FireEye

Datasheet

Threat Analytics Platform

Identifies Threats and Improves Response With Real-Time Threat Intelligence

Highlights

- Identifies threats and accelerates response by layering real-time FireEye threat intelligence over enterprise event streams
- Requires no investment in infrastructure
- Provides a cohesive threat response plan by leveraging events from existing enterprise security infrastructure
- Raises the visibility of the threat landscape by providing rich insights into threat actor profiles
- Manages incidents to improve efficiencies in assigning, tracking, and resolving events with on-demand portal access
- Offers a strategic service portfolio tailor-made to fit the needs of your organization

The FireEye® Threat Analytics Platform (TAP) is a cloud-based solution that enables security teams to identify and effectively respond to cyber threats by layering enterprise-generated event data with real-time threat intelligence from FireEye.

Most security-conscious organizations spend significant resources amassing log and event data to satisfy regulatory and compliance requirements. However, when it comes to analysis and responding to advanced attacks few are able to derive value from these data troves. The FireEye Threat Analytics Platform enables security teams to respond more effectively to threats by combining traditional system-based event data with FireEye threat intelligence.

Real-time threat intelligence to identity threats

The FireEye Threat Analytics Platform applies the largest and most comprehensive source of real-time threat intelligence on the event streams generated from enterprise systems to identify threats who evade traditional security solutions. Security teams get the information they need, when they need it to rapidly investigate and provide effective response.

Raises the level of threat visibility

The FireEye Threat Analytics Platform increases the overall visibility into the threat landscape by leveraging FireEye Threat Prevention Platforms' rich insights into threat actor profiles and behavior.

Prioritized alerts to enhance incident response

The FireEye Threat Analytics Platform delivers prioritized alerts to help accelerate and enhance incident response. The platform quickly determines the scope of a suspected incident so that security teams can respond appropriately. It provides the ability to pivot into any field within an alert to identify related users, endpoints, and attacker infrastructure.

Low cost of ownership

The cloud-based solution requires no investment in infrastructure and can be set-up in existing environments within hours. The costs are proportional to the volume of data analyzed with no hidden costs for more devices or collectors.

Streamlined incident management

The platform streamlines the management and prioritization of incidents by assigning, tracking, and measuring the efficiency in how tasks are resolved. Incident responders can attach newly discovered data to existing incidents, add comments, indicate which assets are involved, and search data related to the incident.

Aggregates event data for incident response

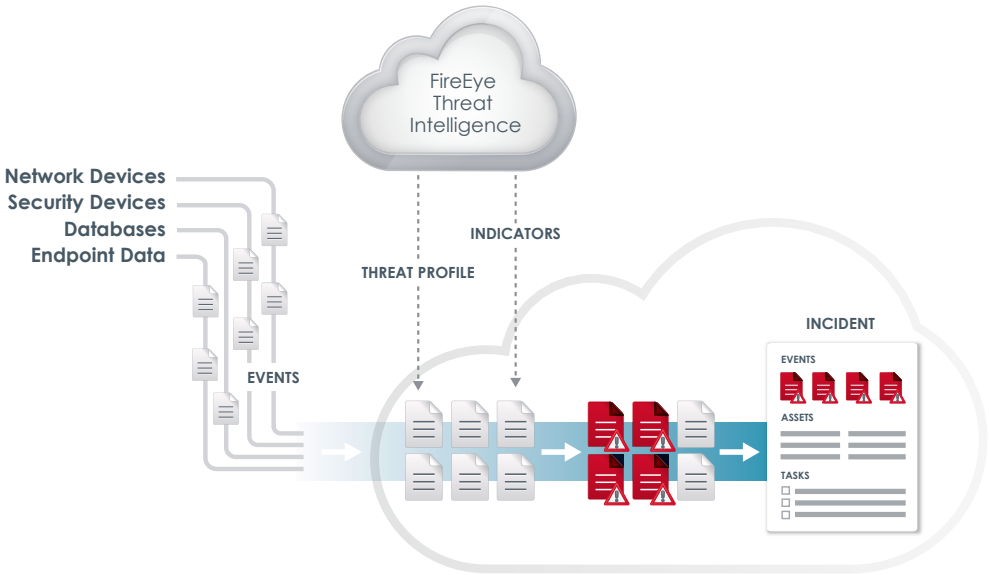
The platform is designed to scale by keeping as much data online and searchable as business needs demand. Search results can be exported from the user interface for use in other incident response management tools as needed.

Faster analysis to determine scope of the threat

The FireEye Threat Analytics Platform enables you to quickly search through billions of events, typically within seconds, and correlates event logs with FireEye threat intelligence to discover the presence and impact of threat. In addition, the TimeWrinkle™ capability shows you what occurred immediately before and after an event.

Tailored strategic service portfolio

Customized service offerings are available for the FireEye Threat Analytics Platform. Mandiant security operations consulting services and foundation services are available. In addition the Threat Analytics Platform jumpstart service is available to quickly accelerate the implementation and integration of the Threat Analytics Platform with customer existing security operations.



FireEye
Threat Analytics Platform