 MSPs or MSIs that are blocking.**
3. **Turn automatic upgrades back on:** Follow the same procedure as step 1, except choose **Enabled** on the menu.

Note: If you are using a third-party software distribution method to upgrade agents, disable that distribution until you approve the blocking files.

If you encounter this situation and are unsure of whether to approve the blocked files, contact Technical Support.

- If you use the "Export to CSV File" feature on the Computers page, there is a limit of 25,000 on the number of rows that can be exported.
- Some or all memory rules are not supported as follows:
  - Memory rules are not supported on Windows Server 2003 64-bit.
  - Kernel Memory Access rules are supported only on computers running Windows XP or Windows Server 2003 without SP1.
  - Dynamic Code Execution rules are supported only on computers running 32-bit versions of Windows XP, Windows Server 2003, Windows Vista, and Windows 7 operating systems. On Windows XP, if the system-wide DEP Policy is set to "AlwaysOff", dynamic code execution memory rules cannot be enforced, but Bit9 Platform will report as though they were enforced. If the policy is set to "OptIn" (the default) or "OptOut", then these rules will be enforced on systems running XP. [CBPTR-27039]
- On Mac OS X, an interoperability issue exists with certain versions of Trend Micro's endpoint security products. You must run Trend Micro's TMSM version 1.5 SP4 or higher. [CPBTR-19207]
- On Mac OS X and Linux platforms, you cannot disable or replace the Bit9 logo in Notifiers. If you disable the logo, you may observe computer management events indicating "Computer failed to receive Notifier Logo: Source[…/GenericLogo.gif]". These should be disregarded. [CBPTR-19177, CBPTR-17607]
- Symantec Endpoint Protection and Bit9 Platform exhibit a conflict on Mac OS X with regard to Software Update. Some Software Updates are intermittently blocked by Bit9 Platform as a result. If an update is blocked, it can be approved using the Bit9 Console and applied again. To avoid future blocks on other endpoints, each blocked update can be globally approved.

  Software Updates blocked by the SEP/Bit9 Platform interaction produce two events in the Bit9 events log: a Discovery event with a file written by installd followed by an Execution

block (unapproved) event with installd as the process that attempted the execution. [CBPTR-19337]

- When a Custom Rule is used to block writes to a specific file or set of files, and the rule is tested with an editor that creates a backup of the original file, it may appear that the rule is not correctly functioning. This is due to the functionality of certain editors, which may use a rename operation to replace the original file with its backup when any modification is aborted by the user. [CBPTR-20972]
- If the Notifier Link field causes the launch of an application that is not DEP compatible, the application may not launch when the link is selected, even if the associated application is already running. This occurs because Bit9 processes require DEP to be enabled as a security measure. Please contact Bit9 Support for assistance in creating Custom Rules if you encounter this issue. [26943, CBPTR-19416]
- Known interactions with the VMware vShield Endpoint driver (*vsepflt*) can cause systems to deadlock in the presence of other filter drivers, such as Bit9. The *vsepflt* driver may be loaded on a virtual machine, even when vShield is not in use. Permanently disabling or removing the *vsepflt* driver will address this issue. [CBPTR-13447, CBPTR-13842]
- Except for upgrades to Windows 10 Anniversary Update and later, changing the major or minor version of any operating system after installing the agent is not supported, and doing so will produce health check failures and in some cases failure of the upgrade. If you need to upgrade your operating system or you see a health check failure that reports a mismatch between the agent and the build platform, contact Bit9 Support for remediation recommendations. Service pack upgrades are fully supported and do not cause health check failures. See Support for Windows 10 Anniversary Update on page 8 for information about other supported upgrades with the agent in place. [CBPTR-21177]
- For Mac and Linux agents, the default uninstall behavior is now to remove all Bit9 agent data. Previous releases required an additional parameter ("-d") for this data to be removed. The same parameter now *prevents* data removal. [CBPTR-20352]
- On Mac, when *chroot* is used, the patterns for script processors may need to be changed to patterns that will be appropriately matched in the re-rooted environment. For example, in place of "/bin/bash", you may want to use "*/bin/bash". Contact Bit9 Support for additional assistance. [CBPTR-21534]
- Carbon Black Response integration applies only to Bit9 Platform Windows agents. Integration with Carbon Black Response Mac and Linux sensors is not available in this release. [CBPTR-24346]
- SCEP integration with Bit9 Server might not be able to always match quarantined files due to a race condition between the Bit9 Agent hashing the file and SCEP moving the file to a quarantine section. The result is that two hashes could be detected for the same file (original and quarantined file hash) at the same location. The quarantined file hash would be marked as potential risk or malware whereas the original file hash would not. [2237]
- Use of the default read-only memory map operation on banned or unapproved executables by .NET applications rules is recommended. These can be seen under Rules > Software Rules > Custom Rules. Alternative solutions, including the rules suggested for resolving the .NET InstallUtil vulnerability (for example, https://community.carbonblack.com/docs/DOC-3198) should be avoided. Using those rules can risk over-promotion and performance degradation due to a known bug that occurs when setting `*.dll` to be the target of a script rule. [1982]

- After an operating system upgrade from Windows 8.1 to Windows 10, the Bit9 agent may generate health check failures that indicate the kernel driver is not running or enforcing properly. These health check failures should go away after a few hours once the agent detects that the operating system was upgraded and performs a repair install to install the correct version of the driver for the new version of the operating system. [29713]

Contacting Support

For your convenience, support for the Bit9 Platform is available through several channels:

Technical Support Contact Options
Web: User eXchange
E-mail: support@carbonblack.com
Phone: 877.248.9098
Fax: 617.393.7499

Reporting Problems

When you call or e-mail technical support, please provide the following information to the support representative:

Required Information	Description
Contact	Your name, company name, telephone number, and e-mail address
Product version	Product name (for example, Bit9 Server or Bit9 Agent) and version number
Hardware configuration	Hardware configuration of the server or endpoint having the issue (processor, memory, and RAM)
Document version	For documentation issues, specify the version of the manual you are using. The date and version of the document appear on the cover page of most documents and after the Copyrights and Notices section of longer manuals.
Problem	Action causing the problem, error message returned, and event log output (as appropriate)
Problem severity	Critical, serious, minor, or enhancement