2024 TREND REPORT

State of Healthcare IT and Print Management

tricerat®

Introduction

As the global healthcare sector confronts a 156% surge in cybersecurity challenges in 2024, the focus intensifies on fortifying IT security frameworks. This escalation highlights an area often overlooked by security protocols: Print Management.

With 60% of all hospital printing stemming from EHR/EMR systems and the stakes of breaches—both financial and operational—rising, healthcare organizations must ask a critical question:

Are we among the 61% of organizations facing print-related data loss this year?

What's Inside

2024 Health IT Trend Report

TREND #1
Cyber Attacks in Healthcare Increased by 156% in 2023

156%

TREND #2
Financial Toll of Data Breaches hits >$7M

>$7M

TREND #3
Global Healthcare's #1 Tech Investment is in Security IT

#1

TREND #4
61% of IT Leaders Report Data Loss Due to Unsecured Printers

TREND #5
Physical Copies are Responsible for 27% of All IT Security Incidents

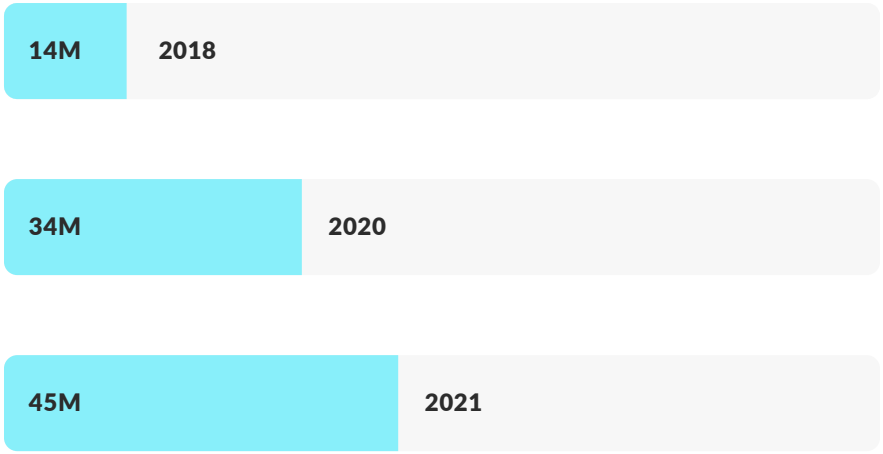
TREND #6
Printing Increases by 11% Post-EMR/EHR Adoption

TREND #7
39% of IT Leaders are Struggling with Printer Security

Cyber Attacks in Healthcare Increased by 156% in 2023

2023 saw a peak in healthcare data breaches, with two incidents occurring per day. With 93% of healthcare organizations reporting breaches in the last three years and the sector comprising 27% of all incidents last year, the critical need for comprehensive measures has never been greater.

In 2021, healthcare data breaches affected 45 million people. This number has tripled in just three years. [1]



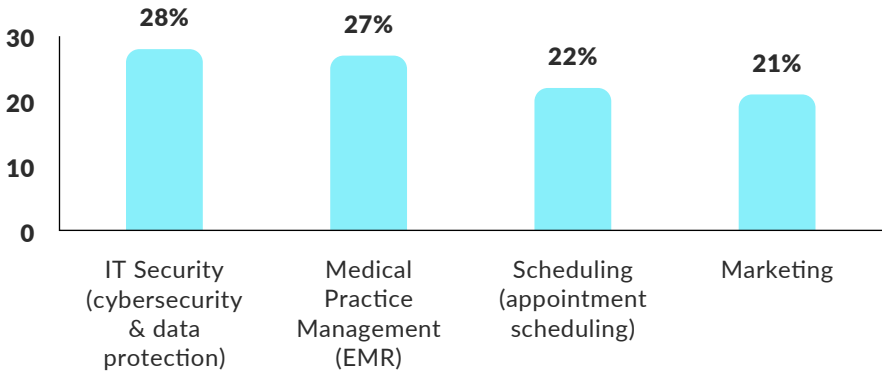
Financial Toll of Data Breaches Hits >$7M

In 2023, healthcare data breaches cost the sector $7.13M, averaging $150 per compromised PHI record. This highlights the sector's substantial financial, operational, and reputational risks and urgency for security protocols and infrastructure to mitigate risks and protect sensitive data.

Global Healthcare's #1 Tech Investment is in Security IT

Responding to growing threats, 28% of healthcare professionals prioritize IT Security as their top tech investment in 2024. The healthcare cybersecurity market is also expected to grow from $8B in 2023 to $17.24B by 2031, reflecting the heightened demand for cybersecurity and data protection solutions.

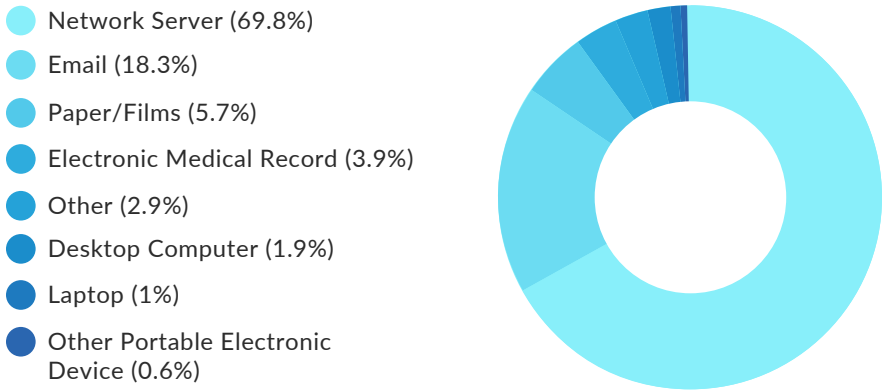
Top priority software for investment in 2024 [2]



Network Printers are Critical Points of Vulnerability

Devices and hardware, like printers, account for half of the cyber attacks in healthcare. Often overlooked by security protocols, multifunction printers with cloud and wireless capabilities are vulnerable to unauthorized access or entry points to broader network intrusions. **In fact, 61% of IT leaders report data losses linked to unsecured printers.**

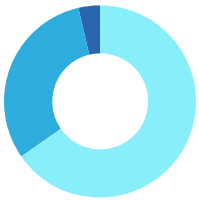
Location of Breached Protected Health Information [3]



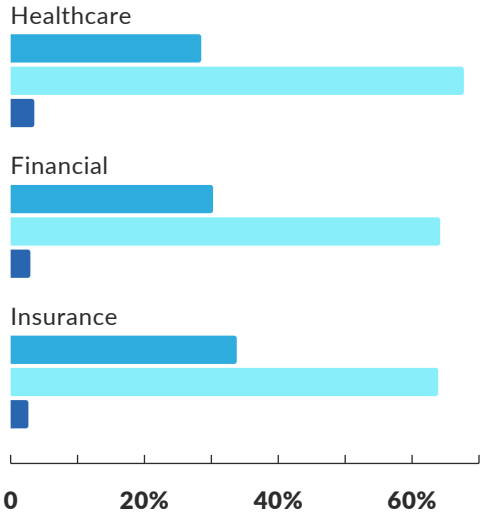
The Persistent Risk of Paper Documents

Despite advancements in digital health records, paper documents continue to present substantial security challenges. **In 2023, physical copies were responsible for 27% of IT security incidents. Printing errors also contribute to 15% of all HIPAA breaches**, indicating the ongoing necessity for stringent print management policies to ensure secure and compliant handling and disposal of documents.

Incident Category
(By Industry)

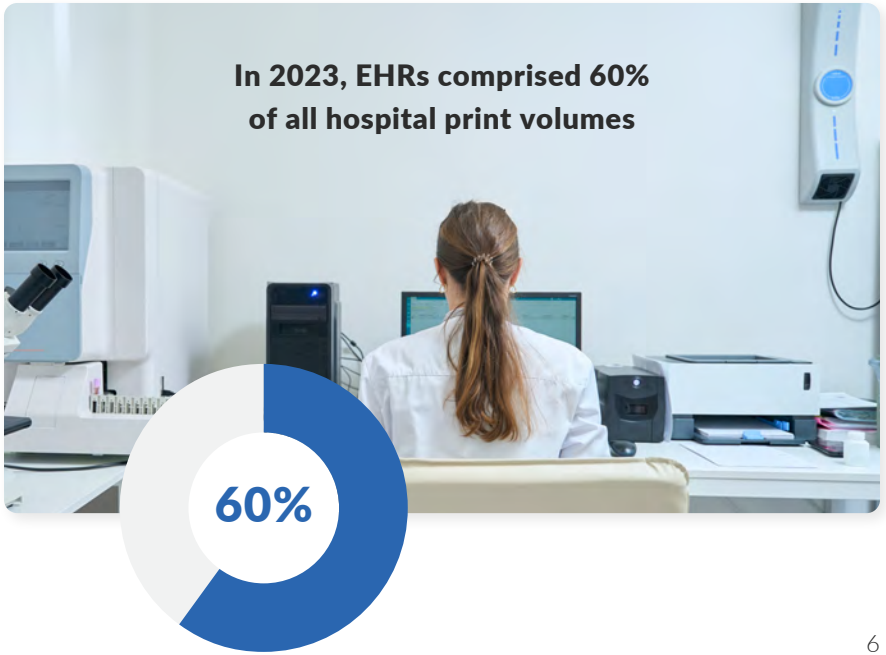


- Electronic (64.09%)
- Paper (30.39%)
- Verbal or Visual (3.52%)



Print Activities Increase After EHR/EMR Implementation

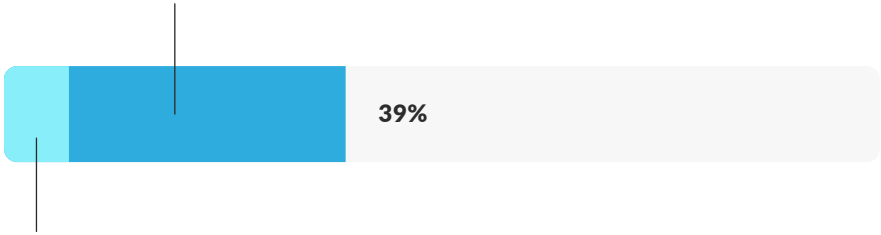
Despite the move towards digital records, healthcare has a surprising uptick in printing. In 2023, EHRs comprised 60% of all hospital print volumes, marked by an 11% rise in user printing activities following EHR/EMR implementation. This highlights the need for secure print management solutions that integrate with EHR systems to secure both digital and printed formats of the patient care process.



Healthcare's Print Security Preparedness Gap

With 39% of IT leaders struggling with printer security and only 19% confident in preventing breaches, healthcare is notably unprepared for print-related threats. With inpatient data set to outpace ICU data by 2027, the sector must upgrade its security practices to manage and protect growing data volumes, emphasizing the critical gap in current print management strategies.

39% of IT leaders struggle with printer security



And only 19% of those are confident in preventing breaches

Stronger Security and Compliance through Print Management in 2024

Understanding Printer-Related Risks

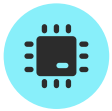
In 2024, the cybersecurity landscape reveals that networked printers extend beyond mere output devices; they are sophisticated machines with operating systems, storage, and software—components that, if not secured, become lucrative targets for hackers. The pathways for unauthorized access include:

Ports: Unsecured USB or network ports are gateways for uploading malicious code to exfiltrate data.

Network Intercepts: Data in transit, such as faxed or sent documents, can be intercepted.

Misconfigurations and Cloud Complexities: Incorrect settings and cloud printing services add layers of risk.

Storage Media: Unprotected drives or hard disks within printers can store sensitive information, making them targets for data theft.



Firmware Vulnerabilities: Unsecured firmware on startup can compromise printers, posing threats to entire networks.

Physical Document Exposure: Documents left uncollected on printers pose significant security risks, potentially exposing sensitive information.

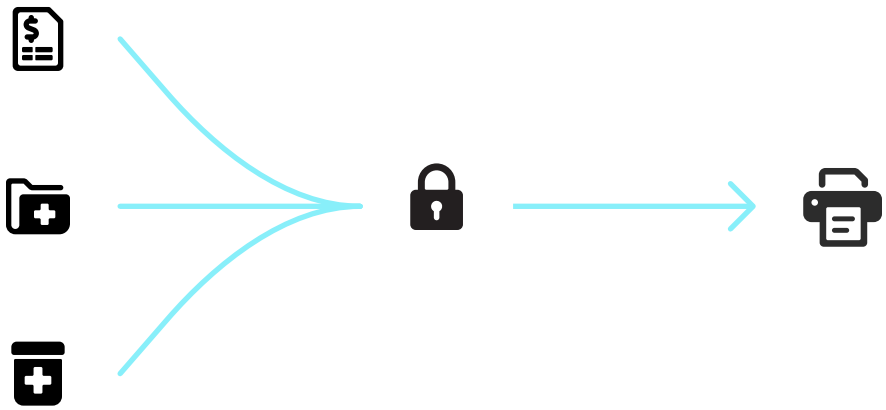
Absence of a Security Strategy: Lack of comprehensive printer security planning leaves gaps in the overall cyber defense posture.

HIPAA-Compliant Printing Checklist

- **HITRUST Common Security Framework Certified**
- **HIPAA Compliant Print Vendors**
- **Print and Mail Security Audits**
- **Secure Data Transfer Portals**
- **Secure Digital and Inkjet VDP Technology**

Elevating Printer Security with Compliance-Driven Solutions

In the ever-tightening regulatory environment of healthcare IT, adopting a security and compliance-focused print management solution is essential. A solution partner with a well-designed security architecture not only safeguards sensitive data but also streamlines adherence to stringent healthcare standards.



Strategic Security Features of Advanced Print Management

ZeroTrust Framework

This security approach is rooted in the principle of "never trust, always verify," offering uncompromising access control and robust user authentication mechanisms that form the bedrock of data integrity and confidentiality.

TLS 1.3 Encryption

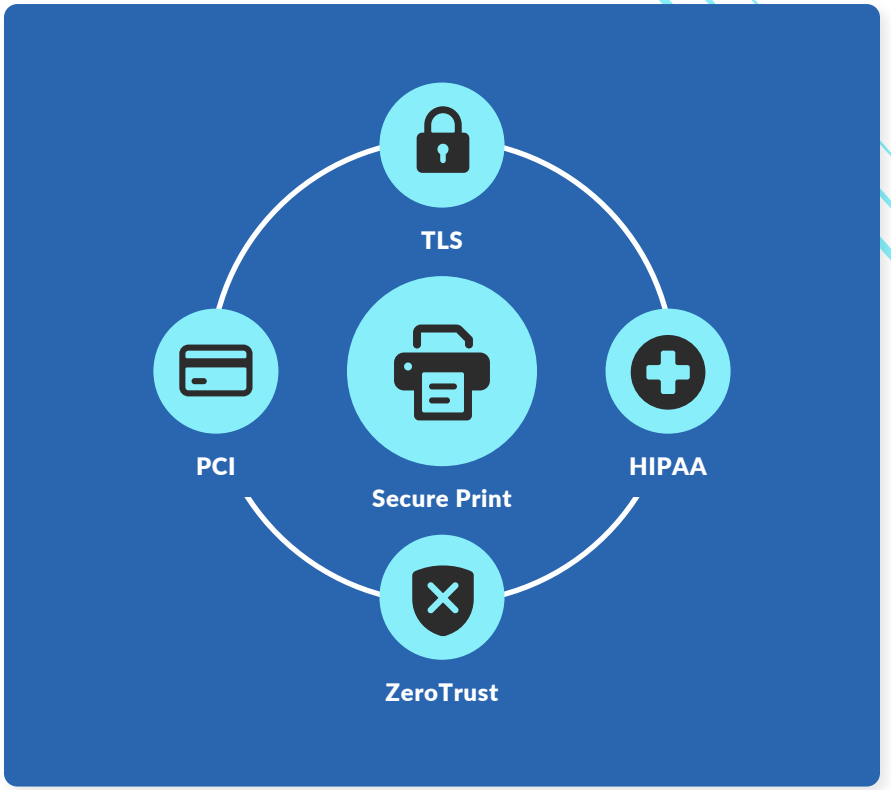
As the newest standard in encryption technology, TLS 1.3 is pivotal in ensuring that data in transit to and from print devices is shrouded in a virtually impenetrable layer of security, thereby maintaining the sanctity of sensitive information.

Cipher Suite Excellence

A meticulously curated suite of encryption algorithms is deployed to thwart attempts at unauthorized data decryption, forming a formidable defense against an array of sophisticated cyber threats that lurk in the digital shadows.

SSL Protocol Integration

Implementing these secure protocols governs data transmission across networks, ensuring that every byte of information is encapsulated within a protective shell, defending against the pervasive risks of data breaches.



In the ever-tightening regulatory environment of healthcare IT, a print management solution partner with a well-designed security architecture not only safeguards sensitive data but also streamlines adherence to stringent healthcare standards.

Tricerat's Security Suite for Modern Healthcare IT

Faced with the complex printer security challenges of 2024, Tricerat's Security Suite offers a robust solution for healthcare.

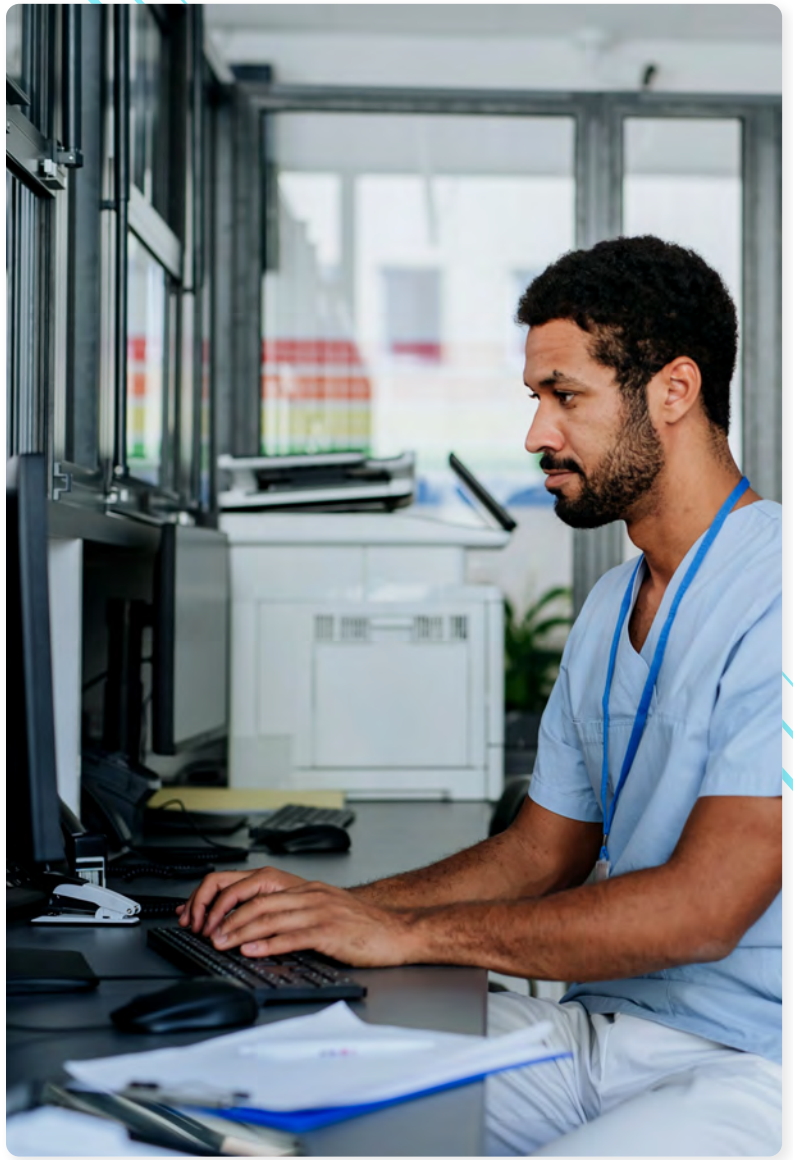
With features designed to address each identified risk—ranging from ZeroTrust encryption and multifactor authentication to comprehensive policy management—Tricerat positions healthcare facilities to safeguard against print-related data breaches and compliance violations.

By adopting our advanced security measures, tech leaders can improve defense mechanisms and ensure the integrity of patient data in an increasingly multifaceted healthcare IT ecosystem.

Secure Your Print Environment with Tricerat's Security Suite, your blueprint for comprehensive print management security.

Get a Demo

See our Healthcare Solutions



tricerat®

Sources: [1] 2021 H2 Healthcare Data Breach Report. [2] Gartner Digital Markets' 2024 Tech Trends Survey. [3] 2024 The HIPAA Journal