LEVERAGING AI
to Protect Hospital IT Infrastructure

A new generation of AI-based threat detection and remediation platforms confront the latest cybersecurity threats

There's a problem in healthcare IT security: incomplete or infrequent software updates and patching that leaves operational and clinical systems vulnerable to cyber threats.

Hospitals can fall behind in updating their software for various reasons. These include the lack of a dedicated staff, to little on-site cybersecurity expertise, to the time and effort needed to test patches before rolling them out to production systems. Across the board, the average time to patch is 102 days, and 43 percent of organizations that have a patch management process say they are taking longer to test and roll out patches in order to avoid issues and assess the impact on performance.[1] Breaking a production system with a patch is especially problematic in a healthcare environment, given patient safety and patient privacy concerns.

The diversity of healthcare IT ecosystems only magnifies the problem. Enterprise workstations in offices; Linux/Solaris systems in the laboratory; Macs in the PR department; tablets and smartphones; all manner of legacy systems; and an ever-expanding number of IoT devices worn by, or implanted in, patients. It's worth noting that security vulnerabilities may be *introduced* every time new users, equipment, applications or components are added – or when a vendor's software patch is applied.

Finally, since they always trail the discovery of vulnerabilities, traditional patching lacks timeliness. In some cases, digitally signed patches from a vendor aren't issued until months or even years after a vulnerability is discovered.

Produced in partnership with

HIMSS Media

"It's certainly true that medical devices aren't patched as proactively as other [systems]. It's easy to lose track of all the devices we have."

Lee Kim | Director, Privacy and Security and Interim Senior Counsel and Data Protection Officer | HIMSS

"Not all vendors are created equal," said Lee Kim, Director, Privacy and Security and Interim Senior Counsel and Data Protection Officer at Healthcare Information and Management Systems Society (HIMSS). "If you, the customer, were to report a problem to the vendor, such as a security or operational bug, the vendor may be responsive, or it may not be. The vendor also may not necessarily understand healthcare and the unique risk to patient safety."

"It's certainly true that medical devices aren't patched as proactively as other [systems]," Kim added, noting that this situation points to the clinical/IT divide. "It's easy to lose track of all the devices we have." In other words, the Windows servers may be identified and monitored, "but not necessarily all of the medical devices." Plus, some systems cannot be patched.

Lack of personnel and budget are issues, too. When asked to identify the biggest barriers to remediating and mitigating security incidents, respondents to the 2018 HIMSS Cybersecurity Survey cited the top five barriers as follows: lack of appropriate cybersecurity personnel (52 percent), lack of financial resources (47 percent), too many application vulnerabilities (29 percent), too many endpoints (28 percent) and too many emerging and new threats (27 percent).

Among respondents from organizations with a specific allocation for cybersecurity within the current IT budget, the top three responses were 1-2 percent and 3-6 percent (both at 21 percent), and 7-10 percent (at 7 percent). Even so, the majority of respondents (80 percent) indicated that they expect their respective organizations' use of resources to address cybersecurity concerns (e.g., people, assets, other resources) to increase in the next year.

The survey also projected that significant security incidents will continue to grow in number, complexity and impact. It found that a majority of respondents (76 percent) indicated that their organizations experienced a significant security incident in the past 12 months.

Consequences

All of this has real-world consequences, exposing healthcare data to disruption, corruption and theft.

By July of this year, 221 data breaches of more than 500 records were reported to the Department of Health and Human Services' Office for Civil Rights, according to the July 2018 Healthcare Data Breach Report from HIPAA Journal.[2] "Those breaches have resulted in the protected health information of 6,112,867 individuals being exposed, stolen, or impermissibly disclosed," the journal wrote, adding that this was 974,688 more records than were exposed in healthcare data breaches in all of 2017.[3]

There's been a sharp uptick in cybersecurity incidents in healthcare since the industry began to transition patient data from paper files locked away in doctors' offices to electronic records accessible from anywhere in the world. Cybercriminals now have a way to access and potentially resell this data, hold it for ransom or commit identity theft for the purpose of obtaining free medical procedures and medications or creating a market for multiple secondary transactions.

"For four or five years, healthcare has gone from a reactive to a proactive posture on cybersecurity," said Rob Bathurst, formerly with Mayo Clinic and now Worldwide Managing Director at Cylance Inc., a software company that applies artificial intelligence to cybersecurity. Big patient data breaches that expose EHR and EMR data, according to Bathurst, are not only bad for business, "they get noticed by government, so organizations realize there are penalties from a privacy and regulatory standpoint."

In contrast to traditional antivirus approaches, machine-learning-based endpoint detection and response (EDR) tools continually

"The typical healthcare organization can't develop a cohesive patch strategy at scale for clinical applications. There's no standard approach or model for legacy risk, which everybody acknowledges is a huge problem."

Rob Bathurst | Worldwide Managing Director | Cylance, Inc.

monitor code and behavior for suspicious activity and block attacks. While traditional software patching is an important practice from an overall data security hygiene perspective, "it may not always be possible, either because these systems are vendor-controlled, home-grown and too old," he said.

For instance, if a typical patch in a corporate IT setting takes three to six months, "on the clinical side, it's anybody's guess," because of the extreme diversity of clinical systems, Bathurst said. "The typical healthcare organization can't develop a cohesive patch strategy at scale for clinical applications." While cybersecurity standards are developing for the latest healthcare devices, "there's no standard approach or model for legacy risk, which everybody acknowledges is a huge problem," he added.

According to Cylance, traditional legacy antivirus security solutions do not take into consideration several critical dynamics within the healthcare industry, starting with the lack of highly trained IT professionals who can monitor and respond to incidents on a 24/7 basis. Even if a healthcare organization has such staffing, "valuable employee time is lost and financial resources consumed while system analysts research events and follow protocols to remediate," Bathurst said.

Apria Healthcare: A new way

That was the experience at Apria Healthcare, which offers home healthcare services and certain medical equipment, including oxygen, inhalation and sleep apnea therapies.

"Our former, traditional AV solution was creating a lot of false positives alerts, which generated a large amount of service tickets to our IT resources," said Vice President and Chief Information Security Officer Jerry Sto. Tomas. After moving to Cylance, these "unnecessary and costly" alerts and services requests were reduced significantly, according to Sto. Tomas, who added, "We outsource our IT operations, so imagine the cost we'd incur on a monthly basis if we were still using the old AV technology."

With a workforce of around 12,000, including employees and partners, another major IT security issue for Apria is what Sto. Tomas calls "insider threat," or malware and phishing attacks against its many endpoint computers, principally laptops and mobile devices. "There are malware and phishing attacks," he said. "Our durable medical equipment devices aren't connected over the Internet, so that's not an issue for us, but we do have a lot of drivers, respiratory therapists, and teleworkers that are always connected to the Internet and the company network."

How AI/ML-based systems works

Instead of waiting on a software vendor's patch, AI/ML-based systems monitor code, comparing millions of features that its model has determined look relevant, and then judging how close these features compare to a malicious binary.

Since malware writers use techniques that mutate their payloads, applying ML techniques to derive common features of malware and detect and block malicious binary payloads is a significant enhancement.

"The model can work in the grey," Bathurst explained. In other words, the determination isn't that code is definitively "malicious" or "not malicious," but rather that "it might be malicious." Advanced threat detection isn't strictly a matter of "yes" or "no," but rather one of high probability vs low probability.

If the model has a high confidence the binary is malicious, it quarantines it and alerts administrators.

Aside from enterprise systems like email systems and web servers, AI/ML models can be applied to a wide range of specialty devices, from IP cameras, network sensors and pharmacy dispensing systems.

"The goal is to correlate different events, both malicious and legitimate, to further reduce false positives. In addition, we're correlating endpoint behaviors against our applications and network environment to increase security and monitoring automations."

Jerry Sto. Tomas | Vice President and Chief Information Security Officer | Apria Healthcare

Enter a new class of software protection solutions that prevent, rather than react, to viruses and malware.

Instead of layers of reactive technology, these AI/ML-based EDR systems are proactive, defending against threats and malware *before* they execute. "AI/ML is preventative medicine, helping prevent the infection in the first place," Bathurst said. This proactive orientation provides continuity of operation and minimization of impact on physicians. For instance, when the WannaCry international cyber-attacks affected some healthcare organizations, not a single Cylance client reported downtime. (See sidebar: "How AI/ML-based systems works")

"Traditional AV is signature based and static," said Sto. Tomas, who switched from a traditional antivirus tool to Cylance when he joined Apria Healthcare three years ago, adding that his most worrisome threats are zero-day attacks. Waiting for a vendor patch or a signature update for AV means playing catch up for a day or two, "during which you're susceptible," he said.

By contrast, Cylance's AI/ML approach to endpoint detection and response (EDR) means "if something changes in the environment, they can protect and block, based on those anomalies and behavior," Sto. Tomas said.

A big project for Sto. Tomas now is to continue expanding the use of Cylance logs as a feed into Apria's user and entity behavior analytics tool. "The goal is to correlate different events, both malicious and legitimate, to further reduce false positives," he said. "In addition, we're correlating endpoint behaviors against our applications and network environment to increase security and monitoring automations."

As healthcare IT faces increasing threats – malicious software code, unauthorized user access, fraudulent use of patient data – vendor patching isn't a sufficient security strategy. It isn't fast enough, and it doesn't emphasize detection and remediation. "Maybe it's not possible to be 100 percent secure," Bathurst said. "But with AI/ML it is possible to have a much more proactive defense."

For more information:
cylance.com

[1] "Expanding Machine Learning Applications on the Endpoint," a 451 Research survey commissioned by Cylance.
[2] "July 2018 Healthcare Data Breach Report." HIPAA Journal. August 24, 2018. https://www.hipaajournal.com/july-2018-healthcare-data-breach-report/https://www.hipaajournal.com/july-2018-healthcare-data-breach-report/
[3] Id.

CYLANCE

About Cylance, Inc.:

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. Learn more at www.cylance.com.

Produced by HIMSS Media | www.himssmedia.com | © 2018