Compliance for Cloud and Virtualized Environments

White Paper

Using 5nine Cloud Security to Meet PCI DSS v3.0 Compliance

Authored By:

Morgan Holm – VP of Product Management at 5nine Software

Dr. Konstantin Malkov – CTO at 5nine Software

Contents

Introduction 1
Overview - PCI DSS v3 2
Cloud 3
Virtualization 5
5nine Cloud Security Mapping to PCI DSS High Level Requirements 6
Summary 8
Appendix A: 5nine Cloud Security Compliance Related Features 9

Introduction

Jurisdictions and industries around the world have put in place regulations that organizations of varying sizes and verticals must conform to. Failure to comply with some of these regulations can lead to damage to reputation, severe fines or even jail time. These regulations cover a wide range of policies and controls that can include the protection of credit card data and patient health records to the verification of published financial data among others. Regulatory compliance indicates how your organization meets specific security standards as mandated by the various regulatory organizations. These regulations should be viewed as the starting position for an organization's security policy.

Many organizations that do not have regulatory compliance mandates may have their own security policies or choose to conform to other published security standards such as ISO, NIST or CSA. No matter if you need to comply with a particular regulation, internal security policy or standard you will need the ability to enforce, track and report on your security settings and changes.

There are many similarities across the various regulations and standards. This document will examine some of the Payment Card Industry Data Security Standard (PCI DSS) requirements for cloud and virtualized environments. Many of these requirements will be applicable to systems that need to comply with other comparable regulations such as the Health Insurance Portability and Accountability Act (HIPAA), Sarbanes Oxley Act (SOX), Gramm-Leach-Bliley Act (GLBA) and the Federal Information Security Management Act (FISMA) among others.

Overview - PCI DSS v3

The PCI DSS standard applies to all organizations that store, process, or transmit cardholder data (CHD), regardless of volume. Merchants, cloud service providers (CSP) that are either storing or working with any aspect of payment card data are required to verify their compliance against over 400 specific test controls that are outlined in the standard.

Table 1 – High Level Overview of PCI DSS [1]

Category	Requirement
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

[1] PCI Security Council - PCI DSS Cloud Computing Guidelines (version 2.0, February 2013) retrieved from https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Cloud_Guidelines.pdf

Cloud

Many organizations of all sizes have been increasing their adoption of cloud computing. The cloud offers many advantages over on premise infrastructure such as the ability to consume computing resources like a utility. There is no need to procure, implement and maintain the computing infrastructure themselves. Some of the main benefits are the ability to quickly provision computing resources for nearly any type of workload (self-service), scale these computing resources up or down as needed (elasticity) and only pay for the resources actually consumed on a very granular level (pay per use).

There has been a reluctance to move some workloads and data to cloud service providers. Some regulations require data sovereignty where data and processing must occur in a particular geopolitical region. There has also been some questions around whether cloud service providers have the necessary policies and controls to meet compliance requirements. Many service providers have addressed these issues and do have the capabilities required by the regulations. Some are even offering security as a service (SECaaS) but it is up to the merchant or client organization to ensure the requirements are satisfied. Depending on the cloud model, control may lie with the service provider, client or both.

There are several different deployment and service models for cloud computing. This document will focus on public and hybrid cloud deployment models. The three most common service models are as follows:

IaaS – Infrastructure as a Service

- Provides the client with the ability to use the service provider's cloud infrastructure compute, memory, storage and network resources to install and run operating systems and software accessible over a network, typically the internet

PaaS – Platform as a Service

- Provides the client with the ability to deploy applications on the service provider's cloud infrastructure using supported application program interface (APIs), programming languages, libraries, services and tools
- PaaS offerings provide these services to clients at a higher layer than IaaS without direct access to low level computing resources accessible over a network, typically the internet

SaaS – Software as a Service

- Provides the client with the ability to use the service provider's application(s) running on cloud infrastructure accessible over a network, typically the internet
- SaaS offerings provide these services to clients at a higher layer than PaaS

Hosting companies, cloud service providers (service providers) may have not exactly followed these deployment and service models. The table below shows an example of how the control may be shared across the cloud service provider (CSP) and client.

Table 2: PCI DSS Shared Responsibilities[2]

Legend
Client
CSP
Client & CSP

PCI DSS Requirements	Example responsibility assignment for management of controls		
	IaaS	PaaS	SaaS
1. Install and maintain a firewall configuration to protect cardholder data	Client & CSP	Client & CSP	CSP
2. Do not use vendor-supplied defaults for system passwords and other security parameters	Client & CSP	Client & CSP	CSP
3. Protect stored cardholder data	Client & CSP	Client & CSP	CSP
4. Encrypt transmission of cardholder data across open, public networks	Client	Client & CSP	CSP
5. Use and regularly update anti-virus software or programs	Client	Client & CSP	CSP
6. Develop and maintain secure systems and applications	Client & CSP	Client & CSP	Client & CSP
7. Restrict access to cardholder data by business need to know	Client & CSP	Client & CSP	Client & CSP
8. Assign a unique ID to each person with computer access	Client & CSP	Client & CSP	Client & CSP
9. Restrict physical access to cardholder data	CSP	CSP	CSP
10. Track and monitor all access to network resources and cardholder data	Client & CSP	Client & CSP	CSP
11. Regularly test security systems and processes	Client & CSP	Client & CSP	CSP
12. Maintain a policy that addresses information security for all personnel	Client & CSP	Client & CSP	Client & CSP
13. PCI DSS Cloud Computing Guidelines (version 2.0, February 2013) - Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers	CSP	CSP	CSP

Note: Use of a PCI DSS compliant CSP does not result in PCI DSS compliance for the clients. The client must still ensure they are using the service in a compliant manner, and is also ultimately responsible for the security of their cardholder data (CHD) – outsourcing daily management of a subset of PCI DSS requirements does not remove the client's responsibility to ensure CHD is properly secured and that PCI DSS controls are met.

[2] PCI Security Council - PCI DSS Cloud Computing Guidelines (version 2.0, February 2013) retrieved from https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Cloud_Guidelines.pdf

Virtualization

The shift to highly virtualized environments makes compliance much harder to ensure and report that the settings are configured per the policy. Virtual environments are highly dynamic, servers can be deployed rapidly and migrated between hosts automatically. Virtualization introduces another layer of technology that must be implemented, administered, maintained, and monitored for compliance.

Microsoft Azure Pack can be implemented with Hyper-V to provide a consistent experience with public Azure. This gives organizations an option to provide a private cloud deployment model and cloud service providers with self-service, elasticity and pay per use (charge back) capabilities.

The Information Supplement: PCI DSS Virtualization Guidelines (June 2011) identifies four "principles associated with the use of virtualization in cardholder data environments": [3]

a. If virtualization technologies are used in a cardholder data environment, PCI DSS requirements apply to those virtualization technologies.
b. Virtualization technology introduces new risks that may not be relevant to other technologies, and that must be assessed when adopting virtualization in cardholder data environments.
c. Implementations of virtual technologies can vary greatly, and entities will need to perform a thorough discovery to identify and document the unique characteristics of their particular virtualized implementation, including all interactions with payment transaction processes and payment card data.
d. There is no one-size-fits-all method or solution to configure virtualized environments to meet PCI DSS requirements. Specific controls and procedures will vary for each environment, according to how virtualization is used and implemented.

[3] PCI Security Council - The Information Supplement: PCI DSS Virtualization Guidelines (June 2011) retrieved from https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf

5nine Cloud Security Mapping to PCI DSS High Level Requirements

1. *Install and maintain a firewall configuration to protect cardholder data* (CHD)
   a. 5nine Cloud Security provides an integrated stateful packet inspection (SPI) firewall to protect CHD.
   b. The 5nine Cloud Security firewall is multi-tenant enabling cloud service providers (CSPs) to automatically and immediately isolate systems and data between customers on shared infrastructure.
   c. 5nine Cloud Security with the Microsoft Azure Pack extension allows clients to control and define firewall rules in accordance with PCI DSS requirements.
   d. The 5nine Cloud Security firewall rules can be bound directly to the Virtual Machine (VM) so that if it is migrated manually or automatically the rules will still be enforced even if its IP addresses have changed.
   e. The solution is designed to enable micro segmentation to only allow traffic and protocols required by the VMs for a particular workload. All traffic is blocked except where allowed by rule configuration.
   f. Firewall rules can be configured to restrict direct inbound traffic to specific designated hosts in a DMZ and restrict unauthorized outbound traffic.
   g. The 5nine Cloud Security firewall is implemented at the Hyper-V virtual switch level enabling the examination of all traffic in and out of the virtual host (North and South bound) and between all VMs on the host, even on a private switch (East and West bound) that traditional firewalls miss.
2. *Do not use vendor-supplied defaults for system passwords and other security parameters*
   a. 5nine Cloud Security leverages Active Directory (AD) integrated authentication enforcing the user to follow the defined AD password policy. No default passwords exist.
   b. 5nine Cloud Security also allows for the creation of custom users and passwords with configurable password strength and lockout capabilities.
3. *Protect stored cardholder data* (CHD)
   a. 5nine Cloud Security does not provide any direct feature to protect CHD
   b. For certain scenarios, 5nine Cloud Security firewall rules could be used to restrict traffic to servers and ports for services that are using encryption like encrypted SQL connections or https.
4. *Encrypt transmission of cardholder data across open, public networks*
   a. 5nine Cloud Security does not provide any direct feature to encrypt traffic.
   b. For certain scenarios, 5nine Cloud Security firewall rules could be used to restrict traffic to servers and ports for services that are using encryption like https.
5. *Use and regularly update anti-virus software or programs*
   a. 5nine Cloud Security provides a selection of three anti-virus (AV) or anti-malware (AM) engines and signatures, Bitdefender, Kaspersky and ThreatTrack Vipre allowing organizations to choose the best solution for their needs based on preference or geopolitical reasons.
   b. The solution is designed specifically to work in cloud and virtualized environments providing agentless scans that are 70 times faster than installing endpoint AV inside of each VM. This approach greatly reduces resource utilization allowing for greater VM density per host.
   c. 5nine Cloud Security leverages a change block tracking (CBT) driver to allow for fast incremental scans, allowing for more frequent scans with minimal impact to cloud or virtual resources.
   d. Configurable update frequency for AV/AM signatures to ensure the product is working against latest known threats.
   e. The system state can be configured to log operations and actions for auditing.
   f. Alerts can be configured when there are failures with the AV/AM services or signature updates. These failure notifications allow for immediate remediation to minimize the risk. Alerts can also be configured for the detection of any virus or malware.

g. Signatures can be downloaded directly from the AV/AM vendor or through a centralized source for efficiency. A manual update utility is also available for systems with no internet connectivity.
h. Cloud service providers can also offer their clients anti-virus as a service (AVaaS) through integration with Azure Pack.

6. *Develop and maintain secure systems and applications*
   a. 5nine Cloud Security is not used for the development of applications.
   b. However, 5nine Cloud Security does include features to verify the integrity of its own operations and data.
   c. 5nine Cloud Security also has an Intrusion Detection System (IDS), Snort that can detect application level attacks through the Snort engine and signatures implemented on the Hyper-V virtual switch.
7. *Restrict access to cardholder data by business need to know*
   a. 5nine Cloud Security does not provide this feature directly, typically accomplished through identification and access control mechanisms such as AD.
   b. 5nine Cloud Security implements roles to manage application access. These roles can be assigned globally or to a particular tenant.
      - Security Administrator – View information and modify settings
      - Auditor – View settings and logs but not make any configuration modifications
8. *Assign a unique ID to each person with computer access*
   a. 5nine Cloud Security typically uses identification and access control mechanisms such as AD which has unique user IDs.
   b. When custom 5nine users are created, each custom user has a unique ID that is referenced in all audit logs.
9. *Restrict physical access to cardholder data*
   a. 5nine Cloud Security does not provide physical access controls.
10. *Track and monitor all access to network resources and cardholder data*
    a. 5nine Cloud Security tracks and logs all operations including modifications of the application whether user initiated or the result of an event.
    b. Integrity of the log data and signatures is verified by the system.
    c. The 5nine Cloud Security firewall can be configured to log all allowed and blocked packets to track and monitor all access and attempts.
    d. 5nine Cloud Security supports output to a Syslog server for integration into external SIEM systems for firewall, AV/AM and IDS logs.
    e. Alerts can also be configured when network anomalies are detected by 5nine Cloud Security.
11. *Regularly test security systems and processes*
    a. 5nine Cloud Security has an integrated Intrusion Detection System (IDS), Snort that can continuously detect intrusions based on the latest Snort signatures.
    b. 5nine Cloud Security automatically analyzes network traffic for anomalies with a heuristics algorithm for notification of potential malicious activity.
12. *Maintain a policy that addresses information security for all personnel*
    a. 5nine Cloud Security enables and maintains a security policy with respect to the cloud or virtual infrastructure.

Summary

5nine Cloud Security provides the required functionality to many of the PCI DSS requirements for virtual and cloud environments. Multi-layered protection is provided with an integrated virtual firewall, anti-virus and Intrusion Detection System (IDS).

5nine Cloud Security provides protection for all Hyper-V networks to help organizations achieve their regulatory compliance mandates, internal security policies or security standards by tracking and reporting against elements of the following regulations and standards:

- PCI DSS (Payment Card Industry Data Security Standard) - https://www.pcisecuritystandards.org/
- HIPAA (Health Insurance Portability and Accountability Act) - http://www.hhs.gov/ocr/privacy/hipaa/understanding/
- SOX Sarbanes-Oxley Act - http://www.sec.gov/about/laws.shtml
- North American Electric Reliability Corporation (NERC) - http://www.nerc.com/Pages/default.aspx
- Federal Energy Regulatory Commission (FERC) - http://www.ferc.gov/
- NIST SP 800 series - http://www.nist.org/nist_plugins/content/content.php?cat.17
- Federal Information Security Management Act (FISMA) - http://csrc.nist.gov/groups/SMA/fisma/
- ISO 27001 - http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
- CSA (Cloud Security Alliance) - https://cloudsecurityalliance.org/
- SANS Institute - https://www.sans.org/

Many other regulations, standards, frameworks and certifications are either based off or are derivations of the above list.

No matter if you are a hosting provider or an organization, multiple tenants in your virtual network will have access to all required resources while being isolated and protected from each other.

- **Provide Hyper-V VM isolation**

With cloud and virtualized environments there are new types of security threats. 5nine Cloud Security allows you to protect your virtual machines from any internal and/or external network security breach using unique, agentless, patent-pending v-Switch filtering technology.

- **Protect Hyper-V with patent-pending agentless antivirus**

5nine Cloud Security provides unique patent-pending agentless anti-virus technology for Hyper-V that allows saving resources and increasing VM density by up to 30-50%. As a result, it leads to a major reduction of capital expenditure on physical infrastructure.

- **Enforce Microsoft Cloud compliance**

For any additional details – please refer to our Resource Center and Product Pages:

http://www.5nine.com/Whitepapers.aspx

http://www.5nine.com/5nine_webinars.aspx

http://www.5nine.com/5nine-security-for-hyper-v-product.aspx

Appendix A: 5nine Cloud Security Compliance Related Features

5nine Cloud Security has many powerful features designed specifically for compliance that allow you to:

•Secure multi-tenant Hyper-V environment and provide VM isolation using patent pending virtual switch filtering extension

•Protect Hyper-V with patent-pending agentless Bitdefender, Kaspersky or Threat Track antivirus now with Real-Time Malware Detection

•Enforce security compliance

5nine Cloud Security's powerful features allow organizations to secure a wide range of Microsoft Cloud environments with flexible management options including Azure Pack, System Center VMM plugin and the 5nine Management Console.

1. Enhanced viewing, sorting and filtering of log data in 5nine Cloud Security

A key characteristic to any regulatory compliance initiative or internal security policy is being able to know what changes are being made to the security systems themselves and any events or alerts these systems generate.

- All columns can be sorted
- Substring search
- Filter data by time
- Additional filters by key fields available for each log

Security administrators need to look through data collected to assess potential threats. Auditors need to verify that the configurations and processes meet specific regulatory compliance and or the organization's internal security policies. When viewing detailed information it is necessary to be able to find the data you are looking for and view it in a way that's easy to consume.

2. Expanded Events and Detailed Event Information in 5nine Cloud Security

To prove and maintain compliance with a regulation, standard or internal security policy, the systems that implement the policies need to track and record the relevant information. This is especially true when security is the focus. 5nine Cloud Security has events for the major areas of functionality. The event detail level is customizable for certain events to allow the desired information to be retained when needed, specifically when certain levels may cause extensive events to be captured.

2.1. Cloud Security Antivirus

2.1.1. Additional fields for scanning jobs

2.1.1.1. Who started the scan

- Specific user
- System

2.1.1.2. Scan Settings

2.1.1.3. Start Mode
- Scheduled
- Manual

2.1.2. Antivirus job logging levels
2.1.2.1. Maximum level – Monitor all scanned files and log any events
2.1.2.2. Standard level – Only files with malware and a general overview
2.1.3. Additional fields for processing infected (quarantined) objects
2.1.3.1. Type of malware
2.1.3.2. Action result – Attempts to move objects into quarantine or remove from system
- Success
- Failure

2.1.4. Subject ID – Antivirus scan task user
2.1.5. Available fields for filtering view:
2.1.5.1. Scan Log
- Time started
- Time finished
- Type
- Label
- Status

2.1.5.2. Processing log (quarantine):
- Event time
- Type
- Event result, "action…"

2.2. Cloud Security Intrusion Detection System (IDS)
2.2.1. Subject ID field – The ID of the virtualization host
2.2.2. Available fields for filtering view:
- Time
- Event type
- Priority
- Subject (host) ID

2.2.3. 5nine Cloud Security saves the statistics in a separate log with the parameter type, the average and receive value, and the time of the suspected exploit/malware.

2.3. User log
2.3.1. Field with the ID of the management server where the action is performed.
2.3.2. Log user's privileges in the user sign-in event.
2.3.3. Log the rights being changed in the user rights changed event.
2.3.4. Available fields for filtering view:
- Date
- Action
- Result
- Event Source (management server) ID
- Access type

2.4. System log
2.4.1. Event Source field (the event source's ID)
2.4.2. Available fields for filtering view:
- Date
- Time
- Operation
- Result
- Event Source
- Target

2.5. Audit Events – 5nine Cloud Security has auditing for the following events:

2.5.1. Starting or stopping 5nine Cloud Security services

2.5.1.1. Audit entry for starting the management service

- Service name
- Start of audit functions
- Service Version #

Audit entry for stopping the management service (when possible).

2.5.1.2. Audit entry for starting the host service

- Service name
- Start of audit functions
- Service Version #

Audit entry for stopping the host service (when possible).

2.5.1.3. Audit entry for starting the antivirus service

- Service name
- Start of audit functions
- Service Version #

Audit entry for stopping the antivirus service (when possible).

2.5.2. Check and log whether the previous termination of the service's operation was unexpected.

2.5.3. When the antivirus service is started the integrity of the antivirus database is verified. The database status of healthy, missing or corrupted is also saved.

2.5.4. Events are logged for the reading of the audit entries for various user actions including failed attempts. This is a configurable option since there is the potential for a large number of entries.

2.5.5. System and State Monitoring

2.5.5.1. Ability to log all of the attempts to query the state of a host

- No logging (default due to potential database and network overhead)
- Logging enabled – Typically only needed in highly regulated environments

2.5.5.2. System also records the component state changes in the log

- No logging
- Logging enabled

2.5.5.3. Logging the switching of a host between servers (in "additional info" to indicate "from where and to where"). This event is also replicated between servers.

2.5.5.4. Logging the version change of the host's software, the antivirus in particular (based on the monitoring data)

2.5.6. Antivirus and IDS

2.5.6.1. 5nine Cloud Security logs all operations on the databases (Management service, hosts, Active Protection), including failed operations and "no updates".

2.5.6.2. Logs all changes in the state of the Active Protection (AP) agent

- Start/Stop operations.

2.5.6.3. In the agent's status, after Start save the status of the databases (healthy/missing/corrupted).

2.5.6.4. Logs all changes in the state of the ‘Lightweight Agent’ used for removal of malware during agentless on demand or scheduled scans

- Start/Stop operations.

2.5.6.5. In the agent's status, after Start save the status of the databases (healthy/missing/corrupted).

2.5.7. Log all changes to the state of the AP databases (based on the heartbeat)

2.5.8. Logs the version of the AP agent upon installation

2.5.9. Logs the version (change in version) of the AP agent (based on the heartbeat)

2.6. 5nine Cloud Security monitors the updates of antivirus databases on hosts and Active Protection agents. Identify (including by analyzing the data collected from events) and log other events (in the system log)

2.6.1. Failures or suspicion of a failure in the Active Protection (AP) agent such as:

- The agent has not been connected for a long time
- The agent has not been started

2.6.2. The databases have not been updated in a long time

- The antivirus databases on the 'AV receiving' host (and thus all other hosts in the environment) are out of date
- The antivirus databases on the host are corrupt (or missing)
- The antivirus databases on the AP agent are out of date
- The antivirus databases on the agent are corrupt (or missing)
- The antivirus databases on the management server are out of date (if using this function of the management server)

2.7. 5nine Cloud Security also monitors updates of the IDS databases (currently Cisco SNORT) on the 'Receiving hosts' and the management server (and thus other monitored and protected hosts in the environment(s)). Identifies and logs other events (in the system log).

- The IDS databases on the host(s) are out of date
- The IDS databases on the management server(s) are out of date (if using this function of the management server)
- The IDS databases on the host(s) are corrupt (or missing)

3. Notifications (Alerts)

5nine Cloud Security provides fine grained control over which events or conditions will generate an alert. It is extremely important to not overwhelm system or security administrators with too many alerts as they will simply be ignored. The important information that should actioned upon will be missed and could lead to unwanted consequences.

3.1. Notifications in the control panel

The control panel has a view where you can see notifications from the system. These notifications are "confirmable" by the administrator either explicitly or by "viewing" events.

The control panel notifications are configurable, so the admin can specify which of the available event types to show and which not to show (for example, don't show events for packets dropped by the firewall). The content of the notification matches the content of the corresponding entry in the log.

3.2. Events notifications

- Virus detection
- Blocking of packets by the firewall (configurable)
- Intrusion detection (using both signatures and KAV or Bitdefender heuristics)
- Antivirus database updates on hosts, Active Protection agents (2.6 events)
- Configurable

- Failure to load AV and IDS updates to the management server(s), virtualization hosts, and AP agent

3.3. In addition to the notification in the control panel, there is a configurable option to send notifications to an email address.

4. Enhanced Functionality

4.1. Centralized database updates for both Antivirus and intrusion detection system databases. ("Centralized updates of signatures “)

4.2. Ability to add newly created VM to various VM Security Groups or apply global Virtual Firewall Rules templates provided the desired security configuration when created.

4.3. Replication of the user action log and the system log provides a consistent view of log information across a redundant implementation.

4.4. Updates to internal security configuration.
- 4.4.1. Verify password strength for custom users (when creating / changing).
- 4.4.2. Timeout after a failed sign-in attempt – for both custom users and windows users.

4.5. Antivirus
- 4.5.1. Antivirus scanning of system areas. For fixed disks (including VM disks), on-demand and scheduled scans.
  - 4.5.1.1. Aide of the existing "scan all files or by file extension" and "scan all “, - provide user a choice of selecting one or more objects for scanning: system areas of disks, critical file paths (OS, loaders), user-specified paths or everything.
- 4.5.2. Deleting (disinfection) of viruses in system areas.
- 4.5.3. Local update of antivirus without automated tools (antivirus databases) on the host as a utility. Includes an ability to check the integrity of existing databases on the virtualization host(s). UAC calls are made from the utility, - similar to integrity verification utilities.
- 4.5.4. Active Protection (AP) agent
  - 4.5.4.1. Monitor the integrity of AP binaries inside of virtual machines
  - 4.5.4.2. Monitor the AP agent's heartbeat – log its absence (events of 2.6 above), display it in the UI
  - 4.5.4.3. Force the update of the Active Protection agent's databases (configurable)
  - 4.5.4.4. Version of the installed agent and the version of the databases is shown in the Active Protection tab.
- 4.5.5. Disinfection of malware. Subjected objects are explicitly specified as: files, system areas of virtual disks, email messages). (See also 4.5.2).