Menlo Security

IT'S SAFE TO CLICK

PREVENTION IS THE BEST FORM OF MEDICINE

IT Security in Healthcare

Overview

Hospitals and other healthcare organizations (HCOs) are increasingly singled out by cyber criminals for ransomware and other attacks. Not only are patients' sensitive records being targeted, but also—as the FBI warns—their intellectual property or credit card information. The primary reasons for HCO vulnerabilities are outdated security architectures, and overall lack of IT security experts. Isolation technology provides an appealing alternative to traditional security methods, and prevents, rather than treats, malware, and phishing attacks.

Why are HCOs Susceptible?

Hospitals pose a relatively easy target due to the high number of network ingress and egress points, which translate into attack vectors.

The majority of today's healthcare-targeted attacks, such as ransomware, are motivated by financial gain rather than simple notoriety. Cybercriminals will always target those organizations with the weakest defenses and the most valuable data. Few industries are as dependent on data and information than healthcare; without patient records, a hospital cannot operate.

Hospitals pose a relatively easy target due to the high number of network ingress and egress points, which translate into attack vectors. Workers routinely access critical information from multiple, often unsecured, devices or networks, which render a perimeter-based security architecture irrelevant.

Compounding the issue, medical institutions often lack sufficient budgets and IT staffing to keep ahead of cyber threats. As a result, many hospitals fail to conduct the regular security audits required to keep them safe from attacks. In essence, they are playing a perpetual game of catch-up while malware infections spread, and increasingly impact HCOs and staff.

The Doctor Has Become Patient-Zero

In medical terms, Patient Zero is loosely defined as the first human infected by a new or recently discovered viral or bacterial outbreak. The term has found its way into the IT security lexicon where its corollary is the first individual to be infected by a new malware strain, or the first victim in a phishing campaign.

It brings to mind a scenario where a single individual is initially infected and rendered contagious. This "patient zero" then comes into contact with others who also become contagious, and in turn, infect multiple others. The illness spreads logarithmically until medical experts are able to cure the disease or limit its propagation. This can take months or years, because even with the luxury of modern medical science, infectious diseases are difficult to treat or cure. Before it is contained, a new virus or bacteria can sicken untold numbers of individuals.

When we refer to patient zero in IT terms, many entertain the notion that if an individual is infected by a new malware strain, or clicks on a new malicious web link, today's state-of-the-art security solutions immediately respond and effectively eliminate the threat. The reality, however, is more analogous to infectious disease.

What better way to stop a disease than to prevent it from happening in the first place?

Today's security solutions rely on detecting good versus bad. Although we have a solid understanding of what is good and bad today, we have no way of knowing what will be good or bad tomorrow. And just as it take time for medical experts to develop a cure or treatment for a never-encountered disease, so too does it take time for security products to develop defenses against new exploits. Even with technologies such as machine learning and AI, there can be a day, week, or months-long gap between initial "patient zero" infection and effective mitigation. During that time, many others can fall victim to the attack. We need to understand that the IT patient zero actually represent tens, hundreds, or even thousands of infected devices.

Polio and smallpox impacted a significant portion of the world's population before they were finally contained. That containment came in the form of a preventative vaccine. What better way to stop a disease than to prevent it from ever happening in the first place? The same holds true for IT security. Because we will never be able to detect every new malicious web link, malware exploit, or email, as with medicine, prevention holds the key.

A Preventative Approach

A new preventative approach to eliminating malware, such as ransomware and the patient-zero problem, is isolation, which implements a secure and trustworthy execution environment (or isolation platform) between the user and potential sources of attack. By executing sessions away from the endpoint and delivering only safely rendered information to devices, users are protected from malware and phishing attacks. In the isolation model, malware has no path to reach an endpoint and legitimate content needn't be blocked in the interest of security. With a native user experience, administrators can open up more of the Internet to their users while simultaneously eliminating the risk of attacks.

Healing Qualities

With the right isolation technology, HCOs can heal their IT security weaknesses and recognize a number of benefits over legacy security products:

- First, isolation is 100 percent effective in preventing malware from web and email links. User sessions are executed in virtual containers within the isolation platform. All content—including any malware—is disposed of along with its container by the platform each time a user completes a session. There's no chance for malware to escape and infect the user's endpoint. As a result, there are no false positives that block legitimate content and generate alerts, or false negatives that allow malware to reach its target.
- Secondly, it delivers a user experience that is indistinguishable from browsing the web directly, with no noticeable latency or impact to browser functionality such as cut and paste, or printing. There is no pixilation, choppy scrolling, or other visual artifacts common with 'screen-scraping' technologies like VDI. Isolation uses the optimal encoding mechanism for each type of content, and delivers it securely to the user's device using industry-standard rendering elements that are compatible with any device, browser, or operating system.
- Thirdly, a cloud-based isolation solution deploys quickly and easily (without appliances or endpoint software) and reduces security complexity and costs by eliminating endpoint software and outdated appliances. It can be turned on in minutes and simplifies operations by eliminating alert fatigue with zero false positives and negatives. And, it can scale to meet the demands of small to global HCOs.
- Finally, isolation can be used in conjunction with existing security infrastructure. Next generation firewalls, for example, which protect against the latest cyber attacks, become even more versatile and effective when integrated with threat isolation.

It's Time for HCOs to Become Immune to Malware and Phishing

Cyber criminals will always target those organizations with the weakest defenses and the most valuable data. Hospitals will always possess valuable data, but by bolstering their cyber immunity posture with new technology such as isolation, they can make themselves a much less appealing target for ransomware and other cyber threats.

Menlo Security
IT'S SAFE TO CLICK

934 Santa Cruz Avenue
Menlo Park, CA 94025
Tel: 650 614 1795
info@menlosecurity.com