FireEye
SECURITY REIMAGINED

Threat Analytics Platform™

Security in the Cloud to Help Ensure Security of the Cloud

SOLUTIONS BRIEF

SECURITY REIMAGINED

HIGHLIGHTS

- Identify threats and accelerate response by layering realtime FireEye intelligence over enterprise event streams
- Cloud-based solution requiring no infrastructure investment
- Rapid deployment in hours instead of months
- Deliver rich insight into threat actor profiles to provide context to threats targetting your organization
- Quickly search through billions of events with sub-second response
- Extensive signature sets curated by FireEye in response to emerging threats
- Integrate custom and/or legacy threat intelligence sources
- Ability to integrate custom intel and/or legacy threat intelligence
- Every customer deployed to a dedicated VPC to avoid data mingling

FireEye's Threat Analytics Platform (TAP) helps detect malicious activity in AWS environments by providing increased simplicity, accessibility, and actionability.

amazon web services | Partner Network
ADVANCED TECHNOLOGY PARTNER

HOW FIREEYE'S THREAT ANALYTICS PLATFORM MONITORS AWS

FireEye's Threat Analytics Platform (TAP™) helps detect malicious activity in AWS environments by providing increased simplicity, accessibility, and actionability to the data and information provided by Amazon's cloud. TAP helps achieves these objectives by harnessing the data from an AWS cloud environment and the detection capabilities prebuilt in the platform.

Simplicity

- Move naturally from alerting to searching to rule creation to incident response
- Easy onboarding of new log sources

Accessibility

- Flexible deployment models to suit virtually any cloud-based or hybrid-cloud infrastructure
- Provides a "single pane of glass" for monitoring cloud activity as well as traditional datacenter logs

Actionability

- Prebuilt rule packs, including one specificially for cloud, and custom rule capabilities
- Alerting and incident response (IR) workflow

SAMPLE USE CASE

Company A works heavily with third party vendors and needs to to quickly determine the actions taken by each vendor.

To meet compliance requirements, Company A needs to maintain records of all actions taken by third party vendors inside of their AWS environment. The third party vendors use cross-account roles to perform various business related tasks. By leveraging TAP, the customer is able to quickly determine what actions are being taken by which vendors. The customer can then create rules to alert on any attempts made to exceed allowed permissions via an assumed role or access AWS from an unauthorized location.

FILLING IN THE VISIBILITY GAP

Amazon Web Services (AWS) has modified the traditional log delivery pattern and instead delivers scheduled batches to locations that ultimately require a pull request of the data in order to make it usable. Due to this pattern change, and the difficulties associated with it, many companies have neglected to collect these logs. Companies lose crucial visibility into their AWS environment, an environment where a malicious actor can steal or destroy everything in a matter of seconds.

FireEye's Threat Analytics Platform (TAP) helps solves this problem, providing a secure manner for log ingestion, where nearly sixty pre-built rules can monitor and alert based on malicious activities or misconfiguration that could provide an opportunity for a malicious actor to gain access to an account.

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | www.fireeye.com

FireEye