VARONIS + FIREEYE TAP

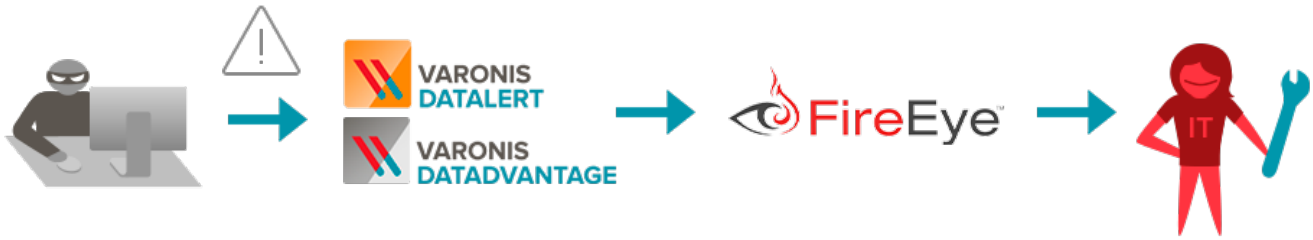
Organizations store massive quantities of unstructured data – files, and emails – comprising some of their most valuable information assets. Unfortunately, these assets are frequently stolen in high-profile breaches, either by insiders who abuse their access (like Snowden), or by outsiders who compromise insiders' credentials (like Sony).

As organizations face an ever-changing technology and threat landscape, they realize that it is no longer realistic to count solely on their perimeter defenses to keep attackers out. Compounding the risk, users already within their walls have access to far more information than they require to do their jobs. Worse still, organizations rarely know they have been compromised until months later, if at all, because users' behavior on many internal systems is rarely monitored or analyzed for abuse.

Varonis has helped thousands of customers protect their unstructured data through analyzing user activity files and emails, permissions and file system metadata, as well as file content. In a recent, informal email survey, of 141 Varonis customers that responded, 31% reported that they had already detected suspicious insider activity or malware with our solutions.

FireEye customers bring together threat intelligence from many sources, including IDS/IPS, DLP, business applications, and firewall logs.

With the integration of Varonis and FireEye TAP, FireEye and Varonis customers gain unprecedented intelligence in the realm of unstructured data – what they typically have the most of and know the least about. From initial reconnaissance through data exfiltration and attack obfuscation, Varonis and FireEye TAP help you spot the warning signs before you end up in the news.



IMMEDIATE DETECTION CAPABILITIES

Easily integrate Varonis DatAdvantage and DatAlert with FireEye TAP, and identify:

- Statistically unusual user behavior
- Mass deletions and modifications
- Malware and Ransomware infections like Cryptolocker and Cryptowall
- Privilege escalations
- Administrative access to user data
- Unusual or administrative access to PII
- Multiple failed login attempts
- Changes made outside of change control windows
- Many more

Installation of Varonis DatAdvantage and DatAlert can take as little as an hour, and integration with FireEye TAP is as simple as configuring an IP address.

ABOUT DATADVANTAGE

Varonis DatAdvantage ensures that only the right people have access to the right data at all times, monitors all activity, and flags abuse.

Varonis secures your data from the inside-out, using machine learning to find patterns and anomalous behavior to stop breaches before they happen.

ABOUT DATALERT

Varonis DatAlert triggers real-time alerts across multiple platforms based on file and email activity, permissions changes, and other critical events - helping you detect potential security breaches, misconfigurations, and other issues in real-time.

ABOUT FIREEYE

FireEye is a leader in providing cyber security solutions, protecting the most valuable assets in the world from those who threaten them. Our combination of technology, intelligence and expertise—reinforced with the most aggressive incident response team—helps eliminate the impact of security breaches.