DYNTEK
DYNAMIC TECHNOLOGY SOLUTIONS

McAfee
by Intel

Healthcare's Growing Cybersecurity Challenge

AS THREATS GROW, AN END-TO-END SECURITY STRATEGY IS A MUST

Long gone are the days when a virus was the greatest threat to cybersecurity. Today, new threats are emerging at a relentless pace, from data theft to ransomware to malicious Trojans and even social engineering attacks.

As new threats and the scale of attacks are accelerating, healthcare organizations are coping with growing security challenges caused by increasingly complex EHR systems, connected medical devices, expanded use of cloud services, and stricter HIPAA compliance regulations, among others. Plus, many healthcare organizations lack the staff, skillsets or strategies to deal with advanced cybersecurity incidents.

DATA THEFT IS AN OLD PROBLEM WITH NEW FACES

The growth of electronic health records, cloud-based doctor/patient communications, and connected Internet of Things (IoT) medical devices open new gateways for data theft and other security threats. A recent Ponemon Institute study showed that an incredible 90% of healthcare organizations experienced a data breach in the past two years; and 40% had more than five data breaches over that time. The theft of personal medical data is particularly alarming because it cannot simply be canceled and replaced as with credit cards.

In the face of the fast-growing rates of data theft, IT teams are still expected to enable new patient-facing services from Wi-Fi network access to advanced digital systems for diagnosis and patient care, all of which exacerbate the spectre of data theft.

INTERNET-ENABLED MEDICAL DEVICES FOSTER NEW THREATS

As the growth and expansion of digital tools and technologies has permeated healthcare, so have the threats to cybersecurity. Everyday devices are now being connected and becoming "smart," and medical professionals are monitoring and controlling them from literally anywhere.

IoT devices are attractive to cybercriminals since they can be easily-accessed gateways to data and intellectual property theft, and to cause disruption to critical infrastructure. Literally billions of IoT devices are coming into regular use, yet many (even most) have weak or no security, or vulnerabilities that cannot be patched or upgraded. Often, seemingly innocuous devices are connected to networks without appropriate isolation or segmentation, inadvertently providing unauthorized access to trusted environments.

RANSOMWARE HAS BECOME A REAL DANGER

Money is the primary motivation for most cyberattacks, and ransomware is one of the most profitable. Healthcare organizations are prime targets for ransomware attackers since healthcare data is estimated to be worth 10 times the value of a credit card number on the black market, thanks primarily to its value in committing insurance fraud.

90%
OF HEALTHCARE ORGANIZATIONS EXPERIENCED A DATA BREACH IN THE PAST 2 YEARS

40% 5
HAD MORE THAN 5 DATA BREACHES OVER THAT TIME

BILLIONS
OF IoT DEVICES ARE COMING INTO REGULAR USE

MANY HAVE WEAK OR NO SECURITY

19
HOSPITAL RANSOMWARE ATTACKS DURING THE FIRST HALF OF 2016

SOME HOSPITALS EXPERIENCED PARTIAL OR COMPLETE NETWORK DOWNTIME OF

5-10 DAYS

McAfee's Foundstone Incident Response team identified at least 19 hospital ransomware attacks during the first half of 2016 alone, across six countries. Some hospitals experienced partial or complete network downtime of five to 10 days. Hospitals simply cannot afford downtime that could be life-threatening to patients relying on medical devices and healthcare data. So it's no surprise that hospitals, when faced with a ransomware attack, often simply pay up to regain access to the critical data. This kind of 'easy' money for attackers only serves to motivate the sponsors of ransomware to further attacks.

THREAT RESPONSE MUST BE AN END-TO-END PRIORITY

Cyberthreats touch all areas of healthcare organizations, yet existing security processes and training are often challenged to keep up with increasingly sophisticated threats. Since downtime can literally be a matter of life and death, security must be an end-to-end strategic priority.

DynTek works with healthcare providers to establish an architecture that extends from the physical to the virtual to the cloud. We start with implementing a broad range of Technical Controls that identify the security gaps and link security strategies to technology spend. Then we leverage our extensive expertise across the core technologies that make up the healthcare IT infrastructure to implement a long-term security strategy aligned with the organization's needs.

Our end-to-end services help healthcare institutions strengthen data protection, streamline backup and recovery, and manage data more effectively – all with key compliance initiatives such as HIPAA in check. Specifically, our security offerings include:

- Risk-based Security Strategy Blueprint for Cybersecurity
- Incident and Breach Response Services
- PCI Compliance Readiness Projects
- HIPAA /OCR Compliance Readiness & Audit Response projects
- Managed Security Services Provider

THERE IS POWER IN PARTNERSHIP

DynTek partners with McAfee to provide cybersecurity solutions for healthcare that are ahead of the threat curve. Our end-to-end approach leverages McAfee's centralized threat management platform to provide visibility into the entire security posture from a single console, which ensures streamlined security administration, enhanced policies and processes, superior compliance reporting and integration across all end points on the network.

A McAfee Platinum Partner, DynTek has been awarded 'McAfee Solution Provider of the Year' for healthcare in each of the past five years.

DON'T WAIT FOR A CYBERTHREAT TO BECOME A CYBERSECURITY INCIDENT

Contact us and let's have a talk.

877.297.3723 marketing@dyntek.com www.dyntek.com

DYNTEK
DYNAMIC TECHNOLOGY SOLUTIONS

McAfee™
by Intel

DynTek Services, Inc.
4440 Von Karman, Suite 200
Newport Beach, CA 92660

877.297.3723

marketing@dyntek.com

www.dyntek.com