DATA SHEET

FortiWeb Cloud Threat Analytics

Available in:

AI-based Threat Analytics Help Zoom In on the Most Important Threats

Security analysts face a rapidly evolving threat landscape that can overwhelm them with security alerts. Threat actors continue to launch increasingly sophisticated attack campaigns that leverage new attack frameworks, vast botnets, and new vulnerabilities. The situation facing the security analyst becomes even more challenging as their organizations move more applications to the cloud, and those applications increasingly deliver critical line of business capabilities. As the attack surface for applications continues its rapid evolution and expansion, security analysts need better tools to keep up with the growing volume of alerts generated by their security tools.

Without better tools, security teams risk becoming overwhelmed by the volume of events, with many of those events turning out to be of low value when seen in isolation – or even worse, turning out to be false positives after further investigation. This alert fatigue can result in critical security events being missed or overlooked.

FortiWeb Cloud Threat Analytics uses machine learning algorithms to identify attack patterns across your entire application attack surface and aggregate them into comprehensible security incidents. The solution separates significant threats from informational alerts and false positives by identifying patterns and assigning a severity to help your security team focus on the threats that matter.

Investigating security alerts requires context and the ability to connect the dots across multiple events over time. FortiWeb Cloud Threat Analytics removes the complexity that comes from manually evaluating alerts by evaluating thousands of alerts and grouping those alerts into incidents based on the patterns identified. With this streamlined view, SOC analysts can focus their efforts on the important threats.

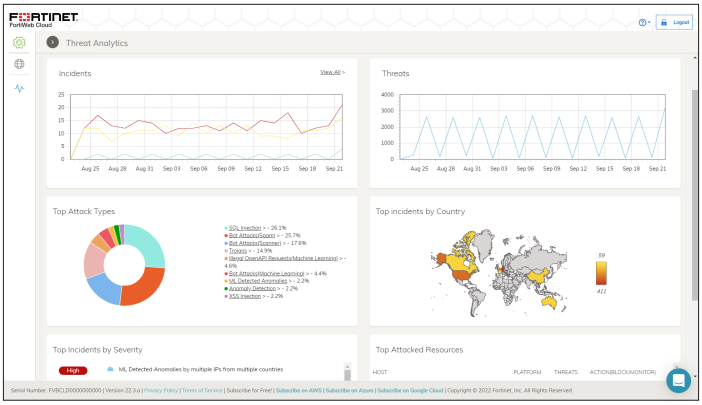
Key Features

- AI based Threat Analytics
- Identifies common characteristics and patterns and groups them into meaningful security incidents
- Incident risk prioritization
- Workflow Integration

Key Benefits

- Simplifies threat detection and response
- Speeds up WAF alerts security investigation
- Helps analysts focus on the most important threats
- Insights provide suggestions to harden security based on findings
- Ingests events from across your entire hybrid cloud environments
- Alleviates alert fatigue

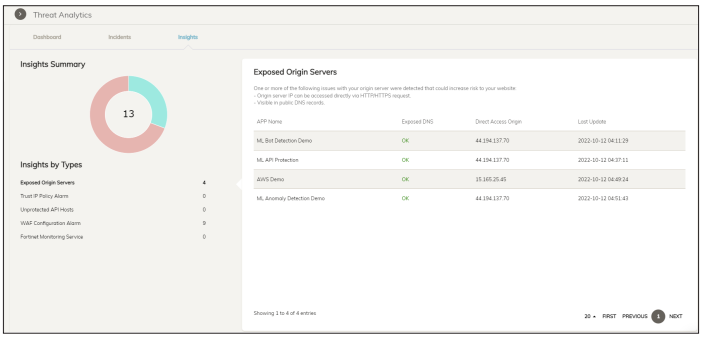
FEATURE HIGHLIGHTS



Threat Analytics Insights and Incident Enrichment

Threat Analytics continuously assess your security posture by monitoring attacks on your web assets together with evaluating your WAF configuration. Attack data is cross referenced across our entire customer base to correlate suspicious and anomalous traffic and alert customers when susceptible to attacks based on their configuration.

Threat Analytics Insights provide recommended actions that can enhance your WAF configuration settings, block future attacks and reduce false positives.



Visibility across SaaS, Cloud, and On-prem Applications

FortiWeb Threat Analytics ingests events from all of your FortiWeb appliances, FortiWeb VMs, and FortiWeb Cloud, delivering the insights that SOC analysts need across the entire web application attack surface. Regardless of where the applications are deployed or which FortiWeb form factor you chose, the solution delivers a unified view of threats from across your application attack surface with a single pane of glass. Threat Analytics aggregates events across the entire enterprise allowing analysts to identify enterprise wide attack campaigns that span multiple locations and web assets.

ORDER INFORMATION

PRODUCT	INDIVIDUAL	BUNDLES	
	A LA CARTE	ADVANCED	STANDARD
Threat Analytics	✓	✓	

The following table provides an example for the FortiWeb-2000F.

PRODUCT	SKU	DESCRIPTION
Bundle	FC-10-FW2KF-580-02-DD	Advanced Bundle (FortiCare Premium plus AV, FortiWeb Security Service, IP Reputation, FortiSandbox Cloud Service, Credential Stuffing Defense Service and Threat Analytics)
A La Carte	FC-10-FW2KF-579-02-DD	Threat Analytics Service

Threat Analytics is included for FortiWeb Cloud applications, and available as part of the advanced bundle or A La Carte for applications protected by FortiWeb appliances and VMs.

www.fortinet.com