VECTRA®

Protecting patient health and privacy from cyber threats

Real-time, automated threat threat detection and response finds attackers before damage is done

Healthcare is now a top target

The healthcare industry today is one of the top targets of cyber attackers. This has been driven in large part by the digitization of healthcare delivery – IoT devices such as x-ray and MRI machines, drug infusion pumps, blood gas analyzers, medication dispensers and anesthesia machines – as well as medical information.

Intended to improve healthcare outcomes and patient access to their own records, electronic medical records are a major draw for attackers because they bring up to 10 times more than stolen credit card numbers on the black market. In 2015, the top three healthcare-related breaches alone affected an estimated 100 million individuals.

Medical records include healthcare-related data and personally identifiable information (PII) such as Social Security and National Insurance numbers, names, dates of birth, and addresses.

In the United States and many other countries, this sensitive data constitutes protected health information (PHI) that is subject to a wide range of breach disclosure laws.

PHI can be collected or created by a healthcare provider, insurer, employer, clearinghouse or other entity – giving attackers a lot to go after. With PHI in hand, criminals can perpetrate identity theft and medical billing fraud, creating major problems for patients and driving up healthcare costs.

At the same time, more and more attackers are employing ransomware to lock up an organization's data, posing potentially life-threatening consequences for patients.

When Hollywood Presbyterian Medical Center was the victim of a ransomware attack early in 2016, attackers took command of servers and encrypted all databases and systems. The medical center was forced to move high-risk patients to other hospitals, patients' test results and treatment histories were inaccessible, and medical staff was reduced to communicating in person and via fax.

And while other industries are just launching IoT initiatives, healthcare providers already have a large number of IoT devices connected to their networks to improve the quality and delivery of patient care.

These smart medical devices, many of which are IP-enabled, are an easy infiltration point for cyber attackers who are looking to establish a persistent undetected proxy for command and control, steal PHI or launch a crippling ransomware attack.

The escalation of attacks presents serious challenges for the healthcare industry. Security and IT staff are forced to manage two critical priorities that compete for time and resources: Teams must simultaneously stay on top of cyber attackers while also meeting an array of regulatory and compliance requirements.

Vectra® offers healthcare organizations a new and stronger class of security solution that finds attackers automatically before they inflict damage. Combining data science, modern machine learning techniques and behavioral analysis, the Cognito™ automated threat detection and response platform detects every phase of a cyber attack in progress.

Cognito also augments security staff by providing automated Tier 1 analysis and intelligence that exposes actual attack behaviors so security teams can act quickly instead of manually hunting for threats.

Challenges facing the healthcare industry

From family doctors and dentists to hospitals and health insurance giants like UnitedHealth Group, Anthem and Aetna, the healthcare industry is a major target of cyber attacks.

According to a recent study by the Ponemon Institute, data breaches in healthcare are consistently high in terms of volume, frequency, impact and cost. Over the past two years, nearly 90% of healthcare organizations in the study had a data breach, and 45% had more than five, costing the industry an estimated $6.2 billion.

Prompted in part by the availability electronic medical records, criminal cyber attacks are now the leading cause of data breaches in healthcare. Among the greatest threats are:

- Malware, including ransomware, and denial-of-service (DoS) attacks
- Persistent attacks that infiltrate networks to steal or damage PHI, PII and payment card data
- Hidden command-and-control (C&C) communication by remote attackers, including the compromise of medical devices
- Botnets, zombie attacks and other threat vectors

Cyber attackers are successfully infiltrating healthcare organizations in a variety of ways, including:

- Direct attacks against employees and assets, including medical IoT devices
- Through smartphones and computers that patients and visitors bring onsite
- Via third-party providers, such as food and laundry services companies, as well as physicians, anesthesiologists and other medical professionals who contract with healthcare facilities

Medical professionals pose a special risk due to their privileged access to medical records and other target assets. In addition, they regularly use BYOD and remote access technologies, which improve patient care but introduce risks.

Key attack vectors

Just a quick look at some recent breaches highlights the scope of the challenges facing the healthcare industry.

Ransomware attacks

Unfortunately, hospitals have become high-value targets for ransomware; with lives literally at stake, medical institutions can't afford to be denied access to systems and data critical to patient care.

After Hollywood Presbyterian Medical Center paid a ransom of 40 bitcoins (about $17,000) to attackers, other facilities became victims of ransomware, including three in California – Los Angeles County Department of Health, Chino Valley Medical Center and its sister site Desert Valley Medical Center; Methodist Hospital in Kentucky; and MedStar Health in Washington, D.C.

Fast, easy and offering an immediate payout for attackers, ransomware attacks are projected to increase 250% in 2016, according to the Beazley Breach Insights 2016 report.

IoT exploits

IP-enabled medical devices provide an easy entry point for cyber attackers who then can move laterally through a healthcare organization in search of PHI and other target assets.

In 2015, cyber attackers infected medical devices at three hospitals – specifically, x-ray equipment, picture archive and communications systems (PACS) and blood gas analyzers – and used that malware in a persistent attack to gain access to servers from which they stole patient data.

As part of their exploits, the attackers used Zeus and Citadel malware to find additional passwords within the hospital, and tried to use the PACS system as a botnet for C&C communication.

Medical IoT devices pose significant security risks for a variety of reasons. For one, they have a long life. Many medical devices are in use for 10 years or more – an eternity in security terms.

Most are closed devices that have limited, outdated or no security software running on them. And they typically run a limited software stack that provides a perfect hiding place for malicious code, creating a permanent backdoor into the network.

Third-party compromises

Another vector for cyber attacks are the many third-party providers employed by the healthcare industry. For example, Phoenix-based Banner Health revealed that attackers gained access to the healthcare, payment and health plan information of up to 3.7 million individuals via payment processing systems for food and beverage purchases.

Similarly, an unauthorized third party accessed a database at 21st Century Oncology, the nation's largest radiation oncology provider, compromising the records of more than 2.2 million individuals.

As of the summer of 2016, 13 separate federal class-action lawsuits had been filed against the Fort Myers-based company on behalf of individuals who have been victimized by identify theft and other scams since the data breach.

The solution

The persistent, internally driven network attack has become the norm, and security products, teams, and processes need to adapt accordingly. Given how rapidly perpetrators modify their malware and launch other advanced persistent threats (APTs), healthcare institutions need a network security solution that identifies and stops attacks in progress.

IT security teams need a real-time, automated threat management system that has visibility into the behavior of all traffic and host devices on the network, including IoT and BYOD devices, and can detect every phase of a cyber attack, such as C&C communication, internal reconnaissance, lateral movement and exfiltration.

Prevention tools at the network perimeter, such as next-generation firewalls, IDS/IPS and malware sandboxes, all help to prevent infection or compromise. But sophisticated attacks have repeatedly shown that they can evade these perimeter security products. To make matters worse, once the infection is successful, these solutions are blind to the reconnaissance, lateral movement and other attack behaviors that cybercriminals use to map out the target network and spread to additional hosts.

Likewise, malware sandbox technologies provide an incomplete approach to managing APTs because they only briefly look for infecting behavior in a virtual environment. What security teams need is a solution that constantly monitors all behavior in the real internal network.

Especially with regard to IoT, behavior monitoring is key to identifying the tell-tale signs of a device behaving maliciously, such as acting as a proxy for routing an attacker's traffic into, out of and across the network. This view of behavior is particularly important as IoT devices cannot run endpoint security agents and will not be protected by IPS signatures.

Challenge: Meeting compliance and regulatory mandates

In the United States and many other countries, PHI is subject to data breach disclosure laws.

The disclosure of PHI triggers a duty to report the breach under the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act and one or more state laws.

Healthcare organizations typically accept payment cards and must also comply with PCI DSS regulations. In addition, new regulations are in the works to address emerging security and privacy issues, such as those raised by medical IoT devices and consumer adoption of mobile health apps, fitness trackers and other technologies.

Given that healthcare is one of the most highly regulated industries, it's understandable that compliance is cited as the main reason for securing sensitive data.

The solution

Healthcare organizations need a security platform that allows them to quickly and easily respond to unique compliance questions.

Comprehensive visibility into all network devices and their behavior is necessary to document compliance for a broad range of technical controls, from asset tracking and security incident reporting to data-loss prevention, and to prove the controls are working.

Security and compliance teams should look for a security solution that continuously monitors all network traffic, both internal and to/from the Internet, from all devices, including BYOD and IoT, and lets them pull up requested compliance data on demand.

Challenge: Protecting assets in an age of encryption

Due to the critical need for privacy, healthcare organizations encrypt the vast majority of traffic on their networks, including medical records, PII and payment data. While encryption provides a layer of protection for sensitive traffic, it also obscures traffic from many network-based security solutions – something attackers are well aware of.

Unfortunately, sophisticated attackers are employing a variety of encryption methods, from standard SSL/TLS to more customized schemes, to hide their malicious code and activities, especially their C&C and exfiltration traffic. In addition, the use of hidden tunnels is on the rise, with cybercriminals preferring HTTPS over other protocols to conceal their attack communications.

Although some organizations use man-in-the-middle techniques to decrypt outbound traffic for inspection, healthcare providers often don't have that option due to strict privacy laws that prohibit inspection of encrypted patient records and other sensitive traffic. Decrypting traffic also exacts a heavy toll on application performance, making it unpopular with users.

In addition, many online service providers, including Google, undermine the use of certificate pinning, a technique that enterprises increasingly use to thwart man-in-the-middle attacks on Web sessions.

In an attempt to deter attackers who have stolen valid certificates, Google and other providers choose to trust only certificates from a specific trusted root certificate authority instead of any recognized certificate authority. This breaks the man-in-the-middle decryption methods used by many security teams.

The solution

To deal with encrypted threats, IT staffs need a way to detect malicious attack behaviors without decrypting packets and inspecting the payload. This requires a new approach to network security based on analyzing traffic behavior and patterns across all applications and devices to reveal the fundamental actions of attackers hidden within network traffic, even encrypted traffic.

Data science, machine learning and behavioral analysis are needed to identify and monitor hidden tunnels, data leaving the environment, malware receiving C&C instructions, outside attackers using remote access tools, and attackers delivering malware updates.

Behavioral traffic analysis can quickly distinguish between human and machine-driven traffic. This capability can flag an attacker using a remote administration tool by revealing that what appears to be an end-user connection is actually a connection being remotely controlled by an outsider.

Challenge: Security teams have a lot on their plates

The majority of security products create work for IT, requiring staff to sift through many thousands of alerts to identify real threats. In many networks, it's common to get 50 alerts per minute.

Faced with lean security teams, it's not humanly possible to sift through and interpret those vast volumes of data, identify the most serious threats, and then mitigate attacks before they spread and do damage.

In the 2016 Vormetric Data Threat Report, a survey of more than 1,100 senior security executives from across the globe, 57% of respondents cited complexity as the number one barrier to wider adoption of data security tools and techniques.

Lack of staff was the second highest barrier, cited by 38% of respondents. The research goes on to note that "a chronic and growing shortage of skilled security personnel" is a problem across the industry.

The solution

Healthcare organizations need a network security solution that reduces the work for overburdened IT staff instead of creating more work. This requires a solution that is comprehensive, easy to deploy, and automates real-time threat detection and reporting.

In particular, security staffs need a solution that streamlines operations by condensing the vast amounts of security-related data down to simple, actionable information, and focuses staff attention on actual attacks in progress by pinpointing the physical devices at the center of an attack and alerting staff of high threat activity.

Cognito detects attacks in progress, streamlines operations

Cognito enables healthcare organizations to detect and respond rapidly to threats, before any damage is done. Picking up where perimeter security leaves off, Cognito provides deep, continuous analysis of internal and Internet network traffic and detects the fundamental actions and behaviors that attackers must perform when they spy and spread across an organization's networks, and steal valuable assets.

Leveraging a unique combination of data science, machine learning and behavioral analysis, Cognito detects all phases of an attack, including C&C communication, internal reconnaissance, lateral movement, data exfiltration, and botnet monetization.

Cognito provides proof of technical controls in multiple fundamental areas

Meet the challenge: Know your business, know your risk

The Vectra Threat Certainty Index™ automatically consolidates all detections and assigns scores that indicate in real time which hosts pose the greatest threat, enabling security teams to immediately focus on the highest risk detections.

Cognito also learns about the naturally occurring behavior patterns in an organization's network and provides a visual map of the relationship between threats, hosts and key assets such as medical records.

The Cognito platform allows healthcare organizations to quickly and easily address the security, compliance and manpower challenges they face.

Address today's dynamic threat landscape

Cognito monitors all network traffic from all devices – internal traffic within the network as well as traffic going to and from the Internet. It also works across all applications, operating systems and devices, including IoT and BYOD devices that are so prevalent in healthcare environments.

Combining machine learning, data science and behavioral analytics, Cognito detects the attack behaviors of known and never-before-seen threats at any stage across the entire attack surface of an organization. Detections are automatically scored and correlated to quickly prioritize the threats so IT can promptly stop the attack and mitigate its impact.

Cognito is unique in that it uncovers the fundamental behaviors of cyber attacks, such as internal reconnaissance, the internal spread of malware, abuse of account credentials, data exfiltration, ransomware activity, and a wide variety of C&C and other hidden communications.

For example, Cognito offers multiple ways to identify ransomware in action, including detecting:

- C&C communication
- The malware update of ransomware binaries on infected hosts
- The internal searching and scanning of file shares
- The theft of administrator credentials to escalate privileges
- The ransomware file encryption activity itself

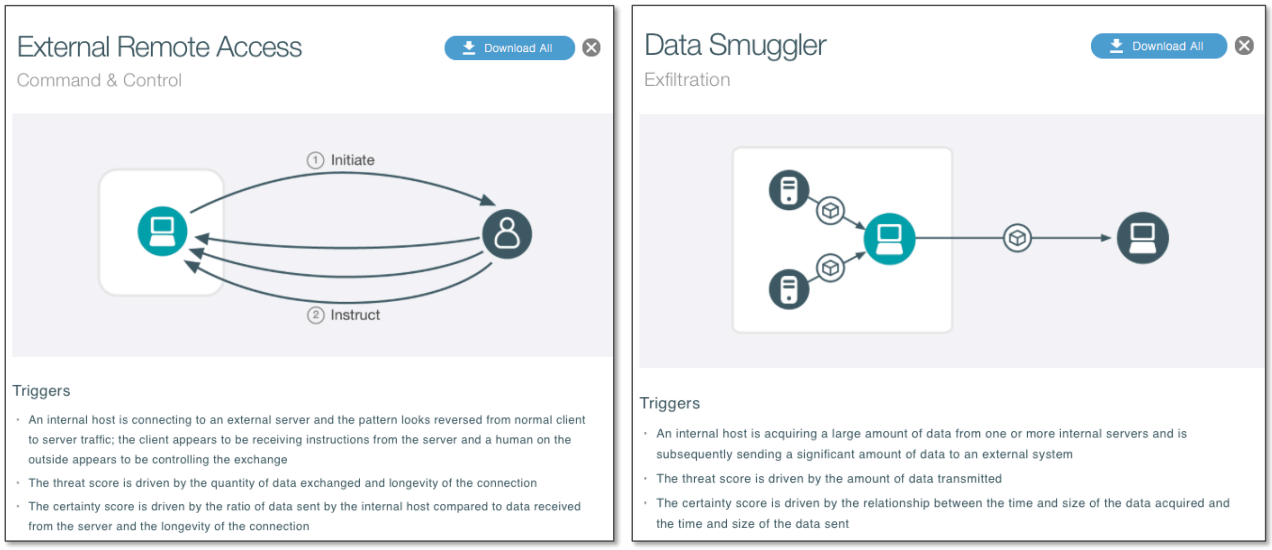
Because Cognito recognizes patterns of traffic, there's no need to crack open packets to see what's inside, preserving data privacy for encrypted traffic. Cognito uses mathematical models and performs a highly sophisticated analysis of network traffic to detect the presence of hidden tunnels within HTTP, HTTPS and DNS traffic.

Similarly, Cognito uses data science, packet-level machine learning and behavioral analysis to identify the presence of external remote access, even malicious remote access tools that are customized or unknown to the security industry.

Streamline operations and save staff time

Understanding that IT and security staff time is at a premium, Cognito is easy to deploy and use. Automation plays a pivotal role.

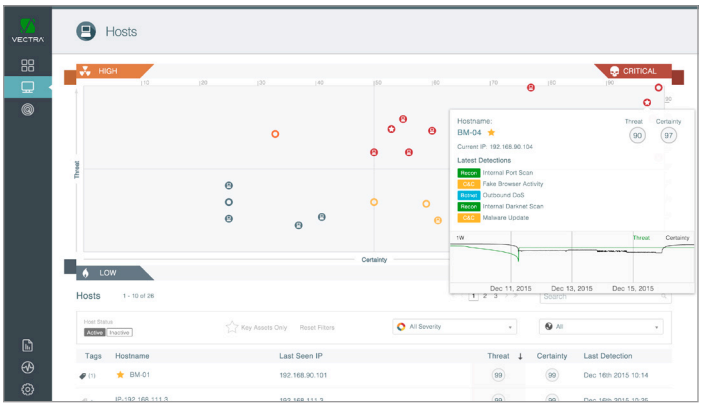
Cognito automates the tedious part of a Tier 1 security analyst's job, empowering security teams by condensing vast amounts of data down to simple, actionable answers that save time, effort and money.



Simple detection explanations: Evidence of technical controls

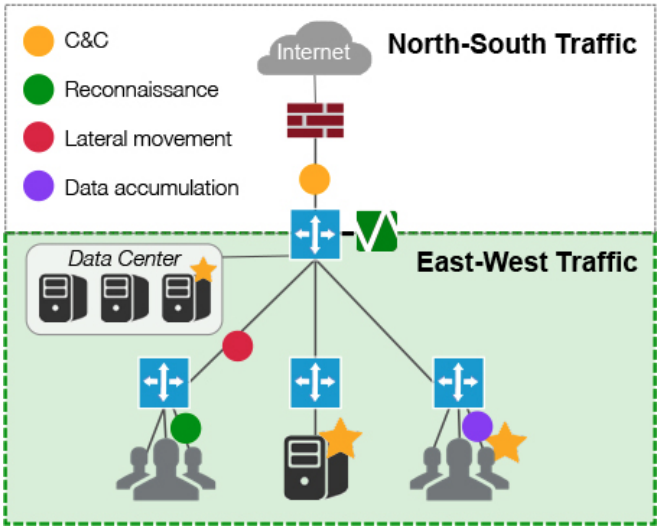
This automation offers two benefits – staff can perform investigations in less time and non-expert staff can handle more investigations. Vectra customers have reported 75-90% reductions in time spent on investigations, and have successfully deferred analysis to IT generalists instead of escalating incidents to higher paid experts.

Cognito pinpoints physical hosts at the center of an attack and automatically tracks and scores threats in context over the full duration of the attack, displaying alerts on the Threat Certainty Index so staff instantly knows which network hosts with attack indicators pose the most significant risk and highest degree of certainty.



Cognito pinpoints physical hosts at the center of an attack and automatically tracks and scores threats in context over the full duration of the attack

Details about an attack are just one-click away, so staff can easily view metadata from the exact packets between the compromised host and other internal assets it is attacking or external parties with which it is communicating, and respond accordingly.



Full visibility ensures knowledge of business risk

Cognito also enables security teams to mark proprietary databases, medical records, credit card databases and other critical assets so they can see threats in the context of target assets and predict the potential impact of an attack.

In addition, Cognito makes it easy to share threat intelligence with other team members and systems. Security teams can be automatically notified via email when devices reach specified threat or certainty score thresholds.

And finally, a robust API allows Cognito to integrate with other third-party security solutions, such as SIEMs, next-generation endpoint security, traffic optimization, and next-generation firewalls. For example, Syslog and Common Event Format (CEF) log integration provides SIEMs with pre-correlated Vectra detections and host scores.

Deliver compliance data on demand

With full visibility into all traffic and the ability to detect any phase of an attack, Cognito is an ideal platform to document compliance for a broad range of technical controls.

Cognito delivers clear, intuitive analysis with one-click access to all supporting evidence, allowing staff to quickly and easily respond to any data request from regulators.

Passive internal deployment

- Leverages TAP or SPAN
- E-W and N-S visibility of traffic
- Sees all phases of behavior

Persistently tracks all devices

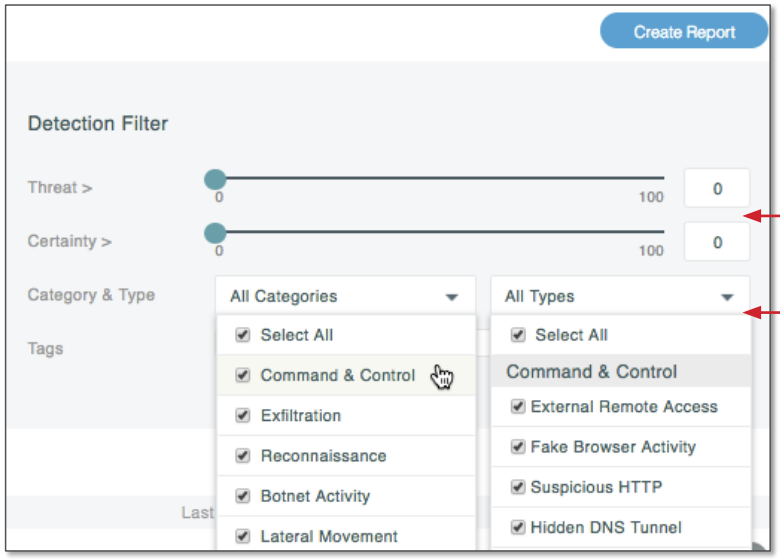
- Any OS, BYOD, IoT

Protects without prying

- Behavioral models find threats without looking into the payload
- Find threats in SSL without decryption

While persistently tracking all target assets and reporting on them, Cognito makes it easy to maintain a compliance trail. Likewise, because Cognito monitors and detects hidden tunnels and data exfiltration behaviors used by attackers, it's easy to document compliance efforts for data-loss prevention.

With Cognito, a powerful reporting engine lets security teams generate reports on the fly as well as schedule specific reports to be compiled on a regular basis. Reports can focus on any timeframe, section of the network, and host or detection. Advanced filtering capabilities can highlight specific data, such as all hosts with threat certainly scores above 50.

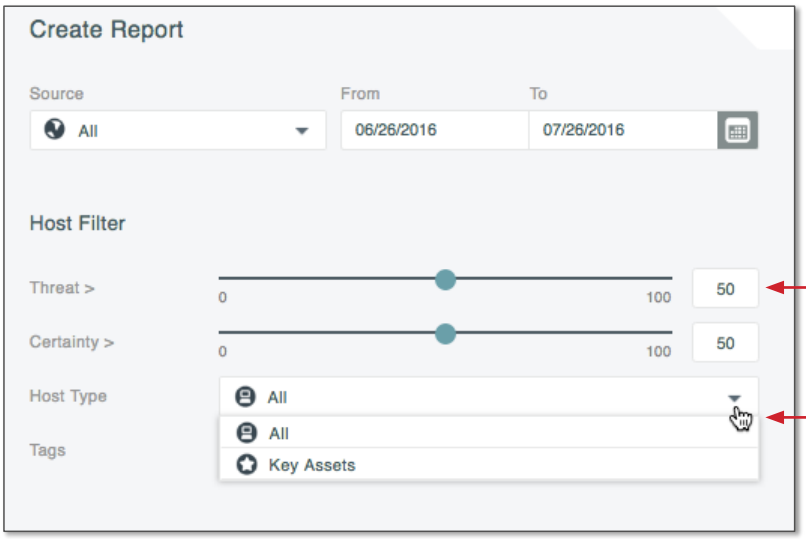


Filter events based on threat level

Easily report on controls specific to any phase of attack:

- Malware behavior
- Lateral movement
- Data loss

Easily document controls based on type of threat



Persistently tracks all devices regardless of device type or OS

Report on all hosts or those with particular risk levels

Report on all hosts, key assets, or any custom category

Track and document any and all hosts in your network

A powerful solution to combat modern threats

Healthcare organizations will continue to be a top target of cyber attacks. Cognito arms security teams with an automated solution that works in real time to rapidly detect known and unknown cyber attacks across the constantly evolving threat landscape.

With the unique ability to detect and mitigate cyber attacks while they are happening, Cognito enables security teams to respond with unprecedented speed, accuracy and efficiency – well before the bad guys endanger patient health, compromise PHI or cause irreparable damage.

Likewise, Cognito gives security teams unparalleled network visibility into malicious attack behaviors and automates the hunt for cyber threats, which lets organizations quickly and easily respond to audits and have more time to focus on keeping target assets safe.

VECTRA®
Security that thinks®

Email info@vectra.ai **Phone** +1 408-326-2020
vectra.ai