SOLUTION BRIEF

Comprehensive Insider Threat Detection and Protection

A joint solution from innerActiv and FireEye

HIGHLIGHTS

- **Protect from within**
  Gain valuable risk analytics and protection against internal threats.
- **Detect advanced threats**
  Integrate over 300 FireEye and non-FireEye security tools and overlay contextual threat intelligence, and behavioral analytics to deliver unparalleled situational awareness.
- **Gain visibility**
  Whether on premise or in the cloud, centralize monitoring and security data with next generation analytics for complete visibility into threats and vulnerabilities.

70% of IT professionals say insider attacks have become more frequent in the past 12 months.[1]

And the average annual cost of all insider threats was 8.7 million dollars.[1] The challenges surrounding security, compliance and data loss continue to grow alongside the increased mobility of both your employees and your data. It doesn't help that many monitoring solutions are limited in scope and require extensive manpower to configure and maintain.

Organizations should be able to proactively address risky workflow practices from both on and offsite employees while enforcing critical security policies.

Together, innerActiv and FireEye combine critical insights into data loss risks from insiders, employee misuse of data and external cyber threats to support:

- **Insider threat management.** Protect your organization's reputation and assets from malicious or accidental insiders, a primary contributor to 69% of breaches at organizations with traditional security in place[1]
- **Simplified HR investigations.** Quickly conduct accurate, objective and forensically sound investigations
- **Data protection.** Track and monitor when employees view, handle or remove sensitive data
- **User activity and behavioral analysis.** Understand how, when and why users interact with sensitive assets, and how those interactions affect your risk

innerActiv is a one-of-a-kind endpoint and behavioral monitoring software platform that helps to secure organizations' most valuable assets by continuously monitoring endpoints, alerting on suspect endpoint activity and providing the option to block critical data loss threats. When innerActiv is combined with the FireEye Helix security operations platform, this critical data set can be combined with data and alerts from over 300 other tools to create a customized and complete view of your organization's security.

[1] Code42 Software (2019). 2019 Data Exposure Report.

Integration Overview

FireEye Helix detects security incidents by consolidating and correlating all incoming data from multiple tools and appliances, and offers additional details when combined with FireEye contextual threat intelligence. The robust data set offered by innerActiv encompasses four main areas: data loss prevention, identity-based events, activity statistics, and infrastructure management. When this data is ingested into Helix, security analysts can get continuous real-time alerts when unusual or dangers behaviors put their organization's users or data at risk. A custom innerActiv parser for Helix, rule-pack and dashboards make this integration turnkey for joint customers.

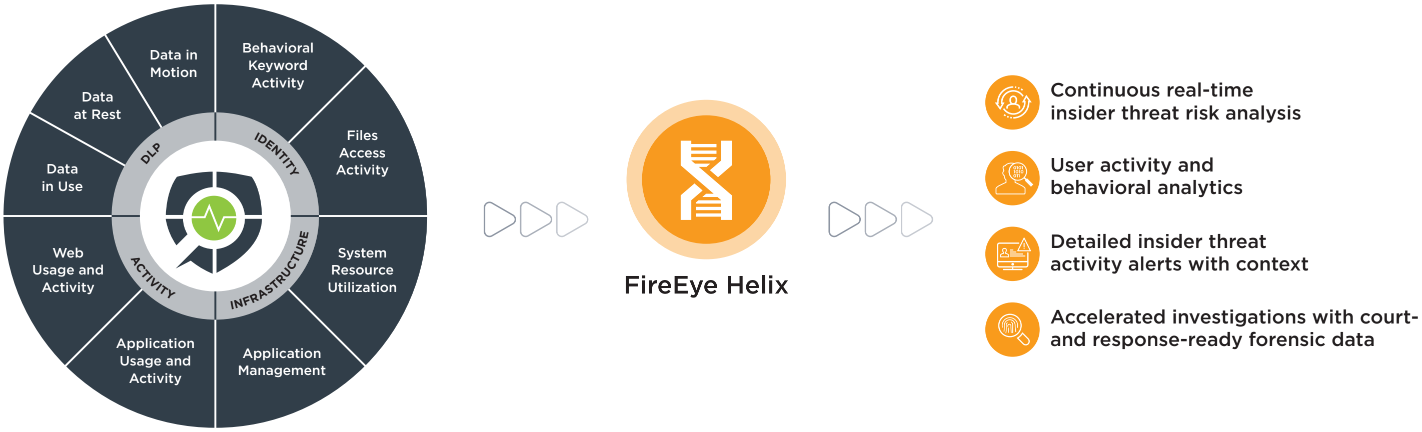
Data in Motion
Behavioral Keyword Activity
Data at Rest
Files Access Activity
Data in Use
DLP
IDENTITY
INFRASTRUCTURE
ACTIVITY
Web Usage and Activity
System Resource Utilization
Application Usage and Activity
Application Management
FireEye Helix
Continuous real-time insider threat risk analysis
User activity and behavioral analytics
Detailed insider threat activity alerts with context
Accelerated investigations with court- and response-ready forensic data

Figure 1. Interactions and outcomes resulting from the partnership between innerActiv and FireEye.

Malicious insider incidents are likely to become an increasing trend given that they involve trusted access, high impact and low cost to execute, combined with organizational cultures with open trust models.[2]

[2] FireEye (2019). M-Trends 2020.

innerActiv

OnGuard Systems, developer of innerActiv, was founded with the primary goal of protecting organizations' endpoints against the rising risk of insider threat and accidental data leakage. The company has expanded to include a robust DLP tool, one-of-a-kind productivity analysis tools, infrastructure monitoring module, and identity monitoring tools, all operating on a low-profile endpoint client. Additional features and components of innerActiv are continually being developed in order to create the most comprehensive and user-friendly endpoint protection software available.

To learn more about FireEye, visit: **www.FireEye.com**
For questions or more information about this integration, contact: **integrate@FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About FireEye, Inc.
FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.

FIREEYE™