Bit9 Security Platform 7.2.2

Release Notes

Product Version *7.2.2.1119*
Patch 2
29 April 2016

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 v7.2.2 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 7.2.2 new and modified features**: This section provides a quick reference to changes in the Bit9 Platform made since Bit9 Platform 7.2.1.
- **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 v7.2.2 that you should be aware of.
- **Contacting Bit9 support:** This section describes ways to contact Bit9 Technical Support, 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 review the "Corrective Content" and the "Known Issues and Limitations" sections carefully.

This release also includes new trusted updaters. See the section "Bit9 Platform v7.2.2: new and modified features" for a list of new and improved updaters for v7.2.2.

Documentation

Your Bit9 Platform documentation set consists of online Help built into the console as well as PDF files included with the product distribution and/or available on the Support Portal. The standard documents include:

- **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

Before you Begin

This section describes preparations you should make before beginning the installation process for Bit9 Server. These include actions you should 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 that applies to upgrades and new installations.

System requirements

The document *Bit9 Security Platform Version 7.2.2 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 v7.2.2* provides the current requirements for systems running the agent. Both are available to customers with login credentials on the Support Portal.

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 v7.2.2. Consult the *Installing the Bit9 Server* guide 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

For more detailed instructions, please refer to *Installing the Bit9 Server*. It is available in the Support Portal.

This section is for upgrades only. If you are not upgrading, see New Bit9 Platform Installations (page 5).

Support for the upgrade process

Bit9 Server and Agent upgrade support is covered under the Customer Bit9 Platform Maintenance Agreement. We recommend contacting Technical Support prior to performing the upgrade for further details on the upgrade process and the latest information that supplements the information contained in this document. Technical Support 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 v7.2.2), 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 process 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. A 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 more details.

Before running the server upgrade

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

- **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 v7.2.2, 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

You should 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 v7.2.2: New and modified features" for a list of new and improved updaters for v7.2.2.
- **Update agent distribution points:** If you use third-party deployment mechanisms (e.g. SCCM), re-enable or re-create them using new agent packages from the upgraded Bit9 Server. Use ParityHostAgent.msi to upgrade from a pre-v7.2.2 agent.
- **Review the new Bit9 Platform installations section:** Although it is for new installations, this section also includes information of possible interest to upgrade customers.
- **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

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

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.

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.
  Note: 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 more 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 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 detailed information 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 v7.2.2 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.

Bit9 Platform v7.2.2: New and modified features

The following sections provide a quick reference to the feature changes made since v7.2.1.

- Some threat Indicator Sets have been upgraded to include 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.
  - Applies to: Server

  See the *Bit9 Platform Events Integration Guide* for details of the QRadar integration.

- Set default size limit for logs [46342]
  - Details: Previously, Bit9 Agent log files were allowed to grow without limit. In this release, the default log rotation size is set to 50 MB. After exceeding this limit, logs are compressed and rotated out. The agent keeps the current "live" log and one old log. This behavior is configurable if you need to capture larger logs; contact Technical Support for details.
  - Applies to: Agent [Windows]

- The following new (in bold) or improved trusted updaters are included in v7.2.2 CD: [47484]
  - Adobe Air
  - **Apple System Performance**
  - Bit9 Agent Tamper Protection
  - Carbon Black Tamper Protection
  - Google Chrome
  - **GoTo Meeting**
  - McAfee Viruscan Enterprise 8.5
  - Webex for Chrome
  - Webex for Firefox
  - Webex for Internet Explorer

- The following new (in bold) or improved trusted updaters are included in v7.2.2 Patch 1:
  - **FlowDock (Mac)**
  - Google Chrome (Mac)
  - Google Drive for Mac
  - GoToMeeting

- The following new (in bold) or improved trusted updaters are included in v7.2.2 Patch 2:
  - Google Chrome (Windows)
  - GoToMeeting (Windows)
  - **Linux System Performance**
  - Mac System Updates
  - **Windows 8, 10, and Server 2012 Updates**

Red Hat / CentOS Agent Support in this Release

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

The Linux agent package is not included in the installer. However, the 7.2.0 Linux agent is compatible with the 7.2.2 Bit9 server. To deploy the 7.2.0 Linux agent, you should download the Linux installer from the Bit9 Customer Portal or the User eXchange, and follow instructions listed below:

1. From the latest 7.2.0 agent, copy these files
   a. b9agent.rpm
   b. b9notifier.rpm
   c. Bit9Redhat6Install.bsx

   into the 7.2.2 server at folder c:\Program Files (x86)\Bit9\Parity Server\hostpkg.
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”.

Corrective Content

Corrective Content in Bit9 Platform 7.2.2 Patch 2 (Build 1116)

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

- 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

- Certificate to communicate with Software Reputation Service (SRS) is expiring [48973]
    - Details: The certificate provided in previous releases to validate communication between the Bit Server and SRS is expiring, which will interrupt the capability to obtain file reputation, threat indicators, and updaters. This release includes an updated certificate that will allow continued SRS-Server communications.
    - Applies to: Server

- Files are not being copied to FireEye to be analyzed [48459]
    - Details: In some cases, file analysis (manual and event-rule based) by a provider that is enabled stops working, stranding files in the queue instead of copying them to the FireEye file share. This occurs when there are more than 1000 pending files waiting for analysis by another provider that is now disabled or removed from the server. In this release, this condition does not prevent analysis by an enabled provider.
    - Applies to: Server

- Compatability failure between existing databases and new 7.2.2 server installations [47902]
    - Details: Some Bit9 Servers experienced problems when doing a database upgrade or reconnect due to a change in database compatibility level. This would prevent upgrade of or reconnection to when compatibility level of the “das” database is lower than the rest of the database (e.g., on the SQL Server 2005 level). This happened when the database version was upgraded to a newer SQL Server on an existing Bit9 database. The issue is fixed in this release.
    - Applies to: Server

- Server upgrade fails if rules have patterns longer than 2048 characters [46918]
    - Details: The config list that stores rules has a limit of 2048 characters per entry. However, the Custom Rules dialog did not limit the length of patterns, and longer patterns could cause server upgrade failure. In this release, validation checks have been added to the Custom Rules Details page to avoid this failure.
    - Applies to: Server

- Microsoft Windows 2003 server will not boot when Bit9 agent is installed [48536]
    - Details: In environments with multiple file system filters installed – for example when other security products or backup systems are installed – a deadlock could occur during system boot if one of those drivers used stream I/O. In this release the issue has been resolved.
    - Applies to: Agent [Windows]

- Kernel queue limit prevents full inventory of files [48450]
    - Details: A messaging limit may have prevented some new files on endpoints from being inventoried when a large number of new files was generated very quickly. The message limit has been removed in this release.
    - Applies to: Agent [Windows]

- Windows 10 updates in the system32 folder blocked [48412]
    - Details: During Windows 10 updates, files in the windows\system32 directory could be blocked. In this release, the Bit9 updater for "Windows 8, 10, and Server 2012 updates" has improved logic to handle ongoing Windows updates.
      Note: If you have machines running these operating systems, make sure that this updater is enabled.
    - Applies to: Agent [Windows]

- Agent causes system crash when processing long path names [48309]
    - Details: When the agent was processing long path names, it was possible for the system to crash due to excessive use of stack space by parity.sys driver. In this release the parity.sys driver has been modifed to avoid using unnecessary stack space when processing a long path name.
    - Applies to: Agent [Windows]

- Agent causes system crash due to memory allocation issue [48308]
    - Details: Previous agent versions could crash due to incorrect memory allocation and release. The issue has been addressed in this release.
    - Applies to: Agent [Windows]

- Reduce kernel memory footprint [47944]
    - Details: An optimization was made in this release to reduce the amount of pageable memory required by the Bit9 agent's kernel driver.
    - Applies to: Agent [All]

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

- Invalid file name information causes file analysis failures [48198]
    - Details: If a process was discovered with an operating system callback intended to notify device drivers of images loaded into a process, the kernel could cache invalid file name information. This caused later file analysis failures and inaccurate information reported to the server. This release includes an additional check to ensure that invalid file name state is not be cached when handling operating system image notify callbacks.
    - Applies to: Agent [Windows]

- Occasional blocks on previously approved files [48117]
    - Details: In previous releases, restarting the agent could lead to multiple copies of the same hash in the agent's inventory, in some cases with different states. This could lead to blocks of previously approved files. This release includes changes to address the issue.
    - Applies to: Agent [Windows]

- Frequent cache check starts causing performance issues on endpoints [47989]
    - Details: Unnecessary cache database consistency checks could run when the same file extension was used in two or more separate script rules. This visibly impacted performance on endpoints. This release corrects the issue.
      Note: In previous releases, the issue could be avoided by making sure there was no more than one script rule with the same target pattern defined.
    - Applies to: Agent [Windows]

- An agent could crash the system due to a NULL pointer in the agent driver [47878]
    - Details: Under rare, conditions, a flaw in internal routines caused the parity.sys driver on Windows agents to attempt to dereference a NULL pointer, which resulted in a system crash. This specific issue has been corrected and the agent has been examined to ensure that other, similar cases do not exist.
    - Applies to: Agent [Windows]

- "Mac System Updates" updater should be enabled by default [48023]
    - Details: In previous releases, the "Mac System Updates" updater on the Updaters page was not enabled by default, leading to blocks when Apple provided updates. This updater is now enabled by default on newly installed instances of the server.
      Note: The enablement state will not be changed on existing instances of the updater. If you are upgrading to this release, confirm that the updater is enabled.
    - Applies to: Agent [Mac]

- Agent on Mac causing kernel panic [47809]
    - Details: In rare cases, the kernel extension could panic with a double-fault, especially in the presence of other security products with kernel extensions, when accessing files on a network share. This issue has been addressed in this release.
    - Applies to: Agent [Mac]

Corrective Content in Bit9 Platform 7.2.2 Patch 1 (Build 799)

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

- Update the Mac Application Behavior indicator set[46985]
    - Details: Additional rules were added to the Mac Application Behavior indicator set in order to detect additional malicious behavior.
    - Applies to: Agent [Mac]

- Update the Mac Shell Activity indicator set [46986]
    - Details: Additional rules were added to the Mac Shell Activity indicator set in order to detect additional malicious behavior.
    - Applies to: Agent [Mac]

- False Tamper Protection events generated by the Bit9 Server Tamper Protection updater [47278]
    - Details: When the Bit9 Server Tamper Protection Updater is enabled, and the agent tamper protection on the server was disabled, false tamper protection events would be generated. These false events will no longer be generated.
    - Applies to: Agent [Windows]

- Built-in alerts for Malicious File Detected and Potential Risk File Detected are not enabled by default [47377]
    - Details: The built-in alerts for Malicious File Detected and Potential Risk File Detected were not active by default in previous releases. These are now enabled by default.
    - Applies to: Server

- The Linux System Performance updater is not enabled by default[47784]
    - Details: The Linux System Performance updater, which was added in the initial release of v7.2.2, is now enabled by default.
    - Applies to: Server

- Avoid deadlocks in the presence of other filter drivers [46775]
    - Details: The system work queue has a fixed number of threads with which to process kernel work items. The combination of a driver which queues numerous items along with the Bit9 filter driver, that needs to finish work on another thread, can cause deadlocks. The Bit9 driver now uses a private thread pool to break the dependency and avoid deadlock.
    - Applies to: Agent [Windows]

- The Windows agent caused the MSI agent to get blocked during upgrade from 7.2.1 Patch 9 [47300]
    - Details: The agent does not detect that the MSI is a Bit9 upgrade if the path to the MSI is not a full path. The agent now detects a Bit9 even with a relative path.
- Applies to: Agent [Windows]

- Files are being blocked after being renamed in both high or medium enforcement [47441]
    - Details: In rare circumstances, the Parity driver would continue to process a file using the old name of the file during a rename operation. This would cause the file analysis to fail and potentially trigger an unwanted file execution block, even for operations that would otherwise be uninteresting.
    - Applies to: Agent [Windows]

- Mac OS X agent could generate assert errors or crash during CL processing [47264]
    - Details: Improperly formatted prints to logs could cause agent crashes when processing invalid config list (CL) entries. Now it will not generate those assert message, and the crash has been fixed.
    - Applies to: Agent [Mac]

- Mac OS X file actions are slower than v7.2.1 Patch 9 or later releases. [47192]
    - Details: File rename, write and delete actions were slower in the initial v7.2.2 version of the Mac OS X agent than they were in the 7.2.1 Patch 9 (or later) releases. The performance issue has been addressed.
    - Applies to: Agent [Mac]

- Upgrading Mac operating system from 10.11.2 to 10.11.3 fails [47467]
    - Details: With the agent installed on Mac OS X 10.11.2, attempts to upgrade the operating system to version 10.11.3 failed. This was due to OS X changing its updater to use system installed instead of the previously used installed.
    - Applies to: Agent [Mac]

- Bit9 Notifier crashes on Mac OS X agents [47806]
    - Details: In some situations, the Bit9 Notifier crashed on agents running on Mac OS X. Previous improvements to our multi-threading neglected to ensure the Bit9 Notifier was fully thread-safe and caused crashes to occur. The crash has been mitigated.
    - Applies to: Agent [Mac]

- When the same file is being modified concurrently by multiple threads, Bit9 could cause a deadlock[46950]
    - Details: Bit9 agent could deadlock a system on extremely rare occasion when a file is being modified concurrently by multiple threads. This issue has been resolved.
    - Applies to: Agent [Windows]

Corrective Content in Bit9 Platform 7.2.2 (Build 515)

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

- Improved Installer handling for remote databases [45526]
    - Details: Error handling related to installations making use of a remote databases has been enhanced to more clearly show connectivity errors in the install logs.
    - Applies to: Installer

- SQL server prerequisite check causes Bit9 Server upgrade to fail [47100]
    - Details: Recent updates to SQL Server changed the format of the SQL Server version number, which resulted in failure of the Bit9 Server installation during the SQL Server version pre-requisite check. In this release, the Bit9 installer will account for the cumulative updates of SQL Server and accommodate the format change.
    - Applies to: Server Installer

- Added expanded logic to help determine connection compatibility for the database for upgrades [44297]
    - Details: The logic that the upgrade wizard uses has been expanded to determine and set the compatibility database connection mode.
    - Applied to: Server Installer

- Health check error for missing key classification on some Windows 2003 systems [46361]
    - Details: In previous releases, an agent health check error similar to the following could appear on Windows 2003 systems: "Bit9 Agent is missing a classification for Key[\systemroot\system32\aepdu.dll]". This error did not have any negative functional impact, but starting in 7.2.2, you should no longer see this error.
    - Applies to: Server

- Agent events are not being seen in the Bit9 Console [44756]
    - Details: If an agent goes back in time, as would be seen when restoring an earlier version of an image, the Bit9 Server would ignore new agent events, considering them duplicates, until the agent's last sent event ID caught up to the server's last event watermark. In this release, both the last sent event ID and its timestamp are tracked, allowing the server to recognize that new events are new, and to handle them properly.
    - Applies to: Server, Agent [Windows]

- Arithmetic overflow in server pre-upgrade script [46504]
    - Details: During a Bit9 Server upgrade, calculations performed by an upgrade script could cause an arithmetic overflow and upgrade failure for databases over 2097 MB. In this release, that error has been eliminated.
    - Applies to: Server

- MSI/MSP Files MSI/MSP Files being blocked despite being approved [45129]
    - Details: Approvals created from the Events page on the console for MSI/MSP files could fail to take effect on the agent. This has been corrected.

  - Applies to: Server

- DailyPruneTask Performance Improvement [47146]
  - Details: A performance enhancement has been added to the daily pruning task, in the location that applied marking the antibody instance groups for deletion.
  - Applies to: Server

- Event rules not saving to specific policy [44792]
  - Details: Under certain conditions, event rules that applied to specific policies were failing to save correctly on the first attempt and were instead saved as applying to all policies. This has been corrected.
  - Applies to: Server

- Last Policy ID field was not exposed for Computers in the Bit9 API [45026]
  - Details: In previous releases, the "last Policy ID" field was not exposed in the Bit9 API for Computer objects. In this release, the field is available, allowing clients using the API to revert computers back to their previous policies after a lockdown.
  - Applies to: Server

- Customized health indicator text depending on the current version of SQL server [45137]
  - Details: The descriptive text for the health indicator "SQL Server Protocol" has been modified to be dynamically produced depending on the type of SQL Server native client installed.
  - Applies to: Server

- Multiple attempts to submit files to WildFire [44900]
  - Details: In previous releases, failed uploads of files submitted for analysis by WildFire could retry indefinitely. This can be seen in the Reporter log with the message: "File MD5 hash not matched against WildFire MD5 hash". In this release, upload retries are prevented after a limited number of attempts.
  - Applies to: Server

- Unable to make agent config changes via the console on the support page [44805]
  - Details: In some previous versions of the Bit9 Server, agent configuration changes made through the console Support page were not saved. This release corrects the problem.
  - Applies to: Server

- Reinstall of server on hardened IIS systems fails [44993]
  - Details: When an IIS deployment is hardened, backup folders for the Bit9 Server are often set to be read-only. This caused attempts to reinstall the server to fail. In this release, the Bit9 installer will change the permissions of these folders when needed.
  - Applies to: Server

- Failure to identify/remove server stats properly causes server upgrade failure. [47222]
  - Details: The Bit9 Server upgrade installer was failing to properly identify and remove an existing statistic from a database table prior to altering the table, which caused

the upgrade to fail in the database migrate script. In this release, the failure should not occur.
    - Applies to: Server

- Server upgrade failure due to reference constraint [46166]
    - Details: Upgrades to Bit9 Server v7.2.1 or later could fail when the installation had pre-7.0 versions in its upgrade history and the following error message was present: A critical database script 'migrate' needed to install Bit9 Server failed with an error. The DELETE statement conflicted with the REFERENCE constraint "FK_console_DashboardPortlets_Portlets". This issue has been corrected.
    - Applies to: Server

- Server upgrade does not capture timestamp for individual scripts [45527]
    - Details: In previous releases, the server upgrade captured a timestamp only for the time the upgrade information was copied to the install log. In this release, server upgrade logging includes timestamps for the execution of each SQL statement.
    - Applies to: Server and Agent

- Blocks on files with missing hash [45639]
    - Details: If Bit9 is unable to hash a new file, the file is treated as unapproved. In this release, if Bit9 is unable to hash a file, an event will be generated indicating the reason why the hash was not obtained.
    - Applies: Agent [Windows]

- File events missing process information [47093]
    - Details: In some cases, Bit9 can be delayed in analyzing a new file. In past releases, if the writing process exited before the new file was processed, Bit9 sometimes discarded the process information and did not record it in related events. In this release, the process information is kept until analysis is complete.
    - Applies to: Agent [Windows]

- File is blocked because path normalization issue prevents hashing [46218]
    - Details: In previous releases, file operations, such as hashing, could fail due to NT token impersonation level errors. The Bit9 Agent has been modified to re-try the file operations under these circumstances.
    - Applies to: Agent [Windows]

- Agent behavior unpredictable if both agent database and backup become corrupt [46754]
    - Details: If both the agent database (cache.db) and agent database transaction log (cache.db-journal) became corrupt, it was possible for the agent to get into a state where the cache.db file was recreated but zero-length and unwritable. Without a database, agent behavior is unpredictable (each file accessed is seen as new, events can't be reported, etc.). In this release, the agent's resiliency has been improved so that it can recover from more scenarios in which the database is corrupt.
    - Applies to: Agent [Windows]

- Agent causing system crash [45132]
    - Details: In a prior release, a required lock on the agent was missing, creating the potential for a system crash (BSOD). In this release, the lock is properly acquired.
    - Applies to: Agent [Windows]

- Agent taking a long time to complete initialization [45619]
    - Details: In this release, agent initialization times should be noticeably faster when performance optimization rules are used to avoid initialization of certain volumes/directories. A side effect of this improvement may be an under-reporting of how far agent initialization has progressed, and a slightly less accurate "initialization percent complete" status in the console.
    - Applies to: Agent [Windows]

- B9_CONFIG or B9_NOCONFIG must be selected on agent install [46611]
    - Details: When doing a command line, fresh installation of the non-branded Bit9 Agent, one of the parameters B9_CONFIG or B9_NOCONFIG must be specified. However, in this release, these no longer need to be specified when *upgrading* an agent, and will be ignored if they are set on an upgrade.
    - Applies to: Agent [Windows]

- Bit9 Agent is not displaying custom logo in notifier window [44338]
    - Details: If a custom logo was specified for a notifier and the agent was unable to download the specified image before restarting, the agent would continue to use the default Bit9 logo on subsequent notifications and not make any further attempts to acquire the specified logo. In this release, the image download location is stored locally, which allows the agent to continue attempting to download the logo after restarting.
    - Applies to: Agent [Windows]

- Bit9 is tracking Carbon Black file activity [44722]
    - Details: The Bit9 Platform includes a default performance optimization rule designed to ignore activity by Carbon Black on Mac systems. This rule was not being applied properly by the OS X agent in past releases, but is fixed in this release.
    - Applies to: Agent [Mac]

- Bit9driver not part of COM Infrastructure service group [46786]
    - Details: Previously, Bit9 agent was not part of the correct Windows service group. This would allow processes such as *trustedinstaller* to write files before Bit9 was active, causing them to be marked as unapproved. In this release, the problem is avoided by making Bit9 a member of the "COM Infrastructure" service group.
    - Applies to: Agent [Windows]

- System process on Citrix VDI endpoint is continuously busy on 1 CPU [47095]
    - Details: An interoperability problem was found with Citrix VDI that could lead to the Bit9 Agent getting stuck and consuming a lot of CPU. This was caused by the Citrix product returning a non-standard error code when a registry key that didn't exist

was deleted. In this release, the Bit9 Agent works around this issue and will no longer get stuck trying to delete keys that don't exist.
    - Applies to: Agent [Windows]

- It is possible to create bans that terminate critical processes [46753]
    - Details: If a policy was configured to terminate processes with banned images, a poorly chosen rule or file ban could have the Bit9 Agent terminating critical system processes such as the system process, which when terminated will take the system down with it. In this release, the agent refuses to terminate any process deemed critical by the operating system.
    - Applies to: Agent [Windows]

- Duplicate "File approval (local approval)" events for the same file [45565]
    - Details: While in local approval mode, if a pre-existing file was moved or copied multiple times, "File approved (local approval)" events were created for each instance of the file. In this release, the events are created once per hash. If the file is created elsewhere or moved around, only the first filename with that hash will generate this event.
    - Applies to: Agent [Windows]

- High memory use during cache DB cleanup [44873]
    - Details: Prior versions of the Bit Agent stored temporary data in memory for database cleanup (VACUUMING). A large cache file would consume a large amount of memory, in some cases crashing the agent (parity.exe). In this release, the temporary data is stored on disk.
    - Applies to: Agent [Windows]

- Increased occurrence of Execution Block (still analyzing) events [45628]
    - Details: Systems under high load might experience an increase in unanalyzed block events, "Execute Block (still analyzing)". In this release, changes were made to reduce the incidence of unanalyzed blocks. They can still occur in some scenarios but should do so at a much lower frequency then past releases.
    - Applies to: Agent [Windows]

- Install failing on Windows 10 after Microsoft KB 3081455 installed [46741]
    - Details: Installation of Microsoft KB 3081455 was causing failure of the agent installer on Windows 10 systems. The agent installer has been modified in this release to handle this Microsoft update.
    - Applies to: Agent [Windows]

- Kernel exclusions don't help with slow network transfers [46867]
    - Details: When internal configuration properties were set to ignore all activity over the network, not all network access was actually ignored. This could result in slower network access or blocks on network files. The internal network exclusions now cover all network-based access.
    - Applies to: Agent [Windows]

- Multiple crashes due to malformed .msi file [45183]
    - Details: If a malformed MSI file contained blank filename entries in its install list, agents attempting to analyze the MSI caused their hosts to crash. In this release, this condition is safely handled without causing a crash.
    - Applies to: Agent [Windows]

- Modification of '..\carbonblack\upgrade\upgrade.exe' blocked because of tamper protection [45598]
    - Details: If a rule exists that prevents file deletion, but it has exclusions, it is possible for a delete operation that was allowed due to the exclusion to be falsely reported as the being blocked by a process that was not excluded. This was most commonly seen when using additional third-party software such as Symantec Norton antivirus. The Bit9 Agent has been corrected to not report invalid file delete block events.
    - Applies to: Agent [Windows]

- Notifier does not display on Citrix VDI machines [45802]
    - Details: On Citrix VDI machines, the Bit9 notifier did not display properly in some cases. The agent was not correctly identifying the user's session. In this release, the notifier should display properly under these circumstances.
    - Applies to: Agent [Windows]

- Bit Agent crashes at service start [47176]
    - Details: Certain invalid certificate co-signer information for a file would cause the Bit9 Agent process parity.exe to crash. In this release, the agent checks if the co-signer valid and does not use the information if it is invalid.
    - Applies to: Agent [Windows]

- Bit9 Agent repeatedly crashes on startup [46521]
    - Details: If an endpoint was misconfigured such that is generated large numbers of logon sessions, the agent would crash from a memory problem when listing the logon sessions. In this release, a change in memory handling avoids the crash.
    - Applies to: Agent [Windows]

- Server won’t install with .NET 4.6 [46393]
    - Details: Bit9 Server can be installed with .NET Framework 4.5 or 4.6 on the system. However when the server checked the version, only .NET 4.5 was accepted, and .NET 4.6 would cause the installer to exit. In this release, both versions are considered valid by the installer.
    - Applies to: Installer

- Support additional versions of TLS [45090]
    - Details: Previously, the Bit9 Platform only supported communication using TLS 1.0 and SSL 3.0 security protocols. In this release, support has been added for SSL 2.0, TLS 1.1, and TLS 1.2.
    - Applies to: Agent [Windows]

- Treat the system drive as non-removable [46155]
    - Details: In past releases, no removable drives were initialized by Bit9. If the operating system was installed on a removable drive, this resulted in blocked OS files. In this release, if the OS is installed on a removable drive, the drive is treated as a fixed drive and its files are initialized, preventing these blocks.
    - Applies to: Agent [Windows]

- Whitespace in agent config properties causes parsing errors [45091]
    - Details: The presence of trailing whitespace in agent configuration properties could cause parsing errors for some properties. In this release, agent configuration properties submitted via the Bit9 Console will have any trailing whitespace trimmed.
    - Applies to: Server

- Windows 10 hangs with a black screen on shutdown [46729]
    - Details: Because of a service tracking problem in the operating system, Windows 10 systems running the Bit9 Agent would hang on shutdown. In this release, service tracking is not used on agents running on Windows 10, and the “Service created” and “Service deleted” events will not appear.
    - Applies to: Agent [Windows]

- Windows agent occasionally spikes CPU [45031]
    - Details: Processing of files for analysis could occasionally trigger a busy loop that caused the agent to use most of a single CPU. The error that caused this condition has been corrected.
    - Applies to: Agent [Windows]

Known Issues and Limitations

- When a temporary overide is generated for an agent, it causes the agent to disconnect. A temporary workaround is to request the agent to reconnect by the cmmand “dascli connect” at the agent. [49290]

- 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. [47500]

- 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. [47068]

- 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.[43766]

- 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. [40145]

- 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. [38051]

- 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** . [37562]

- On Bit9 Console file pages, an underscore at the end of a file name in a search filter is ignored. [18103]

- 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 the **Update** button 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 in a Bit9 Platform table (such as 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 on certain Windows based operating systems:
  - 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 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. [45494]

- On Mac OS X, an interoperability issue exists with certain versions of Trend Micro's endpoint security products. You must be running Trend Micro's TMSM version 1.5 SP4 or higher. [26565]

- On 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. [26502, 24017]

- 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 Platform 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. [26825]

- 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. [29917, 33147]

- On Linux systems, the *ext3* file system does not perform journal checksums, which can lead to file system corruption when the disk controller is using out-of-order write caching. In some circumstances, this can lead to corruption of the Bit9 Agent database. In order to avoid this, the option "*barrier=1*" must be added to /etc/fstab for all *ext3* file systems.

- 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, 26971]

- 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. [33719, 34411]

- 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. [33646]

- 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. [28824]

- 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. [34305]

- Carbon Black integration applies only to Bit9 Platform Windows agents. Integration with Carbon Black Mac and Linux sensors is not available in this release. [39284]

Contacting Support

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

Technical Support Contact Options
Web: Carbon Black (Bit9) Support Portal
E-mail: support@carbonblack.com
Phone: 877.248.9098
Fax: 617.393.7499
Hours: 8 a.m. to 8 p.m. EST

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, Bit9 Agent, or Bit9 Software Reputation Service) 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