FireEye and FairWarning®

Coordinated Threat and Protection Response

SOLUTION BRIEF

INTEGRATED SOLUTION HIGHLIGHTS

When deployed on the same network and integrated, the FireEye and FairWarning joint solution delivers some very specific benefits:

- **Provides a holistic, end-to-end view of health application events within a customer's organization.**
- **Proactively monitors known threats to healthcare organizations.**
- **Detects APTs earlier through the use of proven statistical trend analysis.**
- **Supports lateral investigation of suspected incidents.**
- **Applies intuition and expertise to Electronic Health Records (EHRs) and cloud-based applications through powerful discovery tools.**
- **Responds quickly and efficiently to incidents.**
- **Empowers contextual and efficient decisions for coordinated threat prevention and response.**

OVERVIEW

Advanced Persistent Threats against healthcare organizations are on the rise. These new threats require a holistic view of healthcare organizations to protect against internal and external security breaches. Deploying multiple technologies is required to achieve the defensive depth necessary to prevent data breaches and detect unauthorized access to protected health information. By combining forces, FairWarning and FireEye can better prepare healthcare organizations to deal with the most common threats facing them today.

THE CHALLENGE

Healthcare organizations face a series of challenges as a wide variety of bad actors attempt to compromise and profit from protected health information. Among these challenges are:

- Identity and medical identity theft.
- Sale of patient, employee, and physician data to crime rings.
- Data theft for IRS tax fraud.
- Nation state espionage – state-sponsored attempts to gain access to medical information for blackmail purposes.
- Insider trading – attempts to gain access to information such as investments in research, FDA authorizations, and construction on new research or production facilities.
- Denial of service attacks.

THE INTEGRATED SOLUTION

The FairWarning Patient Privacy Monitoring Platform provides monitoring for over 300 clinical applications. Through FairWarning, security teams can analyze user activities within these applications to identify suspicious activities. Once a suspicious activity is identified, it sends correlation with other infrastructure events to the FireEye Threat Analytics Platform (TAP). FireEye TAP can add context to the malicious event within the application and identify potentially malicious user behaviors.

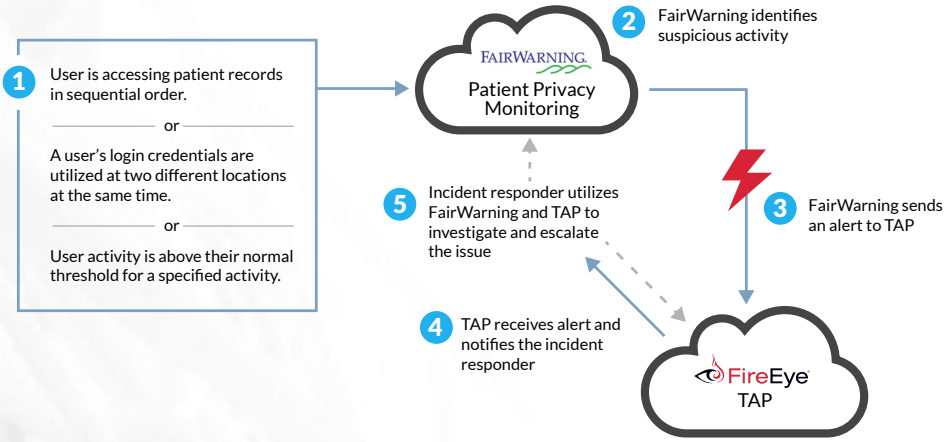
FIREEYE PRODUCT AND VERSION

FireEye Threat Analysis Platform (TAP) 12.0 and later versions

FAIRWARNING PRODUCT AND VERSION

FairWarning Patient Privacy Monitoring Platform

Threats and Joint Solution Response



HOW THE JOINT SOLUTION WORKS TOGETHER

The FairWarning Patient Privacy Monitoring Platform continuously monitors the clinical applications in use by a customer. If an aberration in user behavior is detected, the FairWarning platform will alert FireEye TAP with the detected event information. Examples of aberrant behavior are (1) a user accesses patient records in sequential order (2) a user's login credentials are utilized at different locations at the same time (3) user activity is above the normal threshold for a specified activity. When detected, the FairWarning platform will also alert the incident responder or security analyst and support performance of a lateral forensic investigation on this user. The FireEye TAP can correlate the activities discovered in FairWarning with infrastructure events and help determine whether this user has compromised credentials and determine the scope of the threat. The FireEye TAP enables customers to search quickly through billions of events and correlate event logs. This process allows the analyst to see what happened immediately before and after the event. The combined solution provides end-to-end protection and a quicker and more efficient incident response when faced with a threat, either internally or externally.

THE VALUE OF THIS PARTNERSHIP

The FairWarning and FireEye solution creates a world-class threat prevention and response framework. Our integration allows customers to analyze quickly and respond to both internal and external threats to the organization for better protection and prevention of patient privacy breaches. Together we deliver the best solution for the protection of patient healthcare information and identification and remediation of internal and external compromises of clinical applications and electronic healthcare records.

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. The FireEye Global Defense Community includes 3,700 customers across 67 countries, including 675 of the Forbes Global 2000.

ABOUT FAIRWARNING

FairWarning's solutions are broadly adopted across the healthcare market. This adoption means that patients can share their most sensitive medical information more confidently and enable the best care possible without worrying about who might access their sensitive medical details. Over 1,500 hospitals and 7,400 total medical facilities around the world use FairWarning Patient Privacy Monitoring and Managed Privacy Services to expand trust with their patients.

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**