opentext™

POINT OF VIEW

Cybersecurity for healthcare organizations

An OpenText industry perspective

More information on challenges facing healthcare organizations

U.S. Department of Health and Human Services (HHS)
Healthcare Sector Cybersecurity›

UpGuard
What are the Biggest Cyber Threats in Healthcare? ›

Cureus
Clinicians' Perspectives on Healthcare Cybersecurity and Cyber Threats ›

CISA
Mitigation Guide: Healthcare and Public Health (HPH) Sector ›

Statista
Healthcare and cybercrime in the U.S. - Statistics & Facts ›

Thoughtful.ai
Cybersecurity in Healthcare: AI as a Guard Against Threats ›

In 2024, approximately 67% of healthcare organizations worldwide experienced a ransomware attack, the highest rate since 2021.[1]

Key cybersecurity challenges facing healthcare organizations

Healthcare and pharmaceutical organizations face ever increasing threats from cybercriminals seeking to obtain PHI and other sensitive data through advanced techniques. Organizations also need to comply with regulatory requirements. Here are the key challenges:

Prevent ransomware attacks and data breaches

Cybersecurity has become a critical issue for top executives at hospitals, health plans, medical practices, pharmaceutical companies, and other life sciences firms. Ransomware attacks are rampant. The theft of protected health information (PHI) and intellectual property can devastate an organization's reputation. Even short interruptions to operations can have profound effects on patient care and healthcare stability. Recent history is not reassuring—with massive data breaches in early 2024 of Change Healthcare (a unit of UnitedHealth Group) and Kaiser Foundation Health Plan. To block and contain threats, healthcare organizations need to improve attack detection, accelerate incident analysis and response, and better protect customer and employee identities and credentials.

Comply with expanding regulations

Depending on their location, healthcare organizations may need to comply with evolving versions of HIPAA, HITECH, HITRUST CSF, PCI DSS, NIST, ISO 27001, the EU GDPR, NIS2, the Cyber Resilience Act, and other cybersecurity and privacy regulations. Organizations that manufacture and use medical devices and software must also address standards such as the FDA Quality System Regulations (QSR) and H.R.7084 (the Patch Act of 2022).

Improve patient experiences with online services

As healthcare organizations strive to provide more online and telehealth services and share more PHI online, they must meet patient expectations for simple, secure authentication and authorization without hassles related to passwords and credentials.

AI adoption

AI increases cybersecurity risks and data privacy concerns by relying on sensitive data, creating new attack opportunities and complicating compliance with evolving healthcare regulations

Neutralize insider threats

Healthcare organizations must cope with malicious insiders trying to steal PHI, financial data, and intellectual property, careless insiders inadvertently exposing data and access credentials to outsiders, and clueless insiders violating privacy policies by viewing patient information without authorization. Insiders can also be unwitting pawns of threat actors.

1 Statista, *Share of healthcare organizations worldwide encountering ransomware attacks from 2021 to 2024*, 2024

Most affected organizations—74%— had their data encrypted as a result of these attacks.[2]

Prevent ransomware attacks and data breaches

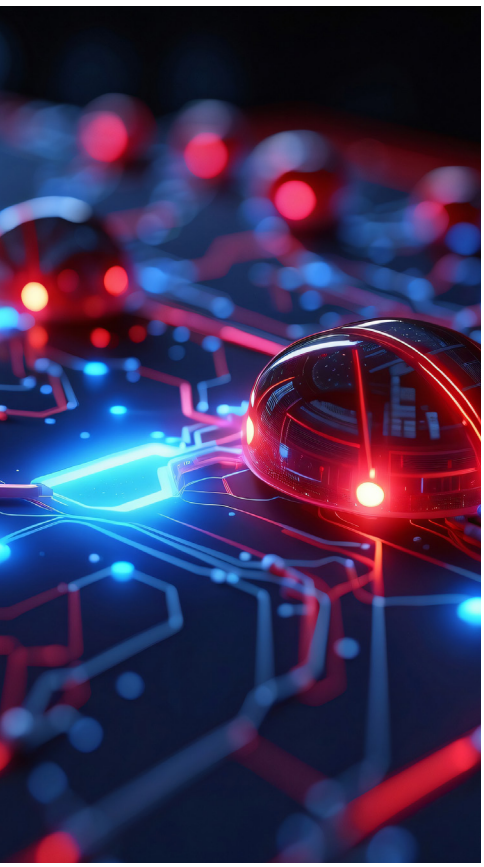
OpenText helps healthcare organizations prevent ransomware attacks and data breaches by strengthening their capabilities to protect identities and data and to deploy secure applications.

Identity protection

Threat actors have discovered that the easiest way to circumvent security controls and anti-fraud measures usually involves capturing and exploiting legitimate customer and user credentials. To minimize the impact of identity-related attacks, healthcare organizations need to:

- Enforce policies that minimize unnecessary access to data and applications.
- Reduce the loss and theft of identity information and credentials.
- Detect and prevent threat actors attempting to impersonate employees, customers, and business partners using stolen credentials.

2 Statista, *Share of healthcare organizations worldwide encountering ransomware attacks from 2021 to 2024*, 2024



Recovery costs for ransomware attacks in the healthcare sector have risen to $2.57 million in 2024, up from $2.2 million in 2023.[3]

OpenText™ Identity and Access Management (IAM) solutions (OpenText Access Manager, OpenText Identity Governance, and OpenText Privileged Access Manager) enable healthcare organizations to implement best practices to:

- Discover identity and credential stores across the enterprise, so they can be consolidated and protected.
- Streamline identity and access management (IAM) by using automated processes and intuitive workflows to define, manage, request, and approve identities, permissions, and credentials throughout their lifecycles.
- Leverage advanced identity governance to detect and address orphaned and inactive accounts, entitlement creep, over-privileged users, and unnecessary group membership
- Use rule sets to discover and retrieve various details of the accounts and help in managing the discovered accounts. Discovery of privileged accounts also enables administrators to add multiple accounts to a preferred resource.
- Detect violations of separation of duties (SoD) policies.
- Ensure that non-human identities are who they claim to be and secure interaction between them.
- Ensure the validity of patients and remote employees with passwordless, attack-resistant multi-factor authentication (MFA).
- Provide cloud infrastructure entitlement management (CIEM) to control access to SaaS applications, cloud file storage systems, and public and private cloud platforms.

Data protection

Threat actors typically target patient PHI and employee data. To safeguard that data, healthcare organizations need to accelerate threat detection and response, discover and secure high-value data everywhere it resides, consistently enforce security policies, and unlock deep insights that foster best practices for security and privacy.

OpenText data security solutions help healthcare organizations implement best practices to:

- Find and control “shadow IT” applications and data repositories that increase the risk of data leakage and data breaches.
- Conduct global discovery so all data stores and repositories can be classified and protected with the appropriate controls.
- Enforce access control and data access governance (DAG) policies consistently across the organization
- Monitor and analyze data access events to uncover suspicious activities and unnecessary permissions, and to identify data that should be moved, better secured, or retired.

3 Sophos, *The State of Ransomware in Healthcare*, 2024

More information about protecting identities, data, and applications

IGA Buyer's Guide: Selecting the Right Identity Governance and Administration Solution ›

Identity Administration Needs Governance ›

OpenText Identity Governance and Administration web page ›

OpenText Data Privacy and Protection web page ›

OpenText Application Security web page ›

Advanced Threat Detection & Insider Threat Management ›

- Facilitate secure testing, analysis, and data sharing through techniques for masking, tokenization, and anonymization.
- Identify opportunities to consolidate data repositories and reduce the data attack surface.
- Assess data-related risks to prioritize remediation activities, justify new data protection initiatives, and improve the organization's data security posture.
- Analyze users' behaviors in context of their current operating environments to automate the discovery of anomalous activities that might be related to data breaches.

Application protection

To prevent threat actors from compromising internet-facing software applications, those applications need to be "secure by design," with security requirements defined, developed, and tested throughout the software development lifecycle (SDLC).

OpenText application security solutions provide healthcare organizations with the tools to implement best practices to:

- Integrate security testing of all types (including SAST, DAST, IAST, MAST, IaC, SCA, API, and penetration testing) into automated development, security and operations (DevSecOps) processes.
- Improve the security of application programming interfaces (APIs).
- Dramatically reduce the time required to analyze and audit static scan results by using AI to automatically classify issues as Exploitable, Not an Issue, or Indeterminate.
- Reduce friction between developers and security teams by allowing software engineers with less security training to quickly remediate many security issues on their own.
- Analyze the risks of application vulnerabilities and security issues to better prioritize remediation actions.
- Prevent software supply chain attacks by ensuring that open-source and purchased custom software have not been compromised and do not contain unlicensed proprietary code.

Scan open-source codebases used for training AI models to identify vulnerabilities and malicious code so they are not replicated in AI-generated software.

- Provide visibility and analysis so the organization can monitor and improve its application security posture.
- Keep development projects on schedule by increasing the productivity of software developers and testers.

Only 22% of healthcare organizations were able to fully recover within a week, 47% fewer than the year before. And 37% took more than a month to recover.[4]

Comply with expanding regulations

Regulators and standards bodies are continually escalating requirements for resilience, privacy, and governance. Healthcare organizations in the US must comply with continually evolving versions of HIPAA, HITECH, HITRUST CSF, PCI DSS, NIST, ISO 27001, and other regulations and frameworks. Institutions that operate in the EU are covered by the GDPR, DORA, NIS2, the Cyber Resilience Act, and national cybersecurity and privacy regulations. Medical device and software developers must also address standards such as the FDA Quality System Regulations (QSR) and H.R.7084 (the Patch Act of 2022).

OpenText solutions for application security, data privacy and protection, identity and access management, and threat detection and response enable healthcare organizations to:

- Streamline the production of compliance reports, certifications, and micro-certifications.

4 Sophos, *Two-Thirds of Healthcare Organizations Hit by Ransomware – A Four-Year High, Sophos Survey Finds*, 2024

- Meet requirements for data protection and business resilience by demonstrating visibility into all types of protected data at every level, consistently enforcing access policies for applications, databases, and data repositories, and managing effective data backup and recovery processes.
- Implement best practices for retaining, archiving, and deleting data and for controlling the flow of data to third parties and across geographical boundaries.
- Implement best practices for enforcing role-based access control (RBAC), separation of duties (SoD), and the principle of least privilege (PoLP).
- Comply with mandates to encrypt, mask, or anonymize data in motion and data shared with payment and data processors, insurance companies, and service providers to maintain data privacy
- Detect all instances of personally identifiable information (PII), protected health information (PHI), payment card industry (PCI) data, and words and phrases associated with specific healthcare regulations and standards so all information assets can be protected by the necessary controls.
- Support compliance with regulations governing personal information, including rights of access, rights to restrict processing of personal information, and “the right to be forgotten.”
- Create comprehensive audit trails of the creation, storage, access, and sharing of data.
- Employ artificial intelligence to collect, sift, analyze, and organize information for compliance reporting and to automatically prefill compliance reports.

More information about improving patient experiences

What is Passwordless Authentication? ›

Experian Health

Patient access technology: how it creates better patient experiences ›

HealthTech

MFA Fatigue: A Growing Headache for Healthcare ›

OpenText Advanced Authentication for Your Business ›

OpenText Advanced Authentication product page ›

- Perform and document all types of security testing during software development, including SAST, DAST, IAST, MAST, IaC, SCA, API, and penetration testing.
- Detect anomalous behaviors prior to attacks and enable faster incident response to effectively prioritize risk and reduce breaches with patented and proven AI/ML powered analytics.
- Use real-time contextual threat intelligence as the foundation for enabling unmatched threat insights and help anticipate and adapt to meet new threats
- Secure sensitive information, access violations, and application vulnerabilities to establish a foundation for secure adoption of AI technologies
- Improve security posture and integrate security across business functions, roles and processes to drive governance
- Prioritize threat investigations with automated and intelligent risk scoring

Improve patient experiences with online services

Unfortunately, complex authentication processes and password-related issues have long frustrated patients and other users of healthcare services. In contrast, frictionless authentication and self-service enrollment and administration increase patient loyalty, improve security, and reduce customer support costs.

OpenText identity security and data protection solutions enable healthcare organizations to adhere to best practices to:

- Improve patient experiences by deploying simple, passwordless, attack-resistant MFA (authentication processes that use biometric recognition rather than inherently insecure, difficult-to-support passwords and password management systems).
- Reduce support costs and patient frustration by providing self-service capabilities to enroll in online services and applications.
- Use adaptive authentication and contextual security data to dynamically create risks scores, provide frictionless authentication when possible, and create step-up validation requests when necessary.
- Use generative AI and AI image generation to gather insights about patient needs and behaviors to create contextual, personalized, and relevant content for everyone.

"With the adoption of digital health technologies, privacy and data protection are more important than ever. Advances in cybersecurity ensure protected health information remains confidential and secure. Healthcare practices are improving patient trust by implementing robust security measures to safeguard patient data, complying with privacy regulations and ensuring peace of mind."

- The Intake [5]

AI adoption

To protect against emerging threats, including those that employ AI, healthcare organizations must fully leverage AI and large language models (LLMs) to identify vulnerabilities and misconfigurations, detect suspicious activities, contain attacks, prioritize remediation activities, generate compliance documentation, recognize AI-based threats, and perform other key tasks. The adoption of AI for security in the healthcare industry is quite significant. Here is where OpenText Security solutions can help:

- Employ AI to identify PHI, financial and insurance records, intellectual property, product designs, credentials, software, and other high-value information everywhere they are created, stored, and processed.
- Use AI/ML and automation to continuously assess the interaction between people and services with sensitive information, to trigger stronger authentication methods when appropriate, and to block suspicious activities when needed.
- Deploy artificial intelligence to automate the preparation of compliance reports.
- Leverage AI to recognize patterns and detect anomalies associated with attacks and fraud.
- Harness AI for threat detection in order to identify suspicious activities and potential breaches faster and accelerate response and mitigation.
- Drastically reduce the time developers spend remediating code security issues by leveraging AI-powered code fix suggestions

5 The Intake, *Future-proof your practice with digital patient experiences*, March 2024

Neutralize insider threats

Healthcare organizations face special challenges policing the actions of employees, contractors, and business partners authorized to access sensitive applications and data. These insiders start with valid credentials, and security teams must be careful not to interfere with their legitimate activities. In many instances, insiders expose protected data to threat actors and violate privacy and security policies inadvertently.

Fortunately, OpenText identity, data protection, threat detection and response, and analytics, solutions allow healthcare organizations to:

- Prevent unauthorized access by insiders to PHI, PII, financial data, and intellectual property through strict access controls.
- Stay ahead of unknown (insider, novel, advanced persistent) threats with patented behavioral analytics and advanced threat hunting service proven to detect more than 80% of Red Team attacks.[6]
- Educate employees about security policies and best practices with training and security awareness programs

6 According to internal OpenText customer engagements that leveraged the experience and domain expertise of our threat hunting team and the behavioral analytics capabilities in OpenText Core Threat Detection and Response.

Summary

Healthcare organizations like yours face the dual challenge of defending against sophisticated ransomware and hacking attempts, while adhering to growing regulatory demands in the realm of digital security and privacy. At the same time, there are opportunities to enhance digital services for patients by making them more secure and user-friendly.

Additionally, it is crucial to harness the potential of AI, while also managing the insider, novel, and advanced persistent threats and risks that arise from threat actors' malicious use of AI technologies.

OpenText offers a comprehensive range of cybersecurity and cyber resilience solutions to support your success. Our solutions include identity and data protection, security by design, automated software testing, resilient multi-factor authentication, and advanced security analytics. We are at the forefront in integrating AI and threat intelligence into our technologies to automate processes and boost productivity. Discover how we can collaborate with you to enhance the security, compliance, and resilience of your organization.

To learn more, go to: OpenText Cybersecurity Cloud.

Copyright © 2025 Open Text • 02.25 | 246-000023-002

opentext™