




# HOW IT WORKS

## Brief



ITD

**personam**  
Always Vigilant. Always Learning.



PERSONAM has developed an advanced new technology that detects threats on a network. We use advanced artificial intelligence to construct behavior profiles for all users and devices and generate alerts when suspicious behavior is identified. Our technology will detect a threat regardless of its origin (external or internal) and regardless of the attack vector (compromised credentials, exploited vulnerability, IoT, etc.). Personam provides security where everyone is most vulnerable – inside the perimeter.

© 2024, All Rights Reserved



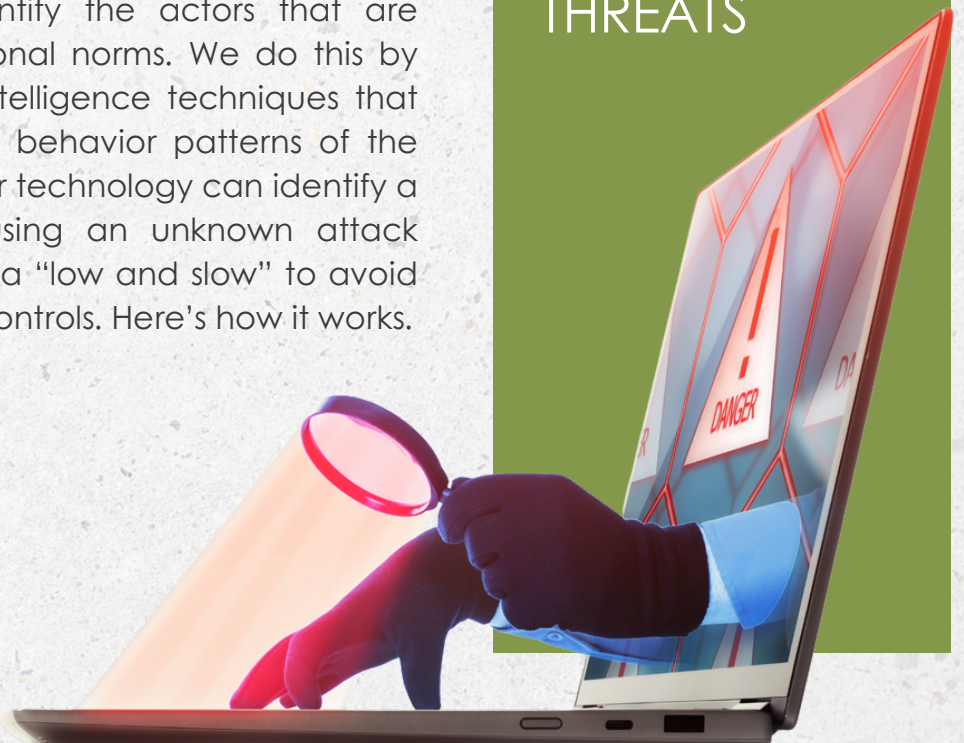
Detecting active threats on a compromised network is an exceptionally difficult task, and very few organizations have been able to accomplish it reliably. Evidence of this is clear from just a few bewildering statistics: it takes, on average, over 200 days for an organization to identify a breach<sup>1</sup>; a whopping 91% of breaches failed to generate an alert<sup>2</sup>; and when breaches are detected, 63% of the time the breached organization did not detect it, but by a third party<sup>3</sup>.

The cause for the failure lies in the approaches used by most cyber products: an over-reliance on rules and signatures. Even the more advanced machine learning methods employed by some products are trained on what to look for, a form of heuristic signature that still leaves them vulnerable to newer threat variants, and zero days are not represented in the training data.

Personam approaches threat detection in an entirely different way. Our models are trained in place on the very network and data it protects. The key to finding a threat is to understand the behaviors of all the actors on a network (users and devices), and identify the actors that are working outside the organizational norms. We do this by applying advanced artificial intelligence techniques that use network data to learn the behavior patterns of the actors and the organization. Our technology can identify a threat even if the actor is using an unknown attack method or is exfiltrating the data “low and slow” to avoid tripping traditional monitoring controls. Here’s how it works.

## SIGNATURE BASED SYSTEMS & ANOMALY DETECTORS DON'T WORK AGAINST KNOWN AND EMERGING THREATS

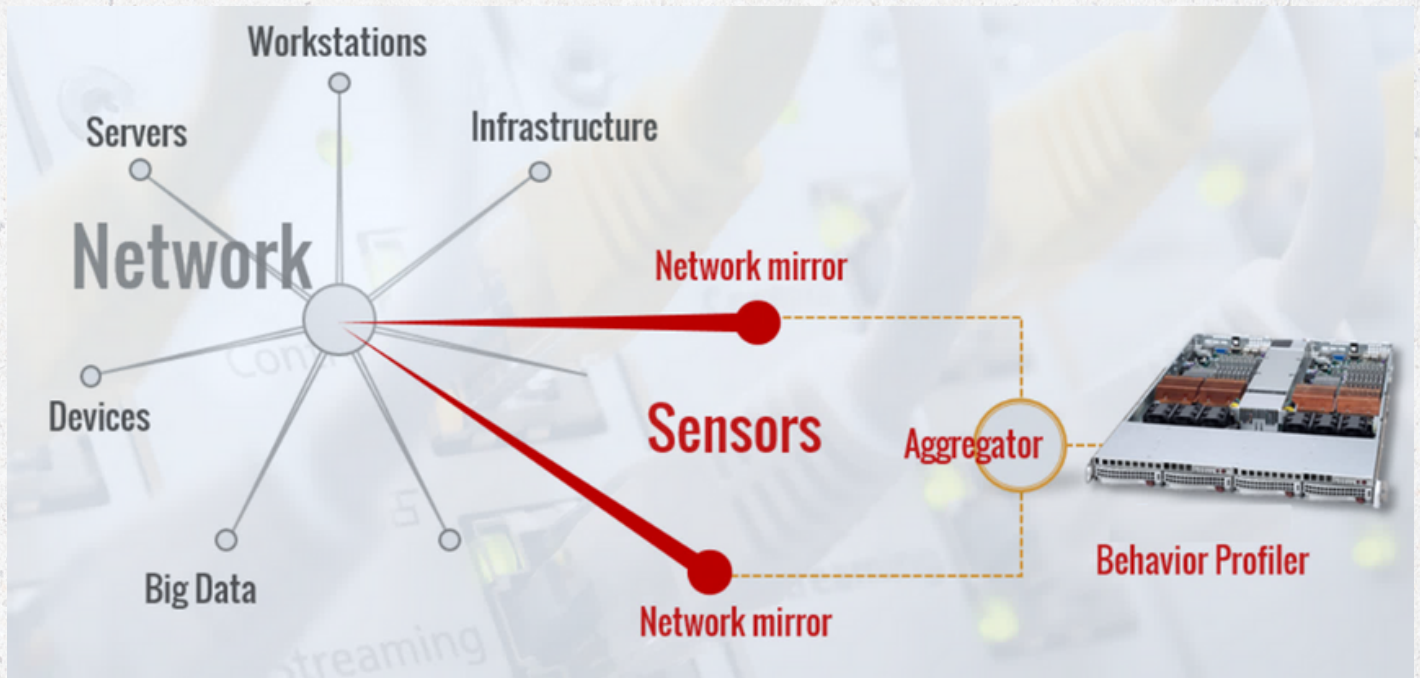
- 
1. Cost of a Data Breach 2023, IBM, [Cost of a data breach 2023 | IBM](#)
  2. Security Effectiveness Report Findings 2020 | [Mandiant Webinar](#)
  3. Top Trends in Cyber Security | [Cyber Attacks Trends | M-Trends \(mandiant.com\)](#)





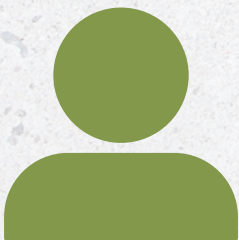
## Network Sensors

Downloadable network Sensor agents are installed at strategic locations on the computer network so that our Detector can observe all data transfers to and from the organization's critical assets, such as the shared file systems, mail servers, CMS applications, and the like. Multiple agents can be installed to cover large or distributed networks.



The Sensor host machines use simple passive Ethernet taps plugged into the ports of a network switch and receive a copy of each data packet transferred through the switch. With the Sensors in place, we have insight into all the critical activity on the network.

The Sensors perform some basic processing steps with each packet: header information is recorded, including source and destination IP addresses, ports, packet size, and others; lookup information is used to identify the user accounts associated with the source of the transmission and IP addresses are resolved to hosts internally or domains externally. Once each session is fully defined, the record is securely forwarded to the behavioral analysis engines running on our cloud-hosted Detector; the contents of the data packet are discarded.



## Behavior Profiles

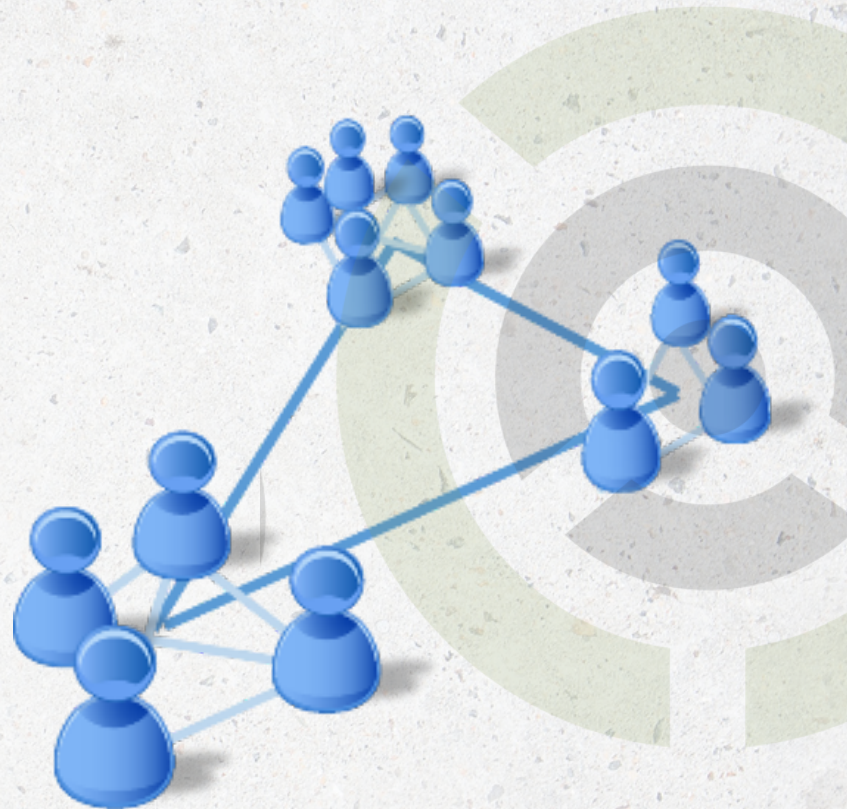
Our advanced algorithms running on the Detector add each data point received from the Sensor agents to the behavior profile of the actor that originated the network activity. This provides us with a rich history of how each actor uses the network.



For a user, we might learn things like which file folders are most frequently accessed, long term and more recently; which websites are preferred; what time of day the user logs into the network or takes a lunch break; and the typical size for transmitted data packets to and from each network resource. For a device: on-prem and cloud-based resources used for backups, API calls made to other servers, etc. We can also label each activity an actor performs as part of either a routine or something more anomalous. And because actors on a network can generate a large number of anomalies, we can also characterize the type and number of anomalies the actor will typically generate in a given timeframe.

## Cohorts

With comprehensive behavior profiles, we can measure the distance of “behavioral similarity” between any two actors (users and devices). The Detector performs this function continuously between each actor and every other actor on the network, placing those with the most similar behaviors together into cohort groups. Our behavior profiles and clustering algorithms for this feature are so effective that the resulting hierarchical diagram will generate a close match to the organization's org chart without any additional input data.



Defining the cohort groups provides additional insight into how the behavior patterns are distributed throughout the organization. This, in turn, gives us an additional perspective to identify outlying and suspicious behavior on the network.

## Identifying Threats

Our system will identify an active threat operating on the network in two powerful ways. The first is through self-consistency monitoring: if the current activity of an actor diverges from its historical baseline, there is a significant risk that either the actor has been compromised or that the actor has begun working counter to their previous efforts. We call this an “Out of Character” behavior. The second method works by comparing the full behavior profile of an actor to the behavior profiles of all other actors in their cohort group. We call this an “Out of Family” behavior.



This approach is even effective for identifying human malicious insider threats because their methods will often include the continuation of their legitimate work (which keeps them associated with their cohort group) while hiding their malicious activity in the noise of daily activity. Our threat detection capability detects all known and unknown threats because we use the organization's data and behaviors to sort out what belongs and what doesn't.



It's important to note that our technology is not a simple anomaly detection mechanism. Other anomaly detection approaches to network threat detection have been attempted in the past and failed due to the high volume of false positives they produced. Computer networks and the people and devices using them generate enormous numbers of anomalies; alerting a security official every time will only result in the system getting turned off. Our advanced behavior profiles are designed to understand the baseline routines and the types and volumes of anomalies an actor typically produces. Our system generates alerts when the behavior profile, complete with its routines and anomaly patterns, indicates threatening activity.

It's the most advanced internal threat detection solution available.

