Bitdefender

WHITEPAPER Jul 2023

How to Tackle PCI DSS Compliance with Bitdefender MDR

Contents

INTRODUCTION 3

CHALLENGES AND THE TRUE COST OF NON-COMPLIANCE 3
- CERTIFICATION AND ASSESSMENT 3
- PENALTIES FOR NON-COMPLIANCE 4

DOES PCI DSS APPLY TO YOU? 4

GOALS, REQUIREMENTS, AND UPDATES 5
- BUILD AND MAINTAIN A SECURE NETWORK AND SYSTEMS 5
- PROTECT ACCOUNT DATA 5
- MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM 6
- IMPLEMENT STRONG ACCESS CONTROL MEASURES 6
- REGULARLY MONITOR AND TEST NETWORKS 6
- MAINTAIN AN INFORMATION SECURITY POLICY 6
- CHANGES TO PCI DSS VERSION 4.0 6

SIMPLIFYING COMPLIANCE 7
- THE NEW STANDARD 8

PCI DSS & MANAGED DETECTION & RESPONSE: BITDEFENDER MDR HELPS YOU COMPLY WITH THE FOLLOWING SECURITY STANDARDS 8

WHY CHOOSE BITDEFENDER MDR? 10

MDR FOR XDR 10
- FEATURES AND BENEFITS OF MDR 11
- SOURCES 12
- OTHER SOURCES USED 12

INTRODUCTION

The Payment Card Industry Data Security Standard (PCI DSS) has served as the de facto standard for protecting cardholder data across the world since its implementation in 2004. The standards were developed by the PCI Security Standards Council (PCI SSC), a global forum that brings together payment industry stakeholders to develop and drive adoption of data security standards and resources for safe payments worldwide[1].

PCI security standards are designed specifically to protect payment account data throughout the payment lifecycle – and to enable technology solutions that devalue this data and remove the incentive for criminals to steal it. And steal it they will. ***According to IBM's 2022 Cost of a Data Breach Report, 2022 revealed costlier and higher-impact data breaches than ever before, with the global average cost of a data breach reaching an all-time high of $4.35 million for studied organizations, and breach costs increasing nearly 13% over the last two years***[2]. Often, actions related to PCI non-compliance are the culprit.

The PCI DSS is a standard, not a law, and it is enforced through contracts between merchants, acquiring banks that process payment card transactions, and the payment brands. And each payment brand has the ability to fine acquiring banks for PCI DSS compliance violations[3].

Compliance, in this case, is a business management discipline, not an information technology discipline, and effective, long-term data security and compliance combines the responsibilities of several roles, including the Chief Information Security Officer, the Chief Risk Officer, and Chief Compliance Officer.

In 2019, consumers and businesses substantially increased business activities conducted online, and they haven't slowed down since[4]. The COVID-19 pandemic escalated the trend and, as a result, the number of payment card transactions increased in tandem. Simultaneously, the abilities and resilience of attackers continues to evolve and increase in severity, paving the way for the successful exploitation of both existing and emerging threats and frailties within payment systems and processes.

Additionally, digital transformations that rely heavily on cloud technologies are introducing new drivers that impact the payment security industry, further complicating the role of CISOs and other security managers and practitioners[5].

In response to these recent challenges, the PCI Security Standards Council (SSC) performed a major rewrite of the PCI DSS v4.0. This refresh will help organizations ensure that data security controls remain current and effective in a changing landscape. It's the most significant update to the PCI DSS since its initial release in 2004 – 18 years ago**.** With changes that include mandating authenticated vulnerability scans, enforcing multifactor authentication (MFA) for all access to card data environments (CDE) and more frequent scope validation for various sectors[6], the effort required to meet PCI DSS 4.0 shouldn't be underestimated. While the enforcement date of March 31, 2024, may seem far off, *now* is an imperative time for business leaders, IT security personnel and compliance officers to begin forming a plan.

The standards, consisting of control objectives and their corresponding requirements, are extensive and can be overwhelming to get a grasp of; version 4.0 consists of 360 pages in total. Understanding how it works and how to successfully demonstrate compliance with each standard is important. The benefits of compliance are ample. Many businesses don't realize that PCI DSS protects more than just payment account data.

It's true that the requirements are designed to focus on environments with payment card account data, but PCI DSS can also be used to protect against threats and secure other elements in the payment ecosystem[7]. This guide provides a comprehensive introduction to payment card industry rules mandated under PCI DSS, as well as how Bitdefender Managed Detection and Response (MDR) can help you tackle compliance like a pro.

CHALLENGES AND THE TRUE COST OF NON-COMPLIANCE

Leaders of a PCI compliance team should be determined by an organization's structure and size. Small businesses who outsource aspects of their payment infrastructures to third parties can usually depend on those same vendors to handle their PCI compliance. Large entities, however, might find it necessary to add executives, IT, legal representatives, and business unit managers. In the world of PCI DSS, one size does not fit all. The PCI Standards Security Council also provides guidance on this topic on their website[8], if needed.

Certification and assessment

Remember, PCI DSS can be tricky because technically, certification doesn't exist. The most frequently used method of demonstrating compliance with PCI DSS is by filling out the appropriate questionnaire and completing an attestation of compliance (AOC)[9]. This is known as a self-assessment.

Penalties for non-compliance

The PCI DSS is a standard, not a law, and is enforced through contracts between merchants, acquiring banks that process payment card transactions and the payment brands. Each payment brand can fine acquiring banks for PCI DSS compliance violations. In turn, acquiring banks can withdraw the ability to accept card payments from non-compliant merchants.

Compliance obligations for merchants also increase substantially in the event of a breach. Cardholder data breach or theft is also a breach of the EU's General Data Protection Regulation (GDPR). Data breaches risk heavy penalties under the regulation: up to €20 million or 4% of annual global turnover – whichever is greater[10].

The payment card industry has established fines of up to $500,000 per incident for security breaches when merchants are not PCI DSS-compliant, and all individuals whose information is believed to have been compromised must be notified in writing to be on alert for fraudulent charges. Failure to effectively comply with PCI DSS standards could lead to a security breach costing more than $500,000 when the cost of customer notification and recovery is accounted for.[11]

The potential cost of a security breach:

- Fines of $500,000 per incident for being PCI non-compliant
- Increased audit requirements
- Potential for campus wide shut down of credit card activity by our merchant bank
- Cost of printing and postage for customer notification mailing
- Cost of staff time (payroll) during security recovery
- Cost of lost business during register or store closures and processing time
- Decreased sales due to marred public image and loss of customer confidence[12]

DOES PCI DSS APPLY TO YOU?

PCI DSS is intended for all entities that store, process, or transmit cardholder data (CHD) and/or sensitive authentication data (SAD) or could impact the security of the cardholder data environment (CDE).

Standards apply to merchants, service providers, and financial institutions on security practices technologies and processes, and standards for developers and vendors to create secure payment products and solutions. Merchants accept debit or credit card payments for goods or services; PCI DSS applies to them, even if they have subcontracted their payment card processing to a third party. Service providers are also directly involved in processing, storing, or transmitting cardholder data on behalf of another entity.

Some requirements apply only when the entity being assessed is a service provider. These are identified within the requirement as "Additional requirement for service providers only" and apply in addition to all other applicable requirements. Where the entity being assessed is both a merchant and a service provider, requirements noted as "Additional requirement for service providers only" apply to the service provider portion of the entity's business. Requirements identified with "Additional requirement for service providers only" are also recommended as best practices for consideration by all entities[13].

Some organizations can be both a merchant and a service provider. For example, an organization that provides data processing services for other merchants will also be a merchant if it accepts card payments.

The payment card industry standards have a significant impact on almost every sector.

This includes all entities involved in payment account processing in those segments – merchants, processors, acquirers, issuers, and other service providers. Cardholder data and sensitive authentication data are considered account data and are defined as follows:[14]

Account Data	
Cardholder Data includes	**Sensitive Authentification Data includes**
• Primary Account Number (PAN) • Cardholder Name • Expiration Date • Service Code	• Full track data (magnetic-stripe data or equivalent on a chip) • Card verification code • PINs/PIN blocks

As mentioned previously, PCI DSS requirements apply to entities with environments where account data (cardholder data and/or sensitive authentication data) is stored, processed, or transmitted, and entities with environments that can impact the security of the CDE.

But some PCI DSS requirements may also apply to entities with environments that do not store, process, or transmit account data – for example, entities that outsource payment operations or management of their CDE. The primary account number (PAN) is the defining factor for cardholder data. The term account data includes: the full PAN, any other elements of cardholder data that are present with the PAN, and any elements of sensitive authentication data. If cardholder name, service code, and/or expiration date are stored, processed, or transmitted with the PAN, or are otherwise present in the CDE, they must be protected in accordance with the PCI DSS requirements applicable to cardholder data[15].

GOALS, REQUIREMENTS, AND UPDATES

In total, there are 12 PCI DSS requirements that revolve around 6 main goals (also called "control objectives"): to build and maintain a secure network, protect cardholder data, maintain a vulnerability management program, implement strong access control measures, regularly monitor and test networks, and maintain an information security policy.

The 12 PCI Security Standards and where they apply to the payment process:

Introduction to PCI DSS

PCI DSS was developed to encourage and enhance payment account data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect payment account data.

Goals	PCI DSS Requirements
Build and Maintain a Secure Network and Systems	1. Install and maintain network security controls 2. Apply secure configurations to all system components
Protect Account Data	3. Protect stored account data 4. Protect cardholder data with strong cryptography during transmission over open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems and networks from malicious software 6. Develop and maintain secure systems and software
Implement Strong Access Control Measures	7. Restrict access to system components and cardholder data by business need to know 8. Identify users and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Log and monitor all access to system components and cardholder data 11. Test security of systems and networks regularly
Maintain an Information Security Policy	12. Support information security with organizational policies and programs

Build and Maintain a Secure Network and Systems

Theft of financial records once required a thief to physically enter an organization's business site. Payment transactions have been updated and now happen with a plethora of electronic devices, including traditional payment terminals, mobile devices, and other Internet-connected computer systems. By using network security controls, entities can prevent criminals from virtually accessing payment system networks and stealing payment account data.

1. **Install and maintain network security controls** in order to prohibit unauthorized access to systems.
2. **Apply secure configuration to all system components**. It might go without saying, but it's especially important to avoid using defaults supplied by vendors for system passwords and addition security elements.

Protect Account Data

This applies to any data printed, processed, transmitted, or stored in any form on a payment card. Account data refers to both cardholder data and sensitive authentication data, and protection of the account data is required where account data is stored, processed, or transmitted. Entities accepting payment cards are expected to protect account data and to prevent its unauthorized use – whether the data is printed or stored locally, or transmitted over an internal or public network to a remote server or service provider.

3. **Protect stored account data.**
4. **Use strong cryptography when transmitting cardholder data across open, public networks.** These requirements ensure you safeguard data at rest *and* in motion.

Maintain a Vulnerability Management Program

Systematically and continuously finding and mitigating weaknesses in an entity's payment card environment is how you manage vulnerability. This includes addressing threats from malicious software as well as consistently identifying and patching vulnerabilities.

5. **Protect systems and networks from malicious software.** Bad actors can (and will) infiltrate access to stored data with malware – proactive vigilance is necessary.
6. **Develop and maintain secure systems and applications.** Make sure you implement security measures and keep them current.

Implement Strong Access Control Measures

This kind of sensitive access should be on a need-to-know basis. Logical access controls are technical means used to permit or deny access to data on computer systems. Physical access controls entail the use of locks or other physical means to restrict access to computer media, paper-based records, and computer systems.

7. **Restrict access to cardholder data by business need-to-know.** You should already be practicing this, but it applies to financial data in particular.
8. **Identify users and authenticate access to system components.** This will allow investigators to determine if an authorized insider misused data while protecting against unauthorized access. Each authorized user should have their own access ID.
9. **Restrict physical access to cardholder data**.

Regularly Monitor and Test Networks

Whether networks are physical, virtual, or wireless, they join all endpoints and servers in the payment architecture. Vulnerabilities in network devices and systems means hackers can gain unauthorized access to payment applications and payment account data. Monitor and test regularly.

10. **Log and monitor all access to network resources and cardholder data.** One of the most commonly violated requirements.
11. Regularly test security systems and processes.

Maintain an Information Security Policy

Your security policy determines the culture of your business. It gives employees an understanding of their security responsibilities.

12. **Maintain a policy that addresses information security.** These last two requirements ensure that the steps you take to meet the previous ten are successful and become part of your organization's institutional culture.

Changes to PCI DSS Version 4.0

In February 2019, online sales overtook traditional store sales for the first time[16] and, commercially, the shift from on-premises IT infrastructure to cloud-based services gave cybercriminals opportunities to profit from the new and expansive landscape.

Demand for online services across every sector accelerated globally in the face of COVID-19. Quick cloud migrations sprung up to support remote working, and contactless payment methods and online shopping became commonplace. PCI DSS has focused on the threats and vulnerabilities within current and emerging technologies to keep it fit for its purpose. One of the most impactful changes is the enhanced emphasis PCI DSS 4.0 places on security, promoting flexible data practices integrated within an organization's wider security posture.

The revised standard recognizes that new technologies don't always encompass a prescriptive, unyielding control framework and introduces more compliance flexibility through a tailored approach. Other significant changes include:

- **Passwords And User Authentication:** Reflecting best password management practices and mandating multi-factor authentication for all access to the CDE.
- **Scope Validation and Data Discovery:** Requiring service providers to revalidate their scope every six months, identifying all locations of cardholder data and designating entities to perform quarterly data discovery exercises.
- **Enhanced Monitoring:** Automating log reviews using log analyzers and SIEM solutions, improving vulnerability scan results with authenticated scans and ensuring service providers support customer penetration testing.
- **Increased Testing of Critical Controls:** Greater frequency of testing per the Designated Entities Supplemental Validation (PCI DSS Appendix A3)[17].

SIMPLIFYING COMPLIANCE

The table below breaks down each PCI DSS requirement and its corresponding testing procedures:

1 Requirements and Testing Procedures		5 Guidance
2 Defined Approach Requirements	**2 Defined Approach Testing Procedures**	**6 Purpose**
3.4.2 When using remote-access technologies, technical controls prevent copy and/or relocation of PAN for all personnel, except for those with documented, explicit authorization and a legitimate, defined business need	3.4.2.a Examine documented policies and procedures and documented evidence for technical controls that prevent copy and/or relocation of PAN when using remote-access technologies onto local hard drives or removable electronic media to verify the following: Technical controls prevent all personnel not specifically authorized from copying and/or relocating PAN. A list of personnel with permission to copy and/or relocate PAN is maintained, together with the documented, explicit authorization and legitimate, defined business need.	Relocation of PAN to unauthorized storage; devices is a common way for this data to be obtained and used fraudulently. Methods to ensure that only those with explicit authorization and a legitimate business reason can copy or relocate PAN minimizes the risk of unauthorized persons gaining access to PAN. **7 Good Practice** Copying and relocation of PAN should only be done to storage devices that are permissible and authorized for that individual.
3 Customized Approach Objective		
PAN cannot be copied or relocated by unauthorized personnel using remote-access technologies.		
4 Applicability Notes	3.4.2.b Examine configurations for remote-access technologies to verify that technical controls to prevent copy and/or relocation of PAN for all personnel, unless explicitly authorized.	**8 Definitions** A virtual desktop is an example of a remote-. access technology. Storage devices include, but are not limited to, local hard drives, virtual drives, removable electronic media, network drives, and cloud storage.
Storing or relocating PAN onto local hard drives, removable electronic media, and other storage devices brings these devices into scope for PCI DSS. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	3.4.2.c Observe processes and interview personnel to verify that only personnel with documented, explicit authorization and a legitimate, defined business need have permission to copy and/or relocate PAN when using remote-access technologies.	**9 Examples** **10 Further Information** Vendor documentation for the remote-access, technology in use will provide information about the system settings needed to implement this requirement.

1 **The Requirement Description** at the X.X level organizes and describes the requirements that fall under it.

2 **The Defined Approach Requirements and Testing Procedures** describes the traditional method for implementing and validating PCI DSS using the Requirements and Testing Procedures defined in the standard.

3 **The Customized Approach Objective** is the intended goal or outcome for the requirement. It must be met by entities using a Customized Approach. Most PCI DSS requirements have this Objective. Appendix D describes expectations for entities and assessors when the Customized Approach is used. Entities following the Defined Approach can refer to the Customized Approach Objective as guidance, but the objective does not replace or supersede the Defined Approach Requirement[18].

4 **Applicability Notes** apply to both the Defined and Customized Approach. Includes information that affects how the requirement

is interpreted in the context of the entity or in scoping. These notes are an integral part of PCI DSS and must be fully considered during an assessment.

5 **Guidance** provides information to understand how to meet a requirement. Guidance is not required to be followed – it does not replace or extend any PCI DSS requirement. Not every Guidance section described here is present for each requirement. Not every section will be present for each requirement.

6 **Purpose** describes the goal, benefit, or threat to be avoided; why the requirement exists.

7 **A Good Practice** can be considered by the entity when meeting a requirement.

8 **Definitions** Terms that may help understand the requirement.

9 **Examples** describe ways a requirement could be met.

10 **Further Information** includes references to relevant external documentation.

The new standard

Decision makers must employ thorough, pragmatic practices to help address the underlying problems behind failing or outdated data security compliance programs. The role of the CISO is to move and roadblocks in achieving objectives. Adaptability and creative thinking have been essential in the past few years – and will continue to be as we move forward.

Compliance is an ongoing process, and the road we take is always shifting, always evolving. Evaluate your compliance status, understand any roadblocks to maintaining compliance, and make sure to educate staff about the changes introduced in PCI DSS 4.0. Remember, the new standard is complex; reading one white paper won't make you an expert. Engaging a specialist to guide you and conduct regular training sessions with all employees is never a bad idea.

PCI DSS 4.0 is around the corner. Don't wait – make it a priority. Educate yourself, get a thorough picture of your organization's data, and help ensure your business stays PCI DSS-compliant.

The worst-performing key requirements are:

- Requirement 11 (Regularly test security systems and processes)
- Requirement 6 (Develop and maintain secure systems)
- Requirement 12 (Security management) where fewer than 70% of organizations maintain those requirements
- Requirement 11 (Regularly test security systems and processes) remains the worst-performing requirement for more than 10 years running but did improve significantly

Bitdefender MDR helps you comply with PCI DSS security standards

The Bitdefender portfolio supports the following sub sections of *Maintain a Vulnerability Management Program*, **Requirement 5**: Protect All Systems and Networks from Malicious Software:

→ **XDR telemetry**

→ **Endpoint agents to monitor activity**

→ **Security Operations Center (SOC) real-time monitoring for incidents**

→ **Patch management add-on for multiple operating systems**

→ **MDR SOC provides passive prevention—identifies and informs when misconfigurations are found or patches are missing**

5.1 Processes and mechanisms for protecting all systems and networks from malicious software are defined and understood.	
5.2 Malicious software (malware) is prevented, or detected and addressed.	5.2.2 The deployed anti-malware solution(s): → Detects all known types of malware → Removes, blocks, or contains all known types of malware
5.3 Anti-malware mechanisms and processes are active, maintained, and monitored.	5.3.2.1 If periodic malware scans are performed to meet Requirement 5.3.2, the frequency of scans is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. → This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.
5.4 Anti-phishing mechanisms protect users against phishing attacks.	The focus of this requirement is on protecting personnel with access to system components in scope for PCI DSS. Meeting this requirement for technical and automated controls to detect and protect personnel against phishing is not the same as Requirement 12.6.3.1 for security awareness training. → This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

Bitdefender supports the following sub sections of *Regularly Monitor and Test Networks*, **Requirement 10**: Log and Monitor All Access to System Components and Cardholder Data

10.1 Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and documented	→ The MDR SOC does not maintain records, but performs auditing and recognizes outliers
10.4 Audit logs are reviewed to identify anomalies or suspicious activity	10.4.1 The following audit logs are reviewed at least once daily: → All security events → Logs of all system components that store, process, or transmit CHD and/or SAD → Logs of all critical system components → Logs of all servers and system components that perform security functions (for example, network security controls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers) **Cardholder Data** (CHD) As defined by the PCI Security Standards Council, CHD is the data allowed to be retained after a transaction validation. A transaction is considered processed once it has been either approved or declined. **Cardholder Data** (CHD) and Sensitive Authentication Data (SAD) are two types of account data (SAD). The cardholder data includes the 16-digit PAN, expiration date, and cardholder's name (CHD). This information is usually printed on the front of the card.
10.7 Failures of critical security control systems are detected, reported, and responded to promptly	10.7.2 Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: → Network security controls → IDS/IPS → Change-detection mechanisms → Anti-malware solutions → Physical access controls → Logical access controls → Audit logging mechanisms → Segmentation controls (if used) → Audit log review mechanisms → Automated security testing tools (if used) This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

WHY CHOOSE BITDEFENDER MDR?

If you feel overwhelmed by the amount of information you need to digest to understand the impact of PCI DSS v4.0 and want to simplify the complexity, you're not alone.

MDR is designed to help support your PCI DSS compliance goals and requirements by analyzing your compliance with the Payment Card Data Security standard and providing real-time analysis and response to security alerts.

Our MDR service helps you meet the requirements for your desired compliance frameworks so you can obtain certifications and perform successful audits, demonstrate compliance with various security/privacy standards to keep your data safe (as their customer), and help you maintain your existing compliance achievements.

Demonstrating PCI DSS compliance is a continuous, ongoing process. Bitdefender Managed Detection & Response (MDR) helps keep organizations safe with continuous security monitoring, advanced attack prevention, detection and remediation, and targeted and risk-based threat hunting by a certified team of security professionals. Staying compliant can be exhausting, but you can consider Bitdefender MDR your compliance partner.

SMBs and mid-market to enterprise organizations can stay one step ahead simply by leaving it to the experts who run our MDR service. Our highly skilled, certified security analysts have experience spanning the U.S. Air Force, U.S. Navy, British Intelligence, and the NSA. They have also created the MDR Cyber Intelligence Fusion Cell (CIFC), which performs extensive monitoring activities to identify company information or high-value employee information that may have been stolen or otherwise leaked. CIFC monitors your domain properties for newly created domains that could indicate "typo-squatting" or URL hijacking behavior by bad actors.

Bitdefender MDR helps ensure organizations have the expertise available to identify threats and respond rapidly to minimize the impact of attacks quickly and effectively – and compliance is a crucial piece of the puzzle. With Bitdefender, you can rest easy, knowing our team of experts is constantly monitoring, evaluating, and remediating to keep you protected.

Reach out to Bitdefender MDR for more info.

MDR for XDR

Managed Detection & Response (MDR) enhances Extended Detection and Response (XDR) with comprehensive coverage across the organization, ensuring wherever data is stored, threat detection and response is in place. GravityZone XDR natively observes and detects attacks across an organization's environment: physical and connected devices, virtual and cloud platforms, and their hosted workloads are all covered. The GravityZone platform combines advanced threat protection with out-of-the-box analytics, adding a rich security context to the correlation of disparate alerts. This enables security teams to rapidly triage and respond to incidents across identity, network, email, cloud, and endpoints. XDR exposes the full scope of all attacks by connecting events and incidents over time and delivering deeper context through automated evidence collection, root cause analysis, and recommended response actions. Modern security operations rely on a combination of context, expertise, and intuition to identify malicious activity that can evade your security tools. Bitdefender MDR for XDR enables our security team to analyze and detect intrusions from across your infrastructure with more accurate, correlated detections. This significantly expands the context available to our cyber threat hunters by providing a more detailed understanding of what 'normal' looks like in the environments we defend. In addition, sensors give our security analysts access to a suite of additional response actions, such as email deletion and user suspension, that allow us to take contextual responses to the next level. Bitdefender MDR for XDR is available by adding any sensor(s) to your MDR service: Productivity App, Identity, Network and Cloud.

FEATURES AND BENEFITS OF MDR

- Event monitoring: MDR monitors and investigates all alerts, responds to detections, and provides a detailed analysis via real-time reporting. Analysts run your security operations 24/7 – including human-led threat hunting, environmental baselining, and threat intelligence and analytics – to help you stay ahead of attackers.
- Threat hunting: MDR uses tactical and strategic threat intelligence paired with Bitdefender expertise to plan and execute threat hunting missions in customers' protected environments. Our proactive, highly skilled and certified security analysts, with experience from the U.S. Air Force, U.S. Navy, British Intelligence, and the NSA, partner with you on the frontlines of your cyber defenses.
- Pre-approved actions: MDR has a set of documented actions that can be executed in response to findings in your protected environment. Bitdefender knows that some endpoints have a significant impact on financial security, so PAAs can be tuned so that the Security Operations Center (SOC) takes action automatically in some cases – and calls you first on others.
- Review and respond based on alerts: MDR actively reviews alerts from customer environments and proactively assesses telemetry searching for evidence of compromise. MDR then takes specific actions on behalf of the customer to lessen the business impact.

MDR makes demonstrating compliance with key aspects of PCI DSS requirements simple. The service fortifies your internal security posture to enhance threat detection for fast, proactive identification and mitigation of threats – before they can become full-scale attacks. This results in a lower likelihood of a data breach, which in turn helps you steer clear of the considerable costs of non-compliance.

When it comes to PCI DSS, your MDR can help you ensure you've got everything you need to keep your tech and data secure, giving you peace of mind at assessment and audit time.

Sources

1 https://www.pcisecuritystandards.org/
2 https://www.ibm.com/account/reg/us-en/signup?formid=urx-51643
3 https://www.pcidssguide.com/whats-new-in-pci-dss-v4-0/
4 https://www.census.gov/retail/marts/www/marts_current.pdf
5 https://www.verizon.com/business/resources/Te93/reports/2022-payment-security-report.pdf
6 https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v3-2-1-to-v4-0-Summary-of-Changes-r2.pdf
7 https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Supporting%20Document/PCI_DSS-QRG-v4_0.pdf
8 https://www.pcisecuritystandards.org/
9 https://www.pcisecuritystandards.org/search/#?cludoquery=AOC&cludopage=1&cludoinputtype=standard
10 https://www.itgovernance.co.uk/data-protection-dpa-and-eu-data-protection-regulation
11 https://www.itgovernance.co.uk/data-breaches
12 https://financial.ucsc.edu/pages/security_penalties.aspx
13 https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Reporting%20Template%20or%20Form/PCI-DSS-v4_0-ROC-AOC-Service-Providers-r1.pdf
14 https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Supporting%20Document/PCI_DSS-QRG-v4_0.pdf
15 https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Supporting%20Document/PCI_DSS-QRG-v4_0.pdf
16 https://www.census.gov/retail/marts/www/marts_current.pdf
17 https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf
18 https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf

Other Sources Used

demystifying-compliance.pdf (splunk.com)
https://townsendsecurity.com/sites/default/files/PCI_WhitePaper.pdf
Business Leaders, Here’s What You Need To Know About PCI DSS 4.0 (forbes.com)
https://pages.nist.gov/800-63-3/sp800-63-3.html
https://www.mymoid.com/blog/pci-non-compliance-consequences/
https://pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/How-do-I-contact-the-payment-card-brands/v

Bitdefender is a cybersecurity leader delivering best-in-class threat prevention, detection, and response solutions worldwide. Guardian over millions of consumer, business, and government environments, Bitdefender is one of the industry’s most trusted experts for eliminating threats, protecting privacy and data, and enabling cyber resilience. With deep investments in research and development, Bitdefender Labs discovers over 400 new threats each minute and validates around 40 billion daily threat queries. The company has pioneered breakthrough innovations in antimalware, IoT security, behavioral analytics, and artificial intelligence, and its technology is licensed by more than 150 of the world’s most recognized technology brands. Launched in 2001, Bitdefender has customers in 170+ countries with offices around the world.

Romania HQ
Orhideea Towers
15A Orhideelor Road,
6th District,
Bucharest 060071
T: +40 21 4412452
F: +40 21 4412453

US HQ
3945 Freedom Circle,
Suite 500, Santa Clara,
CA, 95054

bitdefender.com

Bitdefender-BSG-Whitepaper-PCIDSS_MDR-DEX13963-en_EN