FireEye and Huntsman® Security

Resolves Cyber Attacks in Seconds – Slashes the Time Between Detection and Response

SOLUTION BRIEF

SECURITY
REIMAGINED

INTEGRATED SOLUTION HIGHLIGHTS

- Real-time actionable intelligence through merging internal and external threat information to deliver the context and certainty about any threat.

- Automated incident management and evidential records that provide highly advanced business intelligence and unparalleled reporting options.

- A deep and seamless technology integration that delivers multi-dimensional analysis that yields highly accurate alerts to a single screen.

- Integrating threat detection and response efforts into a forensically reliable incident management and reporting system.

- Shortens the time from threat detection to resolution from months to seconds.

- Automates the collection of contextual information relating to a threat.

- Maintains data integrity and evidential validation across the enterprise.

- Delivers precise security information to operations, management, and audit stakeholders.

OVERVIEW

Whether in a single or multi-tenant environment, it is a challenge to pinpoint security breaches, prevent data loss, and minimize reputational damage. Real-time power of a joint solution where neither element limits the speed or performance of the outcome is significant. The assurance of data sovereignty and an evidential chain of custody are similarly important. The FireEye and Huntsman Analyst Portal™ joint solution meets these objectives to deliver threat resolution in seconds.

THE CHALLENGE

For every organization, it is critical to detect events quickly, understand them, quarantine systems, limit wider infiltration and infection, and prevent data loss. However, many organizations have a response window that can typically extend out to months and leave the enterprise unacceptably exposed.

The longer you take to detect and diagnose an attack — whether it is insider misuse, privilege escalation, external intrusions or data theft — the greater the risk of financial and reputational loss.

Some advanced cyber threat detection technologies like malware sandbox detection systems are extremely powerful but in practice; they generate both true and false positives. These alerts mean security specialists can end up spending too much time addressing benign attacks, rather than focusing on the threats that matter.

The challenge is to improve detection and reduce response time, and the key to delivering this is to enhance the productivity of the security analysts.

THE INTEGRATED SOLUTION

Huntsman Analyst Portal monitors and correlates system activity from across the enterprise in real-time. Using an autonomous decision engine, Huntsman instantly determines breaches of policy and captures trusted evidence of all related events. It's unique artificial intelligence engine baselines to detect and validate suspicious outliers or indicators of compromise that are invariably the first sign of attack.

The proven defense-grade Huntsman Analyst Portal and FireEye platforms unify internal, contextual information with externally sourced threat intelligence to validate and triage relevant threats for immediate response. The combined real-time system evidences the incident and then confirms its nature, severity, and impact in seconds.
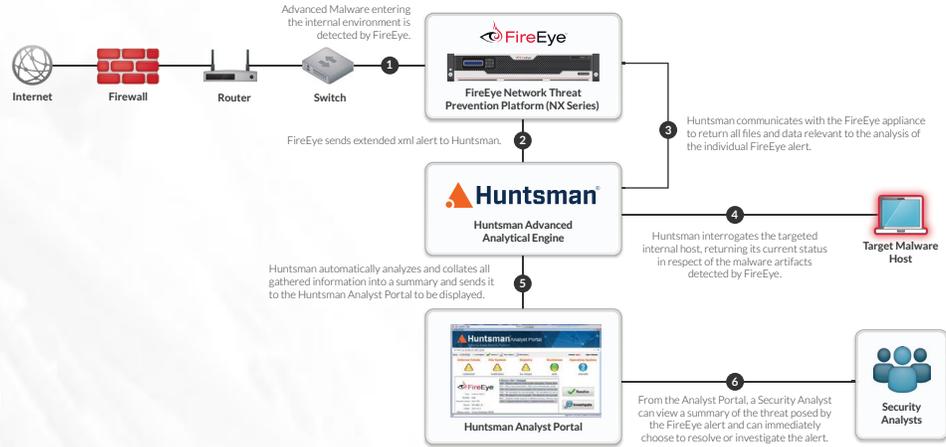
FIREEYE PRODUCT AND VERSION
NX, EX, AX, FX and CM version 7

HUNTSMAN PRODUCT AND VERSION
Huntsman Analyst Portal™

As a result, breaches and potential data loss incidents can be detected and their details retained for remediation. A unique system that assures the integrity of the evidence limits threat management process queuing and maximizes the speed to incident closure. That means, for greater process speed and efficiency, the resources necessary for threat investigation and remediation can be focused only on the risks that matter.

HOW THE JOINT SOLUTION WORKS TOGETHER

FireEye and the Huntsman Analyst Portal™ combine to leverage the best-of-breed capabilities of each solution. The joint solution provides real-time visibility and security management of all devices connected to your network, effective response to APTs, and zero-day threats, and significant levels of automation to efficiently and accurately mitigate threats.

FireEye detects threat activity and prepares an alert that includes comprehensive reporting of the effects the threat will have on the targeted system. Huntsman Analyst Portal™ automatically verifies and resolves the status of the alert in seconds to enable the immediate remediation of the affected system.

High-speed analysis and resolution of FireEye alerts enable the joint solution to deliver massive efficiencies in analyst operations. Turning down the noise for analysts ensures they receive only the key threat information necessary to concisely, accurately and quickly resolve the threat and limit the time at risk.

THE VALUE OF THIS PARTNERSHIP

The FireEye-Huntsman integrated solution provides customers the ability to detect, analyze, and respond in real-time to advanced cyber threats, and then automatically initiate prevention procedures.

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 over 4,000 customers across 67 countries, including more than 650 of the Forbes Global 2000.

ABOUT HUNTSMAN SECURITY

Huntsman Security – whose parent Tier-3 was founded in Sydney, Australia – is a cyber-security pioneer that developed and patented passive machine based behavior anomaly detection (BAD) technology to anticipate and prevent cyber attacks. Huntsman has more than a decade of deployment in mission-critical security environments, national intelligence, border protection, banking and infrastructure. The company offers military-grade protection that proactively detects threats and indicators of compromise in seconds and reduces the time at risk for organizations. Huntsman is deployed in complex, diverse environments across the world, and has offices in North America, Australia, the UK, and Japan.

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**

FireEye