TEVORA™

Intezer Protect

PCI DSS and HIPAA Security Rule Compliance Review

January 5, 2021

Table of Contents

Intezer for PCI DSS & HIPAA Compliance

Overview

Intezer Labs engaged Tevora, a security and risk management consulting firm, and an accredited PCI Qualified Security Assessor (QSA) and HITRUST Assessor, to conduct an independent, in-depth evaluation of Intezer Protect against the applicable PCI DSS and HIPAA Security Rule requirements.

This paper describes the observations and conclusions drawn by Tevora through their independent review of Intezer Protect. This review included an assessment of the key features, including the threat detection engine, event data collection and reporting, incident response support, automated package and configuration auditing, and native cloud stack compatibility.

Furthermore, this report outlines the specific ways Intezer Protect can help organizations fulfill the mandates of the PCI DSS and HIPAA Security Rule.

Current Cloud Security Marketplace

Challenges to Cloud Security

As the use of cloud computing becomes ubiquitous and organizations adapt with great speed to leverage the latest technological advancements, organizations must rely on security solution providers capable of adapting to these changes. Many respected security solutions built for on-premise environments are rendered inadequate when applied to the modern cloud landscape. With the increased scalability, agility, and layers of abstraction that modern cloud deployments entail, many security solutions based on older paradigms are no longer effective.

In an environment of containerized microservices, scalable and dynamic workloads, utilization of container orchestrators, and rapid deployment, standard behavioral anomaly and signature detection mechanisms made for traditional on-premise environments are disadvantaged with limited visibility, incorrect alerting, and wasteful consumption of valuable computing resources.

For instance, many endpoint security solutions currently on the market are primarily capable of detecting threats at the OS level, but organizations may be required to purchase additional solutions to gain visibility into the other layers of the modern native cloud stack. Additionally, many of these solutions are better capable of serving Windows-based environments, with limited focus on protecting systems running Linux distributions that many current native-cloud technologies rely on.

Cloud Workload Security

Cloud workload security solutions are designed for modern cloud-native applications and services, remediating many deficiencies in visibility, compatibility, and efficiency that result from using on-premise solutions. In addition to being compatible all layers of the modern native cloud stack, cloud workload security solutions are designed to apply protection and detection controls that consider modern configuration management and deployment pipelines.

Intezer Protect is a cloud-native workload security system providing a comprehensive set of protection, detection, and response capabilities. Designed to efficiently analyze runtime code execution in dynamically changing and scaling cloud workloads, Intezer offers an innovative threat detection engine capable of defending against sophisticated threats in modern cloud environments.

How Does Intezer Help Customers Meet Compliance Requirements?

Overview

Using technology that pushes the edge of advancement in cloud workload protection, Intezer provides solutions that are designed to help organizations meet PCI DSS and HIPAA compliance requirements. Tevora performed an in-depth evaluation of Intezer Protect and this report summarizes the resulting analysis.

Protect

Intezer Protect is a real-time threat detection engine designed to protect cloud workloads against unauthorized code. Intezer Protect uses a powerful engine managed through simplified and intuitive controls, tuning out false positives without the need to configure policies and rule-sets. Intezer Protect provides threat visibility, comprehensive event data collection, vulnerability management tools, and incident response process augmentation and automation.

Key Features

Advanced Threat Detection

Intezer introduces the “Genetic Software Mapping” threat detection engine that performs memory analysis. Intezer’s threat detection engine analyzes raw binary code against Intezer’s “Genome Database,” a threat intelligence database containing patterns of binary code, profiling both malicious and trusted software. Applying heuristic analysis at the dynamic memory level, Intezer’s threat detection engine is capable of detecting sophisticated threat actors using modern evasion techniques, including code injection and fileless malware.

Visibility

Intezer Protect deploys agent-based sensors that continuously collect and monitor data on process information, including binary executables, shell scripts and commands, executable files and modules from disk or memory, and file permissions.

Intezer Protect first monitors the environment and establishes a trusted baseline, also referred to as the “Genetic Profile,” of expected code execution patterns. Once the baseline is established, Intezer sensors continuously monitor the environment and generate alerts for any malicious or anomalous code executed in memory.

Intezer Protect can be configured to monitor any directory within a Linux filesystem, providing a range of criticality-based alerting depending on the commands that are executed. Its “Audit” function allows an individual to monitor continuously-changing system files, such as logs, for suspicious behaviors or commands which cannot be reasonably alerted on.

Together, the “Alert” and “Audit” functions provide visibility and file-integrity monitoring (FIM) for security teams to more easily monitor the executions of commands, file modifications, and other actions performed on cloud workloads.

Response Augmentation

Intezer Protect augments and automates many aspects of the incident response process. With real-time monitoring, a policy-free and rule-free tuning system, and the Genetic Software Mapping threat detection engine, Intezer Protect provides an effective means for detecting indicators of compromise, eliminating many manual processes required in other detection methods.

Once a threat is detected, Intezer Protect provides a detailed report on the detected alert, which includes a detailed diagnosis of the event and threat intelligence to help the user better understand the nature of the event. This includes verbose log information showing the chain of processes that occurred, the commands run, and the expected behavior of the threat.

If a known strain of malware is recognized, Intezer Protect provides in-depth details such as malware classification, the name of the malware, the associated hacker group, and the behavior patterns one can expect from the detected threat.

For all processes identified, Intezer Protect presents the option to terminate the malicious process directly from the Intezer management console.

Reduced Attack Surface

Intezer Protect provides automated auditing, performing regular scans against the installed packages and configuration files on each protected host to provide insight on attack surface vulnerabilities. Intezer Protect identifies and reports on the Common Vulnerabilities and Exposures (CVE) data associated with the packages installed on each host. Additionally, Intezer Protect reads the host configuration files and audits them against the CIS Benchmarks, reporting on any deviation from the recommended best-practices, while providing a criticality ranking for each potential misconfiguration.

Adaptability to Modern Cloud

Intezer Protect is a cloud-native designed to integrate into the dynamic, agile, and scaling cloud architectures deployed by organizations at the forefront of modern technology. Intezer Protect’s threat detection and attack surface analysis capabilities are functional at all layers of the native cloud stack, including virtual machines, containers, and container orchestrators.

Linux Focused

While the majority of endpoint security solutions specialize on protecting Windows-based operating systems, Intezer Protect is tailored to protect Linux distributions. With Linux focused specialization, Intezer Protect serves as a highly effective security solution for modern cloud environments using the platforms and tools dependent on Linux.

Simplified Tuning

Using Intezer Protect, the time-consuming task of tuning the threat detection engine and reducing false positives is simplified. Intezer monitors all code execution and cross-references the code execution pattern to the Intezer Genome Database to identify malicious or trusted software. If code is not recognized to either be malicious or trusted, such as custom built applications, the end-user simply provides basic input to confirm whether the behavior is “normal,” establishing the organization’s custom and trusted “Genetic Profile.”

Once the Genetic Profile is established, Intezer Protect automatically triages the event data, checking against both the client’s Genetic Profile and the pre-defined behavioral heuristics and malware patterns established in the Intezer Genome Database. The option for continuous tuning is then available for every instance an event or alert is collected, where the Intezer console presents the option to identify an event as malicious, or incorporate an erroneously flagged process to the trusted baseline.

Notice

Intezer’s obligation is to provide a comprehensive feature set that, when configured adequately, can support covered organizations to achieve their compliance obligations. To meet compliance obligations as organizations processing PCI or HIPAA protected data, it is incumbent on covered businesses to configure the solution, as well as establish the necessary supporting processes, to meet their PCI DSS or HIPAA compliance needs. Guidance on how to accomplish this may be found in the next section.

Compliance Requirements

Here is how Intezer Protect addresses each applicable PCI DSS and HIPAA requirement:

PCI DSS

PCI DSS 3.2.1	Intezer Protect Features	Supports Compliance?
Requirement 2: Do not use vendor-supplied defaults for system password and other security parameters		
2.2 – Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.	Intezer Protect performs daily scans against configuration files on each protected host, testing such configurations against the applicable CIS Benchmarks for all layers of the native-cloud stack (i.e., virtual machine, container, container orchestrator). For each configuration that deviates from the CIS Benchmark recommendations, Intezer Protect provides the description, the security related rationale, the remediation steps, and a projected risk ranking. Customers are responsible for defining and implementing internal configuration standards for all in-scope system components. Provided with these reports, customer organizations may use this information help establish these standards and audit the consistency in which these standards are implemented.	Yes
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).	Intezer Protect is available on a number of Linux distributions, including Ubuntu 16.04 LTS (Xenial Xerus)+, Debian 9 (stretch)+, RHEL 7.2+, CentOS 7+, Amazon Linux 2.	Yes
5.1.1 – Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	Intezer Protect monitors code executed in memory, detecting any malicious code execution in real-time, leveraging the threat intel and malicious patterns indexed within the Intezer Genome Database. Intezer Protect automatically terminates processes confirmed to be malicious. For all other unrecognized threats, Intezer Protect provides the option to terminate the process from the management console.	Yes

PCI DSS 3.2.1	Intezer Protect Features	Supports Compliance?
5.2 – Ensure that all anti-virus mechanisms are maintained as follows: • Are kept current, • Perform periodic scans, • Generate audit logs which are retained per PCI DSS Requirement 10.7.	Intezer's Genome Database is continuously updated with threat intel collected both through trusted references and the Intezer security research team. Intezer Protect monitors for malicious code in real-time, exceeding the capabilities of traditional solutions reliant on scanning of static files. Intezer Protect collects audit logs for all malicious code identified. Intezer provides SIEM integration capabilities that allow forwarding of alerts to a SIEM solution capable of storing logs per PCI DSS Requirement 10.7.	Yes
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 regarding sensor agent connectivity, including status and error information. Intezer Protect is designed to protect cloud-based production systems interfaced by authorized administrators. The PCI DSS language differentiates users and administrators, as removing an administrator's ability to manage the system is not feasible.	Yes

PCI DSS 3.2.1	Intezer Protect Features	Supports Compliance?
Requirement 6: Develop and maintain secure systems and applications		
6.1 – Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities.	Intezer Protect performs daily scans against the installed packages and configuration files on each protected host. For each installed package, Intezer Protect reports on the CVEs affecting each package and provides a projected risk ranking. For each configuration, Intezer Protect tests against the applicable CIS Benchmarks for all layers of the native-cloud stack (i.e., virtual machine, container, container orchestrator). For each configuration that deviates from the CIS Benchmark recommendations, Intezer Protect provides the description, the security related rationale, the remediation steps, and the projected risk ranking. Intezer Protect provides a trusted source for identifying security vulnerabilities that the customer organization may incorporate into their vulnerability management program. Customers are responsible for establishing comprehensive vulnerability identification and triaging processes. Customers may use the Intezer reports to aid in these processes.	Yes
6.2 – Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.	Intezer Protect performs daily scans against the installed packages on each protected host. For each installed package, Intezer Protect reports on the CVEs affecting each package and provides a projected risk ranking. Provided with these reports, customer organizations may use this information help identify security vulnerabilities as part of their vulnerability management program. Customers are responsible for applying the applicable security patches for the identified vulnerabilities.	Yes

PCI DSS 3.2.1	Intezer Protect Features	Supports Compliance?
6.4 – Follow change control processes and procedures for all changes to system components.	Intezer Protect establishes a "trusted baseline" of expected activity and code running in the environment. Intezer Protect will alert on any code not established as trusted by the customer or unrecognized in the Intezer Genome Database. Augmenting custom software version control capabilities, Intezer Protect will detect any custom source code introduced into customer environments.	Yes
Requirement 10: Track and monitor all access to network resources and cardholder data		
10.5.5 -- Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	Intezer Protect provides FIM functionality that identifies modifications and deletions to the local /var/log directory. Any changes to log files will be added as an event in the "Audit" tab of the Protect console. Within this area, anomalies can be identified alongside regular system events by examining specific executed commands, users, and other event details.	Yes
10.6 – Review logs and security events for all system components to identify anomalies or suspicious activity.	Intezer Protect sensors continuously monitors protected hosts for threats using the Genetic Software Mapping threat detection engine. When first setting up Intezer Protect, the sensors monitor the environment and establish a trusted baseline of expected code execution patterns. Once the baseline is established, Intezer sensors continuously monitor the environment and generate alerts for any malicious or unauthorized code detected.	Yes
10.6.1 – Review the following at least 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	Intezer Protect sensors monitor and collect event data on all running process information, including shell commands, shell scripts, and binary executables, as well as executable files and modules from disk or memory. Analyzing the data against the Intezer Genome Database and the customer defined trusted baseline, Intezer Protect generates security event alerts for all malicious and potentially malicious activity. All event information is collected as aggregated, non-malicious expected activity.	Yes

PCI DSS 3.2.1	Intezer Protect Features	Supports Compliance?
10.6.2 – Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.	Intezer Protect provides a monitoring dashboard that provides risk analysis information for all alerts generated. This feedback may be used by customer organizations to define their monitoring processes and support their overall risk management strategy.	Yes
10.6.3 – Follow up exceptions and anomalies identified during the review process.	Intezer Protect provides a detailed report for each alert generated, which includes a detailed diagnosis of the event and the relevant threat intel, aiding the anomaly follow-up process. Intezer Protect provides the option to terminate the malicious process from the management console.	Yes
Requirement 11: Regularly test security systems and processes		
11.4 – Use 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 in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.	Intezer Protect sensors continuously monitor protected hosts for threats using the Genetic Software Mapping threat detection engine, including detection of malicious exploit code used for intrusions into systems. Alerts are generated for all malicious and potentially malicious activity. Intezer's Genome Database is continuously updated with threat intel collected both through trusted references and the Intezer security research team. Intezer Protect sensors monitor all process information on each protected host. Customers may deploy sensors on all hosts positioned at the perimeter and critical points in the cardholder data environment to fulfill the intent of this requirement. Whether the use of a host-based IDS/IPS fulfills this requirement, or should be used as a compensating control in lieu of a network-based IDS/IPS, will be determined by a PCI QSA/ISA.	Yes

PCI DSS 3.2.1	Intezer Protect Features	Supports Compliance?
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; and configure the software to perform critical file comparisons at least weekly.	Intezer Protect's Genetic Software Mapping threat detection engine implements dynamic memory-based behavioral heuristic analysis against all process execution on the protected hosts. Suspicious code execution patterns that change critical files will generate an alert. Criteria for determining what activity is suspicious is based on the Intezer Genome Database and the client defined Genetic Profile. Intezer Protect provides FIM functionality that identifies modifications and deletions to the local /var/log directory. Any changes to log files will be added as an event in the "Audit" tab of the Protect console. Within this area, anomalies can be identified alongside regular system events by examining specific executed commands, users, and other event details.	Yes
Requirement 12.10: Implement an incident response plan		
12.10 – Implement an incident response plan. Be prepared to respond immediately to a system breach.	Intezer Protect serves as a tool for real-time threat detection, providing the visibility needed to identify indicators of compromise. Intezer Protect provides threat intelligence for each detected threat, augmenting the triaging process by making available the threat intelligence necessary to understand the relative risk and determine appropriate steps for response.	Yes
12.10.5 – Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems.	Intezer Protect serves as a tool for real-time threat detection, generating alerts for all threats detected through the Genetic Software Mapping detection engine. Intezer Protect provides integration capabilities, allowing you to forward alerts to the relevant personnel via Slack, SIEM, or email.	Yes
12.10.6 – Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	Intezer Protect reports on each alert detected, providing verbose information into the relevant chain of processes and details of the malware or suspicious command identified. Furthermore, Intezer Protect provides the capability to either terminate the detected process or incorporate the process into the trusted baseline.	Yes

HIPAA Security Rule

HIPAA Security	Intezer Protect Features	Supports Compliance?
§164.308 Administrative Safeguards		
§164.308(a)(1)(ii)(D) – Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	Intezer Protect provides real-time threat detection, providing visibility into the process executing in memory on each protected host. Intezer Protect makes available the system activity data collected for both suspicious and non-suspicious processes.	Yes
§164.308(a)(5)(ii)(B) – Procedures for guarding against, detecting, and reporting malicious software.	Intezer Protect monitors code executed in memory, detects any malicious code execution in real-time, and cross-references the threat intel and malicious patterns indexed within the Intezer Genome Database. Intezer Protect provides the real-time option to terminate the malicious process from the management console. Intezer Protect provides valuable information necessary for triaging malware threats, including the malware family classification, a risk assessment of the infection, and insight into the behavior of the malware.	Yes
§164.308(a)(6)(ii) – 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.	Intezer Protect sensors continuously monitor all processes executing in memory on the protected hosts. Analyzing the data against the code-based heuristic models defined in the Intezer Genome Database and the customer defined Genetic Profile, Intezer Protect generates security event alerts for all malicious and potentially malicious activity. For all potential threats detected, Intezer generates an alert including verbose information regarding the relevant chain of processes that occurred and an explanation of the malware or suspicious command detected. Furthermore, Intezer Protect provides the capability to either terminate the detected process or incorporate the process into the trusted baseline. Intezer Protect provides threat intelligence for each detected threat, augmenting the triaging process by making available the threat intelligence necessary to understand the relative risk and determine appropriate steps for response.	Yes

HIPAA Security	Intezer Protect Features	Supports Compliance?
§164.308(a)(8) – Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operations changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart [the Security Rule]."	Intezer Protect performs scans against the installed packages and configuration files on each protected host to provide insight on the attack surface on each host. Intezer Protect identifies and reports on the CVE data associated with the packages installed on each host. Intezer Protect reads the host configuration files and tests them against the CIS Benchmarks, reporting on any deviation from the recommended best-practices.	Yes
§164.312 Technical Safeguards		
§164.312(b) – 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 provides real-time threat detection, providing visibility into the process executing in memory on each protected host. Intezer Protect analyzes the binary code executed in memory using Intezer's Genetic Software Mapping threat detection engine to identify indicators of compromise. This engine, based on code-based heuristic analysis, identifies and alerts on unauthorized processes.	Yes
§164.312(c)(2) – Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	Intezer Protect provides real-time threat detection and prevention, using memory analysis and code-based heuristic analysis, to identify malicious and unauthorized activity occurring on the protected hosts. Intezer Protect will detect and terminate malicious code or suspicious commands used in attempt to gain unauthorized access to system resources. Intezer Protect provides technical capabilities that protect against a subset of methods that may be used to alter and destroy protected health information. Customers may use this to support their overall strategy for addressing this risk.	Yes
HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414		

HIPAA Security	Intezer Protect Features	Supports Compliance?
Generates critical event details to inform accurate risk assessment and reporting of health information compromise.	Intezer Protect deploys agent-based sensors that continuously collects data on process information, including binary executables, shell scripts and commands, executable files and modules from disk or memory, and file permissions. Process execution information, including the malicious, anomalous, and trusted, is compiled and made available to the end-user via the Intezer Protect console. For all alerts, Intezer provides a detailed report on all executions running in the process tree, threat intel context regarding the malware or suspicious command identified, and a projected risk ranking.	Yes

Technical Analysis Methodology

Tevora reviewed the Intezer Protect solution to observe effectiveness for the following compliance areas:

- PCI DSS Requirements:
    - 2: Do not use vendor-supplied defaults for system password and other security parameters
    - 5: Protect all systems against malware and regularly update anti-virus software or programs
    - 6: Develop and maintain secure systems and applications
    - 10: Track and monitor all access to network resources and cardholder data
    - 11: Regularly test security systems and processes
    - 12.10: Implement an incident response plan
- HIPAA Requirements:
    - §164.308 Administrative Safeguards
        - (a)(1)(ii)(D) Information system activity review
        - (a)(5)(ii)(B) Protection from malicious software
        - (a)(6)(ii) Response and reporting
        - (a)(8) Standard
    - §164.312 Technical Safeguards
        - (b)Standard: Audit controls
        - (c)(2) Mechanism to authenticate electronic protected health information
    - HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414

Testing

Methodology

Tevora was provided access to an Intezer Protect lab environment, accompanied with SSH keys used to access the lab bastion host to interact with the protected nodes. Tevora explored the official Intezer documentation and user manuals provided to customers to understand the features available while simultaneously conducting a review of the management console to interact with features documented. SSH access was used to launch various attack simulations, as well as perform authorized commands, to observe the console outputs. Additionally, Tevora interviewed the Director of Product Development to confirm understanding and gain further insight into the underlying mechanisms for each feature.

Results

This section outlines the activities and observations that supported Tevora's conclusions on how Intezer's Key Features support the applicable PCI DSS and HIPAA Security Rule requirements.

Advanced Threat Detection

Using the SSH access provisioned, Tevora launched various attack simulations using common "living off the land" exploits. Tevora reviewed the Intezer Protect console and observed alerts associated with each of these commands, which verified that the threat detection engine functions beyond malware detection.

Intezer also provided a proof-of-concept lab environment containing alerts for fileless malware, a malicious files, and other suspicious commands, further demonstrating the range of detection capabilities.

Through review of Intezer documentation and interviews with the Director of Product Development, Tevora confirmed that the Intezer threat detection engine applies heuristic analysis against the code executed in dynamic memory, identifying patterns in raw binary code.

Visibility

For the various attack simulations launched, Tevora observed the alert details generated on the Intezer Protect console. For each alert, the console provided verbose information, including the machine meta data (i.e., hostname, IP address, OS version, OS release, and cloud platform), the chain of executions at all levels of the running process tree, and the command details.

Tevora confirmed through review of documentation and interviews with the Director of Product Development that the Intezer Protect-based sensors collect all running process information, including binary executables, shell scripts and commands, executable files and modules from disk or memory, and file permissions.

Visibility into unauthorized behavior was observed via examining the Intezer Protect console and sifting through the following categories of code detected: Malicious, Unknown, and Trusted. Tevora reviewed instances of "Unknown" code and identified the option to "Mark as Trusted," providing a simplified option to reduce false positives.

To test Intezer Protect's FIM functionality, Tevora found that Intezer Protect will generate "Sensitive Information Access" alerts when modifying "/etc/hosts" or "/etc/shadow". These alerts only represent a small portion of files that Intezer Protect can monitor for changes by default. In terms of log file monitoring, Tevora deleted and modified log files within /var/log (e.g., "syslog") and found that auditable events were successfully generated within the Intezer Protect console subsequent to these changes.

Tevora further examined the event details available on the console and observed that all process execution data is collected and made available, regardless of whether an alert is generated or not. Due to this feature, seemingly trusted code could be analyzed and manually flagged as malicious.

Response Augmentation

For suspicious commands alerted in Intezer Protect, Tevora identified an explanation of the command details, including a description of the suspicious command used, the associated MITRE tactics and techniques (e.g., exfiltration, command and control, use of standard or alternative protocols), and the available types of shell binding functions (e.g., reverse shell, bind shell, file upload, file download, sudo). Tevora identified an option to "Terminate Process" from the management console.

For malware alerted on, Intezer Protect reports on the malware family, the similarities between the code execution patterns and Genetic Profiles of various strains of malware, the file hashes associated with each malware, and all code strings that were identified to be related to the malware. Tevora identified an option to "Terminate Process" from the management console.

Reduced Attack Surface

On the Intezer Protect console, Tevora examined example Asset reports titled "Installed Packages" and "Configuration Checks." The Installed Packages report revealed a list of findings, with each finding reporting a risk ranking, the package name, the package version, the date and time of finding, and the CVE references associated with each. The Configuration Checks report revealed a list of findings, with each finding reporting a risk ranking, the configuration file-path, the CIS Benchmark referenced, the rationale for the configuration recommendation, and steps on how to remediate the finding.

Adaptability to Modern Cloud

Tevora reviewed Intezer Protect proof-of-concept documentation, which demonstrated various attack simulations affect all layers of the native cloud stack. These attacks included exploitation of an Apache patch related vulnerability, a Docker misconfiguration, and an infected Docker image.

When reviewing the "Installed Packages" and "Configuration Checks" reports supporting the "Reducing Attack Surface" key feature, Tevora observed findings at all layers of the native-cloud stack, identifying those affecting Docker, Kubernetes, Linux, and Nginx within the lab environment.

Conclusion

Intezer Protect is an effective cloud workload security solution that can significantly augment any team's ability to effectively protect, detect, and respond to a wide variety of sophisticated attack vectors. Offering advancements in threat detection technology, Intezer Protect serves as an adaptation to the evasion and obfuscation techniques used by modern threat actors. Intezer Protect supplements any incident response program, aiding with triaging and automating steps in the containment process.

Intezer Protect effectively addresses customer requirements regarding anti-malware and endpoint detection and response and comprehensively fulfills the server-level technology controls mandated by PCI DSS and HIPAA.

Intezer's Protect can provide an organization with a comprehensive set of technological controls to significantly augment the security posture of their cloud workloads and fulfill the PCI DSS and HIPAA requirements identified in this paper.

Appendix

Definitions – Compliance Standards

PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is intended to protect cardholder data wherever it resides to ensure that members, merchants and service providers maintain the highest information security standard. PCI DSS is a set of comprehensive requirements for enhancing payment account data security. The standard was developed by the founding payment brands of the PCI Security Standard Council to help facilitate the broad adoption of consistent data security measures on a global basis.

HIPAA Security Rule

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 requires that Covered Entities must take strong measures to protect the privacy and security of health information. At the endpoint, this translates to ensuring the host is protected from malware. Specifically, the HIPAA Security Rule requires Covered Entities and Business Associates to comply with general security requirements. More specifically, the Administrative Safeguards in §164.308(a)(1), §164.308(a)(5)(ii)(B) and §164.308(a)6(ii), require Covered Entities and Business Associates to implement and maintain procedures to protect, detect, contain, respond, correct, and report on malicious software throughout the environment.

About Intezer

Intezer Protect provides runtime security for cloud and Linux servers. The platform continuously monitors your entire stack in runtime—incl. VMs, containers, and K8s—for every code and application that is running. With so much code running in your systems, from third party libraries to proprietary software, Intezer organizes this mess by giving you full runtime visibility and detecting attacks as they occur. For more information, visit www.intezer.com or follow the company on Twitter at @IntezerLabs.

INTEZER

About Tevora

Tevora is a leading management consulting firm specializing in enterprise risk, compliance, information security solutions, and threat research. We offer a comprehensive portfolio of information security solutions and services to clients in virtually all industries and also serve institutional and government clients.

Tevora's leaders are professionals with years of experience and records of accomplishments in technology as well as business. This dual background means that we understand the importance of growth and profitability and our solutions are designed to enhance both.

As a consulting firm that has the ability to fully implement whatever it recommends, Tevora works with all of the industry's top vendors, yet is beholden to none. We are completely vendor-independent and select best-of-breed products tailored exclusively to our clients' needs. Security is our only business and our single-minded focus on anticipating and solving client problems has been described as "obsessive." We consider this a fair assessment.

Our hard work and dedication has established us as a reliable partner CTOs CIOs, and CISOs can depend on to help protect against threats, both internal and external. With Tevora as a partner, business leaders can devote their energies to enhancing the overall value of information technology to their enterprise.

Tevora is a Qualified Security Assessor (QSA) and Payment Application Qualified Security Assessor (PA-QSA) in good standing with the PCI Security Standards Council. Tevora is also a DVBE (Disabled Veteran Business Enterprise) certified by the California General Services Department (Cert REF# 32786).

For more information please visit www.tevora.com.

TEVORA™

Go forward. We’ve got your back.

Compliance - Enterprise Risk Management - Incident Response
Data Privacy - Security Solutions - Threat Management