DATASHEET

Attack Analytics

Uncover attacks hiding in a sea of security alerts

KEY CAPABILITIES

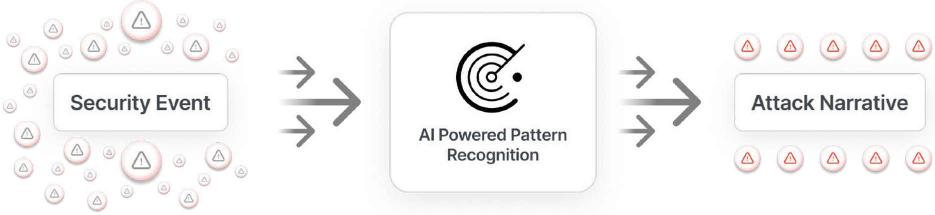
- Correlates and distills thousands of security events into actionable insights
- Displays security events and incidents in an easy-to-understand format
- Unified monitoring of cloud and on-premise WAF
- Collective intelligence from global customer base

Security teams are overwhelmed with the volume and sophistication of emerging threats and attacks. Ideally, they want to receive actionable alerts that provide the entire narrative when a threat is seen. Instead, SOCs are overwhelmed by thousands of vague, unprioritized security events, making it almost impossible to know which alerts are connected and require prioritization. This situation only worsens as applications are moved to the cloud, presenting new security challenges related to cloud-specific or hybrid environments. The need for enterprise-wide visibility has never been greater.

Organizations are looking to increase efficiency while minimizing alert fatigue among security teams. It's imperative to optimize the SOC by prioritizing alerts, reducing time to remediation, and decreasing time spent investigating false positives. This requires a smart analytics tool that can present security events in a meaningful, easy-to-understand way for security teams to be able to act upon immediately. Built-in artificial intelligence would enable SOCs to process large volumes of data almost instantaneously to uncover trends and correlations that are invisible to the naked eye. Such a tool would be invaluable in highlighting, prioritizing, and providing detail on true positive security events from the daily barrage of security alerts.

Imperva's Attack Analytics

Imperva Attack Analytics correlates and distills thousands of security events into a few distinct readable narratives. Imperva machine learning algorithms at every layer in our single stack solution process incoming events to find correlations between them. Events are sorted and grouped into easy-to-understand incidents with context that is prioritized accordingly, taking the mystery out of investigations. Security teams can respond to threats quickly and decisively; they immediately understand an attack and know which incidents require immediate attention. This cloud-based tool has unlimited scaling potential and is already integrated into the Imperva platform.



Optimize security teams

Simplified attack narrative

Vague alerts often provide enough information to start an investigation but lack the necessary detail to promptly and confidently respond. Attack Analytics presents both incidents and security events understandably, minimizing the time an analyst spends determining the scope and severity of an attack. Security events are displayed in easy-to-understand dashboards that highlight the top attack origins, attack tool types, attacked resources, attack timeline, and policy violations. These dashboards can easily be drilled down for more information on specific attack details. Security events are grouped into incidents. Each incident is displayed as a simple narrative: analysts are presented with the type of attack, attack origin, attacker IP reputation, timeframe, tools that were utilized, and any related CVEs. The SOC can get everything they need from a single dashboard or incident.

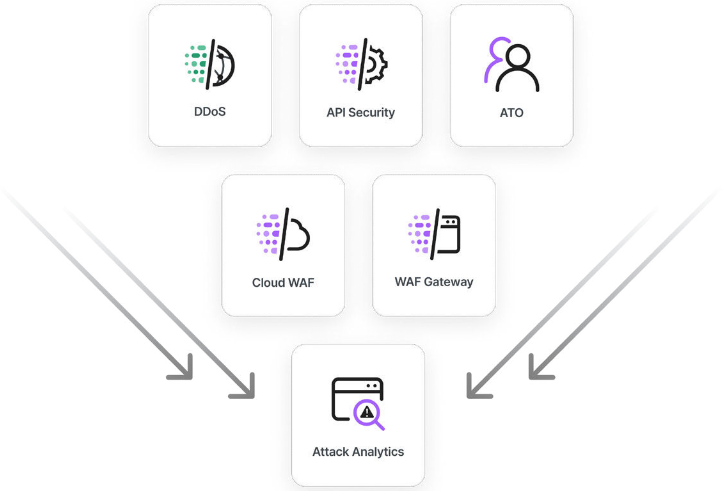
Unified visibility

As more companies migrate to the cloud, it's increasingly difficult to monitor security events enterprise-wide. Attack Analytics provides a unified view to monitoring all security events gathered by Imperva cloud-based and on-prem WAF solutions. This provides organizations with complete visibility across the Imperva platform, simplifying identifying enterprise-wide attack campaigns.

Visibility and integration support with other Imperva solutions include API Security, Account Takeover, DDoS, Cloud WAF, Reputation Intelligence, and WAF Gateway.

Global insights

Helping organizations stay up to date on the latest threats, Attack Analytics analyzes customer data from around the world to identify emerging attack patterns. Rather than having analysts hunt through logs to determine if an organization has been hit with a new attack, this collective intelligence highlights the new attack trends in an environment. When triaging an incident, organizations can see how common this attack is among all Imperva customers. Security teams are informed of what threats they're currently facing and can quickly respond, keeping them proactive.



KEY CAPABILITIES

Cloud WAAP is a key solution of Imperva Application Security, which protects web applicationS and APIs while reducing risk and providing an optimal user experience. The solution safeguards applications in the cloud by:

- Providing actionable security Insights with Attack Analytics
- Providing WAF protection
- Protecting against DDoS attacks
- Mitigating botnet attacks
- Blocking cyber-attacks that target APIs
- Ensuring optimal content delivery
- Providing Account Takeover protection

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.