THINAIR

Identify & Investigate Information Leak Within Seconds

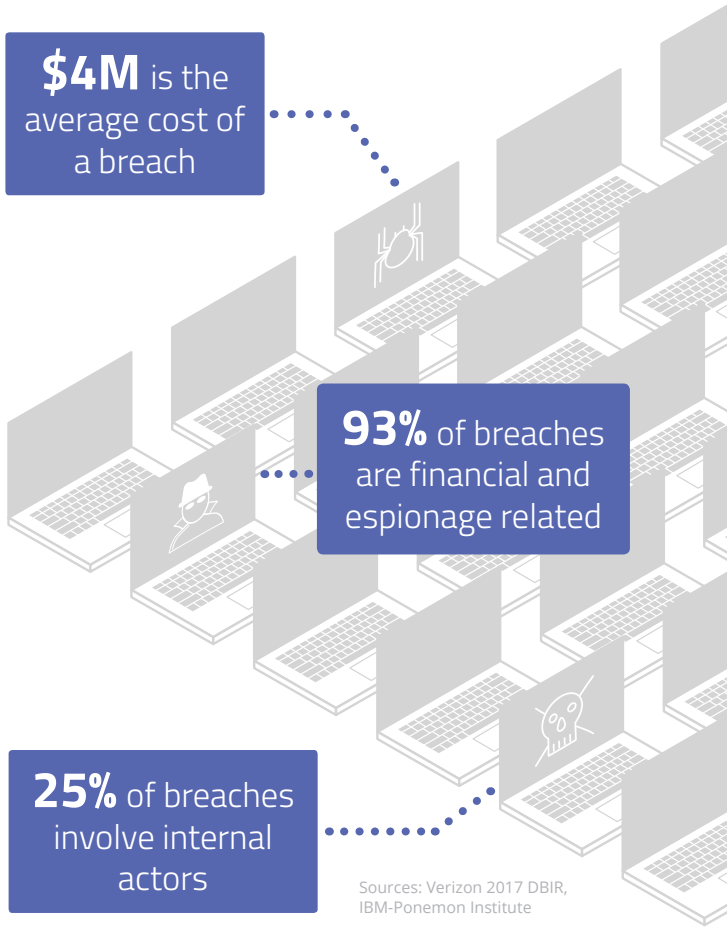
Information Leak is Inevitable

Today's digital economy is driving unprecedented growth of information sharing and access across all sectors of the economy. This information growth brings new challenges for cyber security but more specifically in the critical areas of investigation and forensics as data breach incidents are all but inevitable – it is not "if" but "when" your information will be leaked.

Information security, forensics and investigation teams are stretched thin meanwhile hackers have become highly sophisticated and financially motivated. Additionally, the rising trend of insider threats brings further complexity as insider breaches are even more difficult to identify. And, often the evidence gets tampered with or even destroyed before a formal investigation begins.

Precision and Speed is Critical

While data theft only takes a few minutes, it takes weeks or months to detect, investigate, contain the breach and restore the organization back to normal state. With the average cost of a data breach at its highest ever at $4M today (IBM-Ponemon Institute) it is imperative that organizations prepare internal teams to identify and investigate the scope and impact of a breach – quickly and precisely.



Sources: Verizon 2017 DBIR, IBM-Ponemon Institute

Before, During, and After the Crime

While breaches and information leaks are inevitable, organizations can significantly reduce their losses and compliance fines through proactive assessment and planning before a breach occurs. What if you had continuous auditable footage of every information interaction in your entire organization, like a high-definition video camera? You would then have complete digital visibility into exactly what happened and how it happened - before, during and after the breach. You can reconstruct the entire scene of crime with precise information on the source, root cause and impact of the breach.

Rapid Investigation & Impact Loss

ThinAir simplifies security incident handling by continuously discovering, recording and tracking every information creation, consumption and communication event across your entire fleet. Through its unique patent-pending technology, ThinAir can help your team instantly search and identify the incident, assess its scope and impact on your organization.

Through its simple user interface investigation teams can now ask ThinAir complex questions and get detailed information within seconds. Unlike traditional IR and Forensics tools that focus on a suspected device or person, with ThinAir you can start with simple clues such as a CCN or SSN, file, content, user, device, hash or application. And, ThinAir will instantly search and deliver information that you can filter and drill-down to precisely identify and confirm the incident, and investigate all the associated context and evidence to support your complete forensics and root cause analysis.

ThinAir also swiftly delivers the Risk and Impact of any breach or incident so you know exactly what the risk of that incident is to your organization.

You can now identify, investigate and respond to data leak and security incidents, within seconds!

ThinAir simplifies incident investigation, for example:

1. **Sensitive information leakage?** – Which files on which computers had that data?
2. **Disgruntled employee resigns?** – what has he been doing on his computer?
3. **Your sensitive information on WikiLeaks?** – Check who accessed or even just viewed that information, chronologically.
4. **Malware active on your network?** – Which computers and users were impacted? What sensitive data did the malware interact with?

PRE-BREACH ASSESSMENT

- Discover and tag sensitive information across the fleet
- Track every information creation, access, modification or deletion
- Track compliance and audit information
- Know exactly what your information risk is

BREACH INVESTIGATION

- Identify & confirm the incident - start with any attribute
- Investigate the evidence – files, devices, users, applications
- Root Cause Analysis – exact source, impact and vector of exfiltration

MONITOR POST-BREACH

- Deliver real-time or scheduled alerts
- Monitor suspicious actions and non-compliance
- Create reports to monitor and communicate

"Any organization that is serious about breaches would be smart to take a look at ThinAir"

ENTERPRISE STRATEGY GROUP, FEBRUARY 2017

THINAIR

Learn more at:
www.thinair.com
testdrive@thinair.com

HIPAA AICPA SOC 2