Checklist

Imperva

WAAP CHECKLIST

Essential Capabilities of a Web Application Firewall and API Security Solution

thalestct.com

THALES
Building a future we can all trust

THALES

What is my organization's WAAP (ROSI) - Return on Security Investment?

Category	Description	Imperva	My Current Solution
OWASP Top 10 protection	Tools protect against OWASP Top 10 out of the box with default policies	✓	
Account takeover protection	Identifies and blocks attacks linked to account takeover (credential stuffing, brute force).	✓	
Client-side protection	Identify and block client-side attacks (magecart, formjacking, skimming)	✓	
API discovery	Ability to discover and categorize all APIs in production environment	✓	
Client-side protection	Identify and block client-side attacks (magecart, formjacking, skimming)	✓	
Import Swagger file option	Ability to import Swagger file if customer does not want to do API discovery.	✓	
Data classification	Ability to classify data APIs handle to know which APIs are handling sensitive data (PII)	✓	
Block out of the box	Confidence in product is high enough that policies can be in blocking mode OTTB	✓	
Bad bot protection	Ability to distinguish between good bots, bad bots, and human traffic. Bad bots are blocked.	✓	
JavaScript visibility	Ability to report on what JavaScript is running on sites	✓	
JavaScript risk analysis	Ability to score JS services running on sites based on risk	✓	
DDoS protection	Ability to detect and immediately prevent a high-volume DDoS attack	✓	
DDoS mitigation SLA	5 seconds or less SLA for DDoS mitigation regardless of attack size or origins.	✓	
Reputation intelligence	Ability to provide reputation of attacking IP address	✓	
Dynamic DDoS threshold	Ability to automatically adjust DDoS threshold instead of customers manually adjusting it.	✓	
Low false positive rate	Incident false positive rate is very low. Ideally below 1%.	✓	

Category	Description	Imperva	My Current Solution
Machine learning/AI abilities	Machine learning capabilities. Tools have the ability to create a baseline of normal traffic and alert on deviations from the baseline.	✓	
Threat Intelligence automation	Ability to provide intelligence on latest threats and attacks. Ability to automatically identify and block new attack patterns.	✓	
Advanced attack detection	Ability to detect based on heuristics, anomalies, and signatures	✓	
Uptime	Near 100% uptime with little to no outages	✓	
SIEM Integration	Easy integration with SIEM tools. Ability to customize what is sent to SIEM.	✓	
SOAR Integration	Easy integration with SOAR tools. Ability to have all incidents triaged through SOAR. When incident is closed in SOAR, it is closed in WAAP tool.	x	
ITIL/ISIM Integration	Easy integration into a ticketing tool, like ServiceNow.	✓	
AD Integration	Integration with Microsoft Active Directory.	✓	
RBAC	Ability to create different access groups and customize what they have access to on the portal	✓	
UI ease of use	UI is easy to understand and navigate	✓	
Actionable incidents	Incidents provide enough detail to immediately act upon. Ideally, all incident information is displayed in one screen. Little to no additional research is necessary to triage alert.	✓	
Flexible deployment	Supports on-prem, hybrid, and cloud environments	✓	
TLS 1.3 support	Support for TLS 1.3 or plan to support it in the very near future	✓	
Account insights	Portal automatically reviews current app sec settings and policies and makes recommendations on any possible misconfigurations	✓	
Onboarding ease of use	Quick and easy to onboard sites to WAAP.	✓	
Flexibility around certificates	Customer can bring their own signed certs or vendor can sign them for them	✓	
SSO	Ability to login via SSO	✓	

Category	Description	Imperva	My Current Solution
MFA	Ability to implement MFA for logins. Support for multiple MFA vendors.	✓	
API integration	Tool has an built-in API to connect other applications to (ex: SIEM)	✓	
Audit logs	Audit logs are recorded and can be exported to SIEM	✓	
GeoBlocking	Ability to block countries instead of just IP ranges	✓	
Customized allowlist and blocklist	Ability to add or exclude sites, groups, resources, etc. from policies	✓	
Custom policies	Ability to create custom policies based on any criteria. Policy actions can also be customized	✓	
Meaningful Reporting	Reports are easy-to-understand, provide meaningful information, and have a variety of reports for different levels of employees. Ex: executive summary, SOC summary, etc.	✓	
Container protection	Ability to protect containers	x	
Meaningful dashboards	OOTB dashboards are meaningful. Customers can easily drill down for more information.	✓	
Granular insight	Ability to drill down and see activity and incidents at the granular level (by site, date, account)	✓	
Defined Service SLAs	Service contract has defined SLAs for different incident levels that are strictly adhered to.	✓	
Professional Services not necessary	Tool should be easy enough to use that additional professional services hours do not need to be purchased after tool has been stood up.	✓	
Critical incident/outage support	Ability to always reach vendor by phone in the event of a critical outage/issue. Critical incidents are a priority for vendor no matter what level of support customer has purchased.	✓	
Notification Center	Notification center around important updates or outages	✓	
Documentation	Company has an up-to-date documentation repository that is easy to navigate. Documentation is easy to understand and follow along with.	✓	

Category	Description	Imperva	My Current Solution
Tool integration	Different components of WAAP easily integrate together. Onboading another app security tool from the same vendor is seamless. WAAP components work together to create actionable incidents that are enriched with data from each tool instead of each tool creating its own incidents.	✓	
Single platform	All components of WAAP are in a single platform/console. Onboarding another app security tool does not require standing up another instance	✓	
MSSP support	Ability to support MSSPs. Provide a centralized dashboard for all clients of an MSSP with the ability to drill down into each customer's data. Ability to provide data segmentation for an MSSP so each customers data is segmented.	✓	
Compliance support	Vendor adheres to various compliance standards (SOX, PCI, SOC 2, etc) and allows customers to easily show auditors that they're compliant.	✓	
Scrubbing centers	Vendor has global scrubbing centers for DDoS traffic	✓	
Vendor client relationship	Vendor creates a strong relationship with the client and regularly checks in with them to make sure they're getting as much as they can out of the product. This should include an annual posture check where the vendor and client review the client's instance.	✓	
Global, fully-capable PoPs	Vendor has PoPs around the globe. Each PoP offers full WAAP protection.	✓	

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., is a trusted, U.S. provider of cybersecurity solutions dedicated to U.S. Government. We protect the government's most vital data from the core to the cloud to the edge with a unified approach to data protection. Our solutions reduce the risks associated with the most critical attack vectors and address the government's most stringent encryption, key management, and access control requirements.

For more information, visit www.thalestct.com

©2024 Thales 3.28.24

Contact us - For office location and contact information, please visit thalestct.com/contact-us