Bitdefender®

How to address PCI compliance, security and performance in the datacenter

Overview

The Payment Card Industry Data Security Standard (PCI DSS 3.0) specifies requirements to secure cardholder data that is stored, processed or transmitted by merchants and any other organization. The requirements of PCI include building and maintaining a secure network by: providing endpoint antimalware, installing and maintaining a firewall configuration to protect cardholder data, maintaing a vulnerability management program by using and regularly updating anti-virus software or programs, implementing strong access control measures.

A significant set of problems is encountered when organizations are required to maintain endpoint security across physical, virtualized, and cloud endpoints. Traditional anti-virus software introduces performance and management challenges that increase total cost of ownership, while not gaining robust security.

This document outlines an approach that is tailored to changing environments, while also providing comprehensive insight and control across highly heterogeneous requirements, without sacrificing security.

PCI DSS Requirements

The following are the twelve requirements listed in the Payment Card Industry (PCI) Data Security Standard:

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

3. Protect stored cardholder data

4. Encrypt transmission of cardholder data across open, public networks

5. Use and regularly update anti-virus software

6. Develop and maintain secure systems and applications

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

10. Track and monitor all access to network resources and cardholder data

11. Regularly test security systems and processes

12. Maintain a policy that addresses information security

The Solution

GravityZone is a resource-efficient security solution that provides high performance without sacrificing protection and compliance needs. GravityZone delivers a pioneering centralized management architecture that is easy to deploy, providing GravityZone customers the freedom to choose any combination of virtualization vendors, cloud providers and endpoint devices.

Bitdefender GravityZone provides software-based integrated security and compliance for business that contributes to compliance with requirements 1, 5, 10, 11.

Overview of GravityZone and PCI

Bitdefender GravityZone protects your investment in virtualization and minimizes your administrative effort. Powered by leading detection technologies, the solution delivers resource-efficient security for virtual machines, physical endpoints and mobile devices from the intuitive Control Center. This fully integrated administrative interface is used to deploy, monitor and report on the company's security posture.

In virtualized environments, GravityZone plugs into VMware vCenter, Citrix XenServer, and Microsoft Active Directory, to ensure end-to-end visibility across the datacenter. Turnkey deployment combined with role-based allocation of the GravityZone appliance further increases the scale and streamlines the management operations.

GravityZone is hypervisor-agnostic and delivered as a virtual appliance for quick and easy deployment across any combination of virtualization platforms and devices. Integration with VMware vShield Endpoint provides the option of "agentless" security. In addition, Bitdefender provides centralized endpoint security that offloads scanning functionality to a virtual appliance across heterogeneous hypervisors, including ESXi, Xen, Hyper-V, and others. This deduplication of endpoint antimalware in virtualized environments provides protection with a performance profile that is demonstrably superior to traditional approaches, leading many organizations to choose Bitdefender for Windows and Linux VM security, regardless of the virtualization platform.

Bitdefender helps organizations meet PCI DSS V3.0 requirement 1 by deploying a two-way firewall along with an IDS/IPS (Intrusion Detection/Prevention System) that monitors network packages and blocks intrusion or hijack attempts when connecting to public networks. The firewall protection includes any device directly connected to the internet including laptops, and POS fixed or mobile running embedded windows.

GravityZone is built from the ground up as a hypervisor-agnostic solution on a modular architecture which enables the assignation of primary functions to different physical or virtual servers. Technologies like Application Control and Antivirus Control manage enabling or disabling only mission critical services and address security vulnerabilities. For configuration needs, Application Control delivers all required access standards by enforcing access policies, all these technologies enable requirement 2 compliance.

GravityZone meets requirement 5 by providing top antimalware protection to various operating systems, physical or virtualized, servers and end-user. The latest antivirus signatures are automatically updated from the Bitdefender cloud while the GravityZone Self Protect feature makes it tamper proof.

GravityZone provides a wide array of event logs that include: type of event, date and time, success or failure indication, origination of event, identity or name of affected data system component or resource. Event information can be forwarded to centralized logging servers via syslog in real time for easy and quick access and to meet requirement 10.

Bitdefender GravityZone includes a host-based IDS/IPS module that monitors traffic, prevents intrusions, and issues alerts potential intrusions. Security updates that protect systems from newly discovered vulnerabilities are automatically delivered. GravityZone is able to identify vulnerable applications running on hosts and apply protection rules.

MEETING PCI DSS V 3.0 COMPLIANCE REQUIREMENTS

PCI Requirement	Bitdefender GravityZone compliance support
1.1 Establish firewall and router configuration standards that include: 1.2 Build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment. 1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment. 1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.	Bitdefender GravityZone includes a two-way firewall with IDS/IPS that monitors network activity and blocks intrusion or hijack attempts when connected to public networks
1.4 Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet.	The protection can be extended to any device directly connected to the internet including laptops, POS fixed or mobile running embedded Windows operating systems.
5.1 Deploy anti-virus software on all systems commonly affected by malicious software	GravityZone provides top antimalware protection for multiple platforms (Windows/Linux/Mac) physical and virtualized servers and end-user devices.

PCI Requirement	Bitdefender GravityZone compliance support
5.2 Ensure that all anti-virus mechanisms are current	Antivirus signatures are automatically updated from the Cloud.
5.3 Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.	GravityZone's Self Protect feature makes it tamper proof, while the endpoint is tailored to be managed only by a system admin that controls/enforces policies from the management console taking the load of decision away from the enduser.
10.3 Record at least the following audit trail entries for all system components for each event: - User identification - Type of event - Date and time - Success or failure indication - Origination of event - Identity or name of affected data system component or resource	GravityZone provides a wide array of reports containing information such as: - Type of event - Date and time - Success or failure indication - Origination of event - Identity or name of affected data system component or resource All this information is forwarded to the syslog for easy access.
10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	Event information is forwarded to centralized logging servers via syslog in real time.
11.4 Use IDS, and/or intrusion prevention system (IPS), to monitor all traffic at the perimeter of the CDE as well as at critical points inside the CDE. Keep all intrusion-detection and prevention engines, baselines, and signatures up-to-date.	GravityZone includes a host-based IDS module that monitors traffic, prevents intrusions, and alerts for potential intrusions. Security updates that protect from newly discovered vulnerabilities are automatically delivered to customers and hosts. GravityZone is able to identify vulnerable applications running on hosts and apply default protection rules to protect them.

Bitdefender delivers security technology in more than 100 countries through a cutting-edge network of value-added alliances, distributors and reseller partners. Since 2001, Bitdefender has consistently produced market-leading technologies for businesses and consumers and is one of the top security providers in virtualization and cloud technologies. Bitdefender has matched its award-winning technologies with sales alliances and partnerships and has strengthened its global market position through strategic alliances with some of the world's leading virtualization and cloud technology providers.

FOR MORE INFORMATION VISIT: enterprise.bitdefender.com

BD-Business-Feb.24.2016-TK#: 70595