DATA SHEET

# esINSIDER

***Protect against advanced persistent threats and malicious insiders***

**Comprehensive Threat Awareness**

Automatically maps hosts across on-premises and cloud environments, capturing vital east-west traffic critical for visibility into advanced persistent and insider threat activities.

**Adaptive Behavioral Baselining**

Maintains a deep understanding of normal network activity with continuous modification, contextual to changing business operations and the evolving threat landscape.

**Machine Learning Driven Detection**

Cuts through network noise, identifying potential threats using proprietary machine learning processes that link host interactions and data movement to unavoidable attack chain behaviors.

**Threat Hunting and Co-Remediation**

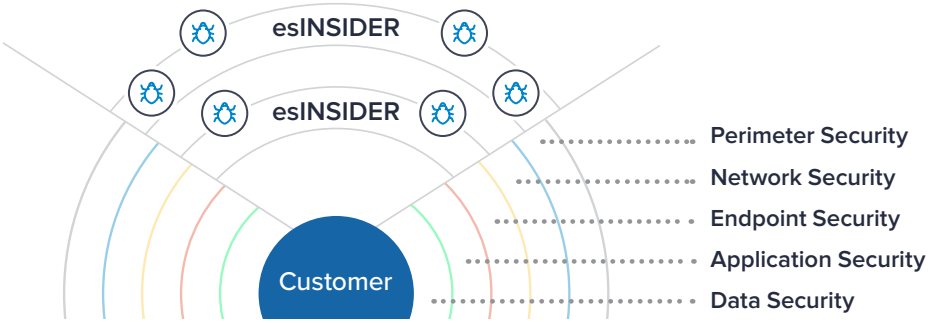
Alleviates resource constraints with a dedicated team of elite eSentire threat hunters that conduct investigations and support co-remediation that ultimately reduces risk to business operations.

esINSIDER is a behavioral-based Managed Detection and Response (MDR) service built to be your last line of defense against attackers already inside your network. esINSIDER pairs proprietary machine learning with dedicated, elite security analysts to identify unavoidable attack behaviors that extend beyond traditional detection methods.

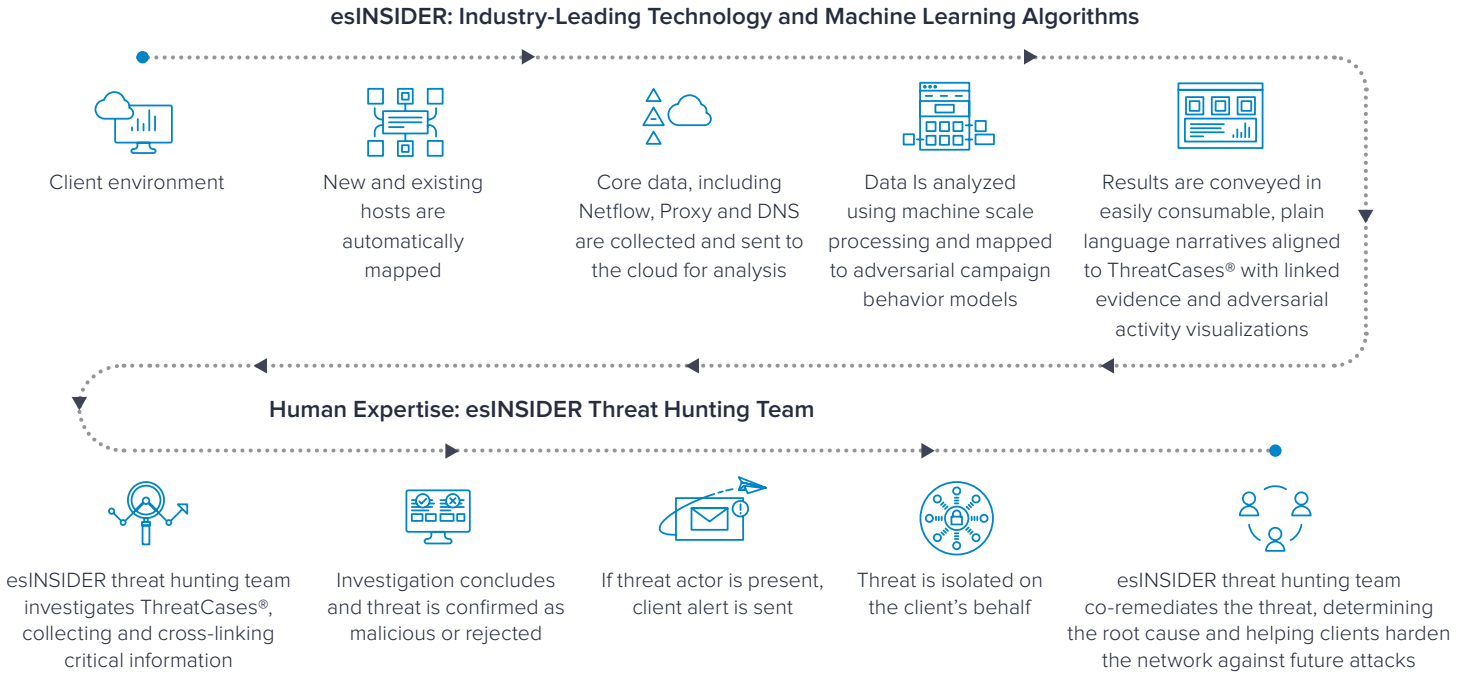
Capturing critical east-west traffic, esINSIDER maintains an understanding of the network norm identifying deviations indicative of unavoidable attacker kill chain stages. Minimizing attacker dwell time, eSentire threat hunters investigate suspicious activity, working with your security teams to neutralize attacks and minimize risk to intellectual property and business operations.

## What does esINSIDER solve for?

- Limited east-west traffic visibility across cloud and on-premises environments
- Risk from threat actors already in your network, such as advanced persistent and insider threats
- Traditional security control blind spots that use approved tooling and live-off-the-land techniques
- Reliance on rules, signatures and IoCs to detect threats that evade advanced network security controls
- Inability to baseline network behavioral norms and maintain continuous situational awareness
- Insufficient capability to identify behavioral anomalies and package event details for investigation
- Resource limitations to conduct investigations, correlate with other network data and confirm threat presence
- Response limitations that extend threat actor dwell time to dangerous levels



## How does esINSIDER work?




## Features

### Automated Network Mapping

Automatically maps new and existing network hosts across your on-premises, cloud and hybrid environments.

### Comprehensive Visibility

Provides unparalleled visibility into east-west traffic, capturing data movement between hosts critical to determining the legitimacy of traffic and the network norm.

### Continuous Situational Awareness

Ingests data from high efficacy sources into an integrated machine learning modifies and redefines understanding of the network norm over time, continually evolving to keep pace with the changing threat landscape and evolving nature of your network.

### Elusive Insider Identification

Integrated machine learning looks deep within your network for entities exhibiting characteristics that match attack chain stages. From reconnaissance to data collection and exfiltration, host activity is mapped to attack stages that exhibit potential malicious behaviors traditional detections and triggers miss.

### Consumable Attack Chain Visualizations

Plain language narratives aligned to ThreatCases® provide visual maps with linked evidence of insider threat campaigns unfolding inside your network.

### Adaptive Human Context

Dedicated threat hunters work in tandem with your internal security teams to establish a deep understanding of network and security operations that improves accuracy and speed of investigations.

### Embedded Threat Hunting and Forensic Investigation*

Embedded threat hunting and forensic investigation by eSentire SOC analysts accelerate precision that eliminates false positives and determines root cause that facilitates focused response and threat containment.

### Co-Managed Remediation*

Leveraging root cause data, eSentire SOC analysts work with your security team post-incident to harden your environment against future attacks and further business disruption.

### Co-Management*

Provides access to esINSIDER ThreatCases® and expert SOC analysts, so you can understand the context and status of an event and investigate alongside eSentire threat hunters.

*Requires esENDPOINT and esLOG+

## esINSIDER vs. Others

| | esINSIDER | Others |
|---|---|---|
| Uses attack chain stages across techniques, tactics and procedures (Recon, data collection and exfiltration ) | ✓ | ✗ |
| Unifies visibility across all east-to-west traffic | ✓ | ✗ |
| Integrates data from virtually any source | ✓ | ✗ |
| Normalizes disparate datasets for analysis | ✓ | Limited |
| Applies user behavior analytics to build a baseline of activity | ✓ | Limited |
| Identifies suspicious behavior whether malicious or not | ✓ | Limited |
| Provides simple straightforward ThreatCases® for easy to interpret information at your fingertips | ✓ | ✗ |
| Cloud operated and deployed | ✓ | Limited |
| Reactive and proactive threat hunting included | ✓ | Limited |

## Making the Case for esINSIDER

- Acts as a last line of defense against advanced persistent and insider threats
- Compliments advanced endpoint and network security controls
- Maintains continuous network awareness across on-premises and cloud environments
- Provides east-west traffic visibility for deep insight into data movement
- Maintains an understanding of legitimate network activity over time
- Identifies advanced persistent and elusive insider threats that circumvent traditional detections
- Alleviates resource constraints to investigate, confirm and respond to threats
- Eliminates alert fatigue and resources wasted on false positives
- Accelerates response and containment minimizing attacker dwell time
- Determines root cause and improves resiliency

**Ready to get started? We're here to help.**

**Reach out to schedule a meeting to learn more about esINSIDER**

eSENTIRE