Bit9 Security Platform Version 7.2.0

Release Notes

Bit9 Security Platform v7.2.0.2227
Patch 14
9 October 2015

Bit9, Inc.
1100 Winter Street, Waltham, MA 02451 USA
Tel: 617.393.7400 Fax: 617.393.7499
E-mail: support@bit9.com
Web: http://www.bit9.com

Introduction

The *Bit9 Security Platform v7.2.0 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 7.2.0 new and modified features**: This section provides a quick references to changes in the Bit9 Platform made since Bit9 Platform 7.0.1.
- **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 Bit9 Platform v7.2.0 that you should be aware of.
- **Contacting Bit9 support:** This section describes ways to contact Bit9 Technical Support and the information to have prepared to 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 and documentation files. The 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.

Documentation

Your Bit9 Platform documentation set consists of online Help built into the Bit9 Console and additional documents in PDF format available on the Bit9 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 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 Platform Console user interface.

Before you begin

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

System requirements

The document *Bit9 Security Platform Version 7.2.0 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 v7.2.0* provides the current requirements for systems running the agent. Both are available on the Bit9 Support Portal.

Please note that v7.2.0 no longer supports servers on Microsoft Windows 2003 operating system. Agents on Microsoft Windows 2003 continue to be supported.

Both upgrade and new customers should be sure to meet the requirements specified in these documents before proceeding.

Additional downloads

This section contains links to download additional software that may be required to install Bit9 Platform version v7.2.0. 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 2008 Express (R2 SP1):

http://www.microsoft.com/en-us/download/details.aspx?id=26729

Bit9 Server upgrades

Bit9 Server upgrades are supported from the following Bit9 Server versions to this 7.2.0 patch:

- V6.0.2.449 Patch 17
- All 7.0.0 GA and Hotfix versions
- All 7.0.1 GA and Hotfix versions

For more detailed instructions, please refer to the *Installing the Bit9 Server* guide. It is available on the Bit9 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. Bit9 recommends 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 v7.0.0 to v7.2.0), ongoing enhancements to "interesting" file identification make it necessary to rescan the fixed drives on all Bit9-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 now 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. Bit9 recommends a gradual upgrade of agents 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 the Bit9 Server database:** Backup the database for your Bit9 Server before you begin the upgrade process. Built-in backup is disabled during upgrade and must be re-enabled once you are sure the upgrade was successful.
- **Backup certificates separately:** In v7.2.0, the 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.x, all Bit9 Platform certificates, on a system other than the 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 the Bit9 Server for upgrading agents; or disable the Bit9 Server from upgrading agents, and use your third party deployment mechanism to upgrade the agents.

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, 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. Note in particular these updater changes:
    - In Parity 6.0.2, there were separate updaters for Java Virtual Machine only and for Java and Bundled Software. In Bit9 Platform v7.0.1 and later, there is a single updater called **Java** that replaces both of these, and when enabled, allows updates to Java and related bundled software.
    - The SMS Software Approval updater has been removed because Microsoft SMS has reached its end of life. The replacement product is Microsoft SCCM, for which there is an updater shown in the Bit9 Console.

- **Enable Indicator Set updates:** This release of the Bit9 Security Platform v7.2.0 includes threat detection Indicator Sets equivalent Bit9 Detection Enhancement version 1.2. There is an automatic update mechanism on the Bit9 Server that uses Bit9 SRS to deliver the latest Indicator Sets if you have enabled SRS and also enabled automatic Indicator Set updates on the System Confirmation/Advanced Options page (enabled by default in v7.2.0). Especially if you are running Bit9 Detection Enhancement version 1.3 or later, you should enable this automatic update after installing the new Bit9 Security Platform to bring the Indicator Sets up to the current version. If you choose not to or cannot use cloud-based updates on your server, you may download the latest Indicator Sets from the Bit9 Customer Support site.
- **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-v7.0 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.

New Bit9 Platform installations

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

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 the account for Bit9 Server installation:** Bit9 recommends that you use a Domain Service Account 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 be assigned Local Administrator privileges on the Bit9 Server.
  Note: Do not change the permissions level of the account with which you install Bit9 Server after installation.
- **Review .NET configuration:** If Microsoft .NET 4 is installed on your Bit9 Server system with Windows 2008 Server, ensure that the IIS DefaultAppPool is set to use ".NET Framework v2.0.50727" by default.
- **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 Bit9 Technical Support. 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 the *Using the Bit9 Platform* guide (or online help) for more details.

Prepare for post-installation tasks

- **Enable Bit9 Agent 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 the *Using the Bit9 Platform* guide (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 be either by Local System or by 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:** The Bit9 Server allows you to use user-supplied certificates for Bit9 Agent-Server communication. To validate this certificate, each agent system must have up-to-date root certificates. Bit9 recommends that you test your new certificates before large-scale Bit9 Agent deployment begins. See "Securing Agent-Server Communications" in the *Using the Bit9 Platform* guide 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 should be configured to exclude the following from on-access scanning: Please refer to the *Using the Bit9 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 Bit9 Agents – contact Bit9 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 the Bit9 Agent pre-installed requires additional steps on the master system. Please consult the "Managing Virtual Machines" chapter in the *Using the Bit9 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 Bit9 Support for more information.

Bit9 Platform v7.2.0: New and modified features

The following sections provide a quick reference to the feature changes made since v7.0.1.

Product Name Changes

Bit9 Parity is now the Bit9 Security Platform. The user interface for version 7.2.0 has been updated to reflect this and related product name changes. These updates include product identification in the console, notifiers, and user documentation, as well as in some file names. Certain file and service names were left unchanged where necessary to facilitate smooth upgrades from previous versions. The following table summarizes key name changes in v7.2.0:

Previous Name	New Name
Parity	The Bit9 Security Platform - or – Bit9 Platform
Parity Server	Bit9 Server
Parity Agent	Bit9 Agent
Parity Console	Bit9 Console
Parity Knowledge Service	Bit9 Software Reputation Service (SRS)

Carbon Black Integration

Bit9 now provides basic integration with Carbon Black version 4.2. This includes the following:

- configuration of connection to a Carbon Black server from the Bit9 Server
- reporting of Carbon Black Watchlist Events on the Bit9 Server
- reporting of Carbon Black sensor status on computers running the Bit9 Agent
- reporting of Carbon Black data for files in the Bit9 Server inventory
- optimizations for coexistence of a Carbon Black sensor and a Bit9 Agent on the same computer
- protection of the Carbon Black sensor from tampering with optionally enabled Bit9 Agent “updater”

Checkpoint Integration

The Bit9 Connector now includes Bit9 for Check Point, which integrates the Bit9 Server with Check Point firewalls and Check Point Threat Emulation Services (local and cloud). This feature, which requires a Bit9 Connector license, allows the Bit9 Server to receive alerts (notifications) from Check Point firewalls, and allows Bit9 Console users to send files to Check Point for analysis. Users can easily scope and investigate Check Point firewall alerts, immediately identifying where malware may have spread across the enterprise, and rapidly investigate with historical data.

Splunk Integration for Data Analytics

Bit9 can now export data for external analytics use. In v7.2.0, this feature is the basis of an analytics integration with Splunk, allowing users to send configurable types and amounts of Bit9 data to a Splunk server, where the data can be monitored, analyzed, and visualized. With this integration, data from a Bit9 Server can be combined with data from other sources, including other Bit9 Servers, for more complex data analysis. In addition, the Splunk App for Bit9 is available for use on the Splunk console, providing pre-configured reports for Bit9 Data.

Additional Agent Operating Systems Support

Bit9 Version 7.2.0 now supports two additional Windows operating systems, Windows 8.1 and Windows Server 2012 R2.

Beginning with Patch 2, Bit9 version 7.2.0 supports agents on Red Hat and CentOS Linux endpoints.

Beginning with Patch 5, Bit9 version 7.2.0 supports agents on OS X 10.10 (Yosemite) endpoints.

See the *Bit9 Agent Supported Operating Systems v7.2.0* for this release for more information.

Procedures to Upgrade to OS X 10.10

There are two ways to upgrade Mac agents to OS X 10.10 (Yosemite):

Procedure 1: Complete Uninstall / Reinstall of Bit9 Agent

1. Uninstall the Bit9 agent.
2. Upgrade the operating system to OS X 10.10.
3. Reinstall the Bit9 agent.
4. Wait for the Bit9 agent to initialize.
5. This will result in two instances of the Bit9 agent on the server. From the console, remove the original instance of the agent.

Procedure 2: Disable/Enable the Bit9 Agent

1. From the Bit9 console, disable the Bit9 agent by moving it to a disabled mode policy.
2. Wait for the agent to confirm it is disabled by running
   "/Applications/Bit9/Tools/b9cli –status".
   NOTE: Starting the upgrade when the Bit9 agent is not disabled can corrupt the database requiring an uninstall/reinstall of the agent.
3. Upgrade the operating system to OS X 10.10.
4. From the Bit9 console, enable the Bit9 agent.
5. Wait for the Bit9 agent to initialize.

Additionally you would need to make sure you have downloaded the latest version of the "Mac App Store Downloads" updater which was delivered through our Software Reputation Service.

Mac Agent Enhancements

The Bit9 Agent for Mac has been enhanced for v7.2.0. Among the enhancements is improved protection against tampering with and disabling the agent, which protects Bit9 and other critical processes on the endpoint even when an end user is running with root permissions.

The agent installer for Mac endpoints is now distributed as a standard OS X installer package (.pkg) contained in a disk image (.dmg)

Threat Detection Enhancements

Bit9 Security Platform v7.2.0 includes built-in Advanced Detection features formerly available as an add-on installation. Bit9 Detection uses Advanced Threat Indicators (ATIs) to identify suspicious or malicious files and actions on an endpoint, and reports threat events to the Bit9 Console.

In addition, Bit9 customers with an SRS subscription now receive Bit9's Threat Intelligence Service. Updates to threat indicators are now pushed from Bit9, keeping every client as up-to-date as possible in the ever-evolving threat landscape.

Enhancements to Bit9 Alerts

Bit9 v7.2.0 now allows customers to create custom alerts based on any event or event rule. All alerts can also be configured with threshold criteria, including time period criteria. Alerts may now be configured on:

- Any event
- Any custom event filter
- Any existing Event Rule

Termination of Banned Processes

Beginning with v.7.2.0, you can configure policies so that banned files on computers in those policies are not only prevented from future execution but are stopped if currently running. This capability provides better control over software in your environment. Because this capability can interrupt important processes or even prevent a computer from running at all, it is configurable per policy, and can be tested in Report Only mode (the default setting) before being fully enabled.

File-Signing Certificate Management

Visibility and management of individual file-signing certificates has been introduced in v7.2.0. Bit9 Certificate Management includes the following specific features:

- In the console menu, you choose **Assets > Certificates** to open the Certificates table page. The Certificates table shows all leaf certificates that have been used to validly sign or cosign files found on agent-managed computers, plus all certificates in the paths for those leaf certificates.
- Clicking on the View Details button next to a certificate in the Certificates table opens the Certificate Details page for that certificate.
- On the Publisher Details page for each publisher, there is an All Certificates for This Publisher panel. This panel shows all certificates that have this publisher name as the CN portion of the certificate Subject Name.
- Certificate-related fields are included on File Details and File Instance Details pages.
- On the Advanced Options tab of the System Configuration page, the Certificate Options panel includes settings that determine what requirements (such as key length and algorithm) a certificate must meet if it is to be used for approving files.
- Certificate-related Events and Alerts may appear when triggering conditions occur.

Event Rules

Event Rules, which were part of the Bit9 Connector in previous releases, are now a standard feature in the Bit9 Platform v7.2.0. With an event rule, you can automatically take certain actions, such as approving, uploading, or sending files for analysis, when specified events occur. File uploading and analysis require an additional license.

Automated Approval Request Workflow

Bit9 Platform (Parity) v7.0 introduced Approval Requests, which allowed an end user who received a blocked file notifier to notify a Bit9 Platform administrator of his or her reasons to have certain software approved. In Bit9 Platform v7.2.0, you can automate the management of these requests by configuring event rules that automatically resolve a request when certain events, like an approval or ban for the file, occur.

Enhanced VDI Handling

Bit9 provides easy provisioning of virtual machines with the Bit9 Agent installed, faster deployment of cloned images to a large number of users with optimized initialization, and quick retirement of images once they are reverted to a snapshot or deleted from the VM infrastructure. In v7.2.0 you will find usability and scalability improvements, including the ability to choose whether to inventory all or only newly appearing files on clone computers.

Enhanced Agent Health Checks

Bit9 v7.2.0 includes additional agent health checks, which provide granular information regarding the health of each agent computer. An administrator can see the health status and all recent health check events for each agent.

Mac OS X 10.9 (Mavericks) Support and Anti-Virus Software

If you run anti-virus software, you should exclude the Bit9 agent installation directories from anti-virus scanning. If you are running OS X 10.9 (Mavericks) or later, the location of the Bit9 *kernel extension directory* has changed. For Mavericks and later, exclude **/Library/Extensions/b9kernel.kext** from scanning.

For earlier OS X releases, you can use the kernel extension path documented in the "Managing Computers" chapter of the *Using Bit9 Security Platform* guide. All of the other Bit9 directories remain the same for all OS X versions.

Corrective Content

Corrective Content in Bit9 Platform 7.2.0 Patch 14 (Build 2227)

- Bit9 Console could not be deployed on IIS during reinstall of Bit9 [45033]
  - Details: When the Bit9 database was migrated to another database server, the server reinstallation process failed with the error "IIS: Bit9 Console could not be deployed on IIS". In this release, the "read only" attribute was removed from certain backup folders, which eliminated the cause of this error condition.
  - Applies to: Server
- Blocks occur on files that are approved by reputation [45119]
  - Details: Some files were blocked due to reputation not being retrieved from Bit9 SRS (Software Reputation Service). The blocked files were shown as having no instances, even as the actual number of instances increased. In this release, the file count listed by Bit9 correctly increases as actual number of instances increases.
  - Applies to: Server
- Blocks occur on files that are approved by policy [45122]
  - Details: In some cases, Microsoft software packages (.msi files, .msp files) were not being approved. Related files would block in high enforcement or would prompt in medium enforcement. In this release, a race condition causing this problem has been eliminated.
  - Applies to: Server
- System crashes on Windows endpoints [45379]
  - Details: In some cases, exhaustion of the memory pool caused system crashes on some Windows endpoints. In this release, the conditions causing the memory pool to be exhausted have been eliminated and the crashes do not occur.
  - Applies to: Agent [Windows]
- Connector and file upload features missing when incremental Bit9 license is used [45563]
  - Details: When an incremental license for Connectors or File Uploads was applied to the Bit9 Server, the features were not being enabled. In this release, the Connector and File Upload features become fully functional when an incremental Bit9 license is applied.
  - Applies to: Server
- Agent crash sometimes coincident to Bit9 7.2.0 P11 upgrade [45937]
  - Details: When agents were upgraded to 7.2.0 P11, system crashes occasionally occurred. In this release, memory buffering has been improved to prevent conflicts with third party applications, which was the cause of the crashes.

    Applies to: Server
- Bit9 agent appears to cause performance lag on Windows 8.1 endpoints [46061]
  - Details: On Windows 8.1 systems running the Bit9 agent and certain attached USB devices, system performance degraded when users typed on the keyboard. This was caused by the agent querying for device metadata on storage devices that did not have a recognized file system. The agent has been modified to eliminate this query and avoid this performance issue.
  - Applies to: Agent [Windows]

Corrective Content in Bit9 Platform 7.2.0 Patch 13 (Build 2101)

- Downloads of interesting files can fail to complete, resulting in file blocks [45659]
  - Details: A problem was identified whereby the agent could compute the hash of a file that was still being written to, which resulted in an incorrect hash and blocking of the file. In this release, this problem has been addressed.
  - Applies to: Agent [Windows]

Corrective Content in Bit9 Platform 7.2.0 Patch 12 (Build 1824)

- Unexpected file block occurs followed by file approval [43679]
  - Details: On rare occasions, some files were blocked due to a failed request for global state information, and then approved when the information became available. To provide a better explanation of such blocks, that agent now generates an event when a request for global information from the server fails.
  - Applies to Agent [Windows]
- Some WebEx update files that should be approved are being blocked [43800]
  - Details: A change in the WebEx installation procedure resulted in the Bit9 file approval process not approving subordinate files in the installed package. In this release, the WebEx updater was redesigned to approve all WebEx update installation files.
  - Applies to: Server
- Large diagnostic package not visible in Data Sync Admin tool [44261]
  - Details: Agent diagnostics files were not available for download using the Data Sync Admin service. This was due to the agent diagnostics files not being reported to Bit9 Software Reputation Service (SRS). In this release, the agent diagnostics files are correctly reported to SRS and become accessible via the Data Sync Admin tool.
  - Applies to: Server
- Agent locks up in rare cases when CTL-ALT-Del entered after moving to low enforcement [44320]
  - Details: It was determined that agent lockups have occurred when input/output was initiated during a code thread exit, requiring an agent reboot. In this release, this condition does not occur and the agent does not lock up.
  - Applies to: Agent [Windows]
- Starting Carbon Black service occasionally fails after reboot with Error 1053 [44511]
  - Details: After upgrading to Bit9 7.2.0.1645 and Carbon Black 5.0.1.5041, attempts to start the Carbon Black service via services.msc following a reboot resulted in Error 1053: “The service did not respond to the start or control request in a timely fashion”. This was due to an interaction with the Carbon Black Tamper Protection “updater”, which is enabled by default, and was only seen with Carbon Black 5.0.1.5041 sensors. In this release, starting the Carbon Black service after reboot will not encounter the condition that caused the error.
  - Applies to: Agent [Windows]
- Invalid filename causes system crash on endpoint [44752]
  - Details: In rare cases, Bit9 allowed a filename that did not contain a valid Unicode string to be sent to Windows run-time library routines, which resulted in a system crash. In this release, file names must contain a valid Unicode string before Bit9 sends them Windows routines.

- Applies to: Agent [Windows]

Corrective Content in Bit9 Platform 7.2.0 Patch 11 (Build 1750)

- Random blocks on Windows system files after upgrading to 7.2.0 Patch 10 [44564]
  - Details: Upgrades to 7.2.0 Patch 10 resulted in occurrences of random Windows system files being blocked. In most instances, the hashes displayed for these files were blank. In this release, the issue that caused the blocks of Windows system files has been eliminated.
  - Applies to: Agent [Windows]

Corrective Content in Bit9 Platform 7.2.0 Patch 10 (Build 1742)

- Crash or loss of connectivity following upgrade from 7.0.1 to 7.2 [43259]
  - Details: Following an agent upgrade to v7.2.0, systems ran out of memory, causing the agent to disconnect from the server or crash. In this release, the amount of memory used by the upgrade process for large databases has been reduced to prevent memory overflow, and memory leaks related to this issue have been identified and resolved.
  - Applies to: Agent [Windows]
- Link from External Notifications page to Computers page fails with HTTP 400 error [43557]
  - Details: If the number of computers on the Computers page was large, clicking on a hyperlink to that page from the External Notifications page caused the error message: “Bad Request – Request Too Long; Http Error 400. The size of the request headers is too long”. In this release, the error no longer occurs.
  - Applies to: Server
- False alert for Bit9 Software Reputation Service Unavailable [43778]
  - Details: The Bit9 Software Reputation Service Unavailable alert was falsely triggered due to a rare race condition when the count of new files was low. In this release, that race condition does not occur and the false alert does not trigger.
  - Applies to: Server
- Console displays HTTP 500 errors after upgrade from 7.0.1. HF50 to 7.2.0 Patch 8 [43802]
  - Details: After the server was upgraded from build 7.0.1.15001 to 7.2.0.1559, HTTP 500 errors occurred preventing access to the Bit9 Console. Updated versions of certain Microsoft runtimes were not being installed automatically by the Bit9 installer. In this release, the Bit9 installer successfully installs the required Microsoft runtime versions, and the HTTP 500 errors do not occur.
  - Applies to:
- Agents show upgrade from 7.0.1 P13 is blocked [43927]
  - Details: Upgrading from 7.0.1 Patch 13 to a later 7.0.1 patch (20) resulted in the database not being accessible. After restoring the database, the console showed “upgrade blocked’ as status for all agents. In this release, upgrades from 7.0.1 P13 resulted in no errors and the database was accessible.
  - Applies to: Server
- File tracking disabled when database size not increased by SQL update [43953]
  - Details: When the server was installed with SQL Server Express, which was later updated to a version with higher database size properties, Bit9 did not recognize the higher database size. This caused file tracking to be disabled because of an incorrect

  database size restriction. In this release, Bit9 does recognize the increased database size and does not prematurely disable File Tracking.
  - Applies to: Server
- Some Windows 7 agents are not completing initialization [43971]
  - Details: After upgrading to 7.2.0 Patch 8, some Windows 7 machines deadlocked during system initialization and the machines became unusable. In order to bring the machines online, the machines had to be rebooted and placed in disabled mode. In this release, the cause of the deadlock has been removed and agent initialization completes successfully.
  - Applies to: Agent
- System crash during certain file delete operations [43975]
  - Details: A Windows 7 32-bit agent machine running Bit9 7.2.0 Patch 5 experienced system crashes during certain file delete operations. In this release, the conditions for that crash have been removed and the system crash does not occur.
  - Applies to: Agent
- Files are being blocked on endpoint, but there are no corresponding console events [44091]
  - Details: A Bit9 server crash caused network connectivity to deteriorate over time resulting in delays of agent events being sent to the server. In a high traffic system, these delays eventually caused a Bit9 server deadlock. In this release, the causes of this deadlock do not occur and agent events are properly sent to the console.
  - Applies to: Server

Corrective Content in Bit9 Platform 7.2.0 Patch 9 (Build 1645)

- Windows API allows users running agents in High Enforcement to bypass execution blocks [43925].
  - Details: With the Windows API, a user whose system had an agent in High Enforcement could activate the Bit9 notifier's "Allow" button, which is normally invisible at this enforcement level. This would permit the execution of any file. In this release, the "Allow" button cannot be activated on systems running in High Enforcement.
  - Applies to: Agent [Windows]
- Large number of tamper protect alerts when upgrading from 7.0.1 Patch 15 to 7.2.0 Patch 5 [42584]
  - Details: An upgrade from 7.0.1 Patch 15 to 7.2.0 Patch 5 resulted in many false tamper protect alerts when Bit9 accessed its own data directory. In this release, these alerts will not occur.
  - Applies to: Server
- Validly signed files are being blocked by Bit9 [42998]
  - Details: If a file with a specific leaf certificate was processed on an agent and then another file instance with the same leaf certificate but a different parent certificate arrived, trusted publisher approvals could fail. This occurred when the new file's signature was validated against a cached certificate chain instead of the chain from that file's signature. This could lead to the signature time on the new file being validated against the wrong certificate chain. In this release, file signatures are validated against the certificate chain presented with their own signature, and the blocking does not occur.

Note: For files already known to the agent that were unapproved because of this issue to get approved, a full Cache Consistency Check with publisher re-evaluation should be performed.

Applies to: Agent [Windows]

- Event rule "Last modified" data not updated when rule is disabled due to invalid FireEye target [43116]
    - Details: When an event rule initiated a file upload to an invalid FireEye analysis target, the event rule would be automatically moved from Enabled to Simulate mode, disabling automatic uploads by the rule. However, this change to the rule would not be indicated with an updated “last modified” user and date.

      In this release, if the rule is automatically disabled the event rule is correctly updated with the last modified user and date.

      Applies to: Server
- Files are blocked due to incorrect hash when a long file write times out. [43121]
    - Details: If a copy of a large file resulted in an extremely long write operation timing out, an incorrect file hash is produced when the file is analyzed prematurely. In this release, file analysis will be performed upon the completed file copy operation.

      Applies to: Agent [Windows]
- Version 7.2.0 Patch 6 consuming high cpu and memory resources [43156]
    - Details: An agent system generating numerous install events, such as from compiling with Visual Studio, could exhaust the available memory. In this release, old install events are periodically removed from memory and the database, increasing the availability of memory and cpu resources.
    - Applies to: Agent [Windows]
- Process name field is empty on console pages [43390]
    - Details: On some Bit9 Console pages, such as the New Installations view on the Events page, the Process Name field appeared blank even though process information should have been available. In this release, the process information is retained in the Bit9 cache long enough to provide the the server with the necessary process information for these pages.
    - Applies to: Agent [Windows]
- Bit9 points to wrong source for files on Carbon Black Watchlist [43562]
    - Details: Bit9 reported incorrect endpoint names for files reported on the CB watchlist. In this release, improvements to the management of deleted hosts has solved this problem.

      Applies to: Server
- Server upgrade fails when installer cannot stop services [43614]
    - Details: During server upgrades, the installer sometimes failed to stop the Bit9 Platform services, resulting in a failed upgrade. In this release, the server will now properly halt if a service cannot be stopped.
    - Applies to: Installer
- SHA-256 hashes from external notifications not accepted for events and event rules [43621]
    - Details: If an event rule was configured to catalog and ban for malicious files reported in external notifications, neither the ban nor the malicious file detected event were generated if the notification reported only a SHA-256 hash. In this

  - release, Bit9 can use SHA-256 hashes from external notifications to record file events and trigger event rules.
  - Applies to: Server
- System crash due to race condition with file operations [43630]
  - Details: In previous releases, certain combinations and volumes of file operations could cause race conditions in the Bit9 Agent that would cause the system to crash. In this release, the management of threads has been improved to avoid these crashes.
  - Applies to: Agent [Windows]

Corrective Content in Bit9 Platform 7.2.0 Patch 8 (Build 1559)

- [Linux] Bit9 Platform slows performance of Apache Tomcat jobs [42690]
  - Details: With Bit9 Platform running, Apache Tomcat jobs take up to three times longer to perform. In this release, the implementation of process exclusions has been modified to eliminate the performance degradation encountered.
  - Applies to: Agent
- Server keeps crashing after agent upgrade to 7.2.0 Patch 5 [42783]
  - Details: After agent upgrade to 7.2.0 Patch 5, the Bit9 endpoint experienced frequent crashes due to low memory. In this release, changes were made in reading memory to avoid the conditions causing this crash.
  - Applies to: Agent
- Agent crash after upgrading agent to 7.2.0 Patch 5 [42826]
  - Details: Under certain circumstances, the Bit9 driver was making invalid references to file names causing the agent to crash. In this release, file name checking was modified to avoid the conditions causing this crash.
  - Applies to: Agent
- After upgrade to 7.2.0 patch 6, excessive certificate error events occurred [43009]
  - Details: After upgrade of Bit9 server from version 7.0.1 to 7.2.0 patch 6, excessive file certificate errors occurred. In this release, these errors did not occur due to a modification to certificate details handling.
  - Applies to: Server
- System crash after upgrading agents to 7.2.0 Patch 5 [43017]
  - Details: A few Windows agents experienced system crashes after upgrading to Bit9 7.2.0 Patch 5. In this release, a race condition was found where memory was simultaneously modified by more than one process, causing a system crash. This race condition has now been eliminated and that crash no longer occurs.
  - Applies to: Agent
- High cpu and memory resources due to large number of install events [43175]
  - Details: When using a monitoring tool which continually wrote new scripts during Bit9 installation, a customer experienced a large number of events, high CPU usage and low memory availability. In this release, unneeded install events have been deleted.
  - Applies to: Agent

Corrective Content in Bit9 Platform 7.2.0 Patch 7 (Build 1492)

- Agents with prioritized updates encountered high CPU utilization [41390]
  - Details: When an agent was prioritzed for updates, CPU utilization was high. This was due to excessive communication between the agent and the server. In this release, agent-server communication was improved to eliminate high CPU rates.
  - Applies to: Server
- Unable to re-use Event Alert names of previously deleted alerts [41463]
  - Details: When deleting event alerts and recreating a new event alert with a previously used name, an error message was produced stating that the event rule creation failed and that the name needed to be changed. In this release, the name of a previously deleted event alert can be reused.
  - Applies to: Server
- Passwords with certain special characters were not accepted during server installation [41579]
  - Details: During server installation, passwords containing one of these special characters were not being accepted: ampersand (&), less than (<), greater than (>), single quote ('), double quote (") or exclamation point (!). In this release, these characters are now correctly encoded in the configuration file and password failures do not occur during the server installation.
  - Applies to: Server
- Upgrade errors when patching from 7.2 P4 to 7.2 P5 [41641]
  - Details: Upgrade errors were encountered when upgrading from 7.2 Patch 4 to 7.2 Patch 5, including ”Cannot resolve the collation conflict…” and “Transaction rolled back…”. In this release, the post-upgrade processing was improved to accommodate user databases with a different collation than the Bit9 default, and so these errors no longer occur.
  - Applies to: Server
- Outlook.exe was marked as malicous because of a FireEye report [41696]
  - Details: FireEye lists all files modified by the software under test. In some cases, for example, if the software kept the target file open beyond FireEye’s time limit, FireEye didn’t report the file hash of the modified file, causing Bit9 to categorize the original file as malicious. In this release, the FireEye listener filters out modified files that do not have a reported hash.
  - Applies to: Server
- Some files discovered during loaded image check block on execution [41837]
  - Details: After a database restore, a CC3 (cache check level 3) is scheduled to approve new files found. Files that were already running might be found by the loaded image check before the CC3 discovered them. Those files would be classified as unapproved and therefore block on execution. In this release, file discovery will not miss these files and they will become approved.
  - Applies to: Agent
- Template clones do not reset all configuration options unless they reconnect to server [41853]
  - Details: When creating a template for computers that will not reconnect back to the Bit9 Server, you must first set a configuration option on the template computer

before disconnecting it and marking it as a template. Contact Bit9 Technical Support, referencing CR 41853, for the technical note containing details on how to do this.
    - Applies to: Server
- Bad manifest stops all manifest processing [41933]
    - Details: During the trusted directory process, a bad (e.g. corrupted) manifest file would prevent new manifests from being processed until the bad manifest file was manually removed. In this release, manifest processing is not interrupted after a bad manifest file is encountered.
    - Applies to: Server
- Agent is not maintaining outstanding event count properly [42076]
    - Details: After an agent restart, the agent had an inaccurate count of events to be sent to the Bit9 Server. Either the agent's event count was too low, in which case not all events were sent to the server, or the agent's event count was too high, in which the agent would keep trying to send events that didn't exist. In this release, the agent's event counting has been corrected.
    - Applies to: Agent
- Agent causing system crashes on rare occasions [42105]
    - Details: On extremely rare occasions, a race condition occurred in the agent causing a system crash. In this release, that race condition has been prevented.
    - Applies to: Agent
- Some users encountered SRS activation failure [42256]
    - Details: For some users, activation of the Bit9 Software Reputation Service failed with the error "SRS activation failure" when they clicked the Verify Activation button. This was due to the verification step using credentials that did not always have access to the Bit9 SRS server. In this release, In this release, the SRS validation check should not encounter this issue.
    - Applies to: Server
- CPU spike on System process after upgrading to 7.2 P3 HF [42310]
    - Details: When the agent was installed on a computer running Windows 7 x64 Enterprise version, and that computer had a USB-connected DisplayLink portable display unit, CPU utilization spiked every 16 minutes. In addition, the display flickered and turned black momentarily. In this release, image refresh software changes prevent this condition.
    - Applies to: Agent
- Policy name is case sensitive when installing an agent through command line [42363]
    - Details: The policy name was being treated as case-sensitive in certain situations where it should not have been, resulting in the policy being installed as the default policy. In this release, that behavior has been corrected.
    - Applies to: Server
- Remounted devices appeared unattached and had file operations blocked [42402]
    - Details: In some cases, unmounting and remounting a removable device would cause the Bit Server to consider the device as unattached, and the device would not appear as attached in the console. This could cause the server to block file

  - operations on that device, even if the device was approved. In this release, unmounting and remounting a device will not cause this condition.
  - Applies to: Agent
- Server connectivity loss and crash due to excessive agent registration and file traffic [42509]
  - Details: When a large number of agents registered with the Bit9 Server at the same time, such as in VDI enviornments, agents could lose connectivity with the server. Rebooting the the SQL server could restore connectivity, but the server could then crash and restart automatically. This situation was especially likely if there were also event rules that caused a large number of files to be analyzed and uploaded. In this release, the conditions causing these crashes have been removed.
  - Applies to: Server
- Upgrade from 7.0.1 to 7.2.0 caused huge volume of tamper protection events [42688]
  - Details: In some cases, upgrading from 7.0.1 to 7.2.0 resulted in a very large number of unnecessary tamper protection events per day. In this release, the tamper protect rules were improved to avoid this situation.
  - Applies to: Server

Corrective Content in Bit9 Platform 7.2.0 Patch 6 (Build 1395)

- Performance issues during initial certificate revocation checking [40539]
  - Details: When the default setting for initial certificate revocation checking was ‘Network’, performance issues occurred. In this release, the default setting for initial certificate revocation checking has been changed to ‘Cache’ to avoid performance issues on machines that either are never connected to the internet or are having network connectivity problems. Note, however, that if you have already modified this setting, the setting is not not overwritten by the new default.

    These issues did not occur during background certificate revocation checking, so the default for background certificate revocation checking was not changed.
  - Applies to: Server
- Processing of PAN connector data could run more efficiently with additional SQL indexes [40999]
  - Details: SQL monitoring of some customer production environments reported that processing of Palo Alto Networks connector data could be improved with additional SQL indexes. In this release, modifications were made to the SQL index for the notifications table, which resulted in improved UI performance of the console External Notifications page.
  - Applies to: Server
- Trusted Directory approvals could be delayed [41018]
  - Details: Approvals of files moved to Trusted Directories could be delayed if the trusted directory’s computer had a low percentage of synchronization with the server, as shown on the Computer Details page Connection History tab. In this release, agent computers with trusted directories are given a high priority for synchronization.
  - Applies to: Server

- Cannot reset alert from Dashboard [41066]
    - Details: Previously, it was not possible to reset triggered alerts from the console Dashboard. In this release, an alert that has been triggered can be reset from the Dashboard.
    - Applies to: Server
- Deleting rule during server upgrade caused upgrade failure [41325]
    - Details: When a Bit9 rule had an extremely large size, and that rule was being deleted during the upgrade of a server, the upgrade could fail. In this release, non-essential data is no longer transmitted from the server to the agent during a configuration list update for rule deletions, which prevents this error condition from happening.
    - Applies to: Server

  Error message when filtering by Computer Name in the Approval Requests section of the server console [41356]
    - Details: When filtering for Computer Name using the options 'is', 'is not' and 'begins with', the following error occurred: "Invalid field:Computer". In this release, using these filter options produces no error.
    - Applies to: Server
- Endpoints are intermittently showing as connected/disconnected in the console [41465]
    - Details: If an agent uploaded a binary file containing a badly formed certificate or if the server received a file certificate not supported by the Windows CryptoAPI, the server would repeatedly try and then fail to validate this certificate. This would cause the server log to balloon rapidly with error messages and the endpoints to intermittently be connected and disconnected. In this release, the badly formed certificate is rescheduled for validation at a later time in the same manner as other erroneous certificates, which prevents the multiple validation failures.
    - Applies to: Server
- Agent crashes or hangs when endpoint uses Microsoft DPM (Data Protection Manager) [41473]
    - Details: When the Bit9 Server was rebooted after an upgrade to 7.2.0 Patch 4, some agents would not reboot properly unless they were booted in Safe Mode and had the Bit9 Agent removed. This was due to a deadlock caused by interaction with Microsoft DPM. In this release, the deadlock no longer occurs and these agents reboot normally.
    - Applies to: Agent
- Unable to remove prioritization from agent computer [41483]
    - Details: From the server console, in the Computer Details page, there is an option under Actions to prioritize updates to that computer. This should toggle between "Prioritize Updates" and "Remove Prioritization of Updates". In previous releases, the option to "Remove Prioritization of Updates” never appeared after selecting “Prioritize Updates”. In this release, the toggling of the option works correctly.
    - Applies to: Server
- SRS Activation times out [41566]

      Details: When Bit9’s SRS (Software Reputation Service) was activated, the proxy configuration on the server console’s “System Configuration/Licensing” page was

being ignored, and the server was going directly to "https://services.bit9.com" when the "Verify Activation" button was clicked. In this release, the "Verify Activation" option functions correctly with the proxy setting.
  - Applies to: Server
- SQL server CPU consistently has high utilization due to FireEye integration [41760]
    - Details: CPU utilization exceeded 100% at times when a request for FireEye analysis of files was sent from the Bit9 Console. In this release, database improvements were made to reduce the CPU usage.
  - Applies to: Server
- Modified files are incorrectly getting blocked by Bit9 Platform [41899]
  - Details: An issue was identified that affects all 7.2 versions up to and including Patch 5 that could cause the agent to miss some modifications to files. When that occurred, the agent could find that the hash of the file is different from expected and block execution of that file in high enforcement. In this release, the issue has been resolved and the files are not blocked from execution.
  - Applies to: Agent
- Endpoint crash can occur when uninstalling or upgrading 7.2 agents [41908]
  - Details: The 7.2 installer could encounter a race condition between multiple processes the would cause the agent to crash while uninstalling or upgrading. In this release, changes have been made to eliminate this race condition, averting the conditions for the crash.
  - Applies to: Agent
- Windows Event Log is missing notification details for file blocks in 7.2 [41940]
  - Details: When a Bit9 notifier (block or prompt) is displayed on an endpoint, an event with ID number 22 is added to the Windows event log to record the blocked file information. The event did not include the notification details, but instead contained a warning that the description for Event ID 22 from source Bit9 Agent Notifier cannot be found. In this release, the notification text is added to the event and the warning is not included.
  - Applies to: Agent
- Files may be blocked on Windows XP and Windows 2003 agents when agent starts in disabled mode and switches to a higher enforcement mode. [42009]
  - Details: When a Bit9 Agent was deployed in disabled mode on Windows XP or Windows 2003 systems, if several user-initiated processes executed and remained open, moving the agent out of disabled mode to a higher enforcement level could cause those processes to be blocked. In this release, moving from disabled to a higher enforcement level no longer causes this blocking to occur.
  - Applies to: Agent
- Rare instances of Windows 7 Agent machines crashing [42112]
  - Details: A rare race condition in the Bit9 agent driver caused agent crashes. In this release, the race condition does not exist and cannot lead to that crash occurring.
  - Applies to: Agent

Corrective Content in Bit9 Platform 7.2.0 Patch 5 (Build 1310)

- File Analysis error “Unsupported WildFire XML format” [41061]
    - Details: In September 2014, Palo Alto Networks version 6.1 was released with Wildfire version 3.0. This new version changes the XML report file format. Any new files analyzed with Wildfire by Bit9 Platform reported the error “Unsupported WildFire XML format”. In this release, Bit9 Platform can process the new XML file format. [41061]
    - Applies to: Server
- Error converting data type timestamp to numeric [41058]
    - Details: Under certain circumstances, pages would fail to load in the Bit9 Console due to an error in a database query. In this release, the error does not occur.
    - Applies to: Server
- Interesting files within .7z files in a trusted directory are not classified as interesting [40991]
    - Details: Files with “.7z” extension within a trusted directory contained interesting files but those files were not classified as interesting. In this release, those files will be classified as interesting.
    - Applies to: Server
- Blank “Identifier” column when exporting Computers page to .csv file [40732]
    - Details: When the “Identifier” column was added to the Assets/Computers page, it would not get properly exported to a CSV file. In this release the column is successfully exported.
    - Applies to: Server
- Computer security alert is consuming high amount of resources [40621]
    - Details: Modifications were made to improve on the performance of Computer Security Alert. Some pruning has been moved to daily pruning task for Alerts. In this release performance of computer security alerts is improved.
    - Applies to: Server
- Server backlog is extremely high [40885]
    - Details: After an agent upgrades, it will often run cache consistency checks to validate or correct the data that was collected by the previous agent version. The number of corrections that need to be made could vary based on a number of factors such as:
        - if the old agent was crashing frequently
        - a high number of files written during agent upgrade
        - if the old agent didn't support the collection of certain information, such as detached signatures

      These and other corrections result in both updates to the agent's local inventory and in the sending of messages from the agent to the server to correct the server’s inventory. When upgrades are pushed in bulk, these messages could cause synchronization percentage to drop while the server tries to process all these corrections, in addition to the normal load. In this release, optimizations were made to reduce the number of messages sent to the server.
    - Applies to: Agent
- Excessive locking during backlog processing [40930]

  - Details: File processing and backlog processing were competing for resources causing a high volume of waits due to file locks. In this release, file processing was improved when the server is also processing a large backlog of files in its database.
  - Applies to: Server

- Connection to Software Reputation Service fails [40713]
  - Details: In some instances, a correct SRS license key was not validated. In this release, the validation procedure used at the Administration/Licensing page has been corrected.
  - Applies to: Server
- Advanced Threat Indicator exclusions not working properly [41190]
  - Details: A regression introduced in 7.2.0 Patch 4 could lead to some ATI rules and exceptions not properly triggering or excluding. In this release, the conditions allowing this issue to occur have been removed and ATI triggers and exclusions now work properly.
  - Applies to: Agent

Corrective Content in Bit9 Platform 7.2.0 Patch 4 (Build 1248)

- Logged events unnecessarly exported to the Analytics folder [40433]
  - Details: On the External Analytics Settings tab of the System Administration page, users can set a time period to limit the backlogged events exported to the analytics folder. Under some circumstances, this time limit could be ignored, causing all logged events available on the server to be exported to the folder. The conditions that caused this problem have been corrected in this release.
  - Applies to: Server
- Navigating to System Configuration->General page results in error 500 [40618]
  - Details: After an upgrade from Bit9 Platform version 7.2 P0 to 7.2 P1, if the Bit9 SQL Service account lacked “VIEW SERVER STATE” permission, an error 500 was returned when navigating to the System Configuration->General page. This error no longer occurs. [40618]
  - Applies to: Server
- Execution of locally approved files occasionally requires notifier response [40668]
  - Details: Agents occasionally displayed the Bit9 Notifier and required the user to choose “Allow” before allowing a locally approved file to run. This issue has been resolved.
  - Applies to: Agent
- Files lost from Agent’s file inventory [40670]
  - Details: On rare occasions, opening a file was classified as creating the file, which could cause the agent to remove the file from its inventory, resulting in possible loss of file state or file history. This issue has been resolved.
  - Applies to: Agent
- Server takes a long time to recognize a new file on the agent [40686]
  - Details: When the server was under high load from the agents, such as when many agents did a resync simultaneously, database processing was slowed. This slow performance has been resolved.
  - Applies to: Server

- Server processing of agent's new file inventory is slow [40687]
    - Details: A previous upgrade of the server did not remove deleted file instances causing slower processing of new agent file inventory. These deleted file instances are now being removed, improving performance.
    - Applies to: Server
- Unauthorized search query in console [40694]
    - Details: When the console timed out after exceeding the "Log Users Out After" limit set in the System Configuration->Advanced Options page, it was still possible to make a new query in the console's search box on the Assets->Computers page. This query is no longer allowed under these conditions.
    - Applies to: Server
- System slowdown with 7.2 Patch 1 installed [40704, 40532]
    - Details: A Bit9 Platform system with version 7.2.0 Patch 1 installed on Windows Server 2008 R2 with a very large set of rules encountered a noticeable decrease in system performance. Rule processing has been streamlined to avoid this performance issue.
    - Applies to: Agent
- Emails from Block Alerts are either not sent at all or are grouped and sent later [40711]
    - Details: In Bit9 Platform 7.2.0 Patch 2, emails from Block Alerts were either not sent at all or appeared in large groups several hours later. Emails from Block Alerts are no longer combined in large groups, which resolves the issue.
    - Applies to: Server
- Filter for policy reverts to Default Policy [40790]
    - Details: If a policy was created with two or more spaces in its name, attempts to filter on it worked the first time but after the page was refreshed, the filter reverted to "Default Policy". The extra spaces in the policy name no longer cause this issue.
    - Applies to: Server
- Server backlog is very high with many state change messages sent from agent to server [40901]
    - Details: An extremely large number of upgrades (over 10,000) performed in a week caused a large server backlog which impacted performance. A change was made to resync more often which remediates the problem.
    - Applies to: Server
- Duplicated rules were created, affecting performance [40950]
    - Details: From the initial 7.2.0 release through Patch 3, many duplicate rules could be created, depending on the number of users logged into the system and the number of user-specific rules in effect. Slower performance could be especially seen with many users logged on via terminal servers. The problem no longer occurs in Patch 4.
    - Applies to: Server
- Agent health events reported on unexpected file versions [40979]
    - Details: Patching a 7.0.0.x system to 7.2.0 versions prior to Patch 4 showed a number of agent health events for file versions left over from previous installations. A change was made in Patch 4 to correct the situation.
    - Applies to: Server
- Agent system freeze [40998]
    - Details: On rare occasions, the agent system could freeze (blue screen or black screen) due to a race condition, especially on high-powered systems with multiple processors. Changes have been made to eliminate this condition.

  - Applies to: Agent

Corrective Content in Bit9 Platform 7.2.0 Patch 3 (Build 1175)

- Backlogs in processing of file hashes from agent cause unanalyzed file blocks [39937]
  - Details: The agent was hashing files in response to uninteresting operations. This could result in a backlog of files to be hashed, and could sometimes result in file blocks on agent computers due to unanalyzed files. This issue has been resolved.
  - Applies to: Agent [Windows]
- Wrong priority for new file operations causes unanalyzed file blocks [40504]
  - Details: Operations related to execution of new files were queued behind low priority background tasks, resulting in delays of hashing new files. This could sometimes result in file blocks on agent computers due to unanalyzed files. This issue has been resolved.
  - Applies to: Server
- Occasional agent crashes [40573]
  - Details: Certain agent activity referenced a null pointer, and this could result in agent crashes under very specific conditions. This issue has been resolved.
  - Applies to: Agent [Windows]
- Some files "marked as installer" lost this setting when upgrading from 7.2.0 P1 or 7.2.0 P2 to 7.2.0 P3 [40535]
  - Details: Affected files will transition back to being installers after upgrade to P3. This issue has been resolved.
  - Applies to: Server
- Daily collection of server health counters was failing occasionally in deployments with extremely large file churn. [40496]
  - Details: This issue has been resolved.
  - Applies to: Server
- Problems had been identified with the new "Carbon Black Tamper Protection" (Version 7) and "Bit9 Server Tamper Protection" (Version 1) updaters. [40409]
  - Details: These updaters could block Carbon Black upgrades and prevent the Bit9 server from operating correctly. This issue has been resolved.
  - Applies to: Server
- Xen Desktop interoperability issue with Bit9 Agent [40359]
  - Details: An interoperability issue with XEN Desktop was found that could result in system freeze and failure to boot the machine. The issue has been resolved.
  - Applies to: Agent
- Server initiated Agent upgrades even when policy based upgrade flag was disabled [40336]
  - Details: Disabling agent upgrades from the Action menu on the Manage Policies page did not actually prevent upgrades from occurring. Disabling agent upgrades from the Policy Details page worked correctly. The issue has been resolved.
  - Applies to: Server
- Server experienced increase in backlog of files from agent after upgrade to 7.2 [40282]
  - Details: The Bit9 server could experience an increase in the backlog of files from an agent when an obsolete 7.0.1 optimization setting was turned on. This issue has been resolved.
  - Applies to: Server

Corrective Content in Bit9 Platform 7.2.0 Patch 2 (Build 1039)

- Agent Performance Problem [40194]
    - Details: A performance problem that only affected 7.2 P0 and 7.2 P1 agents was identified and fixed. Symptoms included slow system responsiveness, periodic high CPU usage attributed to the parity.exe process, and the occasional unanalyzed block.
    - Applies to: Agent

Corrective Content in Bit9 Platform 7.2.0 Patch 1 (Build 1036)

- Sample Server Tamper protect rules block some files [39619]
    - Details: Previously, certain legitimate file actions, some related to use of the Bit9 Connector, were blocked if sample Tamper Protection rules were fully active (i.e., not in Report Only mode). In this release, these Tamper Protection rules have been removed and replaced with rules that may be enabled in the Updaters section of the Software Rules page. This change also allows Bit9 to update the rules through the cloud if improvements are found between releases.
      Note: Because of this change, if previous rules for the sample Bit9 tamper protection rules were modified, those modifications might be overwritten after upgrade. Enabling the new rule implementation via the Updaters page should restore previous tamper protection, but if you created a rule for a special case, you might want to re-implement that as its own custom rule.
    - Applies to: Server
- MESSAGE 1 WITH INVALID TYPE(29811) is displayed in events [39729]
    - Details: An issue with certain previous versions of the Bit9 Agent could cause frequent display of an “invalid type” message. Upgrading to the current 7.2.0 agent should eliminate the issue.
    - Applies to: Agent [Windows]
- Upgrades to OSX 10.9.4 fail because some OS files do not get promoted [40125]
    - Details: During OSX operating system upgrade, some system files may not get approved, causing the upgrade to fail. The conditions that caused this problem have been corrected in this release.
    - Applies to: Agent [Mac]
- Tamper protect rule preventing reboot during Mac OS 10.9.4 upgrade [40127]
    - Details: After a Mac system was upgraded to OSX 10.9.4, rebooting it might freeze the computer. Changes made in this release should eliminate the problem.
    - Applies to: Agent [Mac]
- Path Macro example in the Using Parity document table needs updating [38841]
    - Details: In previous editions of *Using the Bit9 Platform* and online Help, the table of macros that can be used in rules showed paths that apply only to older versions of Windows. In this release, the documentation specifies both the CSIDL and the FOLDERID on which the macros are based.
    - Applies to: Documentation
- Cleanup of deleted uploaded files impacts policy updates [39966]

  - Details: When there were many uploaded filed scheduled to be deleted on the Bit9 Server, the Server would stop sending policy updates for an extended period. In this release, the interaction between these two features has been improved.
  - Applies to: Server
- FireEye version 7.2 Integration with Bit9 no longer works [39925]
  - Details: Changes to the FireEye XML Format for certain date fields in version their version 7.2 caused the Bit9 – FireEye integration to fail. In this release, the Bit9 Server has been modified to accommodate the format change.
  - Applies to: Server

Corrective Content in Bit9 Platform 7.2.0 (Build 891)

- Only in the Bit9 Portlet, filter for full path appears to miss path with special characters [22173]
  - Details: The filter is now able to handle special characters
  - Applies to: Server [Windows]
- Server backlog is affecting UI response [27908]
  - Details: Agent pruning logic ran before fully initialized which caused unnecessary resync with the server. Safeguards were added to avoid the resync loop when the pruning logic runs.
  - Applies to: Agent [All]
- Reported crawler job numbers vary from high to low [28081]
  - Details: Prior to V720, the "jobId" assigned to each trusted directory crawl could be reused if all jobs completed since ids would start back at 0. In V720+, job ids will not be reused.
  - Applies to: Agent [All]
- RSS Feeds in dashboard should use proxy configured for other operations [28848]
  - Details: Dashboard will use the same proxy as configured for Reporter for Portlets : "Bit9 News", "Virus RSS"
  - Applies to: Server [Windows]
- Entering a SAN does not work in the installer when creating a certificate [29017]
  - Details: A help button has been added under SAN label informing the user what needs to be entering in the SAN field and the required format.
  - Applies to: Installer [WIndows]
- Make agent more fault tolerant when kernel communication throws an error [33423]
  - Details: Under low memory situations the agent may need to disconnect from the kernel to prevent system crash. If this occurs, the agent will appear with a "red dot" in the console and event will indicate that the agent was not able to communicate with the server. An agent restart is required to recover.
  - Applies to: Agent [All]
- System Alerts Widget on Dashboard Shows Incorrect Values [33492]
  - Details: The SQL queries have been corrected.
  - Applies to: Server [Windows]
- Date/Time log entries displays the following error: Error converting data type char to datetime [33617]

  - Details: Event insert would fail on the server in case when reporting agent has clock set up to be far in past or future.
  - Applies to: Server [Window]
- Enforcement level portlet is showing incorrect data [33668]
  - Details: The portlet display has been corrected.
  - Applies to: Server [Windows]
- Correllate SQL edition and free disk Space checks [33696]
  - Details: Upgrading to v7.2.0 from a previous version and the database size is 4Gb or greater, and the SQL server is SQL Express. A warning is shown regarding reaching the SQL Express file size limit after upgrading. There is an option to coninue if the customer is aware of the limitations.
  - Applies to: Install [Windows]
- Certain browser files get approved as they are the same publisher as the browser [34477]
  - Details: Prior to v7.2.0 the Bit9 agent could automatically locally approve software that was installed or downloaded by software of the same publisher. The old behavior could lead to unwanted approvals for cases where for example a internet explorer downloaded Microsoft signed installer (e.g. silverlight). The new behavior will not automatically approve this software for security reasons. If customers were relying on this approval mechanism, additional custom rules or updaters may be necessary.
  - Applies to: Agent [All]
- Certificate query is slow due to unneccessary locking [34693]
  - Details: On a recurring basis, the Bit9 Server validates and revalidates the certificates used to sign software. The certificates chosen to be validated are collected by way of a query. On at least one customer installation, this query proved too time consuming.
  - Applies to: Server [Windows]
- Long user lists prevent agent registration [34835]
  - Details: When an agent registered with the server, there was room for only 1024 characters when communicating a comma-separated list of users logged onto the Server. In most circumstances, this turns out to be more than adequate. Under some circumstances, though, there are machines on which a very large number of accounts are logged in simultaneously. Such machines were unable to register with the server because the 1024 character limit was exceeded. As they were unable to register, they were unable to connect.
  - With this change, the buffer can expand to much larger number of characters. If that limit is exceeded, then an internal error is logged.
  - Applies to: Agent [All]
- An automated way to restore and delete cache/backup and force a rebuild is needed [34925]
  - Details: New actions RestoreDB and DeleteDB added to the advanced endpoint detail actions which triggers complete removal, restore and reinit of cache upon next agent restart. Dascli command “restoreDB” "deleteDB" added as well.
  - Applies to: Server and Agent [All]

- Diagnostic upload fails on non-standard port: BulkTransferPort must be set to same value as server port [35084]
    - Details: When a non-standard port was used on the Bit9 Server, file uploads would fail.
    - Applies to: Server [Windows]
- Prevent multiple simultaneous rule expansions [35221]
    - Details: The agent automatically re-evaluates which rules and policies should be active whenever a new user logs onto this system. On systems where user log ons are frequent, the process to expand those rules was being kicked off multiple times in parallel which could cause parity CPU usage to spike.
    - Improvements were made to optimize rule expansion such that only one rule expansion will occur if multiple user logons occur in a short time period.
    - Applies to: Agent [All]
- Saved view "Banned files" on "Files on Computers" page is slow and timing out frequently [35509]
    - Details: Performance on all pages have been addressed
    - Applies to: Server [Windows]
- It is not possible to correct SRS activation key in the user interface [35841]
    - Details: After clean install sometimes it is not possible to enter Bit9 Software Reputation Service Key. The text box for entering the key is not visible in UI. Multiple different reasons can cause this issue, but the underlying cause is that UI attempts to verify that SRS is reachable. If it is not then the textbox is not displayed. The behavior has been changed so that irrespective of whether SRS is available or not, the text box should always be displayed.
    - Applies to: Server [Windows]
- Receiving blocks on GoToMeeting files due to still analyzing state [35934]
    - Details: The agent could deadlock in the presence of other A/V or file inventory products on the system when launching MSI's. This could exhibit a variety of symptoms which include unanalyzed blocks, unresponsive commands and overall system slowness.
    - Applies to: Server [Windows]
- Allow multiple Report rules to fire [36041]
    - Details: Prior to version v7.2.0 the agent was only capable of firing a single event rule per I/O operation. It can now fire up to 10.
    - Applies to: Agent [All]
- The stored procedure InsertPublisher inserts a user_id into a username_id column [36342]
    - Details: The "New Publisher" event would report the wrong originating user name. Now it reports the correct user name.
    - Applies to: Server [Windows]
- Policy based publisher approvals become global when publishers are acknowledged from the list page instead of the details page [36378]
    - Details: Acknowledging publisher that was approved by policy is no longer converted approval to be global (all policies).
    - Applies to: Server [Windows]

- USB Devices are getting blocked [36458]
  - Details: Agent would not properly approve or ban multiple serial numbers for the device.
  - Applies to: Server [Windows]
- The Server UI should perform a case insensitive comparison of Common Name and Server Address in the General Tab on the System Config page [36612]
  - Details: On the General Configuration page, there will no longer be a warning to the user when the Server Address entered by the user and the Common Name in the SSL certificate are the same text with different cases
  - Applies to: Server [Windows]
- After upgrading from v6.0.2 to v7.2.0. The console is no longer accessible and gives IIS 404 error[36716]
  - Details: Bit9 Console is not accessible and gives IIS 404 error after 6.0.2 to 7.0.1 upgrade. This issue was reported only on Windows 2003 SP2. It no longer reports the error.
  - Applies to: Server [Windows]
- When in high enforcement, the notifier is not displayed sometimes [36748]
  - Details: If the Notifer.exe did not successfully connect to the Bit9 agent the Notifier instance remains alive until the agent restart. In some cases this zombie process could prevent upgrade and display of user notifications.
  - The Bit9 agent now properly manages the lifecycle of notifier instances.
  - Applies to: Agent [All]
- Timedoverride.exe crashes if used on cmd with very long string of random characters [37029]
  - Details: It was possible for a user to enter a code that was too long on the command line for the TimedOverride tool, causing the tool to stop working
  - Applies to: Server [Windows]
- Excessive number of locks slow down server backlog performance [37542]
  - Details: high number of open SQL locks causing lowered performance of inventory processing
  - Applies to: Server [Windows]
- File uploads require additional system configuration permissions [37468]
  - Details: In addition to the appropriate file upload permission, *Manage system configuration* permission was required to allow console users to upload files from agents. In this release, *Manage system configuration permission* is not required to upload files.
  - Applies to: Server
- Agent reports incomplete consistency check after upgrade [37778]
  - Details: When an agent is upgraded it can sometimes initiate a cache consistency check to ensure its cached file system data is in tact. If during the initial cache check another check is initiated (usually a result of some configuration change) the first "Cache check complete" event would say that the check was unsuccessful before starting the second check, even though the first check completed successfully.
  - Applies to: Agent [All]

- When attempting to click on Computers from the Computer View and occasionally when trying to make changes to a Computer that does load, the following error is displayed: "No corresponding computer was found in the database” [38719]
  - Details: A message will be displayed when a database error occurs on the computer details page. Previously, the page would appear as if it failed to find a computer with no error message.
  - Applies to: Server [Windows]

Known Issues and Limitations

- If you are using DFS and have installed an agent on a Windows 2003 or XP system, you must reboot the agent system to get full enforcement of Bit9 file rules. Because of an operating system limitation, DFS operations (including file executions) cannot be detected by the Bit9 Agent until the system has been rebooted.

- When Linux is upgraded to a new base minor kernel, the error “Failed to connect to daemon” can occur on systems running the 7.2.0 Bit9 Agent. A second reboot may be required to bypass this error. This issue is being addressed in a future release. [44661]

- Mac and Linux binaries in the Bit9 installation package are automatically globally approved when you install or upgrade the server. In the current release, these files will be displayed in the console as “Global State: Unapproved”, even though they are actually approved. No action is necessary, and the files can execute in high or medium enforcement. [44372]

- Setting the Bit9 Platform agent data path under the agent install directory is not supported and can result in loss of connection to the server after endpoint reboot. For example, installing Bit9 agent to D:\Bit9 and setting the agent data path to D:\Bit9\data is an unsupported configuration. [43019]

- Bit9 no longer supports Bit9 Servers running on the Microsoft Windows 2003 operating system. Agents on Microsoft Windows 2003 continue to be supported.

- If both the Bit9 agent and Microsoft Enhanced Mitigation Experience Toolkit (EMET) are installed on a Windows system, there can be interaction issues between the two, including disabling of Bit9 bans. To avoid these issues, either exclude Bit9 files from being managed by EMET, or install Bit9 prior to installing EMET. [42152]

- If a file approval is created with the same SHA-1 hash used in a file ban, the approval is creating a SHA-256 hash and that approval is overriding the SHA-1 file ban. [41444]

- In OS X 10.10.x, copy/paste or drag/drop of files on the Mac desktop is now implemented by a process owned by ‘root’ (i.e. Desktop Services). As such, the Bit9 Trusted User feature will not work with copy/paste or drag/drop if the trusted user is the logged-in user account. [40869]

- Upgrading from 7.0.1 to 7.2.0 will fail if, in the database table “certificate_state”, there are duplicate values for the fields “cert_id” and “publisher_id. When taken as a pair, these fields must be unique or the install will fail with an error such as “A critical database script (migrate.sql) needed to install Bit9 Server failed.” [41295]

- When creating a custom rule, under the top pulldown for Users and Groups, the ‘Local Adminstrators’ selection functions correctly. If the ‘Specific Users and Groups’ option is selected instead, and 'Local Administrator' is provided in the data entry field, the following error will be displayed at the top of the screen: "Error: SID for 'local administrator' was not found". [41017]

- Upgrades from a Bit9 Platform version 7.0.0.x to version 7.2.0 should be made only to Patch 4 or later builds. [40979]

- If the Bit9 Platform is installed or upgraded when application or system installs or upgrades are being performed it's possible that files will be discovered as unapproved and block in high or medium enforcement. Bit9 recommends deploying new installs and upgrades during a time when the target machine is not currently installing any other applications or doing any system or application updates. Alternatively, you can deploy in a low enforcement level and move to high or medium after initialization is complete. [40859]

- Publishers for files discovered on agent-managed computers are automatically added to the Publishers page on the Bit9 Console. The console also provides a method for manually adding a publisher so that you can approve or ban it before any of its files arrive on your computers.
  If you attempt to use the Add Publisher feature to manually add a publisher whose certificate chain ends in a Microsoft root certificate, the resulting publisher will be incorrectly identified as 'Microsoft Corporation' even though the Subject name field of the signing certificate shows a different name. This is known to happen, for example, with files from Skype. If your server has already identified 'Microsoft Corporation' as a publisher, the attempt to add the new publisher will fail. As a workaround, you can add a (non-threat) file containing the publisher on an agent-managed computer (with an active server connection), and the new publisher will be automatically added to the Publishers page. [40257]

- When agents are upgraded from 7.0.1 or earlier version to 7.2, this results in a cache consistency check on the agents. This can in turn lead to a large number of file messages from agent to server. A large number of agent upgrades in a short duration will lead to a significant drop in Sync % of server. Agent upgrades should be done in a controlled manner. [40901]

- When you upgrade the Server from v6.0.2 to v7.2.0, the agent management password no longer works in the DASCLI command line interface. The password must be reset in the system configuration page after upgrading. [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]

- An underscore at the end of a file name filter is ignored. An underscore in SQL is interpreted as wildcard character. [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 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 Bit9 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 operating systems. On Windows XP, if the system-wide DEP Policy is set to "AlwaysOff", dynamic code execution memory rules cannot be enforced, but the Bit9 Server 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.

- 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 by the Bit9 Platform 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]

- Changes in Bit9 Platform v7.2.0 require that the collation of the Bit9 Server database be set to the default US English collation. If the collation is set to something different, you will not be able to upgrade to v7.2.0, and you will be alerted that you need to contact Bit9 Support for assistance with the upgrade. [27119]

- When upgrading Bit9 Platform 7.0.1 or later from earlier releases, it may be necessary to update certain Microsoft SQL components. In this case, a Microsoft dialog will appear during the upgrade process. Follow the dialogs to update the associated Microsoft SQL components. Bit9 Platform upgrade will continue when this step is complete. [29819, 29822]

- 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 run into 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 Technical Support for remediation recommendations. Service pack upgrades are fully supported and do not cause health check failures. [33646]

- For Mac and Linux, the default Bit9 uninstall behavior is now to remove all Bit9 agent data. Bit9 releases prior to version 7.0.1 Patch 6 required an additional parameter ("-d") for this data to be removed. That same parameter now prevents data removal, if this is required. [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. Mac and Linux integration with Carbon Black is not implemented in Bit9 v7.2.0 [39284]

- On Mac and Linux, when a file is deleted by one process while another process has it opened for update (e.g. script file being edited) and the close occurs after the delete, Bit9 Platform may consider the file to have been deleted until it sees an execute of the target file. [39885]

Contacting Bit9 Support

For your convenience, Bit9 Technical Support offers several channels for resolving support questions:

Technical Support Contact Options
Web: www.bit9.com
E-mail: support@bit9.com
Phone: 877.248.9098 (877.**BIT9**.098)
Fax: 617.393.7499
Hours: 8 a.m. to 8 p.m. EST

Reporting Problems

When you call or e-mail Bit9 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 (Bit9 Server, Bit9 Agent, or Bit9 Software Reputation Service) and version number
Hardware configuration	Hardware configuration of the Bit9 Server or computer (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 after the copyright section of each manual.
Problem	Action causing the problem, error message returned, and event log output (as appropriate)
Problem severity	Critical, serious, minor, or enhancement