# E8 SECURITY FUSION PLATFORM

The E8 Security Fusion Platform cuts the amount of time it takes to investigate security alerts from hours to minutes.

In spite of all the new prevention technologies deployed at the network perimeter, the data center, on endpoints, etc., breaches still occur at record scale. This is not because IT professionals haven't subscribed to the best prevention technologies, or because security analysts defending organizations from inside the Security Operations Center (SOC) aren't highly skilled – it's because security operations is fundamentally broken.

Before analysts can get started, they're placed into an environment that doesn't allow them to succeed. They either have too much data or not enough of it, and no way to quickly and accurately prioritize alerts or understand which alerts are related. Analysts are responsible for protecting a digital environment that's constantly changing, from cyber attackers who are continually creating new ways of circumventing defenses and controls, leaving analysts at a severe disadvantage.

E8 Security is transforming security operations from a reactive function mired in inefficiencies, to a proactive team of cyber defenders able to detect, hunt, and respond to threats before a successful breach occurs.

## Everything you want to know without having to ask.

The E8 Security Fusion Platform is transforming security operations by automating the learning of user and device behaviors to discover malicious activity unknown to security analysts, resulting in improved alert quality and accelerated investigations to make security operations more proactive. Security operations teams are able to reach conclusions quickly by offloading the data mining, analysis, and correlation process, typically done manually, to the Fusion Platform, which provides them with answers to questions they didn't even know to ask.

## Key Features

### Advanced Threat Detection

Surfaces anomalous and suspicious behaviors that indicate threat activity, including malicious insiders, external attackers, and targeted malicious software.

### Retrospective Analysis

Applies machine learning, threat detection and behavior models to current and historical log data providing insight into past events and their relationship to events happening right now.

### One-click Search and Filter

All your data, including historical data, is instantly available and easily searchable — no special search languages required.

### UI Designed for Security Analysts

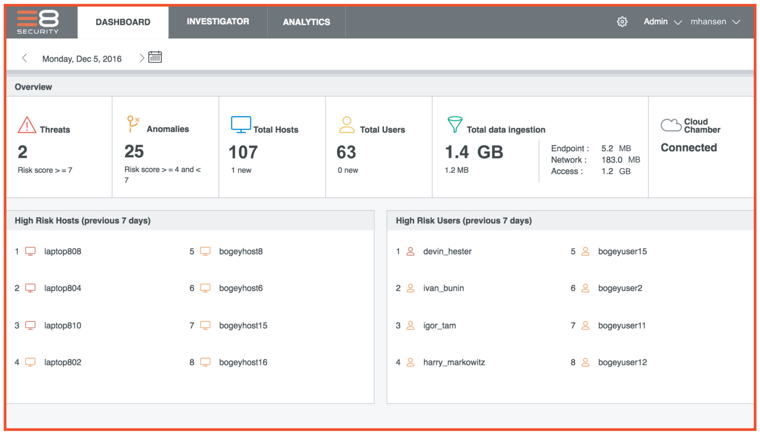
Presents information simply and effectively to guide investigation, save time, and help security teams draw accurate conclusions faster.

### Unsupervised Machine Learning

Learns your network automatically — no rules to create or maintain, or arbitrary thresholds to tweak because of false positives.

### Scalable Big Data Platform

Built on Hadoop infrastructure to easily manage big data from the largest enterprise networks, and integrate into existing data centers.



Monday, Dec 5, 2016

Overview

| Threats | Anomalies | Total Hosts | Total Users | Total data ingestion | Cloud Chamber |
|---|---|---|---|---|---|
| 2 | 25 | 107 | 63 | 1.4 GB | Connected |
| Risk score > = 7 | Risk score > = 4 and < 7 | 1 new | 0 new | 1.2 MB<br>Endpoint : 5.2 MB<br>Network : 183.0 MB<br>Access : 1.2 GB | |

High Risk Hosts (previous 7 days)

| | | | |
|---|---|---|---|
| 1 | laptop808 | 5 | bogeyhost8 |
| 2 | laptop804 | 6 | bogeyhost6 |
| 3 | laptop810 | 7 | bogeyhost15 |
| 4 | laptop802 | 8 | bogeyhost16 |

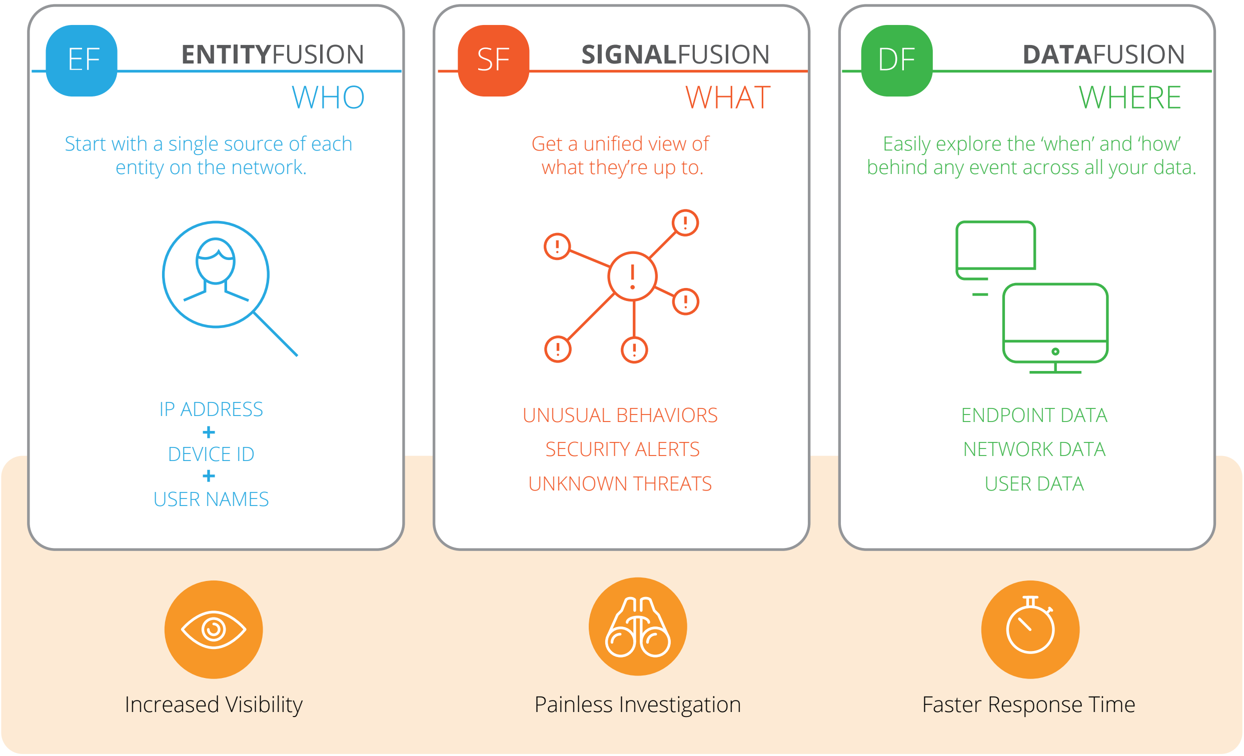
High Risk Users (previous 7 days)

| | | | |
|---|---|---|---|
| 1 | devin_hester | 5 | bogeyuser15 |
| 2 | ivan_bunin | 6 | bogeyuser2 |
| 3 | igor_tam | 7 | bogeyuser11 |
| 4 | harry_markowitz | 8 | bogeyuser12 |

The Fusion Platform is powered by big data and machine learning to identify undetected threats inside the organization at scale as the threat landscape evolves by recognizing the effects a threat has on surrounding resources through unusual behavior patterns. Through the use of advanced analytics, the Fusion Platform gets rid of delayed detection time caused by technology that requires the creation and maintenance of signatures and correlation rules, bringing optimized security intelligence to security operations. By applying self-learning detection models to an organization's security and log data, the Fusion Platform creates baselines for individuals, machines, and user groups, and identifies new, rare, and changed behaviors that indicate hidden threats or risky activity as soon as they happen.

The Fusion Platform provides a focused view of the network, so that analysts can quickly see hidden threats and know where to spend their time, eliminating the long investigative process. In short, E8 helps security teams to detect, hunt, and respond by recognizing what is normal in the network so they can quickly respond to what is not.

## Detect. Hunt. Respond.



EF ENTITYFUSION

WHO

Start with a single source of each entity on the network.

IP ADDRESS
+
DEVICE ID
+
USER NAMES

SF SIGNALFUSION

WHAT

Get a unified view of what they're up to.

UNUSUAL BEHAVIORS
SECURITY ALERTS
UNKNOWN THREATS

DF DATAFUSION

WHERE

Easily explore the 'when' and 'how' behind any event across all your data.

ENDPOINT DATA
NETWORK DATA
USER DATA

Increased Visibility

Painless Investigation

Faster Response Time

## Entity Fusion

### Identifying the “who” behind every alert.

E8’s Fusion Platform brings continuity between usernames, IP addresses and hostnames into a single view. It solves the problem of accurately identifying users who have multiples devices, move between Wi-Fi and wired networks, and change IP addresses throughout their day. In one click, security analysts can see all of a users’ IP addresses, devices and hostnames without exporting data from different systems into a spreadsheet. Behaviors from all security devices are connected by user and hostname without having to create query rules in various systems, providing a single source of “who” behind every event.

## Signal Fusion

### Connecting different events to tell the whole story.

Threat detection isn’t as simple as “threat” or “not a threat,” especially when tactics have never been seen before or seem like legitimate employee activity. For these cases, analysts need to see a series of events — including new, rare, or changed behaviors — before they can decide whether an alert indicates a real threat. The Fusion Platform combines seemingly isolated log entries and alerts from different technologies to show analysts the complete sequence of events, including why a particular action or set of actions was deemed an anomaly or an outright threat.

## Data Fusion

### Improving visibility and exploration across all security data.

All enterprise security data – endpoint, user, and network data – is in one place at your fingertips ready to explore on our platform’s big data infrastructure. Filter and scrutinize log data from multiple sources, seamlessly pivot to interesting data facets, and allow analysts to follow their “threat hunter” intuition without having to switch between different systems or limit their hunting to what they already know. By converging enterprise security data on a Hadoop data lake, E8 Security’s Fusion Platform provides unprecedented visibility into the digital goings-on within an enterprise, so that analysts can easily explore situational information and event details, discover new indicators, and come to conclusions quickly.

E8 Security is transforming security operations by automating the learning of user and device behaviors to discover malicious activity unknown to security analysts, resulting in improved alert quality and accelerated investigations to make security operations more proactive. E8 Security raises the bar, as the first behavioral analytics vendor to make it easier for security teams to quickly identify unknown threat behaviors across endpoints, users and networks. The E8 Security Fusion Platform provides a focused view of the network, so that analysts can quickly see hidden threats and know where to spend their time, reducing the investigation time from hours to minutes. In short, E8 Security helps security teams to detect, hunt, and respond by recognizing what is normal in their network so they can quickly respond to what is not. E8 Security is headquartered in Silicon Valley and is funded by Strategic Cyber Ventures, March Capital Partners, Allegis Capital and The Hive. Find out more at www.e8security.com.

Datasheet Rev 1.0 / January 2017