Compliance Whitepaper

INTEZER PROTECT

Introduction

Conducting business in a cloud environment presents unique challenges for achieving and maintaining compliance with regulations that were designed with traditional computing and business environments in mind.

Intezer Protect provides unparalleled visibility into cloud workloads, allowing for efficient monitoring, protection, auditing, and reporting. These are core components of all common regulatory frameworks.

In this report, we highlight the ways in which implementing Intezer Protect for cloud workloads can help enterprises of all sizes meet and maintain their compliance posture for widely applicable industry standards and regulations.

PCI DSS VERSION 3.2 (REFERENCE)

The PCI Data Security Standard (PCI DSS) requires all organizations that process, store, or transmit payment cardholder data to follow standard security practices in order to accept or process payment cards. The PCI Security Standards Council recognizes that using cloud computing and/or virtualization for processing, storing, or transmitting payment card data requires additional security considerations. As a result, they have developed supplemental guidelines to facilitate maintaining PCI DSS controls in cloud environments. (Ref)

Intezer Protect was designed to specifically address many of the compliance challenges associated with cloud environments mentioned by the PCI Security Standards Council, which include the following:

- Clients may have little or no visibility into the CSP's underlying infrastructure and the related security controls
- Clients may have limited or no oversight or control over cardholder data storage. Organizations might not know where cardholder data is physically stored, or the location(s) can regularly change. For redundancy or high availability reasons, data could be stored in multiple locations at any given time
- Some virtual components do not have the same level of access control, logging, and monitoring as their physical counterparts
- It can be challenging to collect, correlate, and/or archive all of the logs necessary to meet applicable PCI DSS requirements

See PCI DSS Cloud Computing Guidelines, February 2013 for a complete list of compliance challenges identified by the PCI Security Standards Council.

Intezer Protect provides organizations with the ability to effectively assess, repair, and report on PCI DSS compliance for security controls that are difficult to maintain in cloud environments. This cloud-native security solution is designed to help organizations of all sizes meet the following PCI DSS requirements for applicable cloud workloads.

PCI DSS	Intezer Protect
REQUIREMENT 5: PROTECT ALL SYSTEMS AGAINST MALWARE AND REGULARLY UPDATE ANTI-VIRUS SOFTWARE OR PROGRAMS	
5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	The Intezer Protect sensor continuously protects against malicious software code running in the system leveraging Intezer's unique Genetic Malware Analysis technology. Because malware is detected based on code similarities rather than signatures, Intezer Protect can detect new malware variants that can avoid other anti-virus solutions.
5.2 Ensure that all anti-virus mechanisms are kept current, perform periodic scans, generate audit logs, which are retained per PCI DSS Requirement 10.7.	Intezer's Genetic Malware Analysis engine is frequently updated through a range of industry used references and internal research. Because malware is detected based on code similarities rather than signatures, Intezer Protect can detect new malware variants that can avoid other anti-virus solutions.
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.	Intezer Protect generates alerts about the performance of the sensor agent, providing error and status visibility.
REQUIREMENT 6: DEVELOP AND MAINTAIN SECURE SYSTEMS AND APPLICATIONS	
6.4 Follow change control processes and procedures for all changes to system components. Ensure all relevant PCI DSS requirements are implemented on new or changed systems and networks after significant changes.	Intezer Protect continuously identifies the origins of every fragment of code running in a cloud environment and can be rapidly scaled. This deep visibility into cloud runtime can be used to validate that change control procedures are followed for every deployment and immediately flag unauthorized code.
REQUIREMENT 8: IDENTIFY AND AUTHENTICATE ACCESS TO SYSTEM COMPONENTS	
8.7 All access to any database containing cardholder data must be restricted: all user access must be through programmatic methods; only database administrators can have direct or query access; and application IDs for database applications can only be used by the applications (and not by users or non-application processes).	Complements the control: because Intezer Protect provides visibility into every piece of code running inside workloads while monitoring and logging all programs running on a machine, the user can ensure that there is no unauthorized code running which can result in unauthorized access into cardholder storage.

PCI DSS	Intezer Protect
REQUIREMENT 10: TRACK AND MONITOR ALL ACCESS TO NETWORK RESOURCES AND CARDHOLDER DATA	
10.2 Implement automated audit trails for all system components for reconstructing these events: all individual user accesses to cardholder data; all actions taken by any individual with root or administrative privileges; access to all audit trails; invalid logical access attempts; use of and changes to identification and authentication mechanisms (including creation of new accounts, elevation of privileges), and all changes, additions, deletions to accounts with root or administrative privileges; initialization, stopping or pausing of the audit logs; creation and deletion of system-level objects.	Intezer Protect monitors and generates audit trails to every program, process, or code running on a machine, which enables the user to record any operating system command (Shell commands) or unauthorized code that can result in malicious access to cardholder data.
10.3 Record audit trail entries for all system components for each event, including at a minimum: user identification, type of event, date and time, success or failure indication, origination of event, and identity or name of affected data, system component or resource.	Intezer Protect provides an intuitive dashboard with enriched event information such as: alert summary, threat type, attacker, attack goal, attack vector, alert triggers, other attacked servers; response/escalation options, report, index, logged user, timeline that shows the device's status over time, and Intezer's suggested solutions.
10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. Perform critical log reviews at least daily.	The use of Genetic Malware Analysis for identifying security events produces only actionable and high-confidence alerts. This allows security analysts to rapidly identify anomalies and suspicious activity while minimizing time spent investigating false positives. In addition, Intezer Protect monitors and generates audit trails to every program, process, or code running on a machine, which provides a critical log data of a machine running state.
REQUIREMENT 11: REGULARLY TEST SECURITY SYSTEMS AND PROCESSES	
11.4 Use network intrusion detection and/or intrusion prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. IDS/IPS engines, baselines, and signatures must be kept up to date.	Complements the control: Intezer Protect can detect and prevent intrusions at critical points in the cardholder data by continuously scanning for unauthorized code or malicious activity with each fragment of code that is executed, which can result in malicious network activity. While Intezer's code genome database is continuously updated, Genetic Malware Analysis can positively identify never-before-seen variants of malware based on code reuse. This increases the ability to defend against currently unknown threats.

PCI DSS	Intezer Protect
11.5 Deploy a change detection mechanism (for example, file integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files or content files. Configure the software to perform critical file comparisons at least weekly. Implement a process to respond to any alerts generated by the change-detection solution.	Intezer Protect creates a trusted "Genetic Profile" of your infrastructure, then monitors and logs any change in runtime within cloud environments, capturing any unauthorized code or commands that may be used to modify critical system files, configurations, and content files.
REQUIREMENT 12: MAINTAIN A POLICY THAT ADDRESSES INFORMATION SECURITY FOR ALL PERSONNEL	
12.10 Implement an incident response plan. Be prepared to respond immediately to a system breach.	Complements the control: Intezer Protect provides runtime details of a security event within cloud workloads and identifies any malicious or unauthorized code executed during the event, allowing personnel to produce detailed reports in a timely manner and provides thorough context in order to quickly respond to incidents.

HIPAA SECURITY RULE (REFERENCE)

The HIPAA Security Rule requires organizations that handle electronic Personal Health Information (e-PHI) to protect this data using maintain administrative, technical, and physical safeguards that fall into four general requirements. These organizations must:

1. Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
2. Identify and protect against reasonably anticipated threats to the security or integrity of the information;
3. Protect against reasonably anticipated, impermissible uses or disclosures; and
4. Ensure compliance by their workforce.

The Rule does not dictate specific security solutions to use but does require organizations to consider several factors including the technical and software infrastructure used. In addition, security measures must be reviewed and modified whenever changes are made to continuously protect e-PHI.

Organizations that use Intezer Protect can implement administrative and technical security measures to meet multiple HIPAA requirements that pose challenges specifically to cloud environments where e-PHI may be stored, retrieved, and processed.

HIPAA Implementation Requirements	Intezer Protect
164.308 ADMINISTRATIVE SAFEGUARDS (REFERENCE)	
(a)(1)(ii)(D) *Information system activity review (Required).* Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	Intezer Protect provides an intuitive dashboard with enriched event information such as: alert summary, threat type, attacker, attack goal, attack vector, alert triggers, other attacked servers; response/escalation options, report, index, logged user, timeline that shows the device's status over time, and Intezer's suggested solutions.
(a)(4)(ii)(C) *Access establishment and modification (Addressable).* Implement policies and procedures that, based upon the covered entity's or business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	Intezer Protect monitors and logs any change in runtime within cloud environments, capturing any unauthorized code or commands that may be used for attempted unauthorized access to e-PHI.
(a)(5)(ii)(B) *Protection from malicious software (Addressable).* Procedures for guarding against, detecting, and reporting malicious software.	Intezer's Genetic Malware Analysis engine is frequently updated through a range of industry used references and internal research. Because malware is detected based on code similarities rather than signatures, Intezer Protect can detect new malware variants that can avoid other anti-virus solutions.
(a)(3)(ii)(B) *Workforce clearance procedure (Addressable).* Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate. (a)(5)(ii)(C) *Log-in monitoring (Addressable).* Procedures for monitoring log-in attempts and reporting discrepancies.	Intezer Protect monitors and logs any change in runtime within cloud environments, capturing any unauthorized code or commands that may be used for attempted unauthorized access to e-PHI.
(a)(6)(ii) *Response and reporting (Required).* Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. *More information on how Protect can assist with HIPAA incident reporting requirements can be found in the HIPAA Breach Notification Rule section below.*	Intezer Protect provides runtime details of a security event within cloud workloads and identifies any malicious or unauthorized code executed during the event allowing personnel to produce detailed reports in a timely manner.

HIPAA Implementation Requirements	Intezer Protect
(a)(8) Standard: Evaluation. Perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to *environmental* or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.	Intezer Protect monitors and logs any change(s) in runtime within cloud environments, capturing any unauthorized code or commands that may be used to modify critical system files, configurations, and content files related to the security of e-PHI.
164.312 TECHNICAL SAFEGUARDS (REFERENCE)	
(b)*Standard: Audit controls.* Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	Intezer Protect monitors and generates audit trails to every program, process, or code running on a machine, which enables the user to record any operating system command (Shell commands) or unauthorized code that can result in malicious access to cardholder data. Intezer Protect provides an intuitive dashboard with enriched event information such as: alert summary, threat type, attacker, attack goal, attack vector, alert triggers, other attacked servers; response/escalation options, report, index, logged user, timeline that shows the device's status over time, and Intezer's suggested solutions.
(c)(2) *Mechanism to authenticate electronic protected health information (Addressable).* Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed.	Intezer Protect monitors and logs any change in runtime within cloud environments, capturing any unauthorized code or commands that may be used to modify critical system files, configurations, and content files.

HIPAA BREACH NOTIFICATION RULE (REFERENCE)

In addition to the Security Rule, HIPAA also mandates organizations that handle e-PHI to follow the Breach Notification Rule, 45 CFR §§ 164.400-414. This rule establishes notification requirements following a breach of unsecured e-PHI.

Intezer Protect gives organizations the tools necessary to effectively respond to potential breaches. In the event of a breach from a cloud environment, Intezer Protect rapidly generates critical event details to inform the accurate risk assessment and reporting mandated by the HIPAA Breach Notification Rule.

164.410 NOTIFICATION BY A BUSINESS ASSOCIATE (REFERENCE)

(a) Standard —(1) General rule. A business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach.

(b) *Timeliness of notification.* Except as provided in § 164.412, a business associate shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

(c) *Content of notification.* (1) The notification required by paragraph (a) of this section shall include, to the extent possible, the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach. (2) A business associate shall provide the covered entity with any other available information that the covered entity is required to include in notification to the individual under § 164.404(c) at the time of the notification required by paragraph (a) of this section or promptly thereafter as information becomes available.

164.404(c) Content of notification —(1) Elements. The notification required by paragraph (a) of this section shall include, to the extent possible:

(A) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

(B) A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

(C) Any steps individuals should take to protect themselves from potential harm resulting from the breach;

(D) A brief description of what the covered entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and

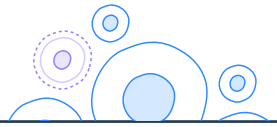
(E) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, web site, or postal address.

SOC 2 (REFERENCE)

SOC 2 is a reporting standard for third party attestations about controls at a service organization. The controls reported in SOC 2 reports are based on the Trust Service Principles defined by the AICPA: security, availability, processing integrity, confidentiality, and privacy.

When an organization is undergoing a type 2 audit, a service auditor will test the operating effectiveness of the organization's controls for up to one year. Limited visibility into cloud workloads introduces significant challenges to completing a SOC 2 audit without receiving exceptions. Intezer Protect enables organizations to gain full visibility into every fragment of code running in cloud environments, which enables them to accurately define and test the operating effectiveness of security controls for cloud workloads.

SOC 2 Trust Service Criteria	Intezer Protect
CC1.0 COMMON CRITERIA RELATED TO ORGANIZATION AND MANAGEMENT	
CC1.1 The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance and monitoring of the system enabling it to meet its commitments and requirements as they relate to security, availability and processing integrity.	Complements the control: Intezer Protect generates alerts for systems that currently have limited visibility, allowing organizations to clearly define reporting lines and responsibilities related to the security and availability of cloud workloads.
CC3.0 COMMON CRITERIA RELATED TO RISK MANAGEMENT AND DESIGN AND IMPLEMENTATION OF CONTROLS	
CC3.1 The entity (1) identifies potential threats that would impair system security, availability and processing integrity commitments and requirements, (2) analyzes the significance of risks associated with the identified threats, and (3) determines mitigation strategies for those risks (including controls and other mitigation strategies).	1. Protect identifies potential threats with high reliability by generating alerts for any unauthorized or malicious code running in a cloud workload. 2. Protect provides rapid analysis of all identified threats through Genetic Malware Analysis, allowing incident response teams to quickly determine the associated risk. 3. Protect generates recommended solutions for mitigating risks posed by unauthorized or malicious code.
CC3.2 The entity designs, develops, and implements controls, including policies and procedures, to implement its risk mitigation strategy.	Complete visibility into cloud workloads is necessary for effectively implementing a risk mitigation strategy. Intezer Protect creates a trusted “Genetic Profile” of your infrastructure, then monitors and logs any change in runtime within cloud environment and provides enriched alerts of unauthorized and malicious code to inform risk assessments and suggests mitigation strategies.
CC3.3 The entity (1) identifies and assesses changes (for example, environmental, regulatory, and technological changes) that could significantly affect the system of internal control for security, availability and processing integrity and reassesses risks and mitigation strategies based on the changes and (2) reassesses the suitability of the design and deployment of control activities based on the operation and monitoring of those activities, and updates them as necessary.	1. Intezer Protect creates a trusted “Genetic Profile” of your infrastructure, then monitors and logs any change in runtime within cloud environments, capturing any unauthorized code or commands that may be used to modify critical system files, configurations and content files.

SOC 2 Trust Service Criteria	Intezer Protect
CC5.0 COMMON CRITERIA RELATED TO LOGICAL AND PHYSICAL ACCESS CONTROLS	
CC5.1 Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized users; (2) restriction of authorized user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access.	Complements the control: (3) Once implemented, Protect continuously monitors for unauthorized access of cloud assets including unauthorized programmatic access.
CC5.6 Logical access security measures have been implemented to protect against security, availability and processing integrity threats from sources outside the boundaries of the system.	Intezer Protect monitors and logs any change in runtime within cloud environments, capturing any unauthorized code or commands that may be used for attempting to gain unauthorized access remotely.
CC5.8 Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software. 	The Intezer Protect sensor continuously protects against malicious software code running in the system leveraging Intezer's unique Genetic Malware Analysis technology. Because malware is detected based on code similarities rather than signatures, Intezer Protect can detect new malware variants that can avoid other anti-virus solutions.
CC6.0 COMMON CRITERIA RELATED TO SYSTEMS OPERATIONS	
CC6.1 Vulnerabilities of system components to security, availability and processing integrity breaches and incidents due to malicious acts, natural disasters, or errors are monitored and evaluated and countermeasures are implemented to compensate for known and new vulnerabilities.	Intezer Protect creates a trusted "Genetic Profile" of your infrastructure, then monitors and logs any change in runtime within cloud environments, capturing any unauthorized code or commands that may be used to modify critical system files, configurations, and content files.
CC6.2 Security, availability and processing integrity incidents, including logical and physical security breaches, failures, concerns, and other complaints, are identified, reported to appropriate personnel, and acted on in accordance with established incident response procedures.	Intezer Protect provides runtime details of a security event within cloud workloads and identifies any malicious or unauthorized code executed during the event, allowing personnel to produce detailed reports in a timely manner and provides thorough context in order to quickly respond to incidents.

SOC 2 Trust Service Criteria	Intezer Protect
CC7.0 COMMON CRITERIA RELATED TO CHANGE MANAGEMENT	
CC.7.1 Security, availability and processing integrity commitments and requirements, are addressed, during the system development lifecycle including design, acquisition, implementation, configuration, testing, modification, and maintenance of system components.	Complements the control: Intezer Protect creates a trusted “Genetic Profile” of your infrastructure, then monitors and logs any change in runtime within cloud environments, capturing any unauthorized code or commands that may be used to modify critical system files, configurations, and content files.
CC7.2 Infrastructure, data, software, and procedures are updated as necessary to remain consistent with the system commitments and requirements as they relate to security, availability and processing integrity.	Same as CC7.1
CC7.3 Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and monitoring.	Intezer Protect provides runtime details of a security event within cloud workloads and identifies any malicious or unauthorized code executed during the event, allowing personnel to produce detailed reports in a timely manner and provides thorough context in order to quickly respond to incidents.
CC6.0 COMMON CRITERIA RELATED TO SYSTEMS OPERATIONS	
CC7.4 Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented in accordance with security, availability and processing integrity commitments and requirements.	Same as CC7.1

References

HIPAA ADMINISTRATIVE SIMPLIFICATION - REGULATION TEXT 45 CFR PARTS 160, 162 AND 164

https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf

SUMMARY OF THE HIPAA SECURITY RULE

https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

PCI SSC QUICK REFERENCE GUIDE VERSION 3.2

https://www.pcisecuritystandards.org/document_library?category=pcidss&subcategory=pcidss_supporting#results

PCI DSS CLOUD COMPUTING GUIDELINES

https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Cloud_Guidelines.pdf

HIPAA BREACH NOTIFICATION RULE

https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

SOC2 - AICPA TRUST SERVICES CRITERIA

https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf