Healthcare IT Security Evaluation Guide

Solution Brief

CYLANCE

Insecure data is a double risk for healthcare institutions.

Healthcare in the Crosshairs

Healthcare IT staff play a critical role in safeguarding protected health information (PHI). Prioritizing data protection can be difficult for IT departments primarily focused on maintaining technology vital for day-to-day operations. Cybersecurity is often an additional responsibility given to healthcare techs who have little or no expertise on security issues. It is important for IT departments to select security solutions that do not overburden their technical resources or overextend their staff. This guide can assist healthcare IT professionals with improving the cybersecurity of their organization.

The healthcare industry's possession of valuable patient data puts it in the crosshairs of both threat actors and regulatory agencies. Threat actors are attracted by the lucrative nature of electronic health records, which often command exponentially more money than other personal information. Owning this sensitive data makes healthcare providers a primary target for advanced persistent threat (APT) groups and other cybercriminals.

Legislators, seeking to protect consumers, have passed numerous regulations governing the protection of PHI. Two well-known examples are the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) Act. Other privacy regulations, like the European Union's General Data Protection Regulation (GDPR), also affect the healthcare industry. Many regulations include hefty fines for organizations that fail to secure sensitive patient data.

Cybersecurity Challenges

Healthcare IT teams face several challenges that make effective cybersecurity difficult to implement.

Diverse Technology

Healthcare institutions rely on diverse technology for providing patient care. Computers perform many specialized roles and may run Windows, MacIntosh, or Linux operating systems. Other medical technology must also be protected, particularly devices administering critical patient care. Securing these systems requires a solution that will protect each device and protect the communications between various platforms.

Imperfect Visibility

Maintaining visibility into the technological environment is a critical aspect of breach prevention. Early threat detection can avert a disastrous system compromise. It is important for security solutions to provide an intuitive, real-time overview of organization technology, down to the individual devices. Solutions that continuously monitor systems and automatically respond to threats can play a critical role on teams with limited technical personnel.

Competition for Resources

Healthcare organizations dedicate the bulk of their resources to providing patient care. This requires strong justifications for every dollar budgeted elsewhere. Convincing executives to invest in security solutions that prevent losses rather than toward directly administering patient care can be challenging. Yet protecting PHI is a form of caring for patients and like medicine, an ounce of prevention is worth a pound of cure.

The Answer Is AI

Healthcare IT professionals are responsible for making security recommendations that meet the needs of their institution. Their expertise is critical for keeping healthcare organizations compliant with privacy regulations and securing patient data.

Cylance® offers an innovative way to protect healthcare technology by using artificial intelligence (AI) to solve cybersecurity challenges. Cylance's AI-based security agents can detect and prevent known, unknown, and zero-day payloads with 99.1% efficacy.

Artificial intelligence (AI) can work with IT teams to maximize productivity and effectiveness.

CylancePROTECT® delivers a machine learning model trained to identify malicious executables directly on devices. Independent testing from SE Labs has proven that CylancePROTECT holds an average predictive advantage of 25 months over major malware families. This means the Cylance 2015 AI model was able to identify and prevent a threat that did not exist until 2017, over two years after the model was trained and deployed.

In addition to predictive advantage, CylancePROTECT provides:

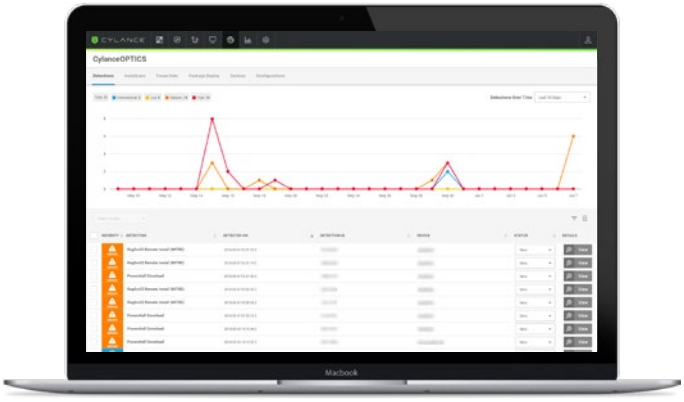
- **Script management and memory exploit prevention —** offering protection against fileless attacks that use legitimate system resources to compromise systems
- **Application control for fixed-function devices —** ensuring unnecessary and possibly insecure software is not installed
- **Automatic detection and blocking of malicious email attachments —** a key feature for preventing phishing attacks
- **Zero-day payload prevention —** detects new and emerging malware and stops cyber attacks before they launch
- **Device control —** Blocks Android, iOS, and USB drives from transferring sensitive data
- **Windows, MAC, and Linux compatible —** supporting a wide range of healthcare technology

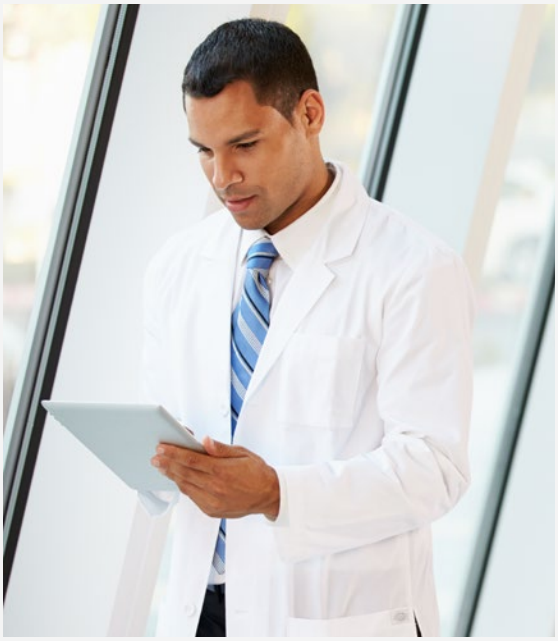
CYLANCE OPTICS

Cylance's endpoint detection and response (EDR) solution, CylanceOPTICS™, also deploys machine learning models that run locally on the endpoint. These models are trained to identify malicious behaviors on the device and take immediate response actions without relying on static behavior rules. By flagging suspicious system behavior, CylanceOPTICS can alert security teams to potential fileless attacks, insider threats, and account abuse.

CylanceOPTICS also provides:

- **Consistent cross-platform visibility**
- **Root Cause Analysis**
  - **InstaQuery —** allows threat responders to compare standard system behavior and new, suspicious behavior
  - **Focus View** — creates a timeline of events leading up to each detection, highlighting security gaps overlooked by routine observations
  - **Enterprise-wide threat hunting**
- **Remote forensic data collection —** individual devices can provide local information, giving context to an attempted attack
- **Automated response —** respond to potential threats or behavioral violations automatically, allowing responders to focus on other issues





Healthcare IT Security Checklist

Healthcare IT professionals are responsible for protecting the infrastructure and data critical to the operation of their organization. Their foresight and expertise can make the difference between surviving a cyber attack and suffering irreparable losses. The following questions can help IT professionals evaluate their organization's current level of cybersecurity and offer focused recommendations:

- What am I responsible for securing?
- Are my existing tools/practices sufficiently protecting patient data and other PHI?
- Does our current security solution proactively prevent threats or react to known threats?
- Does our current security solution alleviate pressure to the current IT team or create additional demands?
- Is our current security solution well integrated with the equipment vital to our core business?

+1-844-CYLANCE
sales@cylance.com
www.cylance.com
400 Spectrum Center Drive, Irvine, CA 92618

CYLANCE

20180926-1204