



Protecting Mobile Healthcare Apps:

How XTD Helps Healthcare
Organizations Thwart Cyberattacks

CHAPTER 1

The Dramatic Rise of Healthcare as a Cyber Target

The healthcare industry is one of those most consistently subject to cyberattacks. Healthcare organizations process vast amounts of data that is valuable to hackers—so valuable that a stolen patient health record can sell for up to ten times more than a stolen credit card number on the dark web.

The broad range of data a healthcare organization typically handles can include patients' personal health information (PHI) like medical records; personally identifying information (PII) like name, address, government ID number, and insurance policy number; and payment and other financial data belonging to patients as well as to the healthcare organization itself. The concentration of so much rich information presents hackers with the tantalizing potential for very profitable fraud, identity theft, and trading on the dark web.

Given that, it's no surprise that healthcare data breach rates have been continually climbing for several years. In 2020, when the COVID-19 pandemic emerged and the use of telehealth soared, healthcare breaches rose by 42%, and 60% of ransomware attacks targeted the healthcare sector¹. The trend has continued since. In 2022, over 50 million patient records were compromised through a total of 905 reported incidents. That was a 44% rise in attacks on healthcare organizations over 2021². As of the end of March 2023, the US Department of Health and Human Services [reported](#) that there had already been 136 health breaches affecting at least 500 people each, with the ten largest of those affecting more than 150,000 individuals.

One of the rising sources of health data risk is mobile devices, as more patients turn to them to access health records and make payments, and more healthcare organizations make use of them for care delivery and myriad other tasks. The number of healthcare apps used across so many mobile devices puts health data security and privacy at greater risk.

¹ U.S. Department of Health and Human Services.

² Protenu Breach Barometer Report.

Characteristics of Healthcare Cyberattacks

Frequency	849 incidents, 571 with confirmed data disclosure
Top patterns	Basic Web Application Attacks, Miscellaneous Errors and System Intrusion represent 76% of breaches
Threat actors	External (61%), Internal (39%) (breaches)
Actor motives	Financial (95%), Espionage (4%), Convenience (1%), Grudge (1%) (breaches)
Data compromised	Personal (58%), Medical (46%), Credentials (29%), Other (29%) (breaches)

Source: 2022 Verizon Data Breach Investigation Report

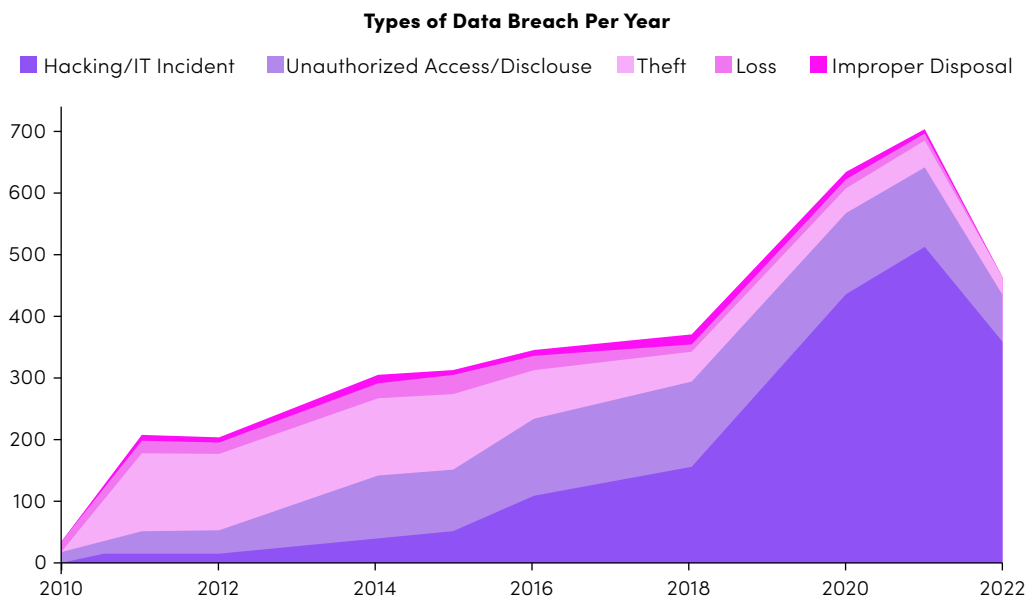
Top Cyber Threats to the Healthcare Industry

There are multiple ways hackers use to get at healthcare data. Some of the most common include:


Ransomware. Ransomware is software that blocks access to a computer system until a payment is made—and sometimes even after that. It’s become a preferred tool for bad actors. Between July and September of 2021, [researchers](#) identified 68 healthcare ransomware attacks, with 60% of those in the US. France, Brazil, Thailand, Australia, and Italy were the next most attacked, demonstrating the global nature of the threat. Encrypting data is a popular technique for successful ransomware attackers, rendering the healthcare organization unable to utilize its vital information. According to research from [Sophos](#), 34% of healthcare organizations whose data was encrypted paid the ransom to get their data back, but on average, only 69% of encrypted data was actually restored after the payment.

Phishing. Phishing is another very common form of attack. Through phishing, hackers try to trick patients or providers into providing the credentials needed to access online health applications. This method is very effective with people who are confused or even fearful (not uncommon for people who are ill), causing them to be less cautious. Per F5’s [Phishing and Fraud Report](#), phishing incidents rose by 220% during the height of the pandemic.

Business Email Compromise. A subset of phishing, business email compromise is a type of attack in which attackers pretend to be an authority figure in a healthcare organization (like the CEO). They use genuine-looking emails to persuade the employee victim to transfer large amounts of money to fraudulent accounts. These kinds of attacks are often thoroughly researched through social engineering methods so that messages convincingly reflect the authority figure’s tone or other relevant information in order to appear legitimate.

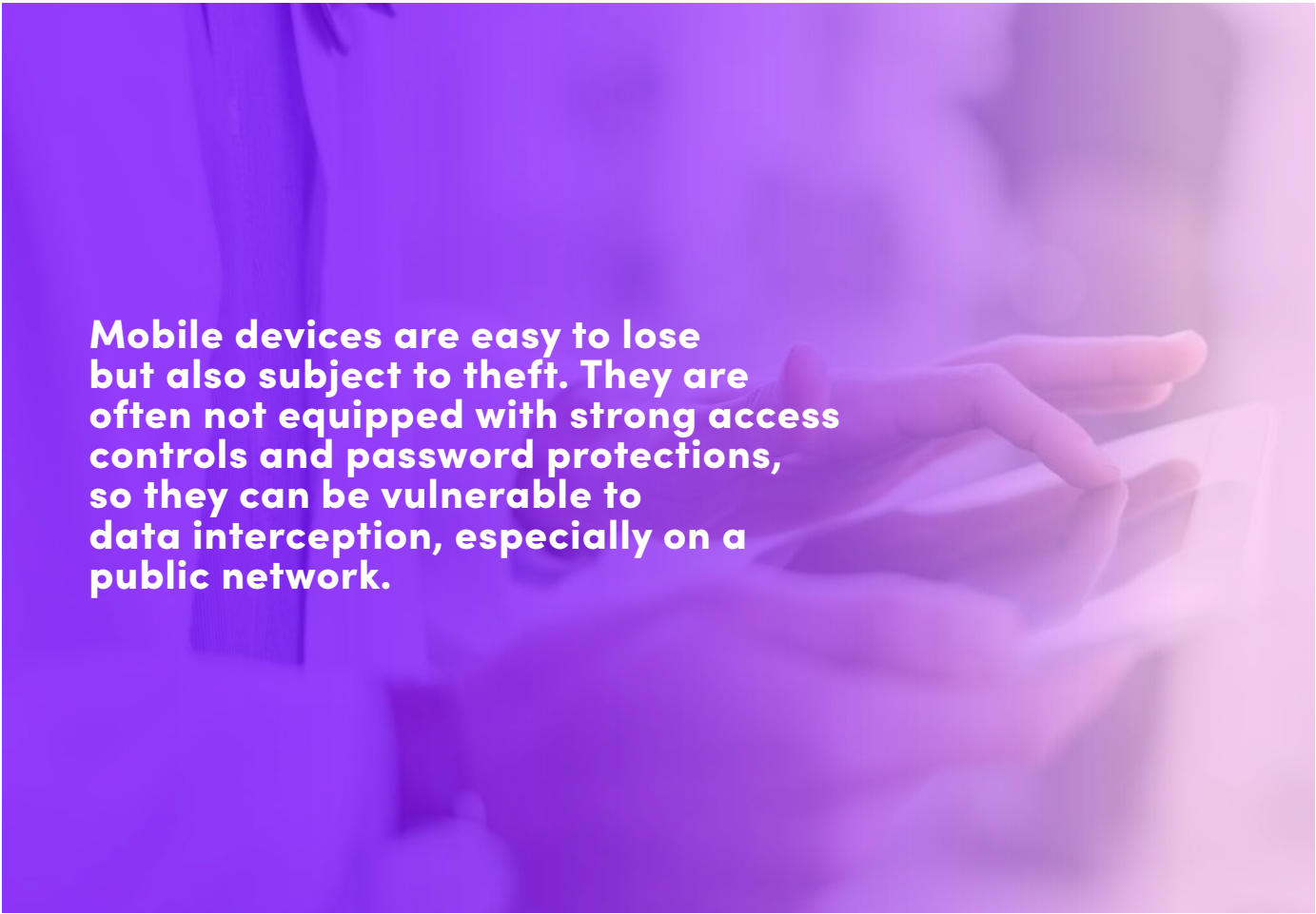


Source: US Department of Health and Human Services Office for Civil Rights



Insider Threats. Insiders can be unwitting or intentional threats. Healthcare environments are high-stress, and well-meaning workers regularly juggle too many demands on their time. They may not understand the breadth of sophisticated cyber threats and risks their organization faces. They use all manner of mobile devices and may sometimes forget to handle them securely. They also often have access to sensitive data on their organization's systems and networks, putting dishonest workers in the perfect position to compromise them. Verizon's [2022 Data Breach Investigations Report](#) noted that 39% of healthcare breaches were caused by insiders.

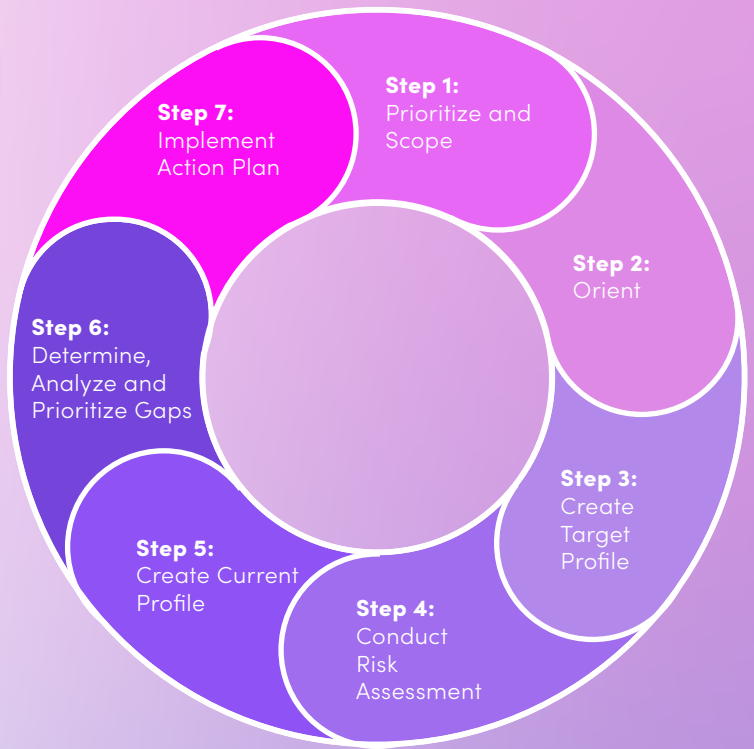
A Growing Threat Vector: Mobile Devices. Healthcare organizations and patients alike use a great variety of mobile and handheld devices to wirelessly transmit sensitive data. Mobile devices are easy to lose but also subject to theft. They are often not equipped with strong access controls and password protections, so they can be vulnerable to data interception, especially on a public network. If patients' mobile devices get compromised, they may unwittingly give attackers direct access to a healthcare network when logging on through the device. But especially in clinical environments where things are moving quickly, healthcare devices should be digitally secured, and workers should take extra care to maintain physical control of mobile devices and prevent the viewing of any health data on them by people who are not authorized to see it. Realistically, in hurried clinical environments, mistakes happen.



Mobile devices are easy to lose but also subject to theft. They are often not equipped with strong access controls and password protections, so they can be vulnerable to data interception, especially on a public network.

Useful Guidance from the Department of Health and Human Services (HHS) Cybersecurity Framework Implementation Guide

The US Department of Health and Human Services' Joint Cybersecurity Working Group published the [Cybersecurity Framework Implementation Guide](#) to help healthcare and public health organizations better implement sound cybersecurity and cyber risk management practices. The guide leverages the industry standard [National Institute of Standards and Technology \(NIST\) Cybersecurity Framework](#) and identifies 7 steps for healthcare organizations to follow for implementing cybersecurity.



Health Care Implementation Activities by Step

Implementation Process Steps	Inputs	Activities	Outputs
Step 1: Prioritize and Scope	<ol style="list-style-type: none"> 1. Risk management strategy 2. Organizational objectives and priorities 3. Asset inventory 4. Informative Reference(s) 	<ol style="list-style-type: none"> 1. Organization determines where it wants to apply the informative Reference(s) to evaluate and potentially guide the improvement of the organization's capabilities 2. Threat analysis 3. Business impact analysis 4. System categorization (based on sensitivity & critically) 	<ol style="list-style-type: none"> 1. Usage scope 2. Unique threats
Step 2: Orient	<ol style="list-style-type: none"> 1. Usage scope 2. Risk management strategy 3. Informative Reference(s) 	<ol style="list-style-type: none"> 1. Organization identifies inscope systems and assets (e.g., people, information, technology, and facilities) and the appropriate regulatory and other authoritative sources (e.g., cybersecurity and risk management standards, tools, methods, and guidelines) 	<ol style="list-style-type: none"> 1. In-scope systems and assets 2. In-scope requirements (e.g., organizational, system, regulatory)

Implementation Process Steps	Inputs	Activities	Outputs
Step 3: Create a Target Profile	<ol style="list-style-type: none"> Organizational objectives Risk management strategy Detailed usage scope Unique threats Informative Reference(s) 	<ol style="list-style-type: none"> Organization selects one or more Informative References and creates a tailored overlay based on a risk analysis that considers the unique threats identified in the prioritization and scoping phase Organization determines level of effectiveness or maturity desired in the selected controls 	<ol style="list-style-type: none"> Target Profile (Tailored overlay of one or more Informative References) Target Tier
Step 4: Conduct a Risk Assessment	<ol style="list-style-type: none"> Detailed usage scope Risk management strategy Target Profile Informative Reference(s) 	<ol style="list-style-type: none"> Perform a risk assessment for in-scope systems and organizational elements 	<ol style="list-style-type: none"> Risk assessment reports
Step 5: Create a Current Profile	<ol style="list-style-type: none"> Risk assessment reports Informative Reference(s) 	<ol style="list-style-type: none"> Organization identifies its current cybersecurity and risk management state 	<ol style="list-style-type: none"> Current Profile (Implementation status of selected controls) Current Tier (Implementation maturity of selected controls, mapped to NIST Cybersecurity Framework Implementation Tier model)
Step 6: Perform Gap Analysis	<ol style="list-style-type: none"> Current Profile Target Profile Organizational objectives Impact to critical infrastructure Gaps and potential consequences Organizational constraints Risk management strategy Risk assessment/analysis reports Informative Reference(s) 	<ol style="list-style-type: none"> Analyze gaps between Current and Target Profiles in organization's context Evaluate potential consequences from gaps Determine which gaps need attention Identify actions to address gaps Perform cost-benefit analysis (CBA) or similar analysis on actions Prioritize actions (CBA) or similar analysis and consequences Plan to implement prioritized actions 	<ol style="list-style-type: none"> Prioritized gaps and potential consequences Prioritized implementation plan
Step 7: Implement Action Plan	<ol style="list-style-type: none"> Prioritized implementation plan Informative Reference(s) 	<ol style="list-style-type: none"> Implement actions by priority Track progress against plan Monitor and evaluate progress against key risks using metrics or other suitable performance indicators 	<ol style="list-style-type: none"> Project tracking data New security measures implemented

CHAPTER 3

Potential Impacts of Cyberattacks on Healthcare Services Institutions

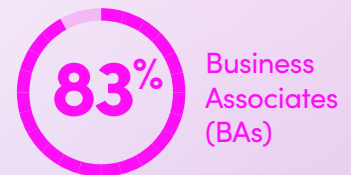
Despite being such attractive targets, many healthcare organizations struggle with implementing effective cybersecurity. An [audit report](#) from the US Department of Health and Human Services Office for Civil Rights found that 86% of Covered Entities (CEs) and 83% of Business Associates (BAs) didn't meet expectations for a cyber risk assessment. Also, 94% of CEs and 88% of BAs didn't meet expectations for effective risk management.

That lack of preparedness, compounded by the rate of attacks, imposes some heavy costs on organizations in this sector. For instance, the average cost for remediating a ransomware attack is \$1.27 million USD, with some studies reporting the total average cost for a ransomware attack in healthcare as being [\\$4.6 million per incident](#). According to the American Hospital Association, remediating a healthcare breach costs nearly three times what it costs for other industries—\$408 on average for a stolen health record vs. \$148 for a stolen non-health record.

Of course, cyberattacks on healthcare organizations can have far more serious and even tragic consequences than financial loss. Patient safety and care delivery can be seriously compromised. In the event of a disruption like a ransomware attack, healthcare organizations can lose access to medical records and even equipment, so patients can't receive the care they need. Shutdowns in hospital systems can and have led to otherwise preventable patient deaths. A study by the Ponemon Institute found that more than 20% of healthcare organizations hit with a ransomware attack or other IT compromise experienced an increase in mortality rates.

Cyberattacks on PHI also pose a risk to patient privacy, which puts the patient at risk as well as the healthcare organization for not complying with regulations like the Health Insurance Portability and Accountability Act (HIPAA) and others to which they are subject.

Failing to protect PHI can have catastrophic consequences. In Finland, for example, a psychotherapy company, Vaastamo, was victim to a ransomware attack whereby the extorters demanded money from both the company and over 30,000 clients. While the extorter was eventually arrested, the Finnish Data Protection Authority fined the company €608,000 for breaching the provisions of the General Data Protection Regulation (GDPR), which led to Vaastamo's bankruptcy in 2021.



didn't meet expectations for a cyber risk assessment.



didn't meet expectations for effective risk management.

Source: US Department of Health and Human Services Office for Civil Rights

The Healthcare Industry Faces Strict Regulations

Personal Health Information (PHI) has long been considered very sensitive, and there are a breadth of rules and regulations enacted to protect it. While the privacy of US citizens' data had traditionally been covered by a patchwork of industry-specific laws, that changed in 1996. Since then, several broad regulations have been put in place:

The **Health Insurance Portability and Accountability Act (HIPAA)** is a US law that requires the creation of national standards to protect sensitive patient health information from being disclosed without the patient's knowledge or consent. All healthcare providers, health insurance plans, and associated businesses that process PHI are required to abide by HIPAA. The US Department of Health and Human Services (HHS) issued the **HIPAA Privacy Rule** to detail the permitted and required uses of PHI. The subsequent **HIPAA Security Rule** detailed requirements for electronically protected health information. And the HIPAA Breach Notification Rule was enacted to require covered entities to provide notification following a breach of PHI.

Title 42 of the Code of Federal Regulations (CFR) Part 2 restricts the disclosure of substance use disorder (SUD) patient records that include the identity, diagnosis, prognosis, or treatment of any patient connected to any substance abuse program or activity conducted, regulated, or directly or indirectly assisted by the US government.

Other countries also have strict regulations that protect PHI. For instance, the **European Union General Data Protection Regulation (GDPR)** protects all data pertaining to the health status of a European citizen that reveals information relating to the individual's past, current, or future physical or mental health status. The GDPR is broader than HIPAA in that it pertains to any type of personal information, of which PHI is only one type. It also applies to controllers and processors of data, so it extends beyond HIPAA's covered entities.

Canada has the **Personal Information Protection and Electronic Documents Act (PIPEDA)**, which applies to private-sector organizations that collect, use, or disclose personal information as part of a commercial activity. Like the European GDPR, PIPEDA's scope is broader than health data but certainly includes it. All clinicians and organizations that collect personal data are required to implement security safeguards to protect it against loss, theft, unauthorized access, use, or disclosure.

Many other countries also have their own laws and regulations to which in-country healthcare providers are subject. But with the widespread use of electronic health records, increasing patient access to those records over mobile devices, and the huge number of cyberattacks on this sector, regulators everywhere are wondering if existing laws are enough. It is quite likely that in the not-too-distant future, tighter regulatory controls may appear.






It is quite likely that in the not-too-distant future, tighter regulatory controls may appear.

The Value of Extended Threat Defense Technology in Combating Healthcare Cyberattacks

The multitude of cyber-related challenges facing healthcare institutions demands an elevated level of security to address the greatly increased risks in the modern environment of mobile devices and telehealth. The current reality is that most mobile applications used by healthcare organizations are not well protected. Since it's becoming more and more difficult for hackers to bypass enterprise-level security solutions deployed by larger healthcare organizations, bad actors look for alternative entry vectors and discover that apps offer a new and easier path.

Extended Threat Defense (XTD) is the leading cybersecurity solution that secures healthcare organizations from risks originating from mobile applications at the edge. While many companies have some form of cybersecurity protection for employer-issued managed devices and personal "bring your own devices" (BYOD), XTD addresses multi-vector threats stemming from unmanaged (consumer/patient) mobile devices like smartphones and tablets.

That specifically includes the range of multi-vector threats that previous cybersecurity solutions like mobile threat defense (MTD) and extended threat detection and response (EDR) miss.

 MTD	 XDR	 XTD
<p>Provides real-time protection against threats and allows organizations to remotely manage and secure their mobile devices.</p>	<p>Provides continuous monitoring of endpoint devices and can detect and respond to a wide range of security threats, including malware, ransomware, and advanced persistent threats.</p>	<p>Helps prevent, detect, respond to and predict cyberattacks originating from the mobile app to the edge, and specifically multi-vector threats.</p>
<p>Works on managed smartphones, laptops and tablets.</p>	<p>Works on managed endpoint devices.</p>	<p>Works on unmanaged devices; any device with an app.</p>
<p>Requires an agent to be installed on the device – protects institution employees' mobile devices, but impractical for end customers.</p>	<p>May take a more comprehensive security approach (continuous monitoring, incident response, and the ability to identify and remediate vulnerabilities). Lacks integration, limiting visibility into the security posture and slowing response.</p>	<p>Uses behavioral analysis like EDR (for detection) combined with other EDR and MTD elements. Ideal when numerous unmanaged consumer devices are connected to a healthcare organization via the app.</p>

XTD monitors new entry vectors from the fastest-growing attack surface—connected apps, APIs, and unmanaged devices. That makes XTD an essential component of effective cyber defenses for healthcare organizations.

Polymorphic Protection: An Important App Security Attribute

An effective XTD platform should include polymorphic protective capabilities. This innovative approach involves constantly changing an application's code and structure to make it more challenging to hack. It's a bit like changing the password of your online accounts every so often to reduce your cyber vulnerability. Some savvy healthcare firms are already protecting their mobile apps with polymorphic protection.

Developers can use various techniques to make an app's code and structure more resistant to attack. One approach is to use obfuscation, which involves modifying the source, byte, or machine code so that it becomes significantly more difficult for hackers to read and understand. In essence, polymorphic protection transforms mobile apps into moving targets, making it much harder—even annoyingly complicated, if not nearly impossible—for hackers to reverse engineer code and develop malware that can penetrate the app's defenses.

That way, the code cannot be used to potentially reveal an app's inner workings or any exploitable vulnerabilities that may be found within it. Obfuscated code is also far less susceptible to tampering. Given the healthcare sector's particular vulnerability to cyberattacks, this approach is crucial for protecting customer information.

To implement polymorphic protection, healthcare organizations must invest in tools that not only shield mobile apps but also provide threat detection and response capabilities.



To implement polymorphic protection, healthcare organizations must invest in tools that not only shield mobile apps but also provide threat detection and response capabilities.

The Verimatrix XTD Approach

Verimatrix XTD offers an affordable and user-friendly solution that utilizes cutting-edge technology to secure mobile apps. With its ability to detect and respond to attacks promptly, Verimatrix XTD ensures the safety of mobile applications and prevents potential damage. Our military-grade, multi-layered security is very difficult for hackers to penetrate. We also help customers monitor the fastest-growing attack surface: consumer endpoints. By analyzing extensive data, Verimatrix XTD can predict future attacks and provide proactive protection.

Covering a Wider Attack Surface with Zero-Code Protection

Verimatrix XTD offers a truly distinct differentiator. Unlike those solutions that necessitate agent installation, Verimatrix XTD offers an agentless, zero-code approach. This capability enables the rich protection, attack detection, and response capabilities to be quickly and easily deployed without cumbersome development or coding—making speed to market a reality.

Addressing Multi-Vector Threats from Consumer Devices

Verimatrix XTD monitors and mitigates cyber threats originating from apps downloaded to unmanaged consumer devices. While many organizations implement cybersecurity measures for managed devices such as BYOD, Verimatrix XTD is one of the few solutions designed to address the multi-vector threats arising from unmanaged mobile devices. XTD can do this because its telemetry is built into its app protection and is automatically passed on to every app instance downloaded. That means any device using the app can be monitored, effectively expanding the coverage of the attack surface into new realms. With Verimatrix XTD, healthcare institutions can secure a broader range of devices, providing comprehensive protection against potential threats.



Detecting and Responding to Active Attacks

Verimatrix XTD's proactive defense strategy involves the swift detection of active attacks and an immediate response to neutralize potential damage. By leveraging advanced threat detection techniques, Verimatrix XTD identifies attacks in real-time, enabling security professionals to disconnect compromised devices promptly. This decisive action safeguards sensitive data and prevents malicious actors from exploiting vulnerabilities.

Proactive Protection through Predictive Analytics

One of the standout features of Verimatrix XTD is its capability to analyze vast amounts of data to predict potential attacks. By employing predictive analytics, the solution can anticipate threats even before they occur. This proactive approach empowers healthcare organizations to stay one step ahead of attackers, ensuring enhanced security for their mobile applications and connected infrastructure.

Understanding Risks and Empowering Security Professionals

Verimatrix XTD is dedicated to helping security professionals comprehend the risks associated with mobile applications and their connections. Highlighting the existence of blind spots by assigning a risk score to every threat found, Verimatrix XTD prompts healthcare organizations to acknowledge and address potential vulnerabilities. XTD provides security professionals with a meticulously designed Software-as-a-Service (SaaS) offering. There is also an optional service incorporating the services of human data scientists to review your account and take response actions on your behalf, adding an extra layer of expert assistance to combat evolving app threats effectively.

A person in a white lab coat is pointing at a tablet computer. The tablet screen displays several medical scans, including what appears to be a brain scan and other anatomical images. The background is a soft, out-of-focus clinical setting.

One of the standout features of Verimatrix XTD is its capability to analyze vast amounts of data to predict potential attacks.

Fight Back with Verimatrix XTD!

As the reliance on mobile applications grows in the healthcare sector, so does the need for robust cybersecurity measures. Verimatrix XTD is an exceptional solution, providing affordable and user-friendly mobile app protection. With its agentless, zero-code approach, it allows for easy and painless deployment, allowing customers to monitor a wider attack surface, including unmanaged patient devices.

Verimatrix XTD effectively detects active attacks and responds promptly, minimizing the potential for damage. By analyzing data and predicting attacks, it enables healthcare organizations to proactively protect their mobile applications. Armed with Verimatrix XTD's comprehensive security offerings and expert support, security professionals can effectively mitigate the risks associated with healthcare app vulnerabilities and secure their digital assets.



Verimatrix – Award-winning Cybersecurity

Verimatrix helps power the modern connected world with security made for people. We protect digital content, applications, and devices with intuitive, people-centered, and frictionless security. We enable the trusted connections our customers depend on to deliver compelling content and experiences to millions of consumers around the world.

We are proud of the market recognition our innovative solutions have earned.



2023 Global Infosec Award for Hot Company in Mobile App Security – Cyber Defense Magazine



2023 Cybersecurity Excellence Awards – Gold Winner for Artificial Intelligence Security and Biggest Brand Growth



2023 Product of the Year, AI and Machine Learning – National Association of Broadcasters (NAB)



2022 Gartner® Hype Cycle™ for Application Security

[Get A Demo](#) of the Verimatrix XTD cloud-native platform, deployed in minutes to protect your apps!

Sources

<https://www.hhs.gov/sites/default/files/2022-retrospective-and-2023-look-ahead.pdf>

<https://www.beckershospitalreview.com/cybersecurity/cyberattacks-in-2022-and-what-hospitals-health-systems-can-learn-going-into-2023.html>

<https://healthitsecurity.com/news/global-cyberattacks-increased-by-38-last-year-healthcare-hit-hard>

<https://www.chiefhealthcareexecutive.com/view/the-11-biggest-health-data-breaches-in-2022>

<https://www.chiefhealthcareexecutive.com/view/nearly-50-million-americans-impacted-by-health-data-breaches-in-2022>

<https://www.aha.org/center/cybersecurity-and-risk-advisory-services/importance-cybersecurity-protecting-patient-safety>

<https://www.securitymagazine.com/articles/99090-experts-warn-of-healthcare-sector-cybersecurity-risks>

<https://www.weforum.org/agenda/2023/05/cyber-attacks-on-healthcare-rise-zero-trust/>

<https://arcticwolf.com/resources/blog/top-healthcare-industry-cyberattacks/>

<https://www.cisecurity.org/insights/blog/cyber-attacks-in-the-healthcare-sector - deep dive stuff if needed on specific threat types>

<https://www.verizon.com/business/resources/T86c/reports/dbir/2022-data-breach-investigations-report-dbir.pdf>

<https://www.verizon.com/business/resources/reports/dbir/2022/healthcare-data-breaches/>

<https://www.insiderintelligence.com/content/healthcare-cybersecurity-2023-hive-s-shutdown-good-news-cyberattacks-only-getting-worse>

<https://expertinsights.com/insights/healthcare-cyber-attack-statistics/>

<https://www.upguard.com/blog/cybersecurity-regulations-and-frameworks-healthcare>

<https://www.himss.org/resources/cybersecurity-healthcare>

<https://www.healthcareitnews.com/news/healthcares-new-roadmap-cybersecurity-resilience>

<https://www.fiercehealthcare.com/health-tech/industry-voices-healthcare-sector-under-constant-cyberattacks-are-tighter-regulations>

<https://healthitsecurity.com/news/addressing-mobile-device-security-risks-in-healthcare>

<https://www.aha.org/system/files/media/file/2022/09/fbi-pin-tlp-white-unpatched-and-outdated-medical-devices-provide-cyber-attack-opportunities-sept-12-2022.pdf>

<https://aspr.hhs.gov/cip/hph-cybersecurity-framework-implementation-guide/Documents/HPH-Sector-CSF-Implementation-Guide-508.pdf>

<https://www.hhs.gov/sites/default/files/hipaa-audits-industry-report.pdf>

https://www.healthit.gov/sites/default/files/Top_10_Tips_for_Cybersecurity.pdf

<https://explore.avertium.com/resource/cyber-threats-in-the-healthcare-industry>

<https://www.healthcaredive.com/news/cyberattacks-hospitals-disrupt-operations-patient-care-Ponemon/631439/>

https://en.wikipedia.org/wiki/Vastaamo_data_breach