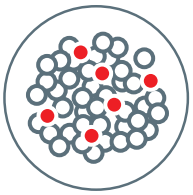
E8 Security Behavioral Intelligence Platform

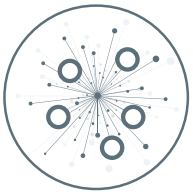
Why Machine-Learning Behavioral Intelligence

E8 Security's behavioral intelligence platform is a self-learning security analytics solution that detects threats hidden in the environment, prioritizes alerts based on risk, and enables security teams to rapidly respond to threats. By combining the scale of big data, the power of behavioral analytics and incorporating human knowledge, E8 Security's solution provides insight into the real risk and nature of security threats within the business environment—closing both insight and action gaps.



Machine-learning analytics solution to identify unknown threats already inside the network

Worldwide, enterprises detect more than 117,000 security incidents every day[1] and the number is rising at a 66% compound annual growth rate (CAGR).[2] Although many security teams are effective at identifying perimeter breaches and patching infected systems and devices, they typically are unable to detect persistent threats hidden in the environment—which have bypassed existing rule-and signature-based systems. In fact, two-thirds of companies[3] don't know they've been breached and are harboring persistent threats until an external source tells them and damage has been done. And by that time, on average, a threat has been present in the system for 229 days.[4]



The insight gap: Too much data

Gartner reports that the data analyzed by enterprise security organizations is doubling every year and that 40% of enterprises will be using data sets of at least 10 terabytes by 2016. That's up from 3% in 2011.[5] This data deluge is effectively burying analysts in a sea of alerts and preventing security teams from finding meaningful insights in the data, creating an "insight gap." This gap is caused by:

- Reliance on manual analytics processes that can't handle big data
- Inability of existing systems to determine what data needs to be analyzed
- Failure of legacy systems to scale and prioritize threats
- Legacy solutions that rely on rules and signatures and can only identify known patterns
- Vulnerabilities created by systems looking at data in siloes versus across the security environment

The action gap: No context

For analysts to progress from insight to effective action and make smart and timely decisions requires prioritization of high-risk threats, context about threats and an understanding of their impact. The methodology used today requires that analysts extract the information they need from multiple systems, users and devices and manually derive context to understand the impact. The volume of threats and the masses of data that need to be analyzed can result in significant delays and erroneous decisions: the "action gap."

E8 Security Behavioral Intelligence Platform

Provides visibility into previously unknown persistent threats —with speed and at scale

E8 Security applies machine-learning and multi-dimensional modeling that examines user and device behaviors to identify anomalous activities. Machine analyses correlate behaviors and relationships, while models track attackers from infiltration to lateral movement to exfiltration. Advanced behavior models expose multiple threat phases such as command and control (C2) communications, lateral movement, credential compromise and establishing persistence. These sophisticated analyses enable machines and humans to optimize their threat identification abilities.

Threats in your environment

Automates threat prioritization based on risk

E8 Security scores threats based on behavioral anomalies and customer-specific contextual information. This provides a risk-prioritized view of security alerts and enables analysts to take action on the most critical ones. Machine-learning algorithms ensure that the system adapts to evolving threats and captures human insight to create a learning loop. As the solution encounters more threats and interacts with security analysts, it becomes smarter, augmenting the intelligence the security team needs to act.

Enables rapid investigation and threat response

E8 Security provides an intuitive user experience to help security teams quickly investigate and validate insights. Analysts can visualize relationships, explore divergent hypotheses and surface hidden patterns. The solution seamlessly integrates with existing security infrastructure, enriching alerts generated by legacy systems. Out-of-the-box integration with leading SIEMs, log management systems, endpoint platforms, web proxy servers and network packet brokers helps customers see value within days of deployment.

Key Features

Data fusion
Identifies user and device behavior and extracts relationships in endpoint, network and access data. Generates rich context and eliminates data siloes by integrating data from legacy systems, internal and third-party sources.

Anomaly and threat detection
Identifies anomalous behaviors and intuitively presents information to guide investigation and exploration of behaviors, threats and anomalies.

Risk scoring and prioritization:
Prioritizes high-risk behaviors and threats so analysts can focus on the most critical ones.

Data exploration
Enables incident response-driven data queries and investigations based on machine- or human-generated context.

Integration
Easily ingests data from any source and enables bi-directional connectivity to feed behavior anomalies, threats and context to the security stack.

Learning loop
Evolves prioritization based on analysts' input, new data and an understanding of the environment.

Scalability:
Easily scales to manage the largest enterprise networks and integrates into existing data centers. Available as an appliance or as software installed on existing off-the-shelf hardware.

[1] The Global State of Information Security® Survey 2015. PwC. Sept. 30, 2014.
[2] Ibid.
[3] Beyond the Breach, 2014 Threat Report. Mandiant. 2014.
[4] Ibid.
[5] MacDonald, N. Information Security Is Becoming a Big Data Analytics Problem. March 2012.

About E8 Security

E8 Security is transforming the effectiveness of enterprise security teams. With scalable machine learning based behavioral analytics platform, E8 Security is empowering security teams to find and prioritize previously unknown threats, provide insight for faster resolution and increase efficacy of the security infrastructure. The company's breakthrough cyber analytics platform transforms burgeoning machine generated security data into actionable intelligence. E8 is headquartered in Silicon Valley and is funded by March Capital Partners, Allegis Capital and The Hive.

E8 SECURITY
100 Marine Parkway, Suite 300 • Redwood City, 94065 • California - +1 (650) 265 7085
www.e8security.com