imperva

CAPABILITY BRIEF

Attack Analytics

Uncover attacks hiding in an avalanche of security alerts

Security teams are often overwhelmed with the volume and sophistication of emerging threats and relentless data breaches. Ideally they want to receive alerts when a potential risk is seen, and be able to take action based on a clear understanding of the context. Instead they labor under a massive overload of security events, making it almost impossible to connect the dots and determine where to spend their time. The situation only gets worse as applications are moved to the cloud, presenting new security challenges related to cloud-specific or hybrid environments and a greater need for enterprise-wide visibility.

Imperva Cloud WAF offers the industry's leading web application security firewall, IT organizations looking for a way to decisively respond to and resolve security events while avoiding "alert fatigue" and wasting valuable time chasing down false positives need a smart analytics tool. One with built-in artificial intelligence would enable them to evaluate large volumes of data almost instantaneously and find commonalities and correlations that are invisible to the naked eye. Such a tool, when trained through machine learning algorithms, would be extremely useful in finding and prioritizing true security events from among the constant barrage of security alerts.

Imperva Attack Analytics

Imperva Attack Analytics correlates and distills thousands of security events into a few distinct readable narratives. Through sophisticated use of artificial intelligence and machine learning, it takes the mystery out of investigating application security events and enables IT organizations to mitigate and respond to real security threats quickly and decisively. Attack Analytics sorts and groups security events into clusters of narratives, assigning each a severity level so teams can quickly investigate.

KEY CAPABILITIES:

Correlates and distills thousands of security events into actionable insights

Cloud-based for fast deployment

Unified monitoring of cloud and on-premises WAF

Collective intelligence from global customer base

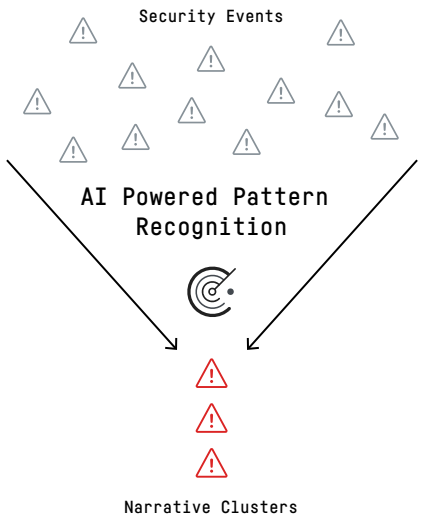

Figure 1: Attack Analytics distill thousands of security events into a few readable narratives.

Make security teams more effective

Reduced risk

By grouping many sec events into narratives and prioritizing them, Attack Analytics removes the complexity associated with investigating these events. Making it easier for analysts to investigate and focus on the few incidents that really matter, contrary to going through thousands of events to identify an attack. This use of AI reduces the risk associated with missing attacks that would otherwise be lost in the alert overload.

Unified visibility

As companies start deploying sec in the cloud to protect their cloud-based apps and APIs, it gets harder to monitor sec events throughout the enterprise. Attack Analytics provides a unified view to monitor all the sec events generated by Imperva cloud-based and on-prem WAF solutions. This enables complete platform visibility and helps in identifying enterprise-wide attack campaigns. Visibility and integration support with other Imperva solutions include Advanced Bot Protection, API Security, DDoS, Cloud WAF, Reputation Intelligence, RASP and WAF Gateway.

Global insights

Using AI, Attack Analytics clusters event data collected globally, on the customer's estate, to identify attack patterns. This info is of tremendous value to determine new or common attack campaigns that hackers are launching. This collective intelligence enables quick attack identification and actionable insights for enhancing a customer's security posture.

Cloud-ready

Attack Analytics is a cloud-based solution that can be deployed with the click of a button. The cloud means unlimited scalability and the ability to accept as many events as an enterprise needs for it to process.

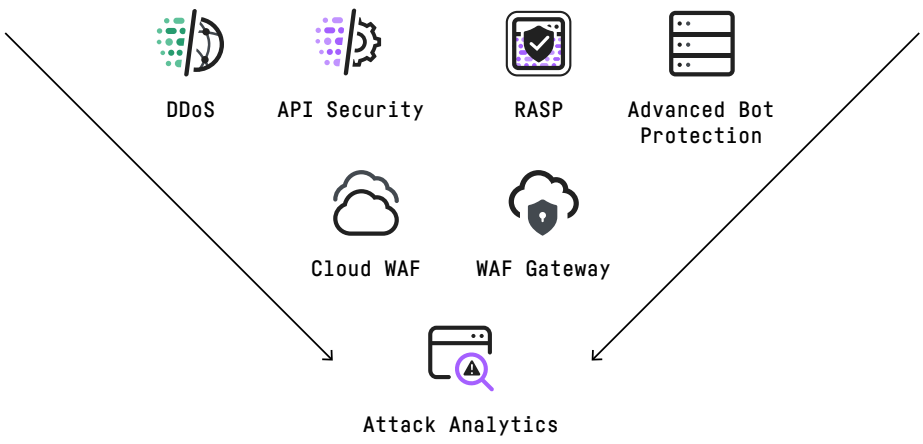

Figure 2: Thousands of security events across multiple sensors filter through Attack Analytics

IMPERVA APPLICATION SECURITY

Cloud WAF is a key component of Imperva Application Security, which reduces risk while providing an optimal user experience. The solution safeguards applications on-premises and in the cloud by:

Providing actionable security insights

Providing WAF protection

Protecting against

DDoS attacks

Mitigating botnet attacks

Blocking cyber-attacks that target APIs

Enabling RASP protection

Ensuring optimal content delivery

Learn more about Imperva Application Security at +1.866.926.4678 or online at imperva.com

Imperva is an analyst-recognized, **cybersecurity leader** championing the fight to **secure data and applications** wherever they reside.