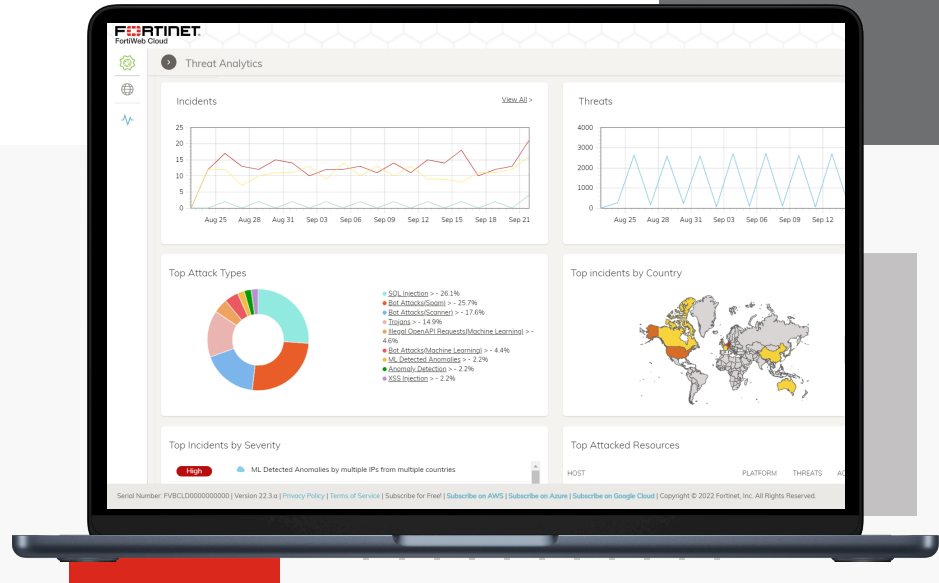


# Fortinet AI Threat Analytics



## Key Features

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

## 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.

**Available in****Appliance****Virtual****Hosted****Cloud**

## Highlights

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.

Fortinet AI 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. Fortinet AI 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 Benefits

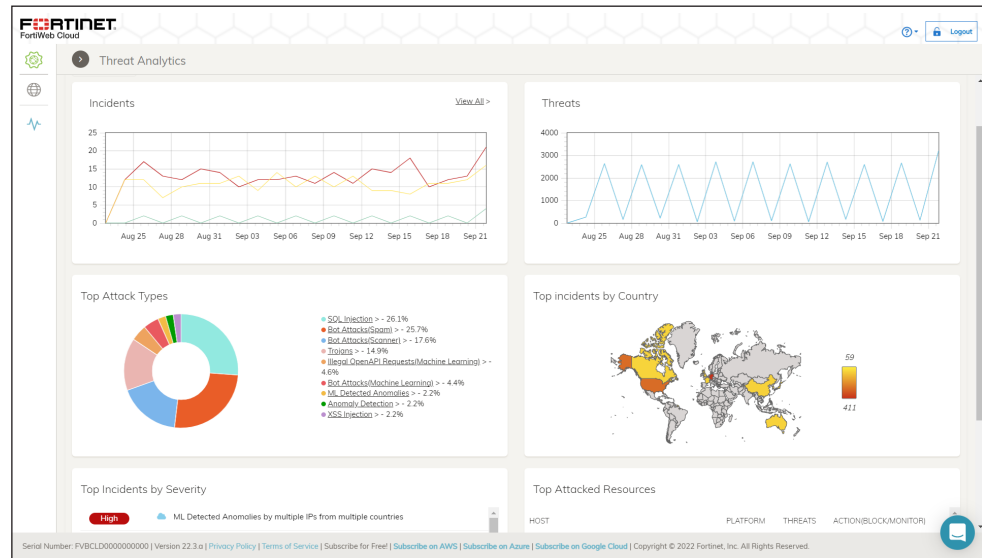
- Simplifies threat detection and response
- Speeds up security alerts investigation
- Helps analysts focus on the most important threats
- Insights provide suggestions to harden security based on findings
- Ingests events from across your entire hybrid cloud environments
- Alleviates alert fatigue

## Features

### Threat Analytics Insights and Incident Enrichment

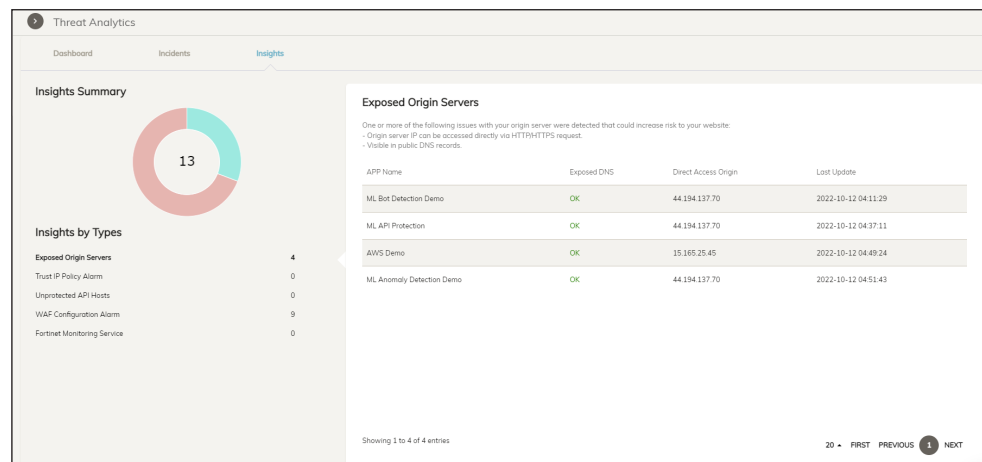
Threat Analytics continuously assess your security posture by monitoring attacks on your web assets together with evaluating your WAF configuration. Attack data is cross referenced across our entire customer base to correlate suspicious and anomalous traffic and alert customers when susceptible to attacks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

Threat Analytics ingests events from all of your FortiWeb/FortiADC appliances and VM, 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 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.



## Ordering Information

PRODUCT	INDIVIDUAL		BUNDLES	
	A LA CARTE	STANDARD	ADVANCED	ENTERPRISE
FortiWeb	✓	✗	✓	✓
	A LA CARTE	Network Security	Application Security	AI Security
FortiADC	✓	✗	✗	✓

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 bundle or A La Carte by FortiWeb/ FortiADC appliances and VMs.

The following table provides an example for the FortiADC-2200F.

PRODUCT	SKU	DESCRIPTION
Bundle	FC-10-AD22F-732-02-DD	AI Security - Application Security Bundle Plus Threat Analytics, FortiGuard Advanced Bot Protection - (2.5M monthly requests), and FortiCare Premium.
A La Carte	FC-10-AD22F-579-02-DD	Threat Analytics Service

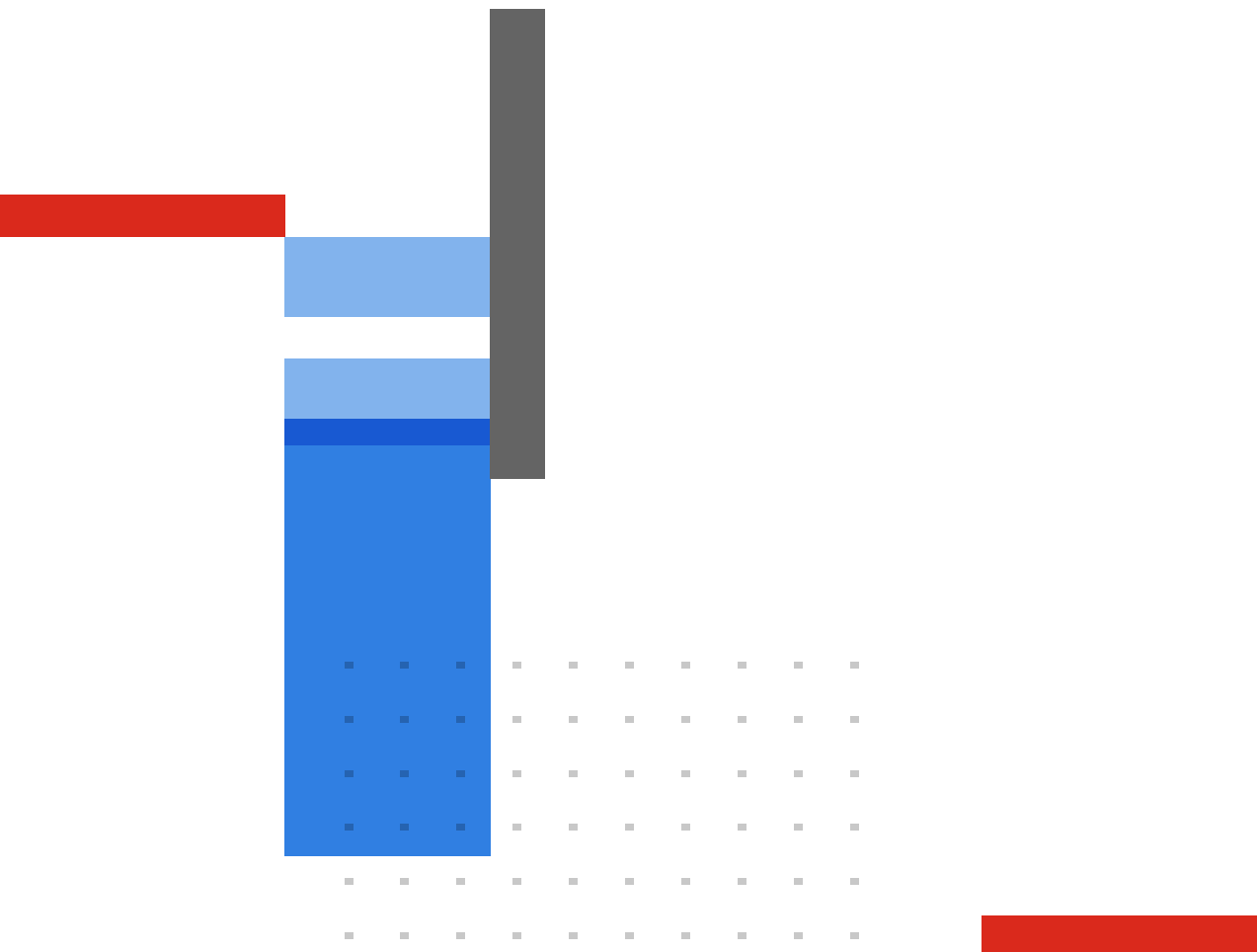
Threat Analytics is included for FortiWeb Cloud applications, and available as part of the bundle or A La Carte by FortiWeb/ FortiADC appliances and VMs.



---

## Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the [Fortinet EULA](#) and report any suspected violations of the EULA via the procedures outlined in the [Fortinet Whistleblower Policy](#).



[www.fortinet.com](http://www.fortinet.com)

Copyright © 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.