Assault On Healthcare

HITECH, Compliance, and the Growth of the Ransomware Economy: A Devastating Assault on Healthcare

CYLANCE™

INTRODUCTION

The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 was designed to be a $27 billion transformation of personal health information (PHI) into electronic health records (EHRs). Yet, one unintended consequence of the landmark legislation is the historic number of assaults by cybercriminals on the healthcare industry. As part of the U.S. Government's 2009 economic stimulus package, HITECH provided incentives for the healthcare industry to transition patient data from paper files locked away in doctors offices to electronic records on the information superhighway, accessible from anywhere in the world.

In theory, EHRs would provide patients and their caregivers with a single source in which to house their medical history and timely data on any current treatments. They would eliminate many of the patient care mistakes that occur due to human error, such as illegible handwriting. They would also supply more efficient patient care by giving healthcare administrators easier access to a holistic picture for each patient.

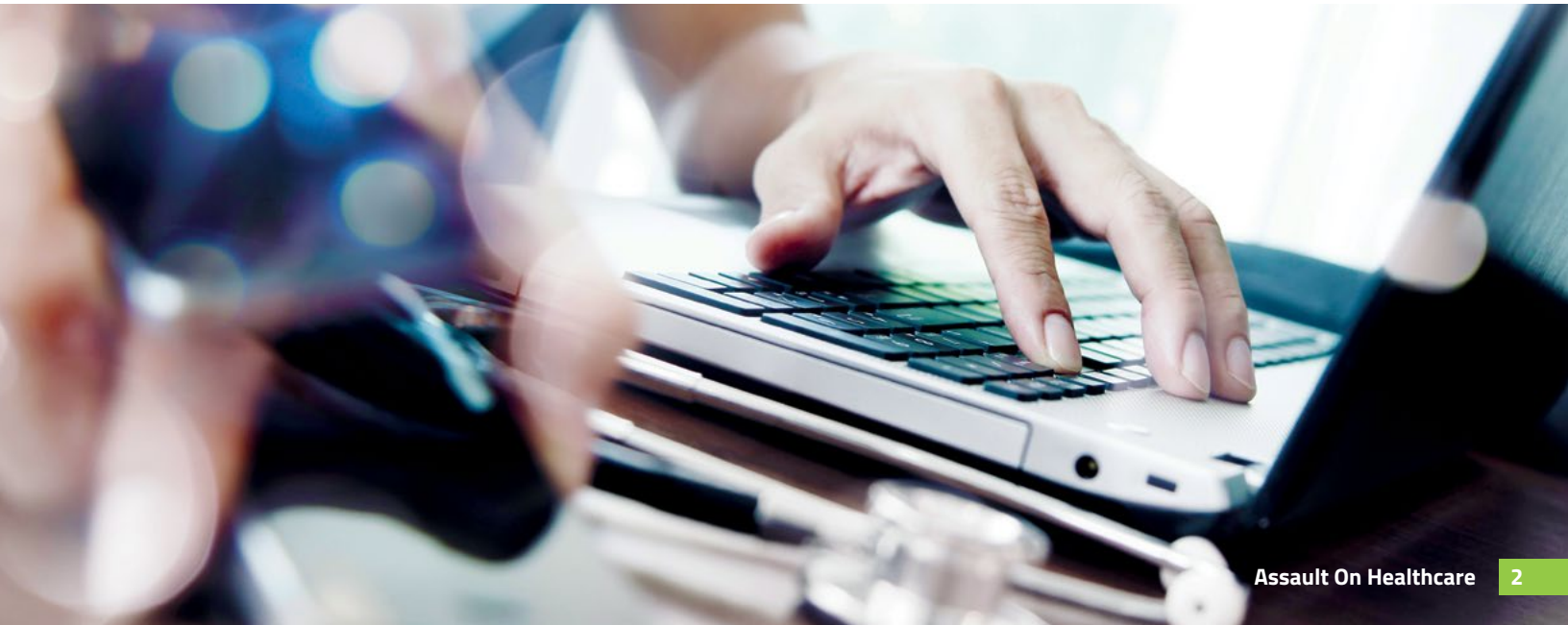
Unfortunately, one of the worst side effects of EHRs has been the movement of personal and critical patient data from secure paper records to easily accessible digital files. What was intended to create accessibility for the benefit of the patient has resulted in accessibility for the benefit of cybercriminals with nefarious intentions, including reselling the information online, holding it ransom for vast sums of money, and committing identity theft for the purpose of obtaining free medical procedures and medications.

With patient data available to hackers on hospital and healthcare provider networks, cyberattacks in the healthcare industry have skyrocketed. The growth in ransomware attacks, in particular, has been a scourge on the U.S. healthcare system. The impact has taken multiple forms, including system and operations downtime, and patient care disruptions.

Ransomware is a type of malware that is typically delivered via a phishing email, which is designed to look like a legitimate email received from a trusted sender. The email will contain an attached file, such as a Microsoft® Word document, that when opened, will launch a piece of ransomware. The attachment itself may look and act normal to delay the victim from noticing the behind the scenes deployment. Meanwhile, the ransomware will seek out and encrypt critical files on the user's machine, as well as on any connected devices.

Once encryption is complete, the ransomware will display an image on-screen with instructions on how the victim can remit a ransom to obtain a decryption code. This ransom is typically paid in bitcoins, which provides the malware author with an untraceable form of instant payment.

Ransomware attacks can lead to dramatic financial losses for hospitals, healthcare providers, and other healthcare-based enterprises. Beyond the ransom that victims may have no choice but to pay in order to regain access to critical operational files, they will also incur the cost of notifying patients of the data breach; plus the expense of regulatory investigations, potential civil litigation, significant system upgrades, and machine restoration; as well as the revenue lost from turning away patients who cannot be processed or treated during a breach. One of the costliest and most disruptive by-products of a healthcare ransomware PHI breach is a judgment by the U.S. Department of Health & Human Services (HHS) that a HIPAA compliance violation has occurred—the fines for which max out at $6 million per year according to the website HIPAA Journal and other corroborating sources.



Ransomware, Technology and Healthcare Trends Converge

In a 2015 report published by the Institute for Critical Infrastructure Technology, researchers explained *new attacks will become common while unattended vulnerabilities that were silently exploited in 2015 will enable invisible adversaries to capitalize upon positions that they have previously laid claim.* Specifically, the report defined healthcare as one critical area where ransomware attacks *will wreak havoc on America's critical infrastructure community.* In addition, researchers at IDC Health Insights predict that during 2016, ***CYBERSECURITY BREACHES WILL TOUCH ONE IN THREE PUBLIC HEALTH RECORDS.***

As predicted, during the first two quarters of 2016, the world was introduced to an advanced level of healthcare ransomware assault that had been unprecedented within the industry. Several large hospitals were hit with attacks that threatened the well-being of patients, and jeopardized each hospital's ability to ensure the integrity of patient PHI.

Hospital	Attack Date	Response	Ransom Demanded
Hollywood Presbyterian Hospital	February 2016	Ransom paid	40 Bitcoins ($17,000)
Methodist Hospital (Henderson, KY)	March 2016	Ransom paid	Undisclosed amount
Prime Healthcare Services, Inc. (Chino Valley Medical Center, Desert Valley Hospital, and Alvarado Hospital Medical Center with service disruptions in other locations)	March 2016	Hospital systems shut down by Locky ransomware	Undisclosed
MedStar Health (10 hospitals in Maryland, Washington, D.C.)	March 2016	Hospital systems infected by Samsam ransomeware; system interfaces of hospital immediately shut down; no ransom paid	45 Bitcoins ($18,500)
Kansas Heart Hospital	May 2016	Ransom paid; second ransom not paid	Undisclosed amount

While healthcare organizations work ardently to improve their cyber risk strategies, the challenge is daunting. An increasingly sophisticated community of ransomware authors, driven by the growth in financial incentives, continues to develop complex and evolving threat vectors.

Recent trends in ransomware, healthcare and technology are converging to help cybercriminals find a wealth of victims:

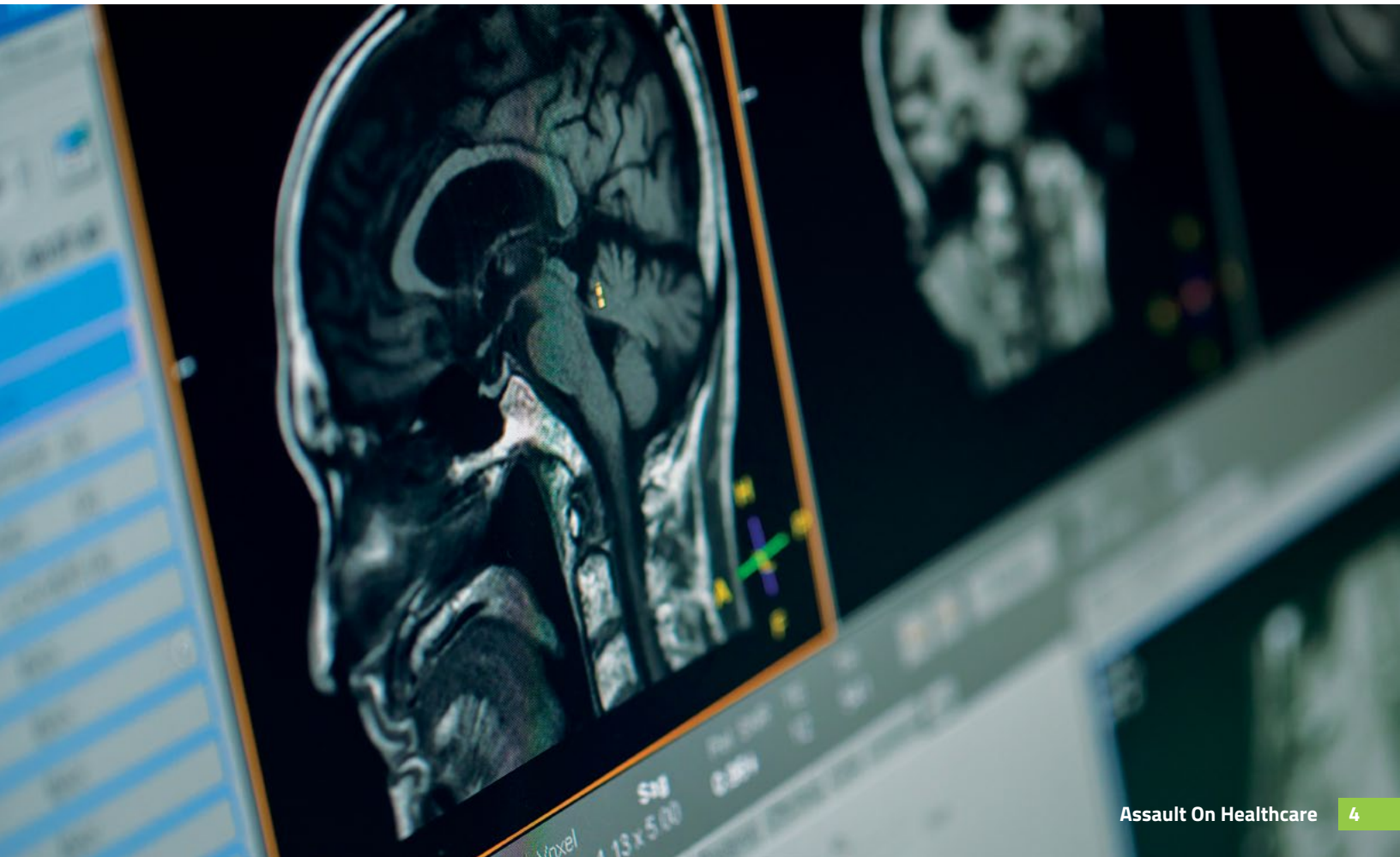
New and Evolving Variants
Early in 2016, the Locky strain of ransomware began to surface. Locky was used to shutdown three Prime Healthcare hospitals in California and disrupt services at several of their affiliate locations. The Locky attack was designed to scramble system files and rename them. Users must then purchase the decryption key using bitcoins. In April 2016, the FBI issued a warning regarding another ransomware infection, Samsam, the ransomware behind an attack on 10 hospitals in the Baltimore and Washington, D.C., area. Samsam is unique in its focus on servers instead of end users. These are only two examples of how new and evolving ransomware code is constantly changing to create a growing landscape of threat vectors.

Ransomware-as-a-service
While some ransomware attacks come from highly skilled programmers with a portfolio of successful attacks, thanks to the proliferation of ransomware-as-a-service, novice cybercriminals are often finding success as well. To expand their reach and operations, ransomware specialists offer their code and expertise to novice hackers online for a nominal fee, no fee at all, or a cut of any ransom obtained.

The Internet of Things & Shrinking Platform Immunity
The expanding reach of ransomware into previously untouched platforms creates new vulnerabilities as the Internet of Things grows. Gone are the days when Windows environments were the only platforms at risk of a cyberattack. Ransomware has now also plagued the users of Android devices, and, in March 2016, researchers discovered the first-ever ransomware attack targeted at Apple's OS X software for Macs.

Medical Technology Velocity
The rate of medical technology innovation puts hospitals and healthcare systems at incredible risk of attacks that can disable the functionality of life-saving equipment and systems. In an attempt to keep up with demand, medical device manufacturers may compromise on risk management practices. This problem can be further complicated by a reliance on a complex global supply chain and vendor network that can also be willing to sacrifice device security for product launch expediency.

Increasing Supply of Bitcoin
The growing availability and use of anonymous digital currency such as bitcoin has made it possible for extortionist cybercriminals to raise the stakes and demand larger and larger ransoms without fear of detection by law enforcement agencies such as the FBI.



Why Healthcare?

The typical healthcare environment is a perfect storm when considering vulnerabilities that attract ransomware attacks:

The Value of PHI
The goal of a healthcare ransomware attack is often to hold prized personal health information hostage in the hopes of either receiving payment, or to sell on the information to third parties. Today, PHI data is more valuable on the black market than personal information from financial institutions. In some industries, the ability to access data from prior system backups is sufficient to return the business to an acceptable state of operational effectiveness. However, the fluid nature of healthcare settings requires the immediate and dependable availability of real-time data. Backups even a few minutes old can put patients at risk.

PHI is also valuable to cybercriminals in creating a market for multiple secondary transactions. As published by the FBI Cyber Division, *cybercriminals sell personal health information on the black market at a rate of $50 for each partial electronic health record, compared to $1 for a stolen social security number or credit card number.*

The Sense of Urgency
The obligation of healthcare organizations to maintain the integrity of patient care environments and the accuracy of medical records is a powerful incentive to return the environment to its original state. This sense of urgency by healthcare providers to return to normal operations as quickly as possible provides a strong advantage to the perpetrators of ransomware attacks.

The Penalty
When hospitals lose control of their data, they risk being in violation of HIPAA regulations as outlined in the HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414. The rule requires HIPAA-covered entities and associates to provide notification following a breach of unsecured PHI.

Older and less sophisticated strains of malware wrap or encrypt the PHI data, never moving it from the server or desktop environment. A party who does not have the proper authorization cannot view it. However, more sophisticated malware variants are able to access the data, and some sit dormant for long periods of time before creating the breach. In such a case, the burden of proof is on each healthcare organization to have solutions in place that can clearly determine whether or not the ransomware viewed or accessed the PHI data, enabling the ransomware author to potentially download or view it. Since September 2009, the HHS Office for Civil Rights has recorded 222 HIPAA cybersecurity breaches that affected 500 or more individuals.

The healthcare industry is not alone in its responsibility to ensure the protection of sensitive and private health information. Any company in possession of health-related information about employees falls under the same HIPAA compliance scrutiny. For example, a Sony Pictures cyberattack that obtained corporate records resulted in a class action lawsuit and undisclosed settlement with 50,000 employees.

The Complexity
Large health systems are particularly vulnerable to attacks on less secure parts of their systems given the siloed nature of the systems and technologies created using software from numerous independently managed vendors.

The Ransomware Payments
A number of high-profile ransomware attacks on hospitals have resulted in some of the victims paying tens of thousands of dollars in ransom money to cybercriminals. Their payment of the ransom has led to multiple new attacks on these same organizations. In addition, the success of these ransomeware attacks has emboldened the cybercriminal community as a whole.

The Lack of Preparation

There is a quote that circulates frequently amongst enterprise workers: "A lack of planning on your part does not constitute an emergency on my part." In the case of healthcare cybersecurity prevention, nothing could be further from the truth. The industry's lack of focus on cybersecurity prevention and the resulting emergencies are well documented by both the media and HHS.

A 2015 study conducted by ABI Research states that *the healthcare sector is ill prepared for the new cyberage. Hospitals, clinics, trusts, and insurers are constantly under attack from malicious online agents … Medical identity theft and fraud are on the rise, and healthcare providers are struggling to cope, with the past two years seeing hundreds of instances of data breaches leaking millions of personal records. And yet the industry spends very little on cybersecurity, comparatively to other regulated critical industries. ABI Research calculates cybersecurity spending for healthcare protection will only reach US$10 billion globally by 2020, just shy of 10% of total spend on critical infrastructure security.*

Examples of these gaps in cybersecurity risk management include the continuing presence of deceptive phishing emails and fake website URLs that entice employees into disclosing login information or downloading malware. Additionally, without the appropriate patches, servers can be vulnerable to threats. Without proper protection, medical devices and industrial control networks can also be accessed with potential impact to life-saving systems.

The Lack of Security Awareness Training

A 2015 survey conducted by the Healthcare Information and Management Systems Society revealed that 64% of 297 respondents—each with some responsibility for information security—had experienced a security incident within their healthcare organization caused by phishing. Healthcare professionals, while highly specialized in their clinical disciplines, are not generally well trained in security awareness. The report indicates *otherwise savvy people click on links due to sophisticated impersonation techniques. For instance, a healthcare phishing attack might involve an email that looks as if it's coming from a familiar vendor such as LabCorp with the subject 'Patient Results Available.' The email will look exactly like a LabCorp email. The link in the email will take the recipient to a perfectly "spoofed," identical copy of the login page on LabCorp.com. When the recipient tries to log in, his or her credentials get stolen. Now, the hacker can log into LabCorp and access PHI from the healthcare organization's patient rolls.*

Without proper security training, employees will struggle to identify threats of this nature.

An Ounce of Prevention

In February 2016, the Ponemon Institute released the results of its 2016 State of Cybersecurity in Healthcare Organizations study. According to researchers:

- Healthcare organizations average one cyberattack per month.
- 48% of respondents said their organizations have experienced a security breach involving the loss or exposure of patient information in the last 12 months.
- Only half indicated that their organization has an incident response plan in place.

With findings like this, the answer seems obvious. Benjamin Franklin said, "By failing to prepare, you are preparing to fail." With the current opportunity for healthcare decision makers to hardwire their enterprises with next-generation endpoint protection solutions, the industry could potentially begin to see the reports of cyberattacks drop significantly within the coming 12 months.

The responsibility to take the appropriate steps toward the right solution now lies is in the hands of board members, C-level executives, and IT security specialists. In parallel, employees must be trained to identify phishing events and address them in a way that reduces security risk.

Cylance: Solutions for Every Step in the Kill Chain

Cyberattacks are planned and delivered in nearly the same manner, seldom straying from a high-level process map known as the "Cyber Kill Chain." The only variable is the amount of technical or personal resources cybercriminals spend on the different stages of an attack. No matter where your current internal infrastructure lies on the spectrum of cybersecurity preparedness, you can have confidence in the fact that Cylance stops malicious files before they can execute.

Most endpoint protection platform (EPP) providers are seeking to do one thing: remediate a threat. The concept of remediation implies one important consideration — the reality that an attack has already taken place. There are impressive dashboards designed to help hospital IT managers and device manufacturers control active cybersecurity events. Yet legacy antivirus security solutions do not take into consideration several critical dynamics within the healthcare industry:

- A remediation-dependent system relies upon the management of highly trained IT professionals who can monitor and respond to incidents on a 24/7 basis. This can be a challenge for resource-constrained support organizations.
- Valuable employee time is lost and financial resources consumed while system analysts research events and follow protocols to remediate.
- Zero-day vulnerabilities often go unaddressed.

In February 2016, Gartner, Inc., reported that by 2018, 60% of EPPs will restrict executables that have not been preinspected for security and privacy risks, a value that is almost triple the current 22%. The stage has been set for providers innovating with disruptive solutions that can detect a growing number of variant threats BEFORE they happen while minimizing the endpoint and network IT management burden.

Taking advantage of a revolutionary artificial intelligence agent, Cylance's products and services proactively prevent the execution of advanced persistent threats and malware.

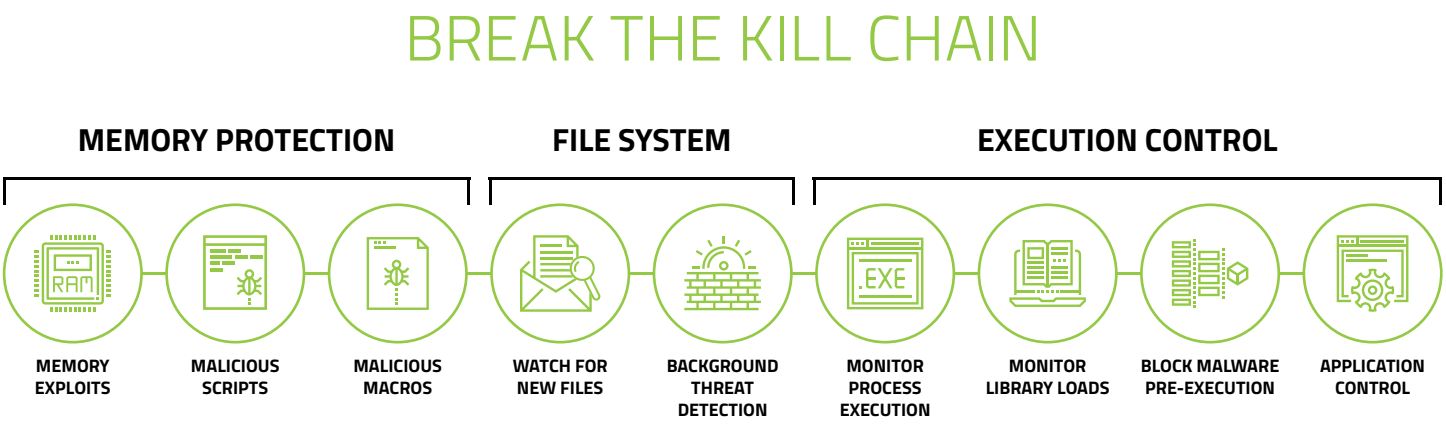
Key Cylance Product and Service Strengths

- Proactively detects new variants and repacked versions of existing malware.
- Delivers a minimal impact on networks and endpoints (continues to work with less than 1% of CPU memory available and no Internet connectivity).
- Offers a cloud-based management console without the requirement of cloud-based detection.
- Generates static file assessment reporting for timely learning across customers and quarantines.
- Expands to OEMs to secure embedded systems and medical devices.
- Supports Windows and Mac devices; Linux available in 4Q16.

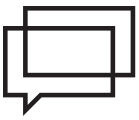
Industry Response

Gartner recognized Cylance as a Visionary in its 2016 EPP Magic Quadrant. Cylance believes this is because it is one of the fastest-growing companies in the history of cybersecurity. In addition, the company provides an innovative new approach that replaces traditional signatures found in legacy antivirus products.

Cylance technology is currently deployed on over six million endpoints and protects over 1,000 clients worldwide, including Fortune 100 organizations and government institutions.



Take the Next Step: PREVENTION



To begin a discussion or for further information on applying artificial intelligence, algorithmic science and machine learning to cybersecurity, please contact:

Chris Coulter
Email: ccoulter@cylance.com
Phone: +1-877-973-3336

Contact Information

To learn more about Cylance, its projects and events, please visit www.cyclance.com.

Cylance
+1-877-973-3336
sales@cylance.com
www.cylance.com
18201 Von Karman, Ste. 700
Irvine, CA 92612

https://www.youtube.com/user/CylanceInc

https://www.linkedin.com/company/cylanceinc

https://www.facebook.com/CylanceInc

https://twitter.com/cylancein