VERITI

THE STATE OF HEALTHCARE CYBERSECURITY 2025

A Veriti Research Report

VERITI.AI

Table of Contents

Executive Summary

The Attack Landscape Under the Scope

Diagnosing the Threats

Breaking Down Exposures

Severely Vulnerable Medical Devices and Applications

Notable Healthcare Events in 2024

Veriti's Predictions and Challenges for 2025

EXECUTIVE SUMMARY

This report, conducted by the Veriti research team, provides a comprehensive analysis of healthcare cybersecurity in 2024, offering critical insights to shape strategies for 2025. Over the past year, healthcare organizations faced an alarming rise in cyberattacks, driven by ransomware groups leveraging sophisticated methods to exploit systemic vulnerabilities.

From IoT misconfigurations to cloud security challenges, the findings in this report underscore the urgent need for proactive cyber defenses.

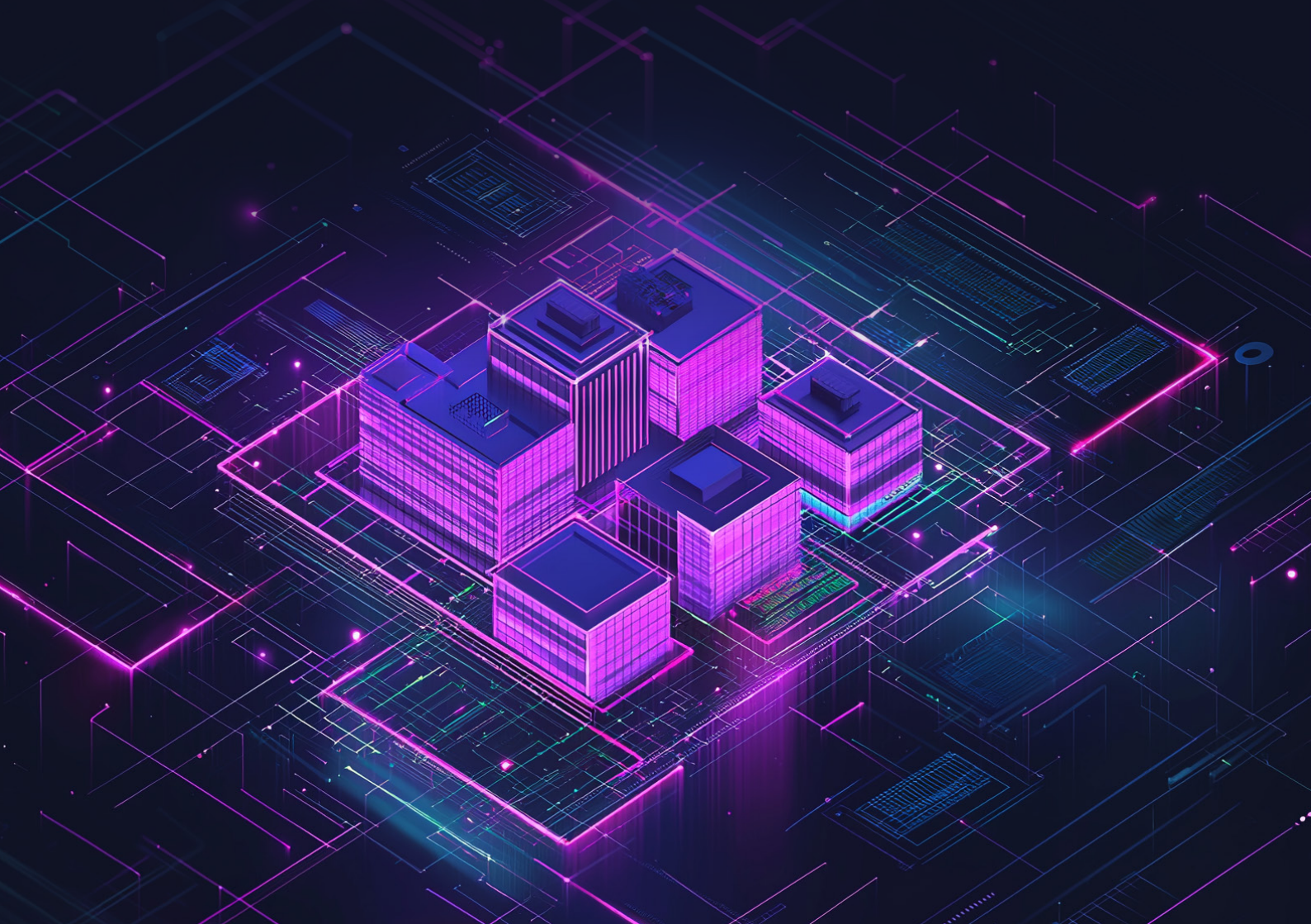
Key findings include:

Rising Threats
Nearly 400 healthcare organizations in the U.S. reported cyberattacks in 2024, driven by ransomware groups such as LockBit 3.0, ALPHV/BlackCat, and BianLian.

Critical Vulnerabilities
Persistent OS and endpoint misconfigurations, combined with outdated medical devices, expose critical infrastructure to exploitation.

Notable Events
High-profile breaches like the ALPHV attack on Change Health and the exploitation of Mirth Connect highlight the urgency of addressing security gaps.

Emerging Trends
The rise of IoT devices, AI integration, and cloud-based PACS systems introduce new attack



THE ATTACK LANDSCAPE UNDER THE SCOPE

The healthcare sector in the United States has experienced a staggering rise in cyberattacks, with nearly 400 healthcare organizations reporting incidents in the past year alone. This alarming trend highlights the vulnerabilities in critical infrastructure and the growing sophistication of attackers.

Attacks on Third-Party Providers on the Rise:

Cybercriminals are increasingly targeting third-party healthcare service providers and suppliers. These entities often have weaker defenses compared to larger healthcare organizations, making them attractive targets. Compromising these suppliers can create ripple effects, exposing sensitive patient data and disrupting healthcare operations on a broader scale.

Collaboration Between Hostile Nation-States and Ransomware Groups:

Emerging evidence points to collaborations between ransomware groups and nation-state actors. These partnerships increase the sophistication and scale of attacks, leveraging advanced techniques to bypass traditional defenses. Healthcare organizations remain a primary target due to the critical nature of their services and the high-value data they store.

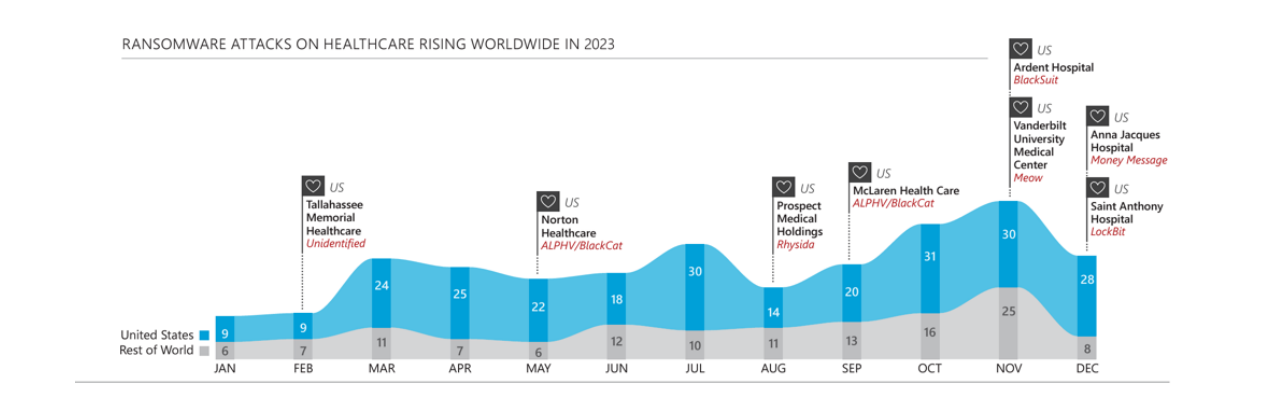
Geopolitical Risks and Their Impact:

Geopolitical tensions continue to drive cyber activity in the healthcare sector. Adversaries use these tensions to disrupt national healthcare operations and steal sensitive information, posing risks that extend beyond financial losses to patient safety and national security.

New Regulations to Strengthen Cybersecurity:

In response to this growing threat landscape, new regulations are being implemented to enforce stronger cybersecurity standards in healthcare. These initiatives aim to ensure that organizations proactively address vulnerabilities, secure sensitive patient data, and reduce the risk of operational disruptions.

The provided graph underscores the significant rise in ransomware attacks on healthcare worldwide, with the United States disproportionately affected. Notable spikes in attacks occurred in October and November 2023, correlating with high-profile incidents at organizations like Vanderbilt University Medical Center and Ardent Hospital.

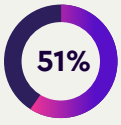


$3.5m *The average cost of a data breach for healthcare organizations*

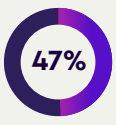
$398 *average cost per exposed record*

of healthcare organizations lack confidence in detecting and resolving data breaches.

lack policies for unauthorized data access prevention.



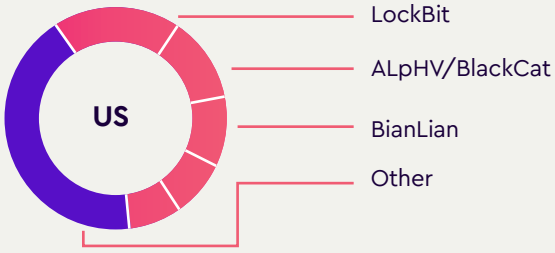
lack the technologies needed for breach prevention.



lack the expertise to resolve breaches effectively.

DIAGNOSING THE THREATS

Healthcare organizations in the U.S. continue to face relentless cyberattacks, with ransomware groups such as LockBit 3.0, ALPHV (BlackCat), and BianLian dominating the threat landscape. These groups target vulnerabilities across IT ecosystems, often leveraging unpatched systems, weak credentials, and well-known attack tactics.



CVE/TTP	Ransomware Group
CVE-2021-44228 (Log4Shell)	LockBit 3.0, ALPHV (BlackCat)
CVE-2018-13379 (Fortinet SSL VPN)	LockBit 3.0, BianLian
CVE-2022-29464 (Wavlink, opennas web server)	ALPHV (BlackCat)
CVE-2019-19781 (Citrix ADC)	ALPHV (BlackCat), BianLian
CVE-2020-1472 (Zerologon)	LockBit 3.0, ALPHV (BlackCat)
Exploiting RDP and weak credentials	LockBit 3.0, BianLian
Double Extortion (data encryption + data theft)	LockBit 3.0, ALPHV (BlackCat), BianLian
Use of Cobalt Strike	LockBit 3.0, ALPHV (BlackCat)
Phishing campaigns for initial access	BianLian, ALPHV (BlackCat)
Living off the land (LOLBins)	LockBit 3.0, ALPHV (BlackCat), BianLian

Commonality Between CVE/TTP and Ransomware Groups

The table highlights the shared tactics and vulnerabilities exploited by ransomware groups to infiltrate healthcare systems:

- LockBit 3.0, ALPHV, and BianLian repeatedly exploit well-known CVEs such as Log4Shell (CVE-2021-44228), Zerologon (CVE-2020-1472), and Citrix ADC (CVE-2019-19781).
- These groups also rely heavily on Remote Desktop Protocol (RDP) exploitation, phishing campaigns, and living off the land (LOLBins) techniques to bypass detection.
- Double extortion tactics, encrypting data and demanding ransom while threatening to release stolen data, are common among all three groups.

Interesting Attacks in 2024

A notable campaign in 2024 involved an unknown attacker targeting smaller healthcare associations by exploiting vulnerabilities in open-source tools such as the DoctorAppointmentSystem SQL Injection Vulnerability (CVE-2021-27314, CVE-2021-27319, CVE-2021-27320). IP Address Identified: 185.23.253.150

These attacks underline the importance of securing all healthcare institutions, not just major hospitals, as attackers increasingly exploit open-source solutions widely used by smaller providers.

Key Statistics and Trends in Ransomware Attacks

Veriti research found that from January to October 2024, there were 149 ransomware attacks on healthcare organizations worldwide, with 52% occurring in the United States. This is a concern for large healthcare institutions but also for smaller institutions that must prioritize cybersecurity, as their reliance on less mature, open-source tools often makes them prime targets.

149 ransomware attacks on healthcare organizations worldwide, with 52% occurring in the United States.

Attack Groups -

ThreeAM	Cloak	RansomHub
BianLian	INC	LockBit
Medusa	RansomHouse	Qilin
BlackSuit	Mad Liberator	Rhysida
Hunters International	Meow	Cicada3301
NoName	Daixin Team	DragonForce
Dispossessor	Everest	Akira
Black Basta	Abyss	Embargo
8Base	Clop	Phobos
ALPHV	BlackCat	Donut

TOP 6 Attack Groups -

20% of attackers are unknown.

Ransom Demands:

$7m
Average ransom

$100
Highest demand

Global Impact: Healthcare accounts for 17% of all ransomware attacks across industries, emphasizing its status as a top target.

BREAKING DOWN EXPOSURES

Hospitals remain highly vulnerable to both outdated configurations and unpatched vulnerabilities, which create exploitable attack surfaces for ransomware groups and cybercriminals.

Active Vulnerabilities in HealthCare

These vulnerabilities, compounded by misconfigurations, leave hospitals exposed to a wide range of exploits and attacks, emphasizing the urgent need for patch management and configuration hardening strategies. The table below illustrates the prevalence of active vulnerabilities across hospitals:

CVE	% of Hospitals Affected
CVE-2021-1675	45%
CVE-2021-34527	42%
CVE-2022-26809	40%
CVE-2023-21554	39%
CVE-2022-34721	36%
CVE-2022-34713	36%
CVE-2022-30190	31%
CVE-2022-26923	26%
CVE-2022-41128	22%
CVE-2022-21971	21%

OS Misconfigurations

The analysis highlights significant misconfigurations at the OS level that are commonly exploited by ransomware groups like ALPHV/BlackCat and LockBit.

NTLMV2 AUTHENTICATION PROTOCOL
Enabled on 1,053 hosts, this setting is leveraged for privilege escalation and lateral movement within networks.

WINDOWS DEFENDER SMARTSCREEN DISABLED: Affecting 1,032 hosts, this increases exposure to phishing campaigns, exploited by groups like LockBit and Ryuk.

MICROSOFT WINDOWS SUPPORT DIAGNOSTIC TOOL (MSDT): Enabled on 947 hosts, it has been targeted by ALPHV and other groups via the Follina vulnerability.

These misconfigurations expose critical weaknesses, making hospitals prime targets for credential harvesting, malware deployment, and unauthorized network access.

OS	Hosts	Ransomware Group reference
NTLMv2 Authentication Protocol is enabled	1053	One ransomware group that has been observed exploiting NTLMv2 authentication is the ALPHV/BlackCat group. They have employed NTLM relay attacks in their operations, leveraging weaknesses in the NTLM authentication protocol to gain elevated privileges within compromised networks. While this doesn't indicate a direct use of NTLMv2 as part of their ransomware payload, these types of attacks exploit the protocol's weaknesses to aid in lateral movement and privilege escalation.

Windows Defender SmartScreen is Disabled	1032	Microsoft Defender SmartScreen helps you browse more safely in Microsoft Edge by: Alerting you to suspicious web pages: As you browse the web, SmartScreen analyzes web pages and determines if they might be suspicious. **LockBit**: The LockBit group has been known to use phishing websites to lure victims into downloading malicious payloads disguised as legitimate software or documents. They often exploit social engineering techniques to convince users to interact with the phishing sites. **Ryuk**: Ryuk ransomware operators have used phishing websites and emails as a primary method to gain initial access. Their phishing campaigns often involve tricking users into downloading malicious attachments or visiting compromised sites.
Microsoft Windows Support Diagnostic Tool (MSDT) is enab	947	**ALPHV/BlackCa**t: This group has used vulnerabilities like Follina to deliver malicious payloads, including ransomware, through phishing attacks and malicious documents that trigger the MSDT exploit. **QakBot (QBot**): While QakBot is primarily a banking Trojan, it is often used as a delivery mechanism for ransomware. It has been observed exploiting MSDT vulnerabilities to spread ransomware payloads like Conti and BlackBasta. **LockBit**: While there is less direct evidence of LockBit exploiting MSDT specifically, the group is known to utilize a variety of exploits in their phishing campaigns,
Disable AllowInsecureGuestAuth	941	**The Vice Society** ransomware group has been observed using the AllowInsecureGuestAuth setting to gain access to vulnerable systems. This setting, if enabled, allows unauthenticated access to shared folders in a Windows environment, which can be exploited by ransomware groups to move laterally across a network and gain access to sensitive files.
EnableVirtualization Turned Off	883	**The BlackByte** ransomware group has been reported to exploit systems where Virtualization-Based Security (VBS) or Hyper-V is turned off. When EnableVirtualization is disabled or not configured, it allows ransomware actors to bypass security mechanisms that rely on virtualization-based protections, such as Credential Guard or Secure Boot.

Endpoint Misconfigurations

Endpoint misconfigurations represent another major area of risk, directly impacting an organization's ability to prevent ransomware propagation.

LACK OF EDR PROTECTION
Numerous hosts lack active endpoint detection and response (EDR) despite having the tools installed, leaving them vulnerable to ransomware like LockBit and ALPHV.

VOLUME SHADOW COPY AND RECOVERY PROCESSES: Misconfigurations affecting 22% of hosts allow attackers to disable recovery options, ensuring encryption impact.

QUARANTINE ON WRITE DISABLED
Impacting 35% of hosts, this prevents isolation of malicious files, increasing the likelihood of full encryption by ransomware.

These endpoint vulnerabilities underscore the importance of consistent configuration management and proactive monitoring to limit ransomware impacts.

EDR Protection	Hosts with no active protection, even though the installed EDR supports protection.	Ransomware Group reference
Quarantine on Write	35% of hosts	This feature can block ransomware families like LockBit, ALPHV/BlackCat, Ryuk, Maze, and REvil, which often rely on creating or modifying files during encryption processes. Quarantine on Write would prevent the malware from successfully encrypting files by isolating the malicious payload before it can execute fully.
Volume Shadow Copy	22%	**LockBit**: Known for deleting Volume Shadow Copies to prevent file recovery, LockBit attempts to use the vssadmin delete shadows or wmic commands to remove these backups. **ALPHV/BlackCat**: Like many ransomware families, BlackCat also attempts to delete Volume Shadow Copies to ensure that the victim cannot use Windows' built-in recovery capabilities to restore files.
Suspicious Processes	21%	**LockBit**: LockBit and similar ransomware often spawn suspicious processes such as vssadmin.exe, wbadmin.exe, or wmic.exe to delete Volume Shadow Copies and disable system recovery. Blocking these processes can stop the ransomware from preventing data recovery. **Ryuk**: Known to use tools like taskkill.exe to terminate security-related processes and services before encryption. Suspicious process monitoring can detect and block these actions. **ALPHV/BlackCat**: This ransomware runs PowerShell and batch scripts to execute payloads and escalate privileges. Detecting and blocking unexpected PowerShell processes can stop the attack.

Force ASLR	17%	**LockBit, ALPHV/BlackCat, and Ryuk**: These ransomware families may try to exploit system or application vulnerabilities as part of their attack chain. By enabling Force ASLR, the memory layout is randomized, making it much harder for these ransomware variants to predictably exploit a vulnerability to gain control over a system. **Maze and REvil:** Both of these ransomware groups have used exploits in their past campaigns. Exploit-based payloads benefit from predictable memory locations to carry out their attacks. Force ASLR significantly reduces the likelihood of these payloads successfully hijacking the control flow of a vulnerable application.
SEH Overwrite Protection	12%	**WannaCry and NotPetya**: These ransomware families relied on exploiting vulnerabilities in Windows systems (such as EternalBlue) to spread. While SEH Overwrite Protection doesn't directly stop the SMB exploit they used, many ransomware variants also rely on buffer overflow or memory corruption vulnerabilities, where SEH overwrite could be a factor. SEH protection mitigates certain stages of these exploits, limiting the ransomware's ability to use this tactic for escalation. **Maze and REvil:** Known for using sophisticated exploit chains to gain access and deliver payloads, some ransomware groups rely on SEH overwriting as part of their attack methodology. SEH Overwrite Protection would prevent these exploits from executing reliably.

SEVERELY VULNERABLE MEDICAL DEVICES AND APPLICATIONS

Healthcare systems are increasingly reliant on medical devices and applications to deliver critical services. However, the growing interconnectivity and reliance on outdated or misconfigured devices create significant vulnerabilities that ransomware groups and other threat actors exploit.

Exposed and Vulnerable Medical Devices

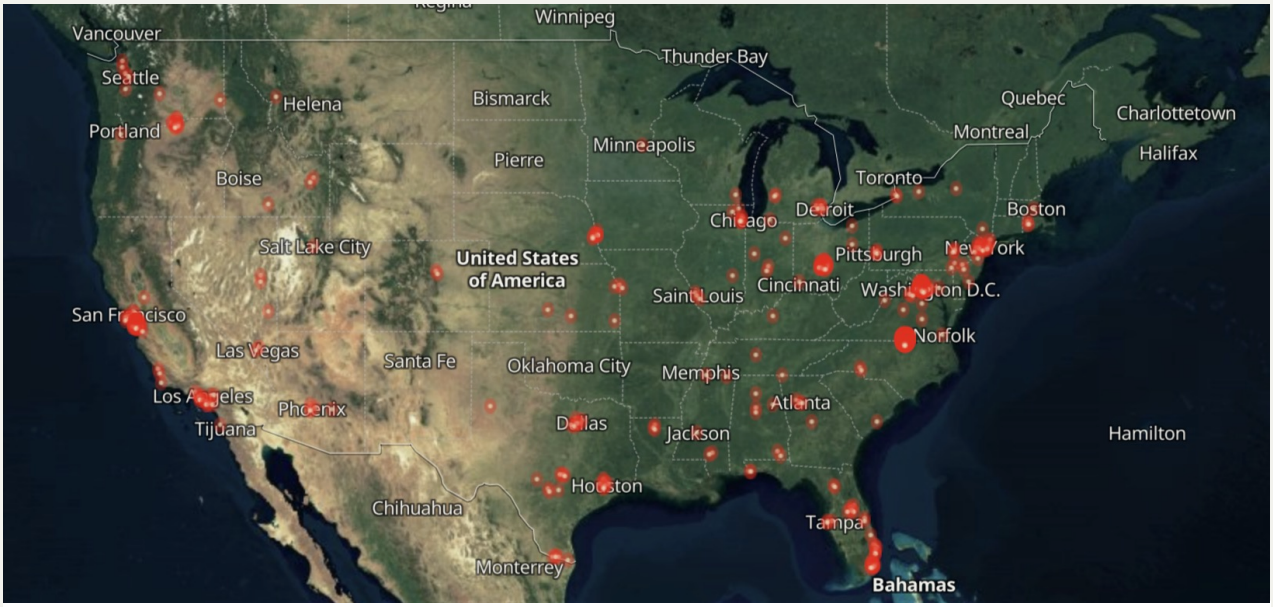
The map above illustrates the widespread exposure of vulnerable healthcare devices across the United States, emphasizing the need for immediate action. Many of these devices run on outdated software or are misconfigured, providing easy entry points for attackers.

1. PACS Systems and DICOM Protocol
Uses: PACS (Picture Archiving and Communication Systems) leverage the DICOM protocol to store and share medical images like X-rays and MRIs.

Misuses: Threat actors exploit unsecured DICOM systems to manipulate or extract sensitive patient data, potentially disrupting diagnostic workflows.

2. Drystar Medical Printers

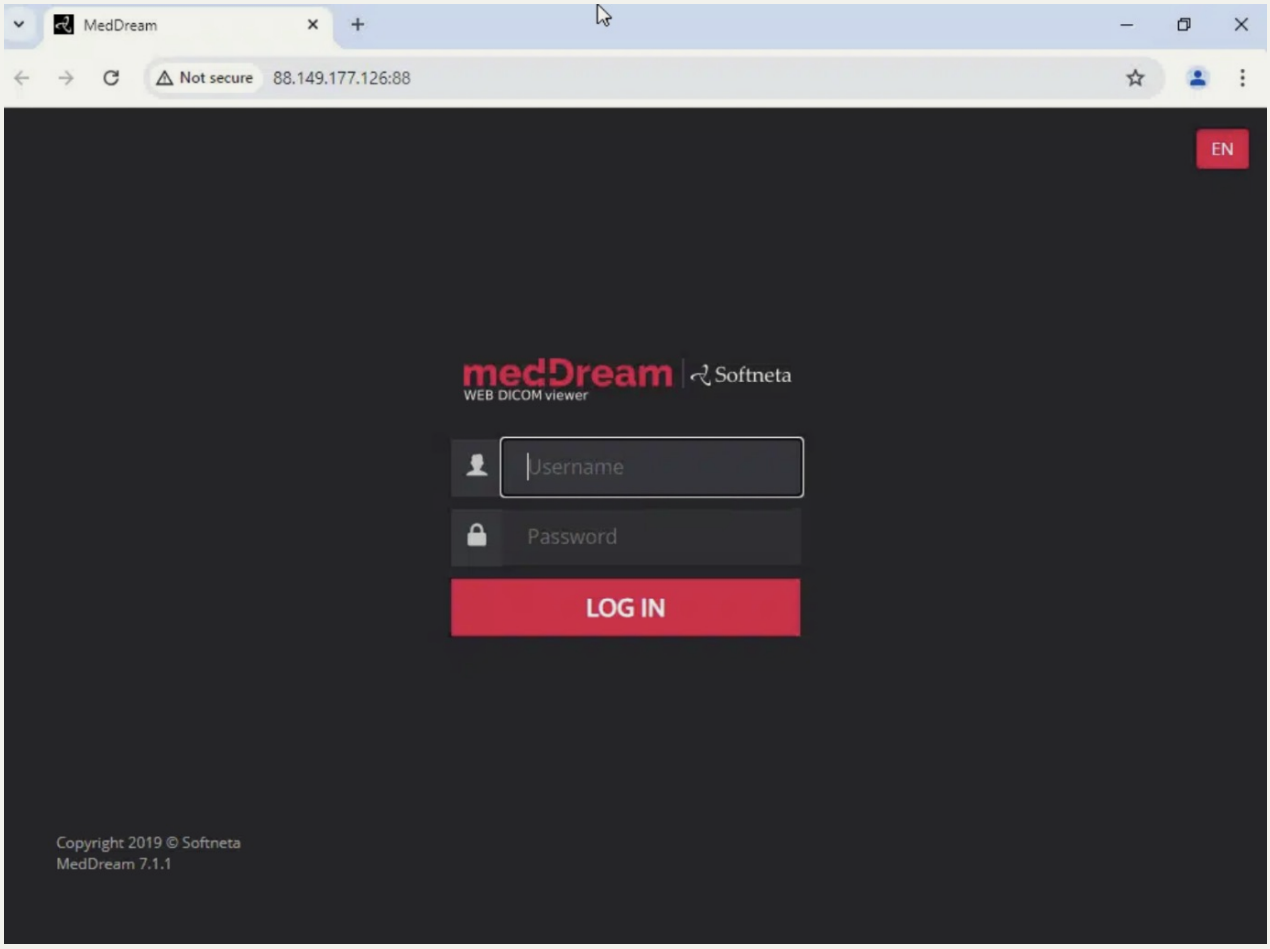
Exposure Risk: Tens of devices are still configured with default passwords, making them accessible to attackers. This lack of basic security hygiene increases the likelihood of unauthorized access and misuse.



Thousands of exposed devices with active vulnerabilities

Vulnerabilities in MedDream and DICOM Applications

MedDream, a popular medical imaging app, has several high-severity vulnerabilities with CVSS scores reaching up to 9.8. These vulnerabilities include issues with authentication and data processing that could allow attackers to gain unauthorized access or execute malicious code. These vulnerabilities, paired with EPSS scores, highlight the critical need to patch and secure such applications promptly to minimize exploitability.



MedDream with Active Vulnerabilities

CVE ID	CVSS Score	EPSS Score
CVE-2024-40898	9.1	0.08%
CVE-2024-38477	7.5	0.02%
CVE-2024-38476	7.5	0.02%
CVE-2024-38474	7.5	0.02%
CVE-2024-27316	7.5	0.02%
CVE-2023-45802	5.9	0.04%
CVE-2023-31122	7.5	0.02%
CVE-2023-25690	7.5	0.02%
CVE-2022-37436	7.5	0.02%
CVE-2022-36760	7.5	0.02%
CVE-2020-13938	7.5	0.02%
CVE-2018-1283	7.5	0.02%
CVE-2022-31813	9.8	1.043%
CVE-2022-23943	9.8	12.813%
CVE-2022-22720	9.8	0.02%
CVE-2021-44790	9.8	0.02%
CVE-2021-39275	9.8	0.02%

CVE-2021-26691	9.8	0.02%
CVE-2019-9517	7.5	0.02%
CVE-2019-0211	8.8	0.02%
CVE-2013-4365	7.5	0.02%
CVE-2011-2688	7.5	0.02%
CVE-2007-4723	7.5	0.02%
CVE-2022-30556	9.8	0.02%
CVE-2022-29404	9.8	0.02%
CVE-2022-28615	9.8	0.02%
CVE-2022-28614	9.8	0.02%
CVE-2022-28330	9.8	0.02%
CVE-2022-26377	9.8	0.02%
CVE-2022-22721	9.8	0.02%
CVE-2022-22719	9.8	0.02%
CVE-2021-44224	7.1	20.479%
CVE-2021-40438	9.1	96.700%
CVE-2021-34798	7.4	0.02%
CVE-2021-33193	7.5	0.02%
CVE-2021-32792	7.5	0.02%
CVE-2021-32791	7.5	0.02%
CVE-2021-32786	7.5	0.02%
CVE-2021-32785	7.5	0.02%
CVE-2021-26690	7.5	0.02%
CVE-2020-35452	7.5	0.02%
CVE-2020-11993	7.5	0.02%
CVE-2020-11023	6.1	0.02%
CVE-2020-11022	6.1	0.02%
CVE-2020-9490	7.5	0.02%
CVE-2020-1934	7.5	0.02%
CVE-2020-1927	7.5	0.02%
CVE-2019-17567	7.5	0.02%
CVE-2019-10098	7.5	0.02%
CVE-2019-10092	7.5	0.02%
CVE-2019-10082	7.5	0.02%
CVE-2019-10081	7.5	0.02%
CVE-2019-0220	5.3	0.02%
CVE-2019-0217	7.5	0.2%
CVE-2019-0196	7.5	0.02%
CVE-2018-17199	7.5	0.02%
CVE-2018-17189	7.5	0.02%
CVE-2018-11763	7.5	0.02%
CVE-2018-1333	7.5	0.02%
CVE-2018-1312	7.5	0.02%

CVE-2018-1303	7.5	0.02%
CVE-2018-1302	7.5	0.02%
CVE-2017-15715	7.5	0.02%
CVE-2017-15710	7.5	0.02%
CVE-2013-2765	7.5	0.02%
CVE-2013-0942	7.5	0.02%
CVE-2012-4360	7.5	0.02%
CVE-2012-4001	7.5	0.02%
CVE-2012-3526	7.5	0.02%
CVE-2011-1176	7.5	0.02%
CVE-2009-2299	7.5	0.02%

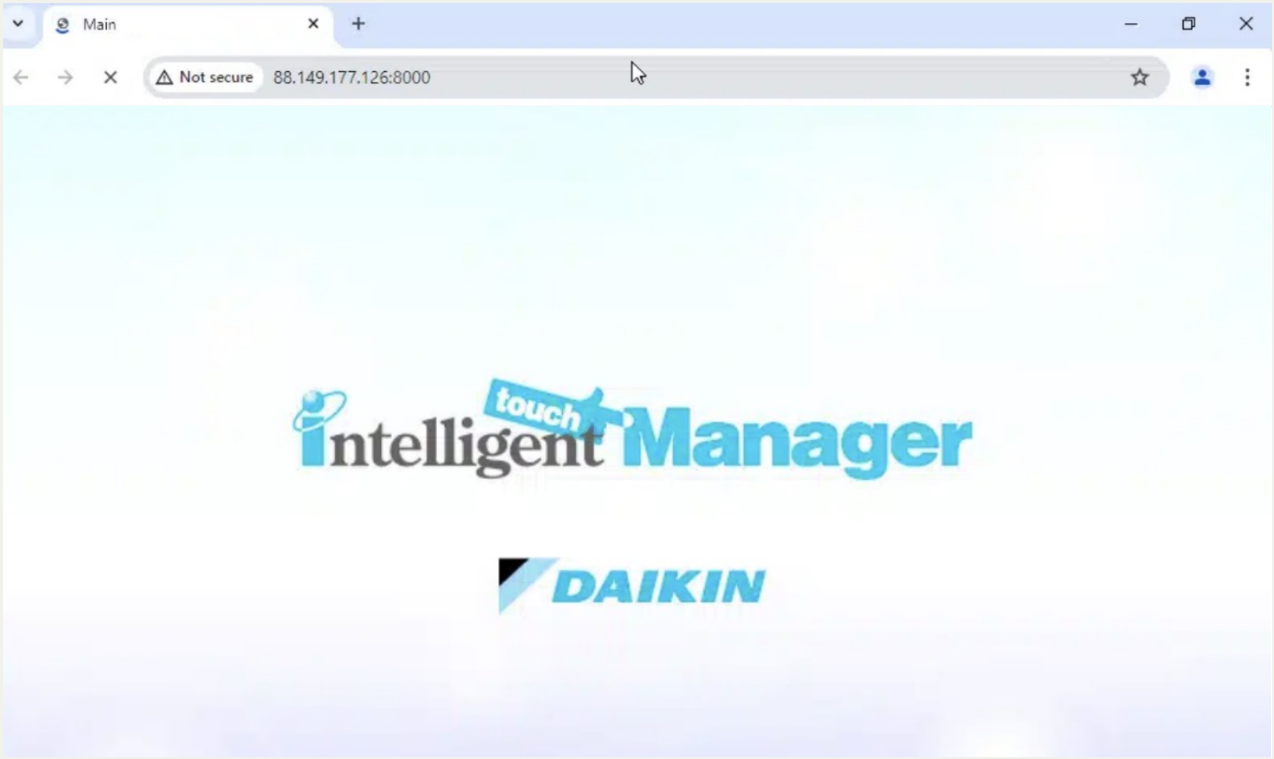
Note: EPSS scores represent the probability of exploitation within the next 30 days and are subject to change as new data becomes available.

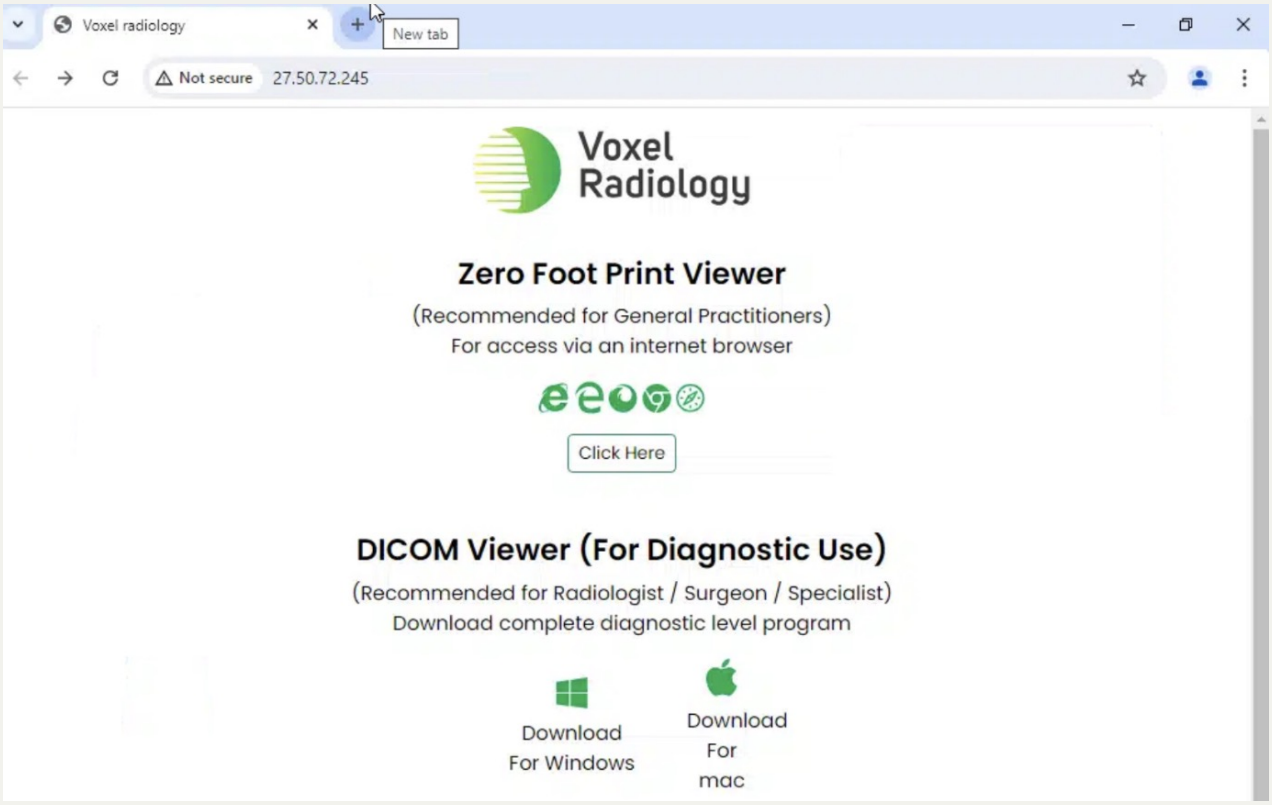
Most Exposed DICOM Web Viewer Interfaces

Research indicates that numerous DICOM web viewer interfaces are publicly exposed, making them prime targets for attackers.

Application	Host Count
OHIF DICOM Viewer	902
Orthanc Server Orthanc	500
NeoLogica RemotEye	215
XERO Viewer	178
Philips IntelliSite Digital Pathology	82
Butterfly Network Ultrasound	14

Drystar medical printers exposed with their default password





Key Takeaways:

Thousands of devices and interfaces are vulnerable due to weak configurations, outdated protocols, and lack of password management.

The DICOM protocol, while integral to healthcare imaging, is increasingly exploited for unauthorized access and data theft.

Immediate focus on patching and securing medical applications like MedDream and DICOM viewers is critical to mitigating risks and maintaining patient safety.

NOTABLE HEALTHCARE EVENTS IN 2024

As this report outlines, cyberattacks targeting the healthcare industry continued to rise in 2024, with attackers leveraging sophisticated tactics to disrupt critical operations, steal sensitive data, and extort victims. Below are two significant events that underscore the sector's vulnerability:

Change Health Breach by ALPHV

In early 2024, Change Health, a major provider of healthcare technology and revenue cycle management services, fell victim to a ransomware attack orchestrated by the notorious ALPHV/BlackCat group.

Attack Details:

ALPHV exploited known misconfigurations and vulnerabilities within Change Health's systems to gain initial access. The attackers encrypted critical operational files, disrupting billing, claims processing, and data exchange services used by healthcare providers nationwide.

Impact:

Patient billing and claims processing were delayed for weeks, affecting millions of healthcare transactions.

Sensitive patient records, including personal identifiers and financial information, were exfiltrated, with threats to release the data unless a multimillion-dollar ransom was paid.

This breach highlighted the critical need for preemptive endpoint protection and vulnerability management in healthcare IT systems.

Mirth Connect Exploited as an Entry Point

In Q1 of 2024, Microsoft issued an alert regarding the active exploitation of vulnerabilities in Mirth Connect, an open-source health information exchange platform widely used in healthcare.

Exploited Vulnerabilities:

- CVE-2023-37679: Allowed remote attackers to execute arbitrary code.
- CVE-2023-43208: Facilitated unauthorized access to sensitive health data through insecure configurations.

Both nation-state actors and cybercrime ransomware groups targeted these flaws as a preferred entry point into healthcare networks.

The platform, maintained by NextGen Healthcare, became a focal point of vulnerability exploitation, underscoring the risks of using tools with inadequate security patching or misconfigured deployments.

Impact

Nation-state attackers leveraged these vulnerabilities to exfiltrate patient records for intelligence operations.

Cybercrime groups used Mirth Connect as a gateway for deploying ransomware, significantly increasing the operational downtime for hospitals and clinics.

Key Takeaways

Attack Surface Management
Vendors and healthcare providers must focus on securing commonly used platforms like Mirth Connect, as they often become systemic points of failure when exploited.

Proactive Patch Management
Both incidents highlight the urgency of identifying and remediating vulnerabilities before attackers can exploit them.

VERITI'S PREDICTIONS AND CHALLENGES FOR 2025

The healthcare industry is poised to face intensified cybersecurity challenges in 2025, driven by the increasing reliance on IoT devices, AI technologies, and cloud-based solutions. These trends highlight the urgent need for preemptive exposure management strategies.

IoT Hardening is Essential

IoT devices remain the Achilles' heel of healthcare cybersecurity. Widely adopted in hospitals for critical operations, these devices are often unpatched and lack the necessary regulatory frameworks for updates. This creates persistent vulnerabilities that attackers will continue to exploit.

Key Risk
Attackers target these devices to ransom critical infrastructure, disrupting essential healthcare services.

Future Outlook
Without standardized patching protocols, IoT vulnerabilities will likely dominate the attack landscape in healthcare.

IoT Bottom Line:

Healthcare organizations must prioritize IoT security by implementing segmentation, regular monitoring, and vendor collaboration to enforce patching protocols.

The Usage of AI in Healthcare

AI is transforming healthcare, enabling advancements like genome mapping and rapid lab result analysis. However, this technological leap comes with significant privacy risks.

Key Concern
The integration of AI often places sensitive patient data outside hospital controlled environments, exposing it to third party systems and potentially unauthorized access.

Implications
Breaches in AI-powered systems could result in widespread exposure of personal medical information, affecting trust in these innovations.

AI Bottom Line:

Safeguarding patient data in AI-driven systems will require stricter controls over data sharing and storage.

Cloud Security First

The shift to cloud-based solutions is reshaping how healthcare organizations store, manage, and analyze patient data. The provided graph illustrates a steady increase in cloud adoption for PACS (Picture Archiving and Communication Systems) devices, highlighting the growing dependence on cloud-managed DICOM applications.

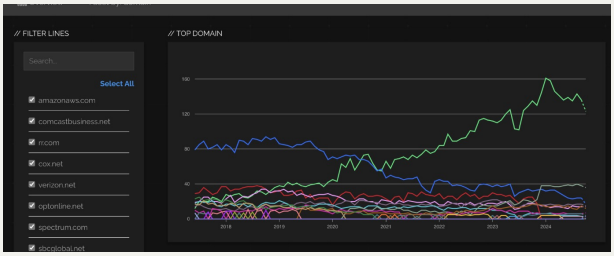
Key Trend
PACS and DICOM-based systems are moving from on-premises setups to cloud-managed environments, improving scalability and operational efficiency.

Challenges
Cloud-based solutions introduce new attack vectors, including misconfigurations, insecure APIs, and data sovereignty concerns

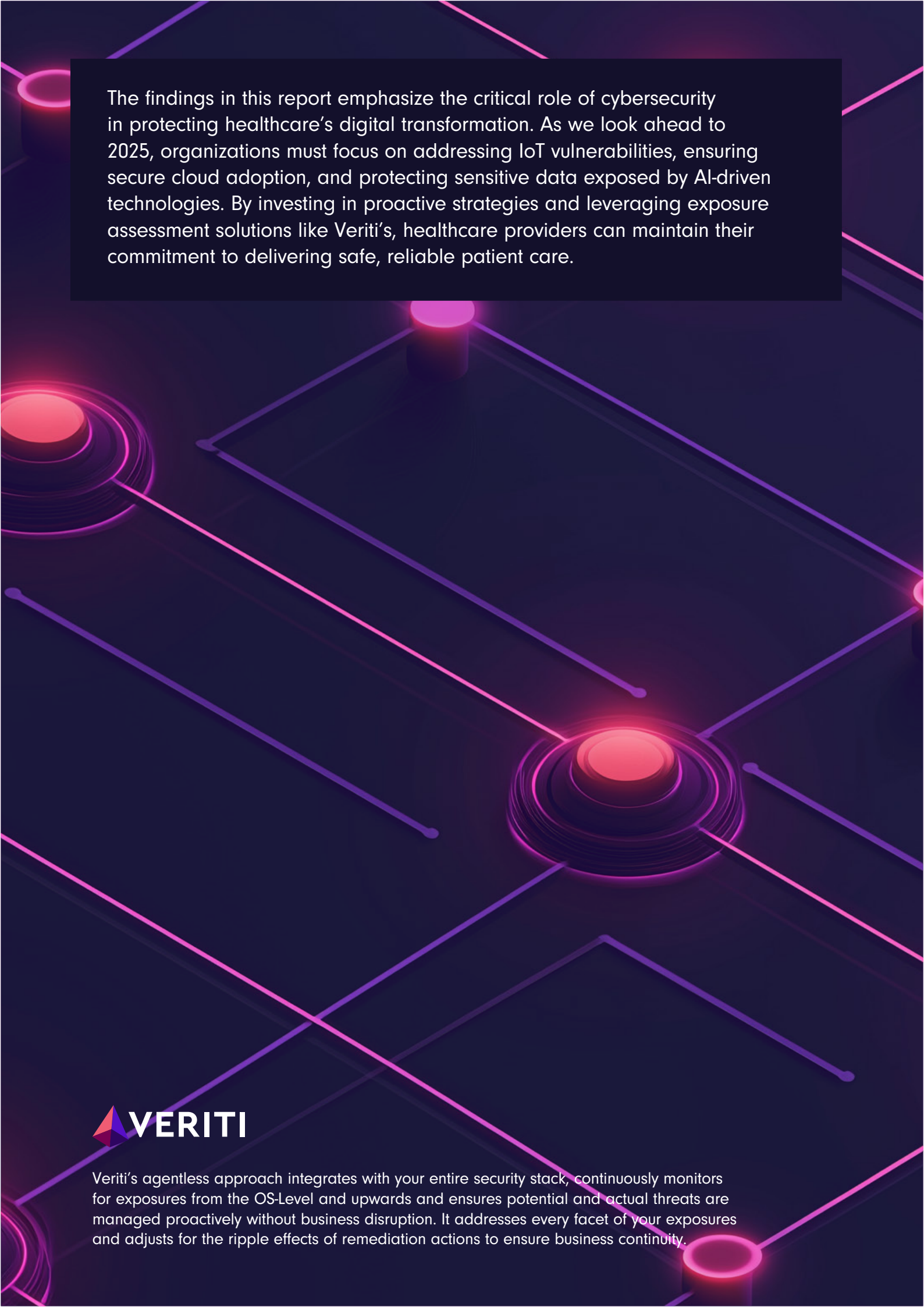
Cloud Bottom Line:

Proactive cloud security measures, including encryption, threat monitoring, and compliance checks, will be vital in safeguarding cloud-hosted healthcare data.

.



The findings in this report emphasize the critical role of cybersecurity in protecting healthcare's digital transformation. As we look ahead to 2025, organizations must focus on addressing IoT vulnerabilities, ensuring secure cloud adoption, and protecting sensitive data exposed by AI-driven technologies. By investing in proactive strategies and leveraging exposure assessment solutions like Veriti's, healthcare providers can maintain their commitment to delivering safe, reliable patient care.



VERITI

Veriti's agentless approach integrates with your entire security stack, continuously monitors for exposures from the OS-Level and upwards and ensures potential and actual threats are managed proactively without business disruption. It addresses every facet of your exposures and adjusts for the ripple effects of remediation actions to ensure business continuity.