

Top 3 Requirements To Turbocharge Your Forensics

Eliminate limitations and complexities within security investigations and make everyone on the team an expert analyst



Executive Summary

Recent years have taught us that no one is immune to security breaches. Organizations from all sectors are under constant pressure to identify successful attacks and respond quickly in order to minimize damage and losses.

Unfortunately the investigation tools that are currently available have failed to meet enterprise business needs. Log-based solutions are inherently incomplete as they are missing the actual data, and packet-based forensics tools are too difficult to use and cannot scale in bandwidth and requisite storage capacity. Even well-funded security teams find it hard to handle the constant alerts triggered by their own security measures.

To overcome today's forensics challenges, security teams must arm themselves with better tools to get access to the detailed information they need, but also save effort and time in the process. To help you find the right solution for your organization, the following set of requirements provides key guidelines for performing successful security investigations.

By 2020 60% of enterprise information security budgets will be allocated for rapid detection and response approaches, up from less than 20% in 2015.

-Gartner Security & Risk Management Summit 2015

IN THIS PAPER, YOU WILL LEARN:

- The blind spots inherent in the traditional forensics approach
- Top 3 considerations when adopting a new forensics technology
- How to overcome the complexities and limitations of security investigations
- How the WireX solution can provide security professionals at all levels the ability to make faster and more informed decisions based on greater context and history



When Under Attack Are You Confident You Can Deal With It?

The increasing volume of sophisticated threats repeatedly demonstrates the inevitability of compromise. Enterprise networks are more vulnerable in the landscape of targeted phishing, fraud scams and vulnerable web applications, meanwhile prevention systems are incapable of providing a silver bullet for protection.

While every organization may expect some of its assets to get compromised, the key question is how fast the security team reacts once the attacker has crossed the first perimeter. This lag between breach and response is critical. Security alerts should be reviewed and once validated as real threats, a detailed investigation must be performed quickly. Security teams need to be able to figure out the attack surface, identify the extent of any data loss and perform root-cause analysis, in order to effectively mitigate the incident before it becomes a full-blown breach. Reducing investigation time exponentially assists in shrinking the damage of potential breaches and exposure to business risks.

Best practices require organizations to adjust to this changing landscape by rebalancing their resources from fortifying security controls to rapid detection and response initiatives. Post-infection analysis methods must be actively embraced, SOC teams need to be reinforced, and incident response processes have to be established - all to keep up with the continued flood of security incidents.

76% of organizations were affected by a successful cyberattack in 2015.

-CyberEdge Group, Cyberthreat Defense Report, 2016

THE CRITICAL LAG TIME BETWEEN BREACH AND RESPONSE






The Forensics Paradox: With Or Without The Data, You Are Left Blind

One of the most critical and persistent challenges in the cyber industry today is lack of quality data. This causes security teams to spend too much time handling potential incidents, and also to miss vital information for the investigation. Unfortunately, today's currently available investigation tools don't make it easy for organizations to speed-up this process:

 **Log-based solutions:
Inherently incomplete as the actual content is missing**

A typical security team deploys dozens of solutions and is provided with countless logs and alerts. As the traditional approach of correlating events using SIEM may be an important step in prioritizing investigations, spending time on log analysis is rarely enough and turns the investigation into guesswork. Security teams are limited to high-level metadata and are left blind to security threats targeting their network.

 **Packet-based forensics tools:
Highly complicated. Limited history. Too slow.**

When trying to gain better visibility in order to support effective investigations, some organizations adopt network forensics solutions that are designed to retain and analyze full packet capture (PCAP) data. However, security teams that are currently using these types of tools report significant barriers when trying to get value from them. First, these tools require advanced skillsets only a few team members possess. Second, recording traffic at an enterprise-scale is often restricted by costly storage investments to only several days. Unfortunately because most security breaches take weeks to months to discover, the value of these tools is therefore greatly diminished.

This reality creates a difficult situation. While conventional approaches do not get the job done, the cost and complexity involved in the adoption of forensics solutions are making them infeasible in most environments. Organizations are left without the ability to investigate the constant alerts triggered by their own security measures.

Nearly 70% of the time spent by security staff responding to malware alerts is wasted because of faulty intelligence.

-Ponemon Research, The Cost Of Malware Containment, 2015



Three Fundamental Requirements For Effective Security Investigations

Most organizations lack the manpower and visibility needed to properly investigate every alert. Security teams are often faced with the choice of ignoring potential incidents, or devoting excessive resources in order to gain more understanding into what has happened. Automated detection followed by correlations to reduce false positives are indeed important steps in mitigating this burden. However, the majority of work still relies on the actual investigation phase. Even the best-equipped analysts find themselves sorting through mountains of packet captures and unrecognized network sessions, unable to provide quick answers to critical questions. So, how does an enterprise change this?

In order to provide security teams with the ability to react quickly and accurately to cyber-attacks and overcome the time, human-resources and technical limitations, here are the three fundamental requirements for consideration:

1 The heavy lifting of data analysis must be automated to overcome skill-set barriers

The current recognized shortage of skills in cybersecurity creates a major bottleneck in facilitating forensics investigations. Organizations must support users who lack deep expertise, so that front-line responders can handle more complex investigations thus escalate fewer tickets. The forensics solution may collect valuable data for investigating a threat, but if further manual analysis is required just to find the relevant data and understand what it means, it is likely to be lost in the shuffle. Security teams should not waste precious time drilling into sessions with Wireshark-like tools when trying to understand what is happening in the network. This is why a key evaluation factor when choosing a forensics tool should be ease of use. Today's solutions should be able to do all the heavy lifting of data analysis to automatically translate network packets and sessions into intuitive, searchable intelligence that can be used without labor-intensive efforts.



2 Organizations need complete visibility into application contents and user activities

The traditional approach of correlating events from different sources using SIEM has proven insufficient for performing investigations. Enterprise visibility should extend beyond logs and flow data in order to validate security alerts and determine the extent of successful attacks. Security teams need immediate access into information traversing the network to be able to answer when data was accessed, by whom, where it traveled to, and what was in it. This includes the actual payloads of network conversations, rather than just the metadata – the content of emails, chats, file transfers, business transactions, DNS lookups, search queries, authentications, as well as remote desktop sessions. All of this is essential intelligence that needs to be available in order to perform effective security investigations.

3 Proper investigations require much greater retention periods of forensics data

The ability to look back in time to investigate historical security incidents is critical, but by the time organizations discover a breach, it's usually too late. According to Mandiant 2015 Threat Report, an attacker has a free rein in breached environments for approximately 205 days before being mitigated. Organizations are doing their best effort to collect data for forensics investigations however they are facing significant storage limitations. As high-level metadata is insufficient, the current approach is to capture and store full packet-data for later analysis. A quick calculation shows that a 10GbE link will require about 110TB of storage for recording a single day of traffic. Security teams are often restricted to merely several days' retention periods, considering the capacity of a typical enterprise infrastructure. While most security breaches take weeks to months to discover, the value of traditional solutions that entail full packet capture is clearly diminished. To overcome this challenge and get access to the historical content required for proper investigations, organizations need to take a different approach and work with solutions that can increase forensics data retention periods from days to many months in order to reveal the full story before, during and after an attack.



WireX: Introducing a New Paradigm Shift Network Forensics. Evolved.

New innovations in security are changing the way organizations can approach security investigations. The WireX Network Forensics Platform (NFP) helps enterprises evolve their forensics to better meet today's demanding requirements with the most advanced, cost-effective, large-scale network forensics solution. WireX's Contextual Capture™ delivers organizations the technology foundation to overcome the challenges associated with collecting and analyzing essential data for security investigations.

Rather than simply capturing raw packets, WireX NFP continuously reconstructs the entire OSI stack into comprehensive intelligence, with details on user behaviors and application contents. By combining massive-scale monitoring, unique analysis technology, big-data analytics and built-in integrations with existing tools and workflows, security teams are able to gain better understanding to the full kill chain of cyber attacks.

REMOVE SKILL-SET BARRIERS

Comprehensive security intelligence delivered in actual human-readable form which can be immediately understood. This allows security professionals at all levels; security managers, SOC operators, analysts and incident response teams – to search, view and interact quickly and intuitively with content-level data without significant manual work requiring deep expertise.

GAIN GREATER VISIBILITY

Optimal content and behavior-aware visibility at both the perimeter and the infrastructure network. Security teams can view the precise information traversing the network and the related user actions performed, while at the same time zoom-in to business transactions within the core network. WireX's customizable analysis modules can provide the same level of visibility into proprietary homegrown applications, as it does for enterprise applications.

BOOST FORENSICS HISTORY

A solution that easily scales to support the needs of the world's largest organizations. Security teams can cost-effectively store many more months of forensics data within the same budget—providing them with up to 25X longer retention periods over traditional solutions with even greater context and visibility.

ACCELERATE SOC AND IR PROCESSES

Adaptive workflows and easy to use investigation tools to streamline forensics processes. The WireX NFP integrates with the existing security infrastructure, such as leading SIEM and threat intelligence solutions, and provides management tools to support the entire investigation life-cycle, as well as collaboration and knowledge sharing across team members.



About **WireX**

WireX is an innovative network intelligence and forensics company that is changing the way businesses resolve cyber-attacks. The company was founded in 2010 to deliver cutting-edge security forensics systems for intelligence agencies across the globe. Today, leading enterprises choose WireX as a key component in their forensics infrastructure to accelerate incident response, mitigate data theft and simplify responding to the magnitude of security alerts they must act on every day. WireX's mission is to deliver the best forensics experience for the enterprise with the greatest amount of context and history to make security investigations easy.

The company is headed by world-class security experts from IDF/8200, Nice Systems, HP and Check Point Software Technologies. WireX is financially-backed by Magma Venture Partners, Vertex Venture Capital, Entrée Ventures, Mickey Boodaei, Rakesh Loonkar and Idan Plotnik.