CASE STUDY

Health and Life Sciences
Trusted: Behavioral Analytics

Strengthening Security with Cybraics* AI-Based Analytics

Using *n*Lighten*, Cybraics' security analytics and artificial intelligence platform, a large healthcare system detected sophisticated malware and medical device attacks that other solutions missed

At a Glance:

Artificial-intelligence-based security analytics from Cybraics* helped a large Midwest health system detect ransomware and infected medical devices that other solutions missed.

By using this platform:

- The health system avoided potentially disruptive and costly breaches that could have threatened patient safety and privacy.
- IT reduced TCO and avoided alert-overload by using Cybraics' analytics-as-a-service deployment model, which provides curated, contextual evidence when the solution finds threats.

REDUCE THE COST OF SECURITY ANALYTIC SOLUTIONS

Cybraics *n*Lighten* reduces security analytics solution costs up to 10x compared to build-it-yourself.[1]

With cyberattacks growing more sophisticated and the number of connected medical devices rising, healthcare security teams need new ways to stay ahead of breaches, ransomware, and device infections. A large US healthcare system found that Cybraics* *n*Lighten*, an innovative behavioral analytics service running on Intel® technologies, quickly uncovered serious threats that the hospital's existing security measures had failed to discover: a ransomware attack and advanced malware on critical medical devices.

Challenge

A large, multisite healthcare system in the US had implemented a variety of security best practices, including segregating its networks, deploying security incident and event management (SIEM) technologies, and working with advanced security service providers. But the healthcare system wanted to do more to detect sophisticated unknown malware and zero-day attacks, as well as computer, device, and user vulnerabilities.

Solution

The healthcare system deployed the Cybraics *n*Lighten platform, which combines artificial intelligence (AI) and advanced security analytics. The *n*Lighten platform analyzes the behavior of networks, users, devices, and other elements in the environment for unknown, advanced, and insider threats, along with vulnerabilities, infections, and targeted attacks. Built on technologies from Intel and Cloudera*, the *n*Lighten platform provides smart, fast detection of threats while helping reduce costs and free up time for healthcare security teams.

Results

The *n*Lighten platform detected dangerous and previously unidentified problems: medical devices infected with unknown ransomware attempting to contact command-and-control servers in Russia and a ransomware-infected management-and-monitoring server for bedside devices, to name a few. The healthcare system's IT department worked with Cybraics to isolate and remediate the threats, helping avoid disruptive and costly breaches, preserve patient safety and privacy, and protect the organization's reputation.

Spotlight on Cybraics*

Cybraics is a security analytics and artificial intelligence company focused on solving the hardest problems in cybersecurity. The company is a collection of like-minded citizens passionate about ensuring that the nation's organizations and citizens can live free of cybercrime. Its comprehensive security analytics and AI platform, *n*Lighten*, is delivered as-a-service. *n*Lighten, combines multiple modes of machine learning with an advanced AI engine to find unknown, advanced, and insider threats, as well as targeted attacks.

For more about Cybraics, visit cybraics.com.

Detecting Ransomware, Protecting Medical Devices

According to the FBI, ransomware—malicious software that blocks access to an organization's critical data until payment is received—was expected to become a billion-dollar-a-year crime in 2016, up from USD 24 million in 2015.[2] The average total cost of a breach has reached USD 4 million, with healthcare leading all industries in terms of per capita impact at USD 355 per patient record breached.[3]

Ransomware has severely disrupted healthcare, with some attacks causing hospitals to shut down or send some of their patients elsewhere.[4] Even when victims of ransomware meet their attackers' demands, the organizations may still be vulnerable. In one survey, some victims of ransomware report being attacked more than three times, suggesting that although the organizations knew about the threats, they could not find and eliminate them.[5]

The healthcare industry is an attractive target for cybercrime. Hackers often view healthcare organizations as vulnerable targets, lagging in security compared to industries such as financial services. Hackers know healthcare organizations are intolerant of disruption and often quick to pay in response to ransomware infections. Medical cybercrime provides lucrative ways to monetize healthcare data, including medical claims fraud, financial fraud, prescription fraud, and extortion.

Ponemon Institute's annual benchmark study on healthcare data security reported in May 2016 that nearly 90 percent of healthcare organizations have experienced a breach in the past two years. The same study found that data breaches could be costing the healthcare industry USD 6.2 billion.[6]

Medical devices are especially inviting targets. Infected devices can threaten patient safety while also enabling adversaries to attack other systems on the network. These devices are more vulnerable than other IT endpoints because they often run older operating systems, are not aggressively patched, and do not have antivirus software installed.

Despite organizational investments in SIEM and other technologies, breaches go undetected for an average of more than six months before being detected.[7] The longer a breach is undetected, the further malware can propagate, the more sensitive patient data can be encrypted or stolen, and the more damage an infected medical device can potentially cause.

> "Medical devices are critical to operations and patient care. It's unsettling that our advanced threat protection suite from a major vendor didn't identify the adversary. Our patients were at risk. It's a good thing *n*Lighten* was able to detect this threat . . . Aside from being the only ones that could identify the threat, the end-to-end service—raw data to actionable results—separates *n*Lighten from other vendors."
>
> **—Head of Security**
> Large US Healthcare System

Sophisticated Analytics Find Advanced Malware

A leading US healthcare system was well aware of the heightened risks faced by today's healthcare providers and wanted to strengthen its environment. The healthcare system implemented the Cybraics *n*Lighten platform to add behavioral analytics to its already-robust security toolkit.

The *n*Lighten platform combines advanced security analytics and AI to improve threat and vulnerability detection. These can range from real-time threats in progress to misconfigured systems that could expose the network to attack. Cybraics offers these capabilities as a service, helping to reduce TCO. Using a variety of machine learning techniques, the Cybraics engine analyzes networks, users, and other elements on the network to detect subtle clues that reveal unknown threats.

When threats are discovered, Cybraics delivers comprehensive evidence to guide the organization's investigation and remediation activities. Cybraics' curated results and contextual evidence help reduce unnecessary alert noise.

Deploying the Cybraics platform, the healthcare system identified serious threats that previous services and technologies missed.

Malware-Infected Medical Device

This threat appeared as a very weak signal within the healthcare system's domain name server (DNS) logs. After identifying DNS resolution requests made by a computer-generated schedule, the Cybraics team used the analytics engine to flag the suspect domain names.

Although these domain names were not registered on any blacklist, Cybraics' unique analytics and dozens of proprietary algorithms determined that the sites were indeed associated with suspected bad actors. Cybraics tracked the problem to an infected medical imaging device on the healthcare system's network. The adversary had gained the ability to alter settings, including modifying radiation levels—a potentially serious result and a direct threat to the safety of patients exposed to the infected device.

Undetected Ransomware

The Cybraics platform analyzed firewall, DNS, and Active Directory logs, and immediately identified behavioral anomalies. The identified host was a network management server responsible for monitoring and managing bedside devices. Cybraics and the healthcare system's IT team isolated a single, low-and-slow beaconing signal that indicated malware actively searching for a command-and-control server. While the signal originated from the management server, the server was acting as a proxy for downstream devices, and the actual origin of the signal was a host on a network that was not included in the original data analysis. Tracing the offending host, Cybraics discovered ransomware that had infected the host and was attempting to connect to its command-and-control for additional instructions.

In each case, the healthcare system detected and remediated the malware infections, removed the associated threats to patient safety, avoided potential ransomware demands, and safeguarded the institution's reputation. The health system's IT team increased its efficiency by receiving high-quality notifications backed by contextual evidence.

Solution Details

Cybraics uses high-performance technologies from Intel and Cloudera to support its enterprise-scale cyber analytics. The platform runs on the Cloudera Enterprise Data Hub* (Cloudera EDH*), based on Apache Hadoop* and Apache Spark*, and powered by the Intel® Xeon® processor E5-2650 v4 and Intel® Solid State Drive Data Center S3500 Series with Non-Volatile Memory Express* support. This infrastructure provides the performance and throughput to analyze large data volumes, along with the scalability to handle ongoing increases in network traffic, devices, and threats. Tightly integrated pods of compute, network, and storage resources help ensure high availability.

Cybraics offers flexible deployment options built on the *n*Lighten platform delivered as a service. Table 1 depicts a typical on-premises configuration, which can be customized to meet a healthcare organization's requirements. Organizations can also engage the Cybraics Managed Security Operations Center to perform full investigation and remediation services.

> Cybraics' *n*Lighten* platform identified serious, undetected threats, including a real-time ransomware attack and advanced malware on critical medical devices.

Table 1. Cybraics* Representative Technology Implementation

	Cybraics* Application Servers	Hadoop* Cluster
Compute	Five servers based on the Intel® Xeon® processor E5-2650 v4, 512 GB RAM	Eight or more servers based on the Intel Xeon processor E5-2650 v4, 512 GB RAM
	Cybraics Platform	Cloudera Enterprise Data Hub* (Cloudera EDH*)
	CentOS* 7.2	CentOS 7.2
	VMware ESXi* plus virtual machines	n/a
	Two-boot Intel® Solid State Drive (Intel® SSD) Data Center (DC) S3500 Series, 200 GB/server	Two-boot Intel SSD DC S3500 Series, 200 GB/server
Storage	Four local Intel SSD DC S3500 Series, 480 GB each	Intel SSD DC S3500 Series
Network	10 GB or higher	10 GB or higher
Software	Cybraics Platform, Elasticsearch*, Logstash*, Kibana*, VMware*, Extract, Transform, Load stack	Apache Impala* (integrated into Cloudera EDH), Core Cloudera EDH components, Cloudera Manager*

Smarter, Faster Cyber Sleuthing

Together, Cybraics' sophisticated platform and Intel® technologies help enable healthcare organizations to strengthen the detection of ransomware and other malware, infected medical devices, and user and system vulnerabilities. The faster that attacks and vulnerabilities are detected, the sooner they can be stopped and remediated. For ransomware, more rapid detection can mean that less data is encrypted and the hospital experiences less disruption.

Whether malware attacks a medical device or another element of the network, robust threat detection can help healthcare organizations mitigate risks to patient safety, reduce the chance of costly breaches, maintain trust in the institution, and concentrate on caring for their patients. Scalable technologies from Intel and Cloudera help healthcare organizations maintain performance and throughput as analytic requirements—and security threats—continue to grow.

Find the solution that is right for your organization. Contact your Intel representative or visit **intel.com/healthcare.**

Learn More

Explore the Intel Security Readiness Program to benchmark your security maturity, priorities, and capabilities against the healthcare industry: intel.com/BreachSecurity

[1] Cybraics cost estimates. Includes hardware and open source and commercial software to create a comparable solution, and staff to install and maintain it over three years.

[2] Herb Weisbaum, "Ransomware: Now a Billion Dollar a Year Crime and Growing," NBC News Tech, January 9, 2017, nbcnews.com/tech/security/ransomware-now-billion-dollar-year-crime-growing-n704646.

[3] Ponemon Institute, "2016 Cost of Data Breach Study," downloadable from ibm.com/security/data-breach.

[4] Steve Ragan, "Ransomware takes Hollywood hospital offline, $3.6M demanded by attackers," CSO from IDG, February 14, 2016, csoonline.com/article/3033160/security/ransomware-takes-hollywood-hospital-offline-36m-demanded-by-attackers.

[5] Sean Michael Kramer, Report: "Half of Organizations Have Been Hit by Ransomware," eWeek, Nov. 18, 2016. eweek.com/security/report-half-of-organizations-have-been-hit-by-ransomware.html.

[6] Ponemon Institute, "Criminals target healthcare data," May 2016, idexpertscorp.com/sixth-annual-ponemon-benchmark-study-on-privacy-security-of-healthcare-data-incidents.

[7] Phil Muncaster, "Hackers Spend 200+ Days Inside Systems Before Discovery," February 2015, infosecurity-magazine.com/news/hackers-spend-over-200-days-inside.

All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps.

Cost reduction scenarios described are intended as examples of how a given Intel- based product, in the specified circumstances and configurations, may affect future costs and provide cost savings. Circumstances will vary. Intel does not guarantee any costs or cost reduction.

Intel processor numbers are not a measure of performance. Processor numbers differentiate features within each processor family, not across different processor families: Learn About Intel® Processor Numbers.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software, or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer, or learn more at intelsecurity.com.

0317/JBLA/KC/PDF ♻ Please Recycle 335486-001US