Network Forensics: Tracking, Investigating and Identifying Threats

What is Network Forensics?

“Network forensics is a science that centers on the discovery and retrieval of information surrounding a cybercrime within a networked environment. Common forensic activities include the capture, recording and analysis of events that occurred on a network in order to establish the source of cyberattacks.”

Infosec Institute

This is one definition by the Infosec Institute but to explain it in simpler terms – Network Forensics is a process where we collect and analyze organizations’ traffic data to detect any potential cyberattack or investigate any cybercrime. You can think of network forensics analysis as putting up CCTV cameras on your network so in case of any data breach you can look at recorded data and track the root cause.

According to the 2023 Annual Data Breach Report, there was a staggering increase of 78 percent in data compromises as the number went from 1,801 in 2022 to 3,205 in 2023.

The increase in the number of data compromises states that network forensics is becoming vital for every organization. It can not only detect and prevent cybercrimes but also helps with ensuring compliance and collecting digital evidence.

How Does Network Forensics Work?

At its core, network forensics works in a set pattern of capturing, storing, and analyzing. Then the security team further investigates into the cyber breach to minimize the damage and intercept any future attack. But if you’re planning to add forensics into your cybersecurity strategy, you should understand the mechanics of Network Forensics in detail:

- ### Deep Session Inspection

  Deep Session Inspection technology helps pay closer attention to ensure that all data circulating your network is accounted for and thoroughly processed for possible cybersecurity threats or data leakage. Fidelis goes through all this data with painstaking detail to find any theoretical weaknesses and ways to secure your enterprise.

- ### Data Capturing

  Tracking metadata is important as it allows us to index large amounts of data traffic and quickly find it. Not only does this help us become more responsive to possible issues, but by capturing metadata comprehensively, we can also identify anomalies better.

- ### Data Storage

  The type of storage solution must be robust so that when data is collected – it can easily be stored and analyzed– this will enable your SOC teams to make the right decisions

quickly.

- **Data Analysis**

  This wealth of network metadata gives our analysts the ability to perform retrospective analysis. By examining past incidents and patterns, we gain invaluable insights into emerging threats. In addition, Fidelis uses our special correlation techniques and state of the art machine learning algorithms to provide full-spectrum traffic analysis. Fidelis Network® employs human intelligence combined with state-of-the-art technology to outmaneuver cyber adversaries.

- **Correlation and Reconstruction**

  Ultimately, how far we can trace an event back to its inception is invaluable in understanding the full complexity of the attack. Our system allows for detailed correlation and reconstruction of incidents, providing a clear view of how an attack unfolded. This process not only helps with immediate response but makes us better at identifying threats overall.

- **Reporting and Legal Compliance**

  The last part of our network forensics methodology includes elaborate incident reporting and legal recourse if needed. We have to comply with legal standards and rules in cybersecurity awareness. Our detailed reporting ensures that all findings are documented comprehensively, enabling your organization to respond appropriately while adhering to industry guidelines.

Key Applications of Network Forensics

Network forensics is the analysis of all network traffic to investigate security incidents. It’s like being a digital detective – you are gathering clues and piecing together what happened.

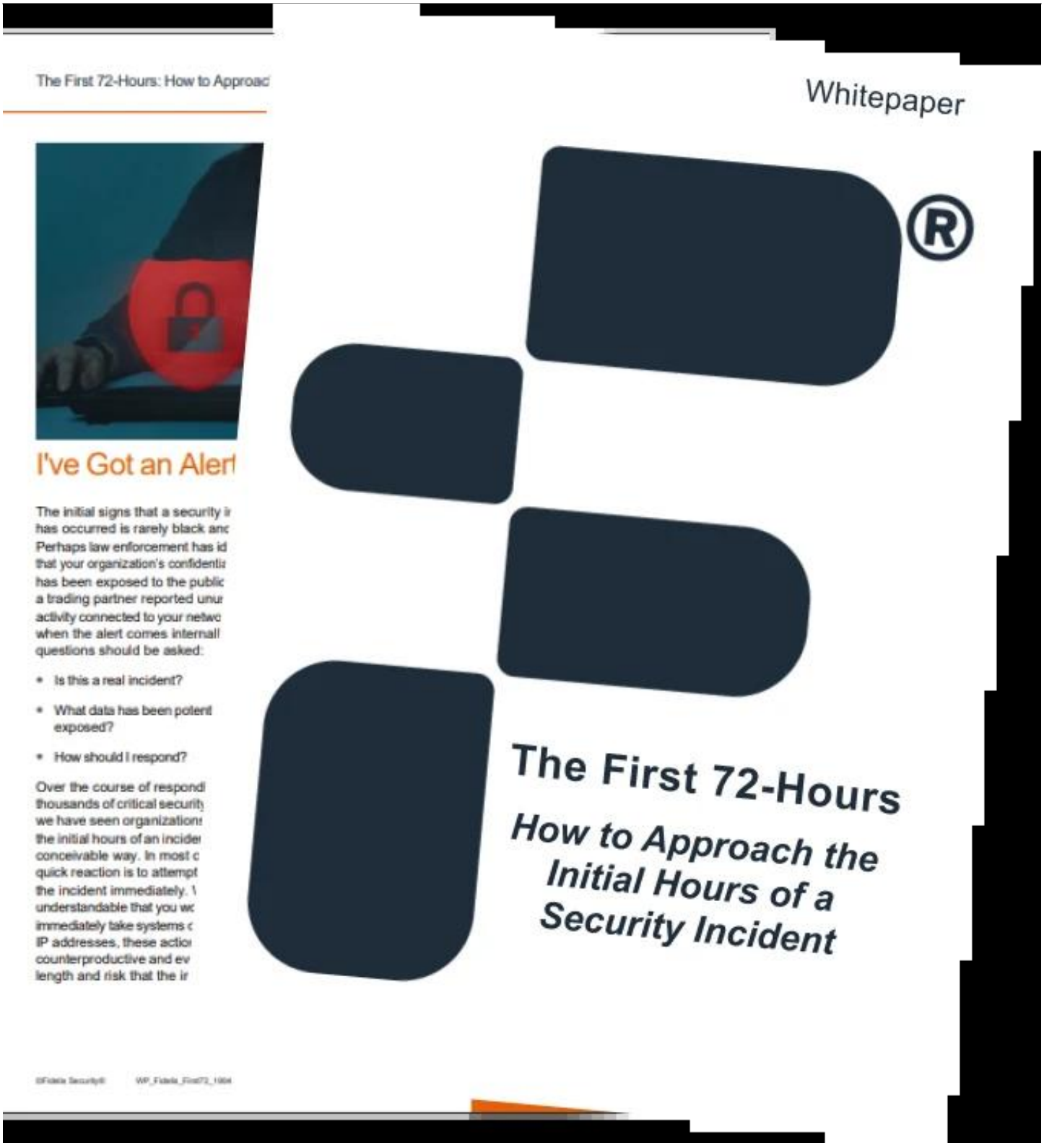
Incident response

One of the key applications is *incident response*. In case of a security breach, you can identify the root cause of the issue with the help of network forensics. After finding the origin of the problem you can take appropriate action to mitigate the damage.

Critical Incident Response: Key Steps for the First 72 Hours

- What data has been potentially exposed?
- Incursion detection and Persistence detection
- How should I respond?

Download the Whitepaper



Compliance and regulatory investigations

Another important use case is compliance and regulatory investigations. The rules around data privacy are getting more rigorous so network forensics analysis can help an organization with forensic evidence that they're meeting those requirements.

Threat Hunting

Network forensics can also support Network threat detection efforts. It can analyze network

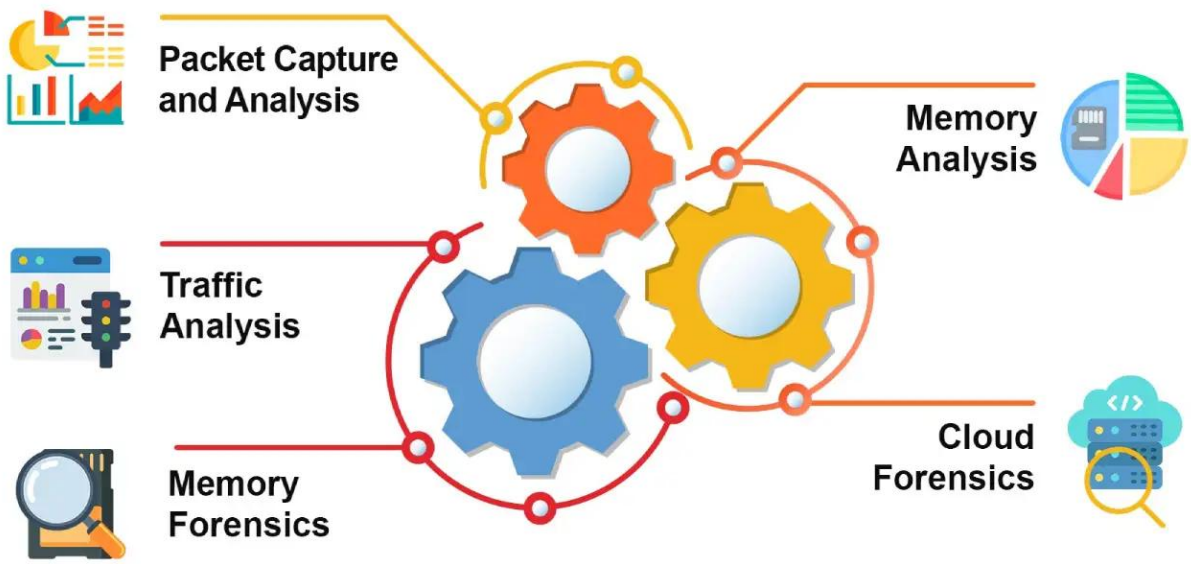
traffic patterns and assist you identify signs of deviation from standard patterns. You can add Fidelis Network® to your forensic security strategy as it enhances the threat hunting capability by utilizing machine learning and advanced analytics to detect anomalies and identify potential threats before they escalate.

Performance Troubleshooting

One the most overlooked applications of network forensics is that it allows you to quickly find and fix issues that could be impacting on business productivity or customer experience. The Fidelis system records key information to support performance troubleshooting.

Overall, network forensics is a powerful tool that can give you a comprehensive view of what's happening on your network.

Advanced Network Forensics Techniques



Network forensics uses various techniques and strategies to capture, analyze, and investigate a network system, A few of those techniques are given below:

1. Packet Capture and Analysis

This process involves monitoring the flow of data through your system and closely inspecting the contents to identify any red flags. Fidelis Security's patented Deep Session Inspection eliminates the need for analysts to spend time decoding network traffic. Our session reassembly allows us to provide visibility far beyond a Deep Packet Inspection (DPI).

2. Traffic Analysis

This technique involves looking for unusual spikes or trends in network traffic. Fidelis will record key pieces of information such as IP addresses and protocols that will allow you to put them together to trace the path of an attack across your network.

3. Memory Forensics

This process involves two key steps. First, you'll capture an image of the system's RAM, known as Memory Image Capture, that will give you a comprehensive view of the system's state, which you can then analyze offline.

4. Memory Analysis

Next, you'll dig into the Network Connection Analysis. Here, you'll extract all the active network connections and related artifacts directly from the memory to identify any suspicious activity that may lead to breach. Fidelis Elevate® can help with the process and memory analysis of endpoints within your organization.

5. Cloud Forensics

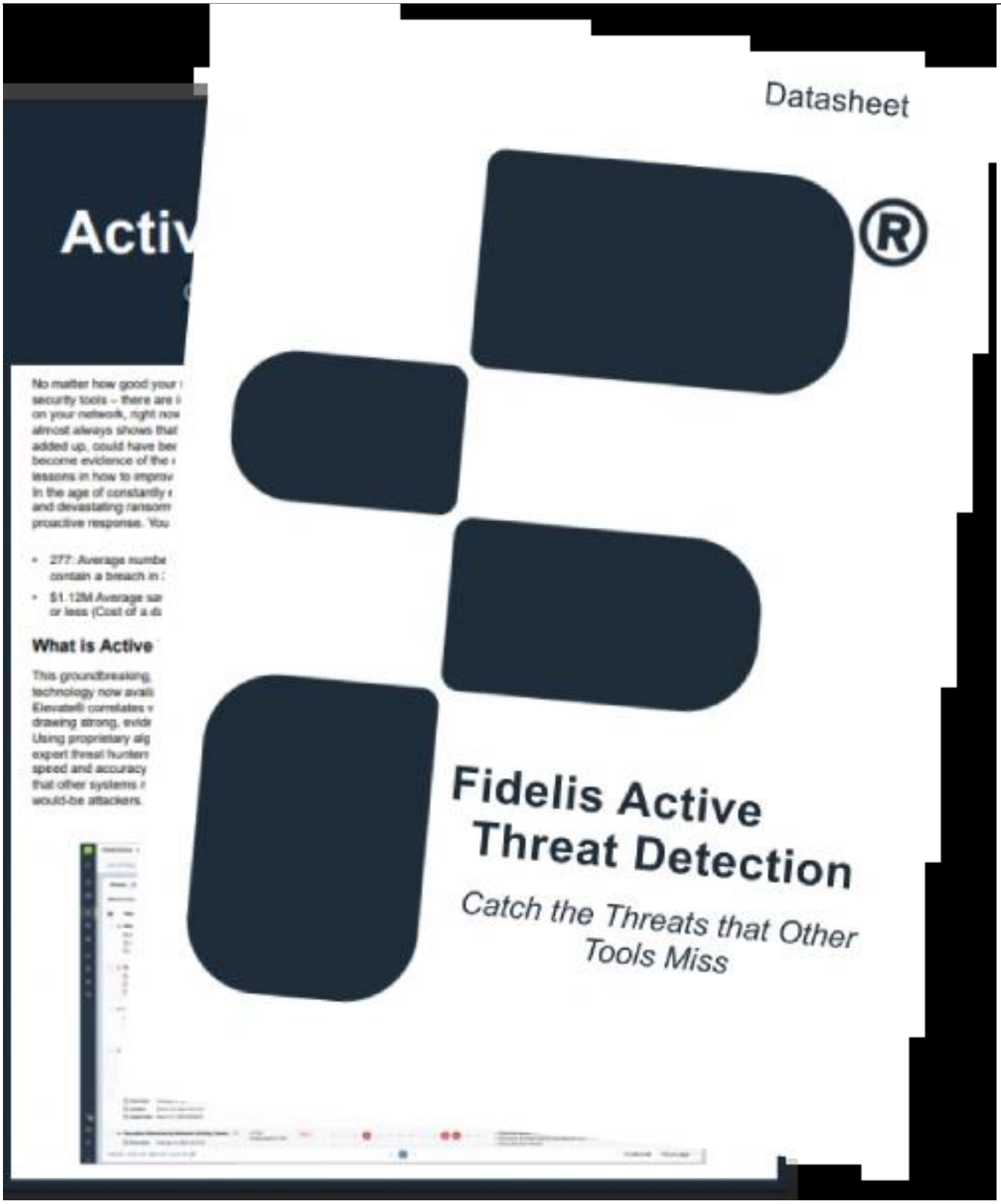
When it comes to cloud environments, traditional network forensic methods may not always be applicable. That's where cloud forensics is applied.

Fidelis supports network cloud forensics, allowing sensors to be deployed in public clouds.

Discover how Active Threat Detection safeguards your network. Get insights on:

- Identifying threats in real-time
- Automating responses
- Strengthening threat defense

Download Now



Future Trends in Network Forensics

These are some of the key trends that may shape and change the landscape of network forensics.

AI and Machine Learning

With the advancement in AI and ML, Network forensics is able to analyze data faster and give

more accurate results. And the more cyberattacks it is experiencing; it is becoming effective to stop future cybercrimes.

Blockchain Integration

Blockchain has garnered a lot of attention due to the recent spike in cryptocurrency exchange. But not many people know that forensic evidence can be recorded on blockchain making them secure against any tampering.

Cloud-Native Forensics

As the data is moving on cloud-based storages, Cloud-Native Forensics is becoming the future of traditional network forensics. Organizations are focused on securing their data in their cloud infrastructure.

IoT Forensics

IoT is the weakest link in any organization, most prone to getting attacked. IoT forensics is a subbranch of network forensics that involves capturing and analyzing data from connected devices to understand and secure any vulnerabilities.

Fidelis Network® – Revolutionizing Network Forensics for Proactive Threat Detection and Response

Network forensics plays a crucial role in contemporary cybersecurity and provides insightful information about the detection, tracking, investigation, and identification of threats. Fidelis Network® Detection and Response (NDR) is a revolutionary tool for network forensics. Through the use of Deep Session Inspection technology, advanced AI (artificial intelligence) analytics, and machine learning (ML), Fidelis' NDR solution provides security teams with an unprecedented view into network traffic to capture and analyze extensive amounts of data at previously unattainable rates.

Our NDR solution not only supports its customers with retrospective analysis after a breach but also delivers real-time threat detection and prevention, identifying potentially dangerous patterns and anomalous behavior as it unfolds.

Here's what sets the Fidelis Network apart:

- Fully integrated intelligence that automates and correlates data across your entire security infrastructure.
- An automated platform specifically designed for threat detection and proactive hunting.
- Comprehensive mapping of the entire terrain, encompassing cloud environments, enterprise networks, and remote work settings.
- In-depth visibility into all embedded content flowing in and out across various ports and protocols.
- Capabilities for both real-time detection and historical investigation of threats.
- Detection of lateral movement within networks to identify potential intrusions swiftly.

- Utilization of multiple detection methods spanning the entire attack kill chain.
- Embedded sandboxing features that allow for safe analysis of suspicious files.
- Robust network data loss prevention measures to safeguard sensitive information.

By combatting the most sophisticated cyber threats, Fidelis Network® equips organizations with what they need not only to detect and respond to today's threats but also predict and train for those of tomorrow.

Unlock Powerful Network Security with Fidelis NDR
See how Fidelis NDR boosts security with:

- Comprehensive Threat Detection & Analysis
- Data Loss Prevention (DLP) & Email Security
- Deep Session Inspection & TLS Profiling

Download the Datasheet

Datasheet

Fide

Deep Visibility, A

Networks continuously grow in both size
ticularly as digital transformation extends
the cloud. This creates the ideal environ
actors to hide. Finding and stopping the
seem like an impossible task. Often, it is
breach will occur, but when.

How Fidelis Network Work

Fidelis Network is a proactive network
(NDR) solution that provides unmatche
threat detection, and faster response t
stand-alone, or as part of the compreh
open and active eXtended Detection a
platform, Fidelis Network integrates se
security stack.

Fidelis Network automatically groups
critical time and provide malware ana
hunting. Fidelis Network also provide
forensics, DLP (Data Loss Preventic
and automated security rules in one
users aggregated alerts, context, an
investigation, deeper analysis, and

By collecting more than 300 metad
and files, Fidelis Network provides
threat defense than competitors' N
Detection correlates alerts that mi
and maps them

Fidelis Network®

Deep Visibility, Advanced Threat Detection and Response