FireEye
SECURITY REIMAGINED

FireEye Threat Analytics Platform (TAP)™ and Varonis

User Behavior Analytics (UBA) Deliver Unprecedented Insight Into Security of Unstructured Data

SOLUTION BRIEF

SECURITY REIMAGINED

INTEGRATED SOLUTION HIGHLIGHTS

These two solutions together provide the alerts that matter, the context to understand attackers, and a tool to track the event to remediation.

- Provides user behavior analytics and visualizations that help customers see anomalies in their environment.
- Utilizes over 1,300 rules developed from the front lines of Mandiant incident response work and FireEye hunt teams.
- Provides context on alerts to help customers understand their attacker.
- Guides workflows that allow customers to monitor an event from identification to remediation.

OVERVIEW

Organizations store massive quantities of unstructured, human-generated data such as files, emails, spreadsheets, and presentations. This data comprises some of their most valuable and sensitive information assets. These assets are frequently exposed or stolen in high-profile breaches, either by insiders who abuse their access or by outsiders who compromise insiders' credentials.

THE CHALLENGE

Because hackers are getting better at their jobs, today's threat intelligence equation needs to combine several technologies in response. With the new interoperability between FireEye Threat Analytics Platform (TAP) and Varonis DatAdvantage and DatAlert, customers can combine critical security insight from FireEye with Varonis intelligence about their unstructured data. Customers typically have the highest quantity and least knowledge about this kind of data.

THE INTEGRATED SOLUTION

Together, the joint solution can help customers protect their unstructured data, through analyzing user behavior with files and emails, permissions and file system metadata, as well as file content.

Varonis and FireEye Threat Analytics Platform (TAP) can help organizations proactively spot the warning signs before they experience an impactful and costly data breach.

Joint customers are now able to send alerts quickly from Varonis DatAdvantage and DatAlert into FireEye Threat Analytics Platform (TAP) to identify statistically unusual user behavior surrounding this data. Installation of Varonis DatAdvantage and DatAlert can take as little as one hour. The connection to FireEye Threat Analytics Platform (TAP) is as simple as configuring an IP address.

HOW THE JOINT SOLUTION WORKS TOGETHER

Varonis DatAdvantage collects metadata of activity related to all specified files. This metadata is shared with the Varonis DatAlert solution to identify suspicious behavior using advanced user behavior analytics (UBA).

This metadata and any resulting alerts are sent into FireEye Threat Analytics Platform (TAP) to identify statistically unusual user behavior surrounding this data. The anomalous activity could include mass deletions and modifications, malware and ransomware infections like CryptoLocker and Cryptowall, privilege escalations, unusual access to PII, multiple failed login attempts, and many more potential warning signs.

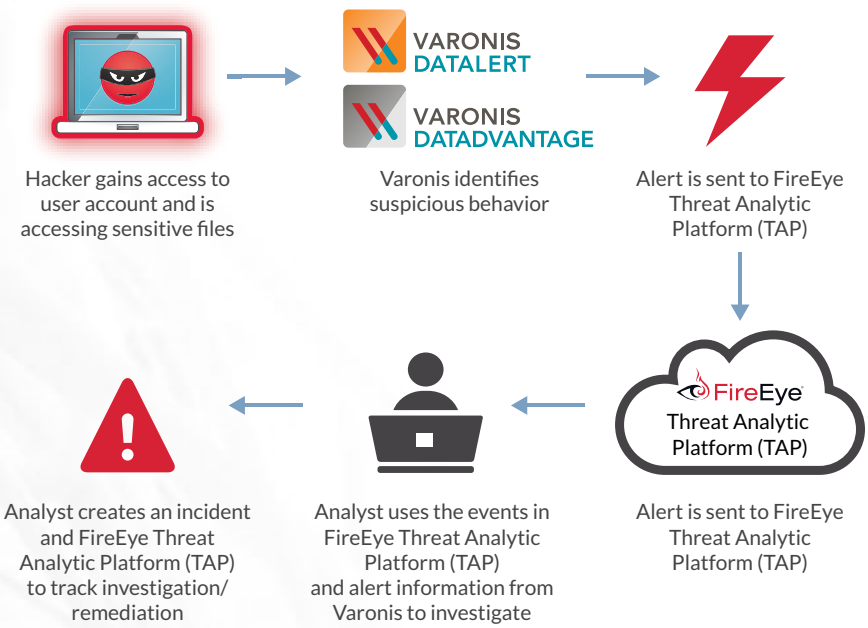
VARONIS

FIREEYE PRODUCT AND VERSION

FireEye Threat Analytics Platform (TAP)

VARONIS PRODUCT AND VERSION

DatAdvantage and DatAlert



FireEye Threat Analytics Platform (TAP) applies advanced threat intelligence to the metadata and additional analysis of the DatAlerts. Use of FireEye Threat Analytics Platform (TAP) accelerates the detection and investigation of cyber-attacks by correlating events from a broad range of devices and locations. It also applies threat intelligence to pinpoint critical threats, including the hunt for threat indicators within unstructured data sources.

This threat information and specifics about the threat move to the incident responder for remediation.

THE VALUE OF THIS PARTNERSHIP

With the interoperability of Varonis DatAdvantage, DatAlert, and FireEye Threat Analytics Platform (TAP), customers can gain unprecedented intelligence in the realm of unstructured data. FireEye Threat Analytics Platform (TAP) enables faster identification of attacks on or threats to all forms of data files containing valuable customer information. The advanced security intelligence information provided by FireEye Threat Analytics Platform (TAP) analyzes threats in the broader context of comprehensive threat intelligence. By integrating FireEye to identify anomalous data activity, Varonis provides its customers with valuable insight into the security of their high-value information.

ABOUT FIREEYE

FireEye protects the most valuable assets in the world from today's cyber attackers. Our combination of technology, intelligence, and expertise — reinforced with an aggressive incident response team — helps eliminate the impact of breaches. FireEye has over 4,000 customers across 67 countries, including more than 650 of the Forbes Global 2000.

ABOUT VARONIS

Varonis is the leading provider of software solutions for unstructured enterprise data. Varonis provides an innovative software platform that allows enterprises to map, analyze, manage, and migrate their unstructured data. Varonis specializes in human-generated data, a type of unstructured data that includes an enterprise's spreadsheets, word processing documents, presentations, audio files, video files, emails, text messages, and any other data created by employees. Varonis has over 3,750 customers, spanning leading firms in the financial services, public, healthcare, industrial, energy & utilities, technology, consumer and retail, education, and media & entertainment sectors.

For more information contact CSC@fireeye.com.

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