CyberRes

Flyer

Accelerating Trusted, Secure Electronic Healthcare

In an era of innovation, scale, and patient-centric enhancement of healthcare services, a provider's growth is based on their ability to securely automate, digitally engage, and provide new levels of AI-led services to their patients. Healthcare providers that can "go to where patients are" can generate new revenue models and drive better patient adoption and loyalty.

Reimagine Trusted Healthcare

A trusted electronic healthcare provider is characterized by the ability to provide a secure, robust, transparent, and traceable patient care experience from the clinic to the ER.

Patient Care

A key aspect of patient care is knowing where data exists, how it is being used, and who has access—from onboarding, to records management, to telemedicine, to the use of modern SDN-enabled healthcare.

Patient Trust

A key aspect of trusted healthcare is the provider's ability to secure the entire digital experience of the healthcare provider, clinician, and patient—from how they access their records online, to telemedicine, to how hospital staff access their records.

Patient Access Transparency

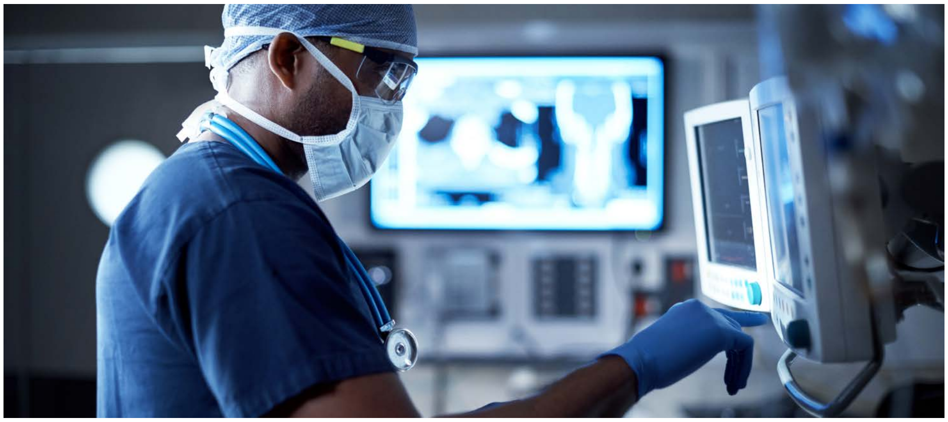
In the age of telemedicine, complex medical supply chains, and digitalization of services, patient trust is established through access transparency. This enables a patient to know who accessed their data, for what purpose, and how they can withdraw access.

Digital Lifecycle Visibility

Healthcare networks are complex, extending to various providers, insurers, affiliate providers, university healthcare programs, and other parties. In addition, a typical hospital has various extended networks to support patient data access, connected medical devices, and other related networks. A key aspect of gaining trust and assurance is having an end-to-end view of the holistic digital footprint.

Digital Records Visibility

A key aspect of establishing trust, demonstrating patient care, and enabling records access and healthcare is lifecycle transparency from the beginning of the patient's experience to how their personal records are destroyed. A comprehensive digital resiliency program should include end-to-end, verifiable visibility.



A trusted electronic healthcare provider is characterized by its ability to provide a robust, transparent, and traceable patient care experience from the clinic to the ER. Such a provider has the ability to automate and provide real-time capability to trace and protect each patient's medical journey through the healthcare system. The CyberRes Trusted Healthcare offering is a comprehensive ecosystem solution, supported by a partner Privacy Operating Center capability to enable trusted electronic healthcare.

Patient Care

Securing the healthcare value chain (the entire flow of processes through the various healthcare lines of business) requires comprehensive digital lifecycle visibility, granular access control, robust controls and patient access, data governance, and protection. A healthcare provider must address the entire patient journey—from onboarding, to records management, to telemedicine, to the use of modern SDN-enabled healthcare, such as remote (5G-enabled) surgery and digital patient care.

A key aspect of patient care is knowing where data exists, how it is being used, and who has access. However, health records standards such as HL7 and other proprietary methods pose unique challenges for typical cyber operations. These challenges extend to sophisticated schema, behavior mapping, and the persistence of records.

Patient Trust

Ensuring that Electronic Health Records (EHR) and Personal Health Records (PHI) are secure throughout the entire medical interaction of a patient is key to ensuring trust. This includes ensuring the trust and integrity of next-generation healthcare such as robotics, patient care analytics, and telemedicine. CyberRes Trusted Electronic Healthcare provides an integrated fabric to secure data (CyberRes Voltage SecureData), tokenize records so that clinicians can access only the fields that are required for their role, and trace the use of that data in a secure manner (CyberRes ArcSight).

Patient Access Transparency

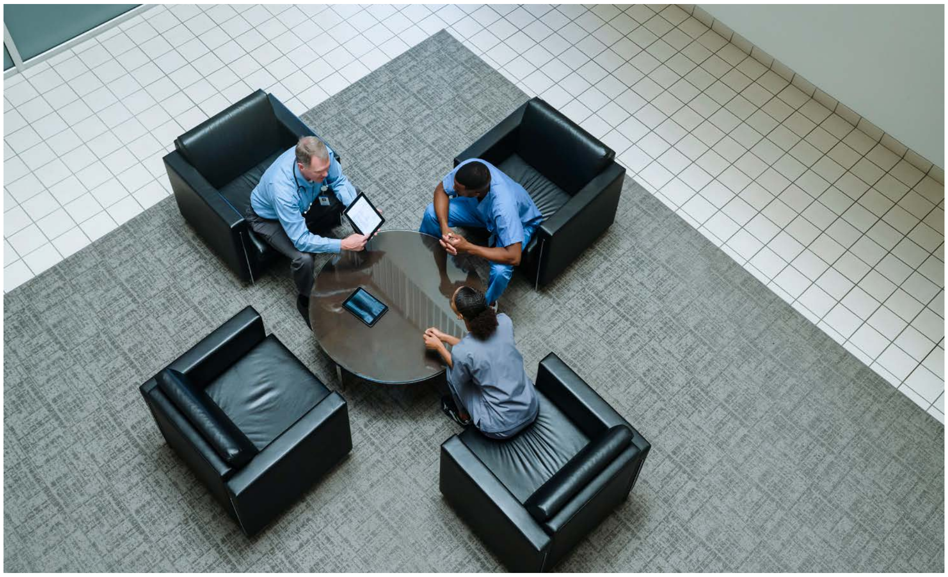
In an era of hyper digitalization of patient care, medical providers require end-to-end secure and privacy-enabled transparency of the entire patient care experience. The challenge is the ability to trace risks and threats without causing any impact to patient privacy. CyberRes Trusted Electronic Healthcare provides a powerful capability to trace the full lifecycle of a patient care record, but still maintain privacy of the record using tokenization, obfuscation, and field-based access control. The automated pattern and anomaly recognition systems can follow a patient without affecting the privacy of the patient record. The patient should also have the ability to determine and opt out of who has access to their data.

Digital Lifecycle Visibility

Electronic Healthcare is increasingly expanding the use of connected devices, complex supply chains, medical Internet of Things (IoT), and other technologies. The healthcare CISO has to contend with an increasingly expansive and diverse set of challenges. CyberRes Trusted Healthcare provides an end-to-end visibility layer for electronic healthcare from the Connected Medical Device (IoT), to ER, to Tele-Medicine, to 5G URLLC-enabled robotics. This visibility enables the capability to detect and respond to long-term patterns of suspicious access to patient care, such as record spoofing, escalation of privilege, clinical access to unexpected hospitals, and other unsupervised detection of anomalies.

Healthcare Risk Management

Custodial and healthcare records are increasingly being targeted by advanced adversaries. Patient record surfing, access to medical history, and even vaccination schedules are an appealing target. These adversaries aren't bound by single healthcare channels; they have been known to cross over from administration, to IT (e.g., hospital wireless network), to clinical networks. A healthcare CISO needs to ensure that the solution is robust enough to connect the dots from a complex threat surface.



CyberRes Trusted Healthcare provides an integrated ability to "stich" threats, detect patterns and anomalies, and use powerful step-up authentication methods for access that crosses over healthcare channels. For example, access to the hospital network using the public wireless zone into other protected parts of the healthcare infrastructure, providing a holistic view of electronic health monitoring.

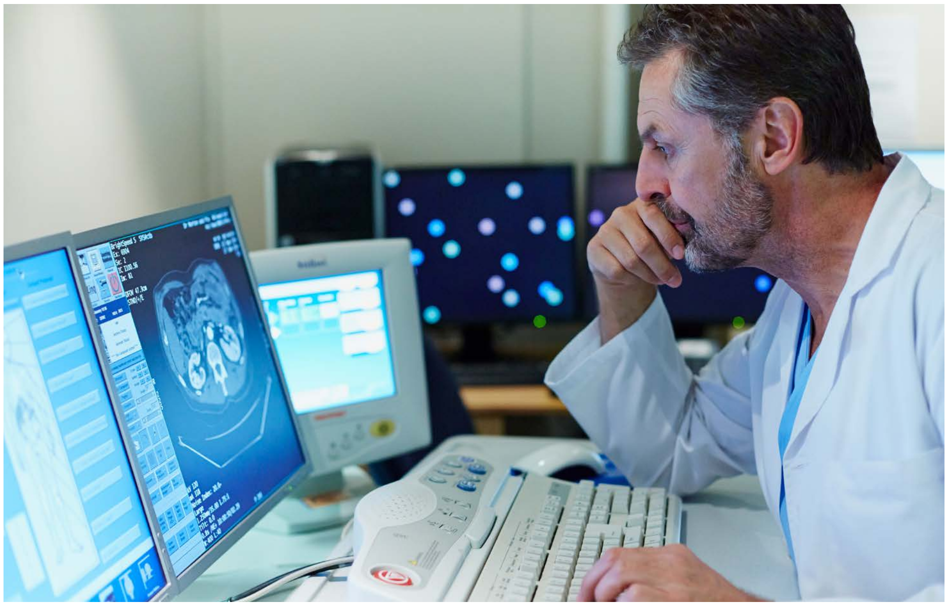
CyberRes Capabilities for Securing Trusted Healthcare

CyberRes is a Micro Focus line of business. We bring the expertise of one of the world's largest security portfolios to helping our customers navigate the changing threat landscape by driving both cyber and business resiliency within their teams and organizations. We are here to help enterprises accelerate trust, reliability, and survivability through times of adversity, crisis, and business volatility.

We are part of a larger set of digital transformation solutions that fight adverse conditions so businesses can continue to run today to keep the lights on and transform to grow and take advantage of tomorrow's opportunities. CyberRes offers a host of capabilities for securing trusted digital patient care.

Healthcare Cyber Data Platform

The CyberRes Data Platform provides one of the most sophisticated, flexible, and scalable data platforms to enable the ingest, analysis, and processing of proprietary healthcare messaging formats such as HL7 and others. The CyberRes data platform not only has the ability to monitor for persistent record changes, but to also apply enrichment along patient rights, intelligence context (e.g., exposure of medical IoT devices), and other enrichment that can be used by machine learning risk models.



Healthcare Privacy Operations

CyberRes solutions for Healthcare Services provide a robust backbone capability, content, and data model for providers to launch a “Privacy Operations Center” (POC) or Healthcare “Trust Operations Center” (TOC). Unlike typical Security Operations Centers (SOC’s), this specialized offering enables providers to use a rich set of privacy models, machine learning, data protection, classification, and data access withdrawal capability to secure the patient experience lifecycle.

Healthcare Data Protection

Healthcare providers today are hybrid IT and multi-cloud and need protection for high-value data that travels with the data. CyberRes Voltage encryption techniques encrypt or anonymize data in files, databases, applications, and analytics platforms so that business workflows continue to operate and data maintains usability and utility in its protected form. Yet, when exfiltrated, the encrypted data is useless to the cyber attacker. Voltage thus neutralizes the impacts of data breach (“safe breach”). Persistent data security enables privacy and safely increases data use to drive value for the business.

Healthcare Data Classification

A key aspect of addressing the handling of electronic health records is to know your patient (KYP). A core aspect of KYP is to trace and classify patient data through complex processing environments. CyberRes Voltage know your patient (KYP). Data Discovery uses AI-driven analytics to build a rich inventory of data. CyberRes Voltage Structured Data Manager (SDM) automatically discovers sensitive data across all repositories and acts on it to reduce the data footprint and lower TCO.

Patient (Opt-Out) Policy Management

Modern digital healthcare provides a platform to enable patient transparency and control. This digital platform not only allows a healthcare provider to equip patients with access profiles for their own data, but also allows the patient to “opt out” of who has access to their data. CyberRes Voltage Secure Privacy Policy Management allows patients to workflow-driven privacy policies to opt out of who has access to their data.

Healthcare Secure Supply Chain

Healthcare applications have complex dependencies with upstream and downstream systems, repositories, NetBeans, and other dependent code farms.

Modern healthcare applications are subject to open source security issues and with most organizations implementing hundreds of apps, CyberRes Open Source Scanning tools put a spotlight on general security risks associated with open source components. Susceptibility analysis enables healthcare facilities to automate the workflow to determine if open source weaknesses can affect the healthcare value chain.

Healthcare Secure J2C

In order to drive on-demand and elastic healthcare services, providers are accelerating their migration to the cloud in a secure manner. CyberRes Data provides insight into patient behavior, trends, and opportunities for new products and services that support Secure Journey to Cloud (SJ2C).

CyberRes Format-Preserving Encryption (FPE) seamlessly integrates with big data analytics platforms on premises, in the cloud, and in cloud-native services to enable secure analytics on data in its protected form. Analytics teams, DBAs, and business users can safely access high-value data, perform most analytics on encrypted data, and produce faster insights and time to value.

Healthcare Secure Development

At the core of healthcare modernization is the trust, integrity, and survivability of the microservices, healthcare applications, and (in modern environments) infrastructure as code.

The CyberRes Secure Development portfolio enables healthcare providers to shift left. Addressing security earlier in the software development lifecycle (SDLC) is the most efficient means of engineering secure applications. However, the velocity of development can make this a daunting

> “ArcSight Intelligence found a previously dormant active GUEST account which had not been locked despite failing hundreds of authentication attempts, all made outside of working hours. It attempted to access a classified server and our team was able to neutralize the activity before any breach occurred.”
>
> CHIEF INFORMATION SECURITY OFFICER
> Large Healthcare Organization

Contact us at **CyberRes.com**
Like what you read? Share it.

task. Integrating security intelligence into development pipelines optimizes the power of automation for agility, speed, innovation, and delivery to efficiently identify software risks, enforce policies, and remediate any found vulnerabilities.

Healthcare Secure Identity
Healthcare providers are encountering an ever-expanding healthcare agent and employee landscape. With an increase in teleworkers, institutions are addressing the complexity of third-party labor providers, work-from-home risks, and other challenges.

CyberRes Identity Governance provides healthcare institutions with a lifecycle-based, analytical, and machine learning-aided set of capabilities to provide visibility and controls of roles, access, and certification of employees.

Learn more at
cyberres.com/industry/healthcare