Healthcare Solution Brief

Higher economic rewards drive attackers to target healthcare organizations and patient data

Summary

Healthcare organizations present special security challenges that vary from other traditional manufacturing or office environments. The costs associated with failure to provide adequate security can be exponentially higher than other similarly-sized businesses.

The healthcare industry is a vast, complex network including very large health systems, single physician practices, public and private payers, research institutions, medical device developers and software companies, and a diverse and widespread patient population. These bodies are governed by international, federal, and state regulations that can complicate security measures, making value judgments on security products difficult.

Compliance Mandates

Due to the sensitive nature of health information, healthcare organizations fall under many stringent regulations. NIST, HIPAA, HITECH, PCI-DSS, and private insurance regulations are in place to ensure fundamental security provisions are enacted and followed, but compliance with mandates does not always equate to security. Medical device security, personnel issues, ransomware attacks, and mobile device protection further complicate security and privacy matters. A recent report by *CSO Online* cites as evidence of this that the profit from sales of records on the dark web is 10 times that of regular identity theft. This increased economic motive drives the increased likelihood of attacks on healthcare organizations. Additionally, the private information found within healthcare organizations can be leveraged to commit fraud. Information such as insurance and Medicare numbers can be used to file false claims. According to the Medical Identity Fraud Alliance, Medicare fraud cost $6 billion over a two-year period. All this has led to a massive increase in cyber attacks on healthcare organizations, up 125% since 2010.

Ransomware

Healthcare organizations have found themselves in the crosshairs of several costly ransomware attacks. Often, a well-intended mouse click on a seemingly innocuous hyperlink has resulted in victims paying tens of thousands of dollars to liberate their data from unscrupulous attackers bent on encrypting this information in exchange for payment. A recent study by the Ponemon Institute indicates that the average healthcare organization experiences more than one ransomware attack per month. Further, the cost of a security breach is more than 2.5 times as compared to breaches in other organizations, and estimated to be $380 per record.

The Cylance® Approach

Cylance has proven effective against such cyber attacks and data breaches. This is due to the architecture of the solution. Historically, security providers relied on virus definition signatures developed from a historical view of malware. AV-TEST reports new malware exceeding 120 million variants in 2017, making signatures based on historical views ineffective and obsolete. Cylance takes a different approach. At the core of Cylance's unique malware identification capabilities is a revolutionary machine learning research platform that harnesses the power of algorithmic science and artificial intelligence. It analyzes and classifies hundreds of thousands of characteristics per file in real time, breaking them down to an atomic level to discern whether a file is safe to run.

About Cylance

Cylance develops artificial intelligence to deliver prevention-first, predictive security products and smart, simple, secure solutions that change how organizations approach endpoint security. Cylance provides full-spectrum predictive threat prevention and visibility across the enterprise to combat the most notorious and advanced cybersecurity attacks, fortifying endpoints to promote security hygiene in the security operations center, throughout global networks, and even on employees' home networks. With AI-based malware prevention, threat hunting, automated detection and response, and expert security services, Cylance protects the endpoint without increasing staff workload or costs. We call it the Science of Safe. .

Cylance doesn't employ this technology at the expense of simplicity, ease of use, or burden on the endpoint or administrator. CylancePROTECT's architecture consists of a small agent that integrates with existing software management systems or Cylance's own cloud console. The endpoint will detect and prevent malware through the use of tested mathematical models on the host, independent of a cloud or signatures. It is capable of detecting and quarantining malware in both open and isolated networks without the need for continual signature updates. Cylance's mathematical approach stops the execution of ransomware regardless of having prior knowledge or employing an unknown obfuscation technique. No other anti-malware product compares to the accuracy, ease of management, and effectiveness of CylancePROTECT.®

Conclusion

Recognizing the healthcare industry's unique set of challenges, Cylance has responded to this demand with lightweight and easy-to-use security products and specialized security services. Cylance does this by leveraging artificial intelligence to predict attacks, seeking first to prevent successful attacks rather than respond, and offering scalable threat detection and response for root cause analysis and threat hunting. Cylance's AI-based algorithm resides in a miniature model on the endpoint and is updated only semi-annually, requiring no daily deep scans that bog down endpoint and network performance. Deployment, management, and reporting are executed through an intuitive, cloud-based console for simplicity without compromise of efficacy. This is why numerous healthcare organizations leverage CylancePROTECT and CylanceOPTICS,™ and often deploy Cylance Consulting Services to assist with deployment and configuration, as well as compromise assessments and penetration tests.

Contact

To learn more about how Cylance can help with these and other healthcare security challenges, please visit www.cylance.com or call +1-877-973-3336 for a discussion with a Cylance representative.

+1-844-CYLANCE
sales@cylance.com
www.cylance.com

CYLANCE

20190110-0384