Simplify PCI 4.0 Compliance

WITH THE OLIGO APPLICATION DEFENSE PLATFORM

PCI SIMPLIFIED

Stay PCI Compliant with Oligo

Getting in compliance with PCI DSS 4.0 requires adherence to dozens of new standards. How can security teams maintain compliance when the standards require managing all existing vulnerabilities - **regardless of their level of severity?**

The Oligo Application Defense Platform, with exploitability-based vulnerability management as well as application attack detection and response, **simplifies PCI 4.0 compliance** and its risk management requirements.

INVENTORY UPDATE

Maintain Up-to-Date Inventories

PCI standards also require maintaining an inventory of not only your own first-party software, **but also third-party software components.**

The Oligo Application Defense Platform goes further than any other product on the market to **create comprehensive software inventories for first- and third-party applications.** Using Oligo, you can identify all components in first- and third-party software used at runtime, including software applications where you do not have access to the source code. This enables you to have full visibility over all components without relying on third-party SBOMs that could be out-of-date.

PCI 4.0 Standard	The Oligo Solution
6.3.2 An inventory of bespoke and custom software, and third-party software components incorporated into bespoke and custom software is maintained to facilitate vulnerability and patch management.	Oligo inventories all first- and third-party software components - so you can see every part of your applications.

RISK PRIORITIZATION

Keep Vulnerabilities Under Control

To comply with PCI 4.0, you'll need to scan for vulnerabilities, with a scanner that rates their severity and risk. Critical and high-risk vulnerabilities must be resolved **within a month of a new security patch** being available, while less-risky vulnerabilities must be "managed."

The Oligo Application Defense Platform provides information on which vulnerable libraries and functions are **actually executed at runtime** - allowing non-executed vulnerabilities (which can be as much as 99% of the total vulnerabilities present in an application) to be assigned a lower risk score.

Simply being assessed by the Oligo Application Defense Platform as a non-executed vulnerable function or library allows a vulnerability to be considered "managed" by PCI 4.0 standards. This enables developers to keep working on features, instead of being **bogged down by constant demands** to patch vulnerabilities that could never actually be exploited.

PCI 4.0 Standard	The Oligo Solution
6.3.1 Security vulnerabilities are identified and managed as follows: • New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). • Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. • Risk rankings identify, at a minimum, all vulnerabilities considered to be a high risk or critical to the environment. • Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.	Risk rankings in the Oligo Application Defense Platform are assigned based not only on the vulnerability severity, but whether the vulnerable library and function are loaded and executed. Using Oligo to identify vulnerabilities relying on non-executed libraries or functions means these vulnerabilities can be considered no longer high-risk or critical.
11.3.1 Internal vulnerability scans are performed as follows: • At least once every three months. • High-risk and critical vulnerabilities (per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are resolved. • Rescans are performed that confirm all high-risk and critical vulnerabilities (as noted above) have been resolved. • Scan tool is kept up to date with latest vulnerability information. • Scans are performed by qualified personnel and organizational independence of the tester exists.	Scan for vulnerabilities while also detecting whether vulnerable libraries & functions are executed. No execution = non-exploitable, no risk. Non-exploitable vulnerabilities can be considered lower-risk and "managed" in compliance - no need to patch to stay compliant.
11.3.1.1 All other applicable vulnerabilities (those not ranked as high-risk or critical per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are managed as follows: • Addressed based on the risk defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. • Rescans are conducted as needed.	"Managing" risks for these lower-risk vulnerabilities can include simply identifying them as non-exploitable using the Oligo Application Defense Platform.

ATTACK PREVENTION

Detect and Block Application Attacks

In addition to maintaining software inventories and managing vulnerabilities, PCI 4.0 also requires **active detection or prevention of attacks** on public-facing web applications.

For designated entities requiring supplemental validation, including those that store or transmit large volumes of account data or who have "suffered significant or repeated breaches of account data," additional requirements include implementing a methodology to **identify suspicious application behavior** and alert security teams when this behavior occurs.

Oligo Application Detection & Response (Oligo ADR) - included in the Oligo Application Defense Platform - continuously scans applications at runtime to **reveal anomalous behavior** and alert security teams when anomalies are detected.

PCI 4.0 Standard	The Oligo Solution
6.4.2 For public-facing web applications, an automated technical solution is deployed that continually detects and prevents web-based attacks, with at least the following: • Is installed in front of public-facing web applications and is configured to detect and prevent web-based attacks. • Actively running and up to date as applicable. • Generating audit logs. • Configured to either block web-based attacks or generate an alert that is immediately investigated	The Oligo Application Defense Platform continually detects and prevents attacks on web-based applications. Oligo can alert to a range of remote code execution (RCE) attacks and detect anomalous runtime behavior indicating an attack has been initiated.
A3.5.1 A methodology is implemented for the prompt identification of attack patterns and undesirable behavior across systems that includes: • Identification of anomalies or suspicious activity as it occurs. • Issuance of prompt alerts upon detection of suspicious activity or anomaly to responsible personnel. • Response to alerts in accordance with documented response procedures.	Oligo ADR identifies anomalous or suspicious behavior patterns in runtime and triggers alerts when any suspicious behavior is detected (for example, a library being used to execute code that is not typically used this way).

SWIFT SETUP

Get Started With the Oligo Application Defense Platform

With Oligo, you can enhance compliance fast - our platform offers **simple, quick deployment and value** you can see right away.

With low technical overhead (<1%) and **very low maintenance requirements** (<¼ FTE), the Oligo Application Defense Platform is all gain, no pain for your security team.