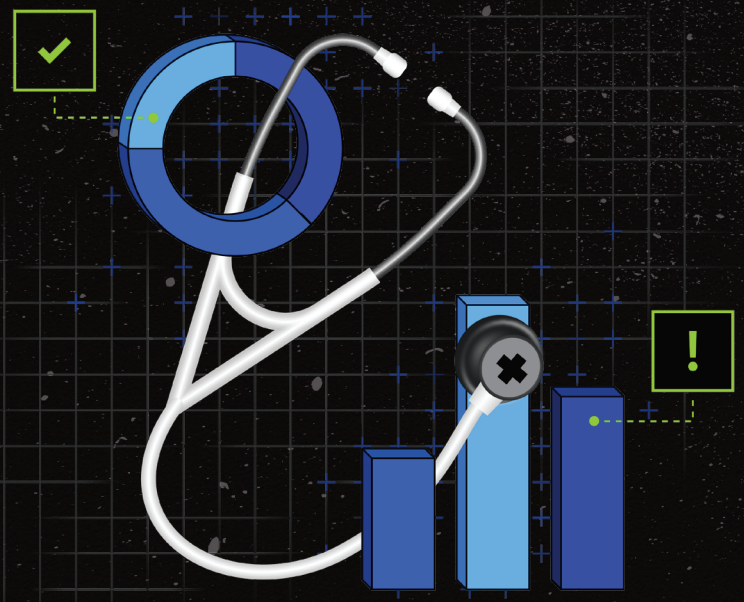
VARONIS

THE RISING THREAT OF DATA BREACHES IN HEALTHCARE



Introduction

In recent years, the healthcare sector has witnessed substantial technological advancements and an increased reliance on digital cloud-based systems for core business functions such as appointment scheduling, telehealth visits, and patient records management.

However, with these advancements comes a rise in data breaches, posing severe risks to patient privacy and organizational integrity.

Looking at some of the largest healthcare breaches in recent years, often attacks begin with compromised identities, leading to unauthorized access to sensitive personal and medical information, resulting in substantial financial and reputational damage. The increasing frequency of such incidents underscores the urgent need for a new approach to data security.

In this guide, we'll review data breach trends in the healthcare industry and discover how integrated identity and data security measures help stop threats.

Healthcare data landscape

Healthcare organizations are prime targets for cybercriminals due to the vast amounts of sensitive data they hold. **One month into 2025, healthcare organizations in twenty-one states reported being affected by cyber-attacks.** Also in January, there were several high-profile data breaches involving over 1.4 million individuals.

Another trend in the last decade showing no signs of slowing is mergers and acquisitions (M&A). Numbers have fluctuated but reports show annual M&A deal volume is nearly 70% higher than the pre-pandemic trendline. The consolidation of healthcare providers means that a single breach can now compromise the data of hundreds of thousands, or even millions, of patients. This was most evident in a January filing where a collection of two dozen senior living companies operating across multiple states succumbed to a ransomware attack that affected nearly 70,000 residents.

In all these cases, bad actors have been able to extract sensitive patient health records which includes names, addresses, social security numbers, phone numbers, email addresses, test results, treatment information, and health insurance information. As a result, these organizations are now facing two proposed class action lawsuits.

The rise of AI risks

AI will also increasingly provide value to the health industry and patients, yet complicate cybersecurity for healthcare organizations. More solutions are entering the market annually. Microsoft just announced **Dragon Copilot** for example, and Salesforce **announced** Agentforce for Healthcare in March 2025. Agentforce for Healthcare is enabling several new outcomes:

PATIENT SUMMARIES

Care coordinators and call center agents can generate comprehensive patient summaries, including conditions, allergies, and care plans, without navigating multiple tabs.

MEDICATION SUMMARIES

Provides a detailed view of all medications a patient is taking or has been prescribed.

PRE-CALL SUMMARIES

Summarizes care plans and care gaps to prepare care coordinators for more contextual conversations with patients.

PROVIDER SUMMARIES

Summarizes provider information such as specialties and working locations.

These collective summaries reduce the workloads of many healthcare professionals. However, it is imperative in 2025 for organizations to prevent improper user access to agents and improper agent access to data.

Varonis for Agentforce is the first data security solution to cover autonomous AI agents allowing security teams to monitor agent activity, detect abnormal usage, and continuously minimize blast radius.

All it takes is an identity.

With the organizations adding new cloud and AI applications regularly, we can anticipate more identity-based attacks targeting sensitive information by taking advantage of this complexity. In more than half (57%) of the cyberattacks examined by a recent Varonis **report**, attackers compromised an identity to gain access to protected environments. Healthcare organizations must prioritize monitoring sensitive data access, managing privileged identities, safeguarding credentials and permissions, and detecting abnormal behaviors to stay ahead of these threats.

READ THE FULL IDENTITY CRISIS REPORT

Download report

The largest breach in 2024 impacted 190 million patient records, and it started with one compromised account that did not have MFA required. **Identity posture and threat detection** are critical in protecting data.

By focusing on these areas, health organizations can better protect patient data, ensure compliance with regulatory requirements, and maintain the trust of their patients and partners. Implementing advanced security measures and staying vigilant against emerging threats will be crucial in navigating the evolving cybersecurity landscape.

190M **THE LARGEST BREACH IN 2024 IMPACTED 190 MILLION PATIENT RECORDS**

How Varonis secures healthcare data

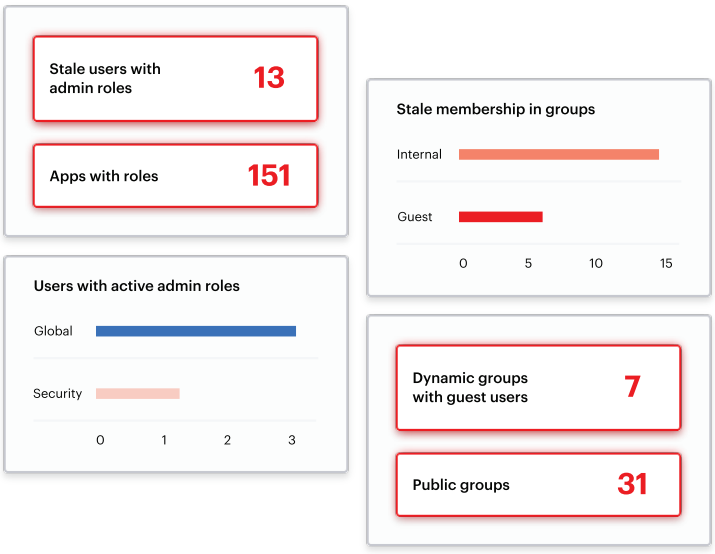
Nearly two-thirds of organizations are now multi-cloud with cloud data expected to surge even more. This growth will result in more complex cloud environments, creating additional attack vectors and putting more sensitive patient data at risk.

In this threat environment, organizations must be protected through every phase of a cyberattack's lifecycle, from the initial breach to data exfiltration. Varonis enables security teams to stay ahead of bad actors with a data-centric approach to security that can stop attackers at every step in every cloud environment.

SAFEGUARDING IDENTITIES AND RIGHT-SIZING PERMISSIONS

Most cyberattacks start with an identity. With that in mind, the first step is to unravel permissions structures and ensure that only the right people can access important files, folders, and mailboxes. **Varonis' identity protection capabilities** seamlessly map identities and users across cloud, SaaS, and data centers in a single interface. Varonis enables Zero Trust at scale by giving visibility into identity risks and vulnerabilities, automatically remediating access misconfigurations for least privilege, and reducing the attack surface.

For instance, Varonis can automatically remove permissions and memberships from stale or disabled users to resources and remediate inconsistent permissions amongst varying identities. The platform is able to find overexposed resources and automatically remediate permissions and proactively mitigate the risk.



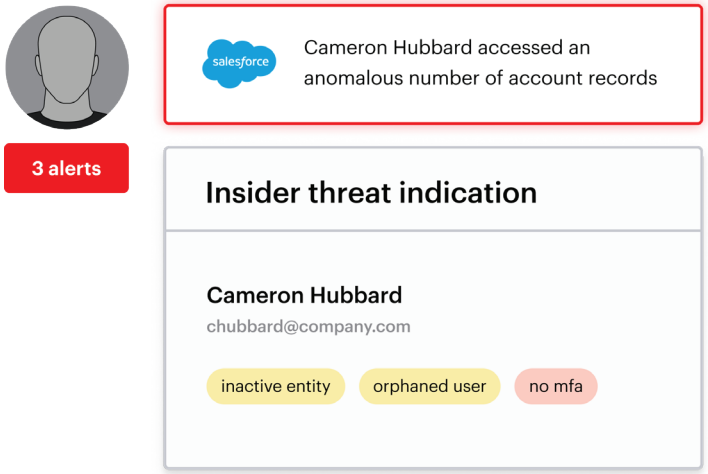
Detecting abnormal behavior and insider threats

Once a bad actor with legitimate credentials is in your environment, it can be incredibly challenging to identify the threat.

Varonis provides a central dashboard that shows potential threats, risks, and top alerted identities and maps those against the MITRE attack framework. In addition, users can also benefit from a posture dashboard aligned to each identity provider like Microsoft Entra ID, Okta, and on-premises active directory. In a single pane, users can discover identity-related misconfigurations to improve the overall posture of managed identities.

Users can also benefit from a unified alerts dashboard that intuitively combines identity threats with data access threats for complete context. Varonis uses behavior-based detections to alert you to abnormal behaviors that indicate a bad actor in your environment. Hundreds of expert-built threat models automatically detect anomalies, alerting you to unusual file access activity, email send/receive actions, permissions changes, and geo-hopping.

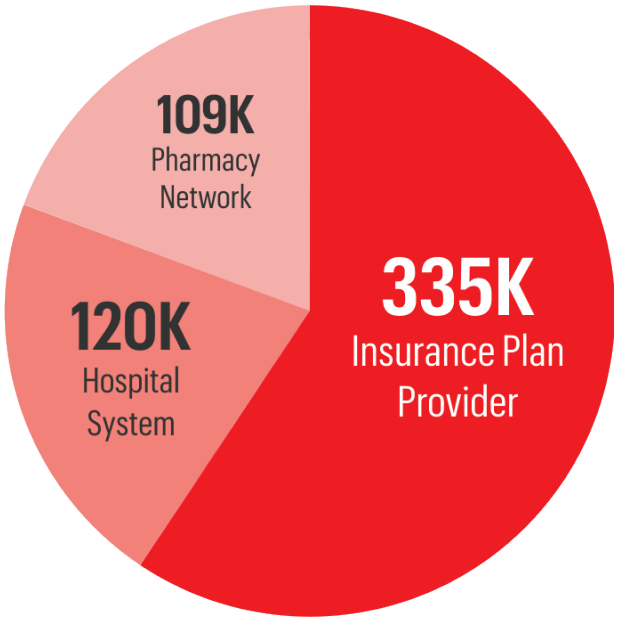
You can track threats and conduct advanced investigations with a complete forensics log of actions, including file access, email activity, and permissions changes.



Don’t wait for a breach to occur.

Cyberthreat groups have shown little discretion on who they attack. The top three breaches reported to OCR in the month of February (1. 335K, 2. 120K, 3. 109K) were from an insurance plan provider, hospital system, and pharmacy network respectively.

TOP THREE BREACH VERTICALS IN FEBRUARY 2025



The healthcare sector’s reliance on digital systems and the increasing frequency of data breaches underscores the urgent need for a new approach to data security. By adopting integrated identity and data security measures, healthcare organizations can protect sensitive patient information, comply with regulatory requirements, and maintain the trust of their patients and partners.

SOURCES

SecurityWeek.com. (2025, February). 1 Million Impacted by Data Breach at Connecticut Healthcare Provider.

bankinfosecurity.com. (2025, January). Nursing Home, Rehab Chain Says Hack Affects Nearly 70,000.

hipaajournalcom. (2025, February). Asheville Eye Associates Hacking Incident Impacts 193K Patients.

hipaajournal.com. (2024, July 12). Tens of Thousands of Residents Affected HCF Management Cyberattack.

VARONIS

Ready to experience the Varonis difference?

Reduce your risk without taking any. Contact our team to learn what will be covered in your **free** Data Risk Assessment.

Get your assessment

ABOUT VARONIS

Varonis (Nasdaq: VRNS) is the leader in data security, fighting a different battle than conventional cybersecurity companies. Our cloud-native Data Security Platform continuously discovers and classifies critical data, removes exposures, and detects advanced threats with AI-powered automation.

Thousands of organizations worldwide trust Varonis to defend their data wherever it lives — across SaaS, IaaS, and hybrid cloud environments. Customers use Varonis to automate a wide range of security outcomes, including data security posture management (DSPM), data classification, data access governance (DAG), data detection and response (DDR), data loss prevention (DLP), and insider risk management.

Varonis protects data first, not last. Learn more at www.varonis.com.