eSENTIRE

DATA SHEET

esINSIDER

Protect against advanced persistent threats and malicious insiders.

Ever-expanding digital networks provide areas of grey where advanced persistent and elusive insider threats thrive. From nation-state attacks to skilled malicious insiders, technology continues to fall short. Human intuition and expertise can't scale to pick up the slack as advanced threat actors look to achieve objectives leaving business disruption in their wake. It's time for a new layer of protection. Illuminate the grey, leave attackers nowhere to hide with esINSIDER.

CONTINUOUS INSIDER THREAT AWARENESS

Automatically map new and existing network hosts across on-premise, cloud and hybrid environments for continuous threat visibility across your expanding business environment.

UNAVOIDABLE BEHAVIORAL IDENTIFICATION

Identify advanced persistent and elusive insiders using proprietary machine learning processes that look deep within your network, linking key unavoidable adversarial behaviors with suspicious hosts.

CONSUMABLE ATTACK CHAIN VISUALIZATIONS

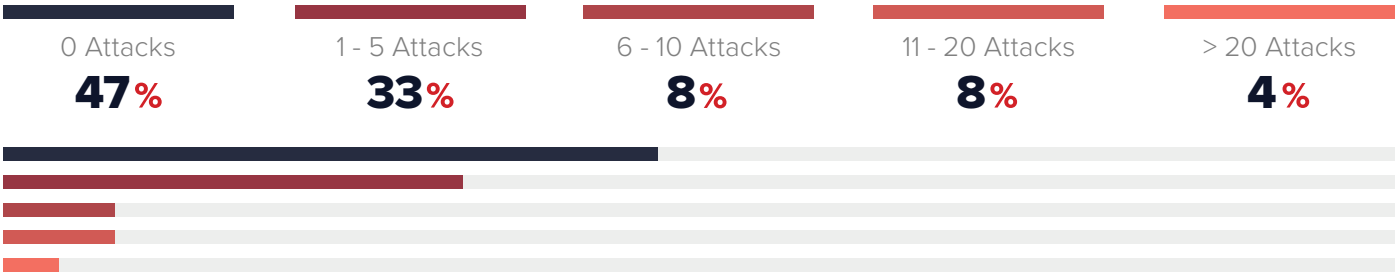
Focus response with plain language narratives aligned to ThreatCase® visualizations with linked evidence and adversarial activity.

EMBEDDED INCIDENT RESPONSE

Contain advanced persistent and elusive insider threats with human expertise that coordinates co-remediation to harden your environment against future attack and business disruption.

THE PROBLEM

FREQUENCY OF INSIDER ATTACKS[1]



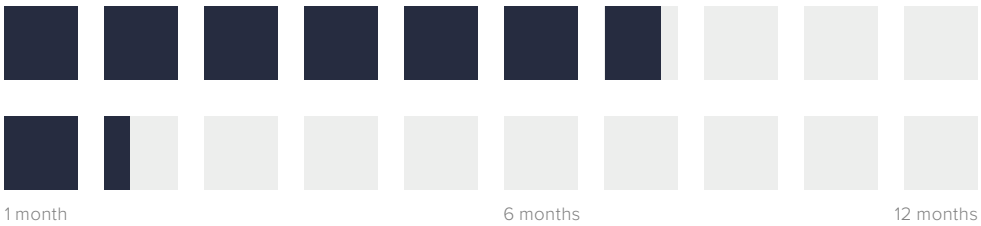
EFFECTIVENESS IN CONTAINING ADVANCED THREATS (1-10 SCALE)[2]

[1] *Cybersecurity Insiders: 2018 Insider Threat Report*
[2] *Ponemon: The Cost of Time to Identify & Contain Advanced Threats*

TIME IT TAKES TO DETECT AND CONTAIN ADVANCED THREATS[3]

Mean time to investigate
196.5 days

Mean time to contain
38.5 days



BARRIERS TO REMEDIATION[4]

Lack of in-house expertise
55%

Inability to prioritize
63%

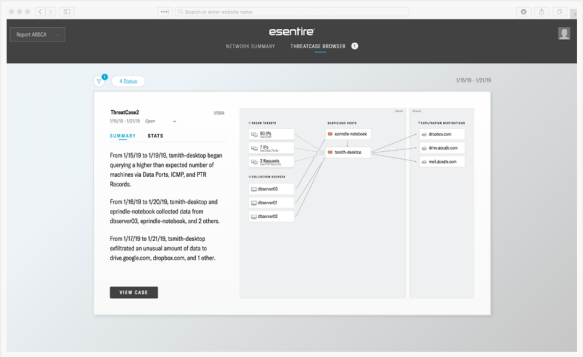
Lack of visibility of threat activity acrosss the enterprise
76%

THE SOLUTION

Whether your data is on-premise, in the cloud or somewhere in between, eSentire esINSIDER evolves with the requirements of your modern hybrid IT environment to illuminate advanced persistent threats and malicious insiders that evade traditional detection technologies.

Using industry leading machine learning algorithms, esINSIDER automatically maps and continuously redefines situational awareness of the network norm that facilitates continuous understanding of your environment. esINSIDER's machine learning processes look deep within your network for entities exhibiting characteristics that match attack chain stages no threat actor can avoid. From internal reconnaissance to data collection and exfiltration, attack stages are mapped to hosts that exhibit potential malicious behaviors. Activity is automatically organized and displayed in easy to understand incident visualizations termed ThreatCases®.

esINSIDER's embedded incident response team leverages ThreatCases®, automatically created investigatory spaces that cross-link information across network and host data, to facilitate threat context, confirmation and containment performed by eSentire Security Operation Center (SOC) analysts. As a co-managed model, your organization has complete insight to all ThreatCases® and access to the esINSIDER analyst team to understand the extent of the attack that facilitates hardening against repeat or future attacks and avoidance of business disruption.



ThreatCases® are actionable maps of campaigns already unfolding inside your network. ThreatCases® give your team and the eSentire analyst team the information they need to act quickly and stop adversaries before damage is done.

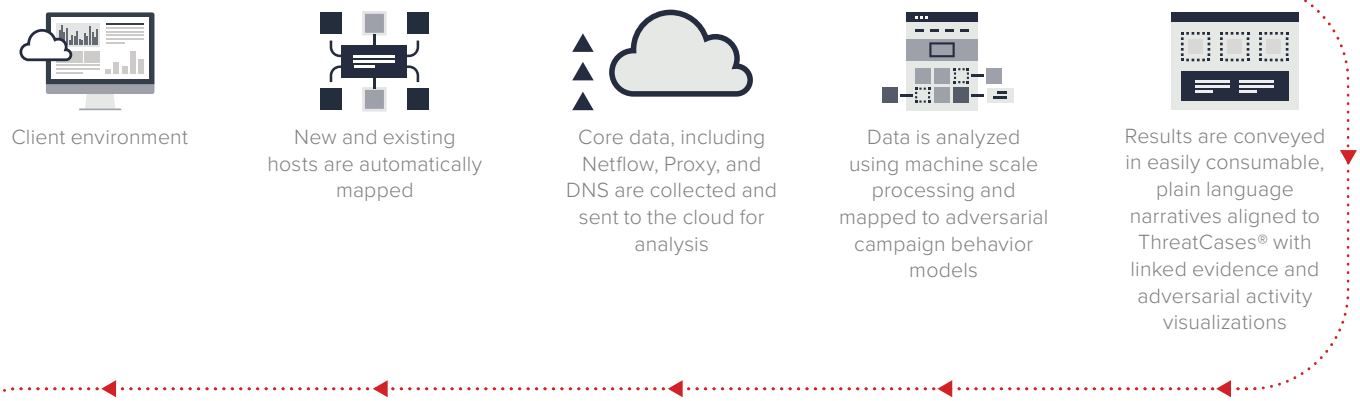
[3] *Ponemon: The Cost of Time of Identify & Contain Advanced Threats*
[4] *Ponemon Study: State of Malware Detection & Prevention March 2016*

WHAT DOES esINSIDER SOLVER FOR?

- Malicious advanced persistent and elusive insider threat identification that evades controls such as DLP, IPS/IDS, IAM, etc.
- Continuous data acquisition and situational awareness of the network norm
- Automated network mapping across cloud, on-premise and hybrid environments
- Scalable analytics that identifies signals in the noise
- Alleviating resource constraints, the eSentire esINSIDER analysts team acts as extension of your team
- Threat visualizations that map, categorize, prioritize and narrate context
- Threat data that facilitates ease of investigation and focused response
- Deep visibility into east-west traffic

HOW DOES IT WORK?

INDUSTRY LEADING TECHNOLOGY AND MACHINE LEARNING ALGORITHMS: esINSIDER SECURITY ENGINE



Client environment

New and existing hosts are automatically mapped

Core data, including Netflow, Proxy, and DNS are collected and sent to the cloud for analysis

Data is analyzed using machine scale processing and mapped to adversarial campaign behavior models

Results are conveyed in easily consumable, plain language narratives aligned to ThreatCases® with linked evidence and adversarial activity visualizations

HUMAN EXPERTISE: esINSIDER THREAT HUNTING TEAM

esINSIDER Threat Hunting Team investigates ThreatCases®, collecting and cross-linking critical information

Investigation concludes and threat is confirmed or repudiated

If threat actor is present, client alert is sent

Threat is isolated on the client's behalf

esINSIDER analyst team co-remediates the threat and helping the client harden the network against future attacks

FEATURES

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

Continuous Situational Awareness
Integrated machine learning modifies and redefines understanding of the network norm over time, continually evolving to keep pace with the changing 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 network reconnaissance to data collection and exfiltration, attack stages are mapped to hosts that exhibit potential malicious behaviors, leaving advanced persistent and elusive insider threats nowhere to hide.

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

Embedded Threat Hunting and Forensic Investigation
Embedded threat hunting and forensic investigation by the esINSIDER analyst team - a Tier 3 SOC team - reduces false positives and facilitates focused response and threat containment.

Tactical Threat Containment
esINSIDER analyst team locks down and isolate threats on your behalf to prevent the spread of attack.*

Co-managed Remediation
Leveraging root cause data, esINSIDER analyst team works with your security team post incident to harden your environment against future attacks and further business disruption.

Co-Management
Provides access to ThreatCases® and esINSIDER analyst team so you can understand the context and status of an event and investigate alongside eSentire investigators.

*Requries esENDPOINT

MAKE THE CASE FOR esINSIDER

- Automatically maps new and existing hosts for continuous network awareness
- Modifies and redefines understanding of your network norm over time
- Provides east-west traffic visibility
- Identifies advanced persistent and elusive insider threats no matter what tools, tactics or exploits used
- Facilitates focused response and containment with narrative threat visualizations
- Hunts, investigates and confirms threats with embedded human expertise
- Contains threats on your behalf
- Determines root cause and hardens against future attacks

eSENTIRE

eSentire is the largest pure-play Managed Detection and Response (MDR) service provider, keeping organizations safe from constantly evolving cyber-attacks that technology alone cannot prevent. Its 24x7 Security Operations Center (SOC), staffed by elite security analysts, hunts, investigates, and responds in real-time to known and unknown threats before they become business-disrupting events. Protecting more than $6 trillion in corporate assets, eSentire absorbs the complexity of cybersecurity, delivering enterprise-grade protection and the ability to comply with growing regulatory requirements. For more information, visit **www.eSentire.com** and follow **@eSentire**.