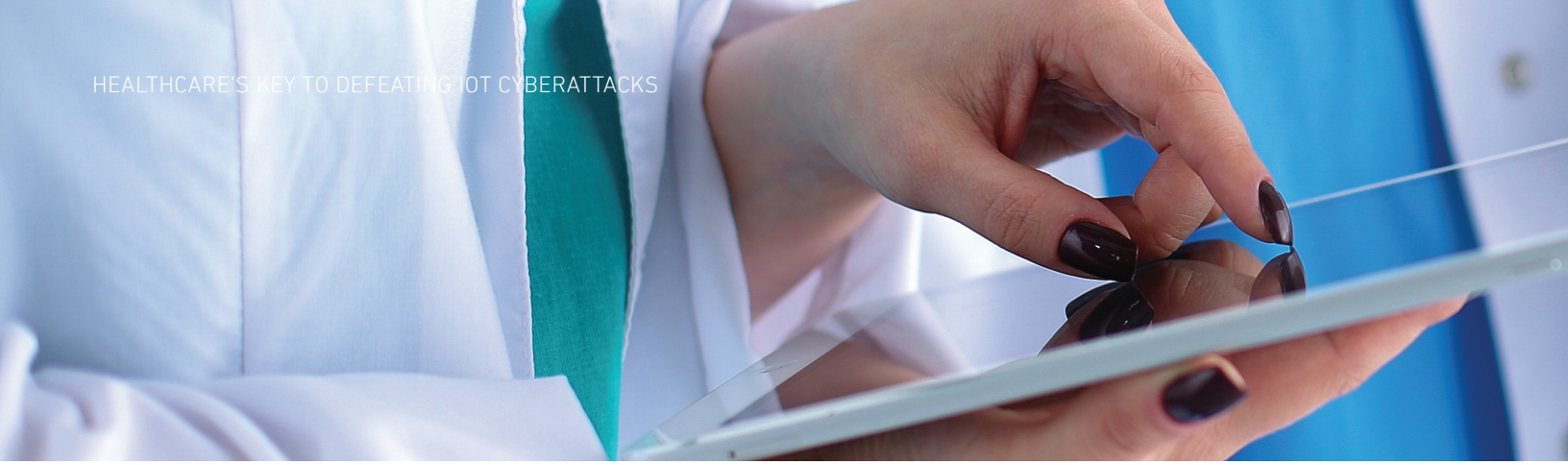
July 2018

ARMOR™

WHITEPAPER

HEALTHCARE'S KEY TO DEFEATING CYBERATTACKS

JUST WHAT THE DOCTOR ORDERED... PROTECT PATIENT DATA, CLINICAL RESEARCH AND CRITICAL INFRASTRUCTURE



INTRODUCTION

The healthcare industry is a double-edged sword when it comes to cybersecurity. On one hand, networks are kept open enough so that doctors can easily obtain patient healthcare records, patients can connect with their healthcare providers, and network connected medical machines can enhance patient care. On the other hand, this interconnected framework makes it easy for attackers to break into medical networks, steal patient data, and sabotage medical devices, which could prove to be fatal. Healthcare attacks affect hospitals of all sizes, including mall practices and rural hospitals, which dominate the healthcare industry[1]. Smaller and medium-sized healthcare organizations are often easy targets as they typically lack the budget, technology, and qualified people to prevent, detect and remediate threats.

Securing healthcare networks is becoming more difficult as more applications and devices connect to them. Artificial intelligence (AI), the internet of healthcare things (IoHT), and Real-Time Health System (RTHS) solutions, will exponentially grow attack avenues. The value of IoHT is expected to top $163 billion by 2020, with a Compound Annual Growth Rate (CAGR) of 38.1 percent between 2015 and 2020[2]. Gartner predicts by the end of this decade 30 percent of nurse call systems will have been replaced by real-time health system solutions[3]. MRI and dialysis machines, heart rate monitors, and smart beds are just a small sample of devices that are connected to hospital networks that could become attack targets. In the best situations, IoHT devices improve patient outcomes, making them popular. However, in the worst situation —a medjack attack— these connected devices may be compromised by attackers and then used as pivot points to move laterally throughout the network.

Fortunately, even though the attack surface is changing, so are cybersecurity solutions. While device makers are slow at adding security to their products, there is finally a way to see all incoming and outgoing traffic on any devices without the need to buy or manage new equipment, firewalls, intrusion detection/prevention systems (IDS/IPS) and other security tools. And remediation happens in a flash.

DIFFICULTIES SECURING THE NETWORK

Even without these new medical devices, already healthcare is the No. 1 U.S. industry attacked more than any other by cybercriminals[4]. Ponemon Institute reports that U.S. healthcare organizations experienced an average of 16 cyberattacks each in 2017, up from 11 the year before[5]. According to the Identity Theft Resource Center 2017 Annual Data Breach Year-End Review, 66 percent of hospitals had between 10,000 and 100,000 network connected devices. Sixty-five percent of surveyed healthcare organizations surveyed by the Ponemon Institute responded "no" or "unsure" when asked whether the security of medical devices is part of their overall cybersecurity strategy[6].

In April 2018, researchers at Symantec publicly identified an attack group called Orangeworm and linked it to malware attacks on the healthcare industry. In other instances over the years, attackers and researchers alike have discovered ways to compromise a variety of medical devices. Most medical devices run on proprietary, embedded operating systems and leave all updating under the control of the device vendor. In addition, scanning these devices for vulnerabilities and security threats is challenging because most antivirus vendors do not support these systems. This is why defense-in-depth strategies must be deployed to protect this type of equipment, including consideration for the data on the device, network segmentation, and stringent logical access controls.

Medical devices are just one potential hole in a healthcare organization's network. Ponemon Institute's "The State of Cybersecurity in Healthcare Organizations in 2018" reports that the existence of legacy systems and disruptive technologies — such as cloud, mobile, big data and the Internet of Things — put patient information at risk by increasing the complexity of managing and securing the environment.

In Ponemon's report "The State of Cybersecurity in Healthcare Organizations in 2018," when asked, "Has your organization experienced an incident involving the loss or exposure of patient information in the past 12 months," 51% of healthcare organizations said yes compared to 48% in 2016. Other respondents weren't sure or said no.

HEALTHCARE INDUSTRY UNDER ATTACK

The healthcare industry was the victim of 88% of all ransomware attacks in U.S. industries in 2016, according to Solutionary, an NTT Group security company. And 89% of studied healthcare organizations have experienced a data breach, which involved patient data being stolen or lost, over the past two years, a report from the Ponemon Institute shows.

88%

of all ransomware attacks in the U.S. in 2016 were in the healthcare industry

89%

of studied healthcare organizations have experienced a data breach

THE FIX

Whether the cause of healthcare threats is due to open networks, social engineering attacks, or employee error, organizations need to remediate threats immediately. It's actually possible to detect and remediate ransomware before any files have been encrypted. The first step in securing an environment — on-premise, in the cloud or in a hybrid environment — is the same as it's always been: monitor 24/7/365, and once suspicious activity is spotted, an highly experienced analyst needs to review and understand the massive lines of code to put the suspicious activities together to reveal the big picture. Once the analyst is sure there's been a breach, remediation needs to be immediate. The faster the data breach can be identified and contained, the lower the costs of loss and remediation.

All from the cloud, Security-as-a-Service (SECaaS) providers can monitor, analyze, and remediate attacks quickly, and they can do it much faster than any organization could do it on its own. With a portfolio of services that simplifies regulatory compliance and leverages the speed and scalability enabled by the cloud, a SECaaS provider armed with a global view of the threat landscape can deliver from the cloud the scalability, speedy security protections and cost savings.

By leveraging the power of the cloud, Security-as-a-Service (SECaaS) providers automatically scale up as a healthcare provider's environment grows with the newest devices and applications. A team of trusted experts that specialize in protecting cloud, on-premises, and hybrid IT environments watch over environments 24/7/365 to monitor the entire network, detect threats as soon as they appear and automatically remediate them. These outsourced security providers alleviate the need to hire and maintain security researchers and analysts, and to purchase and manage expensive equipment like IDS/IPS, firewalls and SIEM tools.

A SECaaS can also provide numerous services like the ones listed below:

- Intrusion detection
- Malware protection with constant updates
- Log and event monitoring
- Active threat hunting
- Vulnerability scanning and patch monitoring

When choosing an SECaaS, look for one that provides the following benefits:

- Intelligence-driven, proactive security that alerts, responds and resolves threats
- Unified visibility and control for any environment
- Simplified, continuous audit-ready compliance
- Reduce dwell time for attackers
- Pay-per-use consumption
- Supported environments (On-prem, Cloud, and Hybrid)

REFERENCES

[1] Health Care Industry Cybersecurity Task Force, Report on Improving Cybersecurity in the Health Care Industry, June 2017.

[2] The Internet Of Medical Things–What Healthcare Marketers Need to Know Now," January 2016, Victoria Petrock: Contributors: Annalise Clayton, Maria Minsker, Jennifer Pearson, eMarketer.

[3] Is Nurse Call Still Necessary?, Barry Runyon, Gartner, April 18, 2016.

[4] 2016 IBM X-Force Cyber Security Intelligence Index

[5] Ponemon's The State of Cybersecurity in Healthcare Organizations in 2018

[6] Ponemon's The State of Cybersecurity in Healthcare Organizations in 2018

ARMOR.COM | (US) +1 844 682 2858 | (UK) +44 800 500 3167