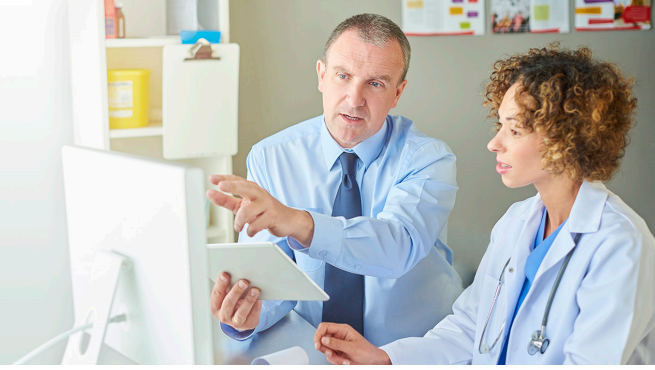
THINAIR

Safeguarding Healthcare Information



Patient Data At Risk

The healthcare industry is the second biggest victim of cybercrime with Insider and Privilege Misuse, Physical Theft and Loss, and Unintentional Actions accounting for 81% of the breaches, as per the latest Verizon 2017 Data Breach Investigation Report.

Providers were the prime target in top 10 healthcare cyber-attacks in 2016 affecting millions of patient records.

Healthcare organizations continue to struggle to protect the patients' health information. As per a recent Poneman study, eighty-nine percent of healthcare organizations had at least one data breach involving the loss or theft of patient data in the past two years, and 45 percent had more than five data breaches in the same time period.

This trend is not likely to abate any time soon as adoption of medical devices and technology, increased sharing of data for treatment, payment and operations, and the growing ransomware threat poses higher risk of data loss and theft.

81%

Breaches are privilege misuse and physical theft

#1 Target

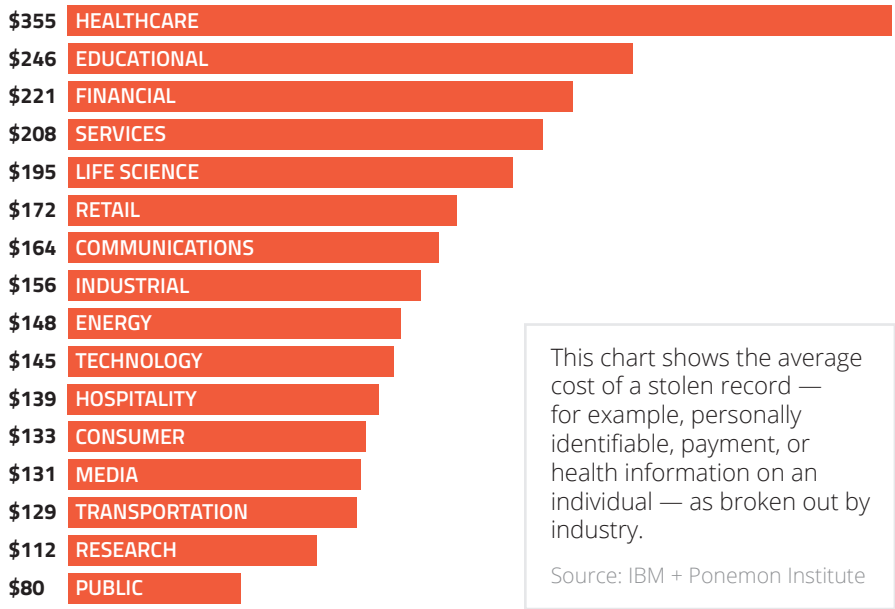
Providers are prime for healthcare breaches

45%

Organizations had more than 5 breaches in 2 years

Healthcare Breach Cost

The fact that Healthcare faces the highest cost for breach at $355 per stolen record which can include patient names, medical histories, credit card data, and social security numbers makes this even more difficult for the industry. About half of all organizations have little or no confidence that they can detect all patient data loss or theft and most of them still don't have sufficient security budget to curtail or minimize data breach incidents.



This chart shows the average cost of a stolen record — for example, personally identifiable, payment, or health information on an individual — as broken out by industry.

Source: IBM + Ponemon Institute

$6.2 billion cost of healthcare breaches over 2 years

$355
average cost of breach per healthcare record

$2.2m
average cost of a company's healthcare breach

90%
of healthcare organizations that will suffer data breaches

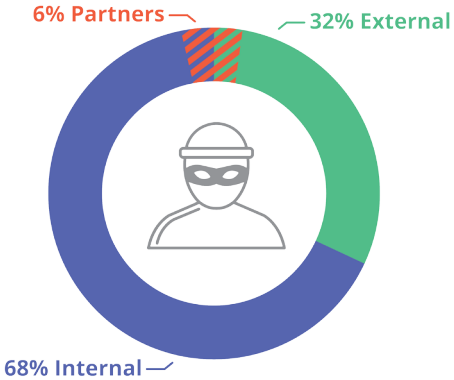
112m
electronic healthcare records breached in 2015

Time is Critical

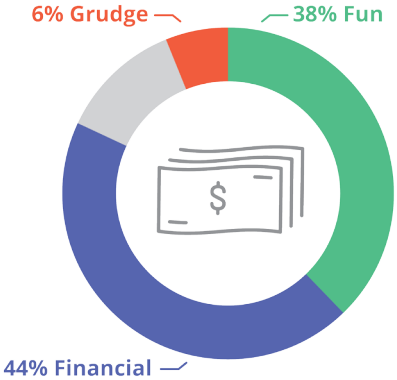
It takes an average of 201 days to identify and 70 days to contain a breach which directly impacts the total cost of a breach or security incident. Conducting investigations and forensics to determine the root cause of the data breach and the probable loss are two of the major costs besides the lawsuits, customer churn, and brand damage, the effects of which can continue for years.

Healthcare has the unenviable task of balancing protection of large amounts of personal and medical data with the need for quick access to practicioners. Internal actors are well represented with employees accessing patient data out of curiousity, or to commit identity fraud. Insider misuse is a major issue for the Healthcare industry; in fact it is the only industry where employees are the predominant threat actors in breaches.

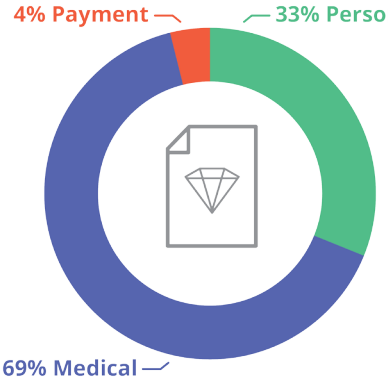
THREAT ACTORS



ACTOR MOTIVES



DATA COMPROMISED



Source: Verizon 2017 Data Breach Investigation Report

ThinAir Simplifies Data Security

ThinAir answers sophisticated questions about information creation, consumption and communication through easy to use search and analytics, tracking and reporting capabilities.

We help you quickly answer the critical questions you need to address in case a security incident or breach strikes your organization:

What happened?

Tell me who, what touched the data... in real time and historically

- A credit card number was stolen from your organization. Who accessed it and had opportunity to take it?
- A file appears on the Dark Web from your organization. How do you identify who leaked the file?
- When an employee leaves your organization how do you find out what they accessed in the 2 weeks before they left? Was something sensitive compromised?

What can happen?

Tell me what and where is my data... who can access it...

- I want to know where all my sensitive data is, what devices and users have it?
- Jerry has over 100 files on his laptop that are tagged as company confidential. How much risk is acceptable for your organization?
- Your organization has data storage and usage policies. How do you know that they are being followed?

What is happening?

Tell me if anything changes... anomaly, threshold, violation, non-compliance

- Doctor uploads sensitive data to DropBox in order to do research at home
- Assistant copies sensitive information to a local computer from an EHR system
- Someone downloads a copy of database as a csv file

You are in complete control of your incident investigation and response as you discover, analyze, scope and respond to the breach. You know exactly when there's a violation or noncompliance, with instant access to the events of interest and the entire footage of what happened.

TAKE BACK CONTROL OF YOUR DATA

Investigate Exfiltration

ThinAir allows admins to rewind the "tape" of all data interactions from real time to years into the past. Investigation can be started from any piece of data that was suspected as leaked or an application name.

Identify Insider & Privilege Misuse

ThinAir investigation capabilities can instantly identify everyone that had access and the opportunity to exfiltrate any piece of data. It reduces investigations from months to seconds.

Assess Human Error Loss

With ThinAir it is extremely easy to get the full scope of the leak as well as to see who, when and using what application interacted with the data at any point in time.

Minimize risk and safety issues in your organization while minimizing the escalating cost of breaches and fines.

Investigate

KNOW THE SOURCE, IMPACT, AND VECTOR OF EXFILTRATION... WITHIN SECONDS.

You can start your breach investigation using any attribute — file name, person, device, file hash or any file content. ThinAir will quickly search and show you all matching files, even if they were deleted and reveal the entire sequence of events, associated with the data. You can now quickly attribute the data exfiltration to a person or a process and understand the total scope of the breach, within seconds.

Assess

SENSITIVE DATA DISCOVERY AND DATA ACCESS TRACKING...ANYWHERE

ThinAir can be easily configured to monitor every information creation, access, modification, deletion or copy event across your entire organization. It automatically tags files based on content or other identifier (e.g. type, name, location). You will know where your sensitive information (e.g. patient personal information, payment information, medical data and other sensitive data) is located in your environment.

Monitor

REAL-TIME ALERTING AND REPORTS ON ANY DATA ACTIVITY...AS IT OCCURS

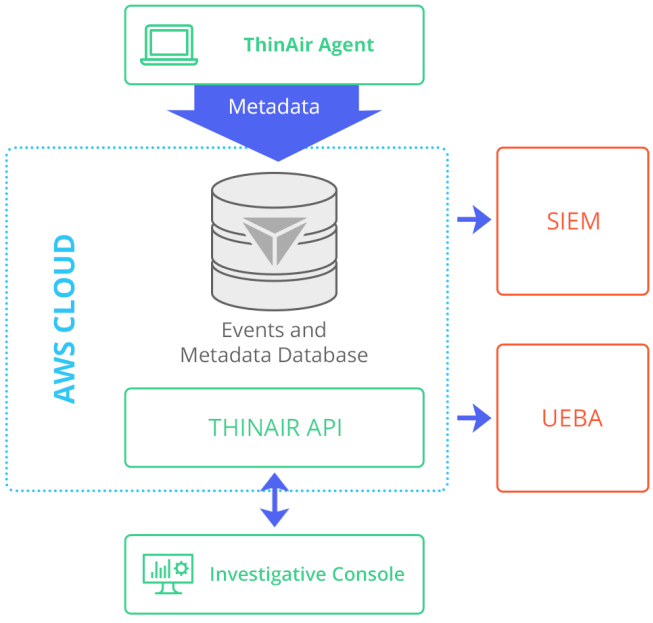
ThinAir can deliver real-time or scheduled alerts based on any query and help you keep track of when, where, how, and who accessed your data. It can also help you identify suspicious actions on your most critical data, or any violation and noncompliance.

THINAIR IS SCALABLE AND EASY TO DEPLOY

ThinAir can be deployed and functional in less than 5 minutes on any Windows or MacOS system using a lightweight kernel-level agent. The cloud-based console (AWS) stores meta-data only ensuring scalability and security while minimizing on-premises infrastructure and maintenance/support.

All information related actions are tracked and infused with metadata (application, timestamp, data elements impacted, etc). The events are immutable, timestamped and sequenced so you have complete visibility of the incident.

ThinAir is licensed for endpoint nodes and data retention, offering you complete flexibility while meeting all your needs no matter how small or large your deployment.



THINAIR

Request a demo at: **www.thinair.com**

HIPAA

AICPA SOC 2