IT SECURITY GURU PRODUCT REVIEW

PerimeterX Code Defender

Scores

Performance - 5/5
Features - 5/5
Value for Money - 4.5/5
Ease of Use- 5/5

Overall - 5/5

Supplier: PerimeterX

Website: www.perimeterx.com

Price: Based on website traffic

Verdict

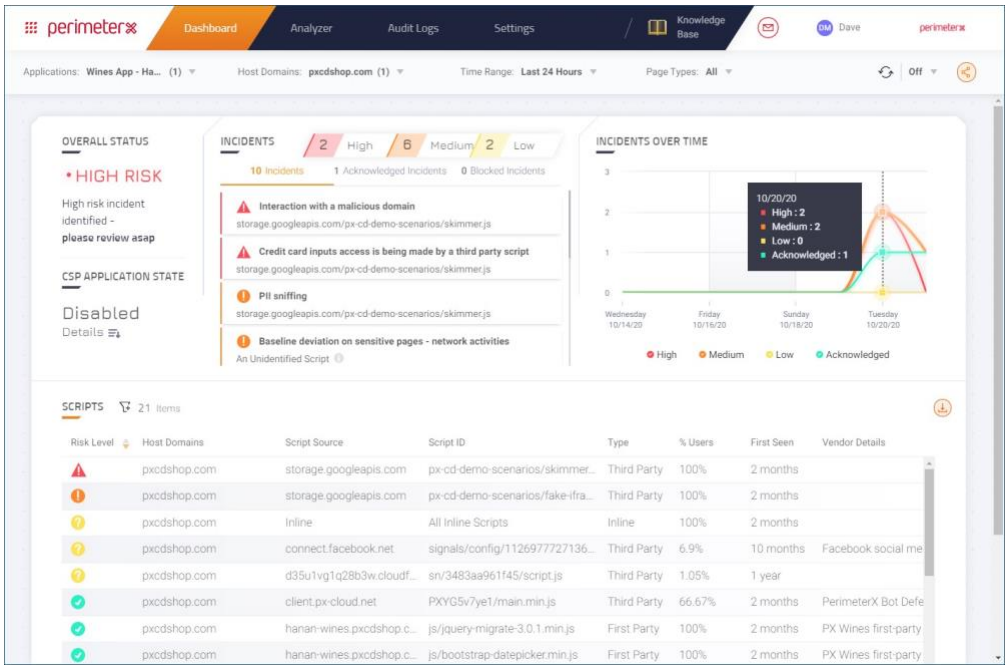
What's on your web site? PerimeterX Code Defender takes the worry out of e commerce with a simple yet highly effective client-side script analysis and risk mitigation solution.

Cybercriminals always prey on our fears in times of crisis and you can rest assured they won't be cutting your business any slack during the coronavirus pandemic and in the ensuing aftermath. The numbers back this up as attacks have increased exponentially this year and it's crystal clear that absolutely nothing is sacred.

Organisations that rely heavily on e-commerce are at extreme risk levels with clientside data breaches such as Magecart attacks growing in frequency and sophistication. Compliance with data protection regulations isn't optional and, as one global airline recently found to its cost, failure to do so will lead to punitive fines.

PerimeterX offers a powerful protection solution as its Code Defender continuously monitors all client-side activity on your web sites, detects attempts to sniff data, stops malicious scripts from exfiltrating data and alerts you in real-time. Unlike many competing solutions, it doesn't rely on cumbersome sandboxes but employs a lightweight JavaScript sensor embedded in the web pages.

The sensor collects information from client-side browsers including all script activity and passes this to a cloud-based Detector for further analysis. The smart part comes next as the Detector uses advanced machine learning to ascertain threat levels and employs an out-of-band Enforcer to automatically modify and apply CSP (content security policy) rules for continuous real-time protection.



Picture 1: *The Code Defender portal dashboard shows you everything you need to know about scripts running on your web site.*

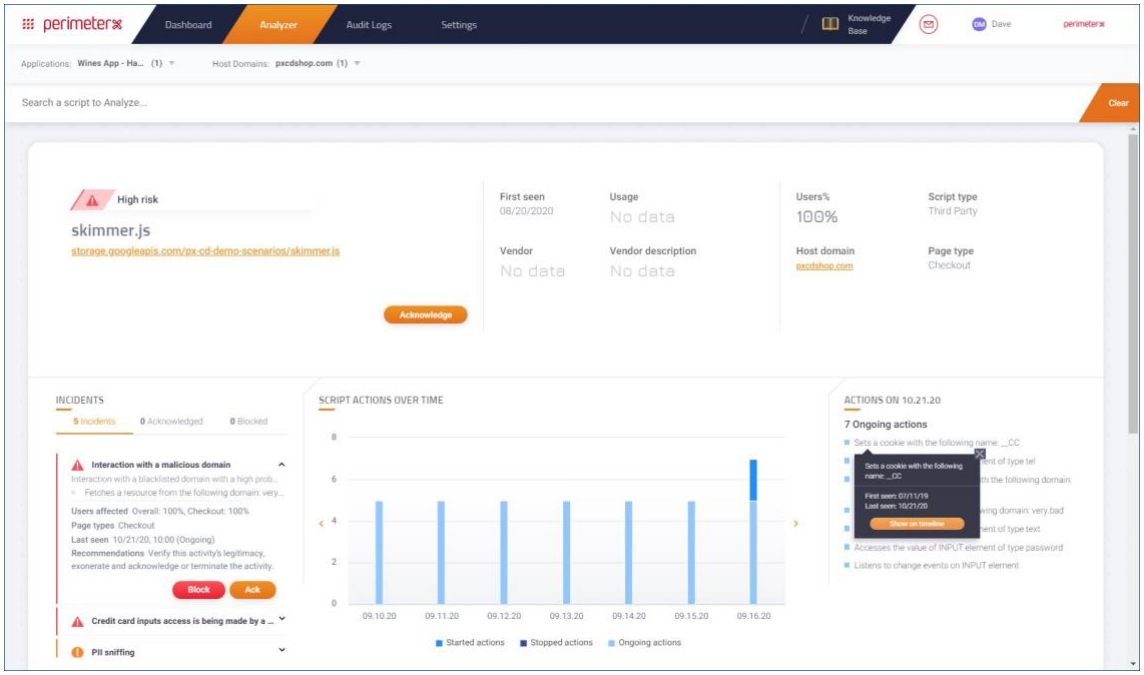
The PerimeterX Platform

Along with Code Defender, the PerimeterX suite includes PerimeterX Bot Defender and PerimeterX Page Defender protection applications and all three are managed from the same web portal. Where appropriate, they use the same JavaScript sensor, Detector and Enforcer making it simple to augment Code Defender with other components if required.

Sensor deployment is a swift process and it can be embedded in web pages easily using page templates. PerimeterX supplies the sensor which could be as small as a couple of lines of JavaScript code and its 24/7 SOC teams will provide assistance if required.

The sensor collects data on DOM change, code injection and lookup events, storage accesses, methods and origins of script execution plus network communications related to third-party domains. It does not collect information on user inputs when form filling, any PII (personally identifiable information) or credit card transactions.

All data collection is asynchronous and has no impact on a user's experience. Blocking actions are transparent and the Enforcer ensures scripts will be allowed to run legitimate actions so customers can continue to make their purchases with no knowledge that malicious communication is being blocked behind the scenes.



Picture 2: *The Analyzer page provides deep insights into script actions and who it is trying to communicate with.*

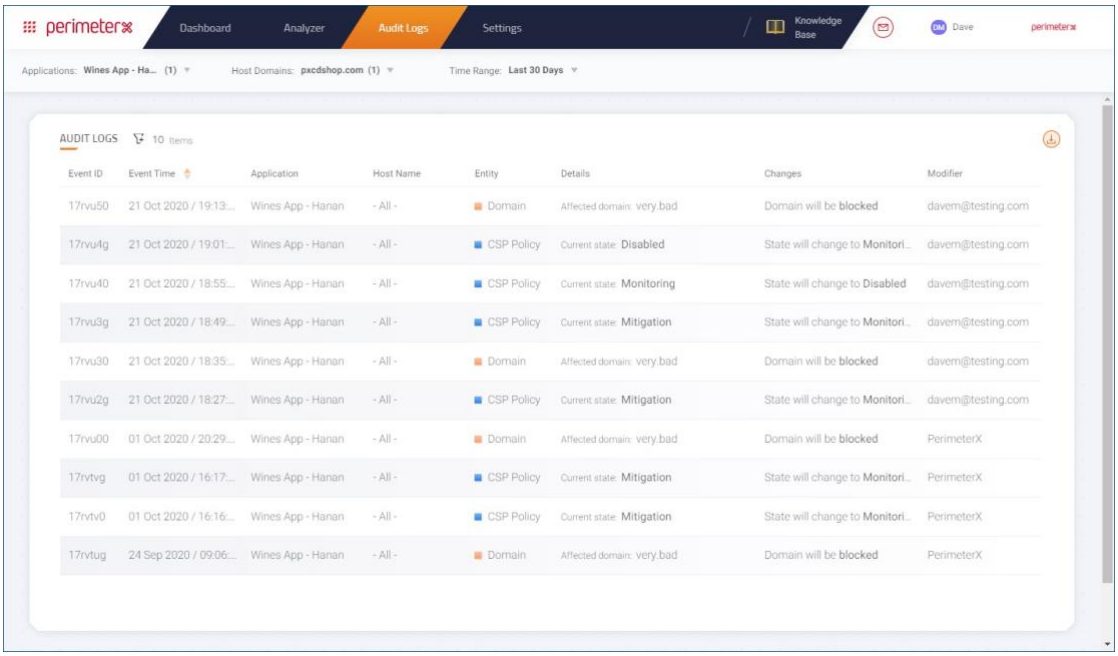
The Platform Portal

When your account is assigned, Code Defender creates a custom JavaScript snippet. This can be inserted into all pages on your web site and it's preferable that if not the first script, it's placed as high up in the HTML as possible.

When web pages containing the sensor are loaded, client-side statistics are gathered and presented in the Portal's dashboard. To create a site baseline, PerimeterX recommends allowing it to run for a few days, up to a week or two, so it can establish a clear picture of all running scripts and actions.

The dashboard presents a detailed inventory of all scripts running on the web pages - InfoSec teams will love this as it provides levels of information many rarely get to see. Instead of having to vet all web site changes their analytics and marketing teams want to make, they can let them go ahead and have full visibility on all their activities.

A status panel provides a heads-up view of the web site's risk level and whether Code Defender is in monitoring or mitigation mode. Scripts that generate alerts are shown in an incidents panel alongside in high, medium or low risk categories while a graph next door shows all incidents over the selected time period.



Picture 3: *Code Defender provides a full audit trail of all user activity and any modifications made.*

Risk analysis and mitigation

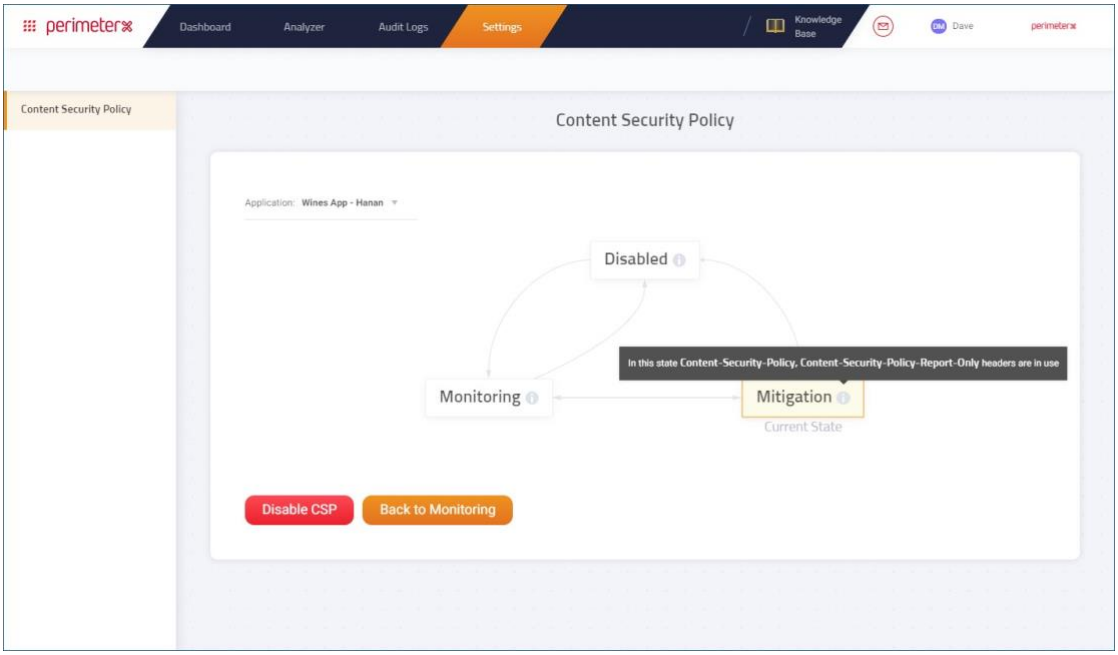
Colour-coded icons denote script risk levels and the dashboard's table list shows their source, the script ID, whether they are first- or third-party, the percentage of users impacted, when they were first seen and the vendor's details. Hovering the mouse over a risk icon loads a pop-up window showing the reason for the classification and scripts can be blocked or acknowledged directly from the incidents panel.

Script IDs can be selected from the table or in the incidents view and a full analysis conducted. The Analyzer tab provides a complete breakdown of the script showing what it is attempting to do and how often it has been run.

The script analysis presents a behavioural chart where you can see if it is trying to access details such as credit card information, what other scripts it is loading and the external domains it is attempting to communicate with. This makes it easy to analyse the script code without deep knowledge and Code Defender provides sage advice on how to deal with it.

From here, you can acknowledge the script so it becomes part of your behavioural baseline or block it with one click. Choose the latter and Code Defender's mitigation processes swing into action and stop it communicating with the suspicious domains instantly. This kills the chain and prevents exfiltration of data but allows the rest of the script to function normally.

Code Defender provides full auditing of all activities which includes actions, event times and the person responsible for the modification. It can integrate with customer's Slack channels for instant event notifications, team up with incident management platforms such as OpsGenie or ServiceNow and use APIs to export information into your SIEM (security information and event management) solution.



Picture 4 : *The Settings page provides an overview of Code Defender where you can see whether it is disabled, in monitoring mode or enforcing mitigation with CSPs.*

Conclusion

With today's web sites containing huge amounts of third-party code, it is essential that businesses, and especially those dependent on e-commerce, understand their impact on security and mitigate risk. Too many are unaware of what's running on their web sites and with Magecart and supply chain attacks on the increase, they cannot afford to remain in the dark.

PerimeterX Code Defender is an elegant solution to this growing problem as it provides complete visibility into all script activity and swift risk mitigation with automated CSP rule enforcement. It's remarkably easy to deploy, doesn't require architectural changes to the web site and, crucially, won't impact on your user's experiences.