tenable®

USE CASE:

SECURING THE HEALTHCARE INDUSTRY

Data Points:

- Financially motivated cybercriminals continue to target the healthcare industry via ransomware attacks[1]
- The number of confirmed data breaches increased by 71% over last year
- Healthcare has the highest number of internal adversaries, with nearly as many internal cybercriminals as there are externally

Recent Events:

- **May 2020:** Nearly 288,000 patient records compromised due to a successful spear-phishing attack that targeted BJC Health System
- **April 2020:** 550,000 patient records exposed when a third-party secure record storage and disposal vendor improperly disposed of patient files
- **January 2020:** Nearly 233,000 patient records compromised due to a successful email attack at Ambry Genetics
- **1H 2020:** 41 hospitals and healthcare providers report impacts from successful ransomware attacks, a more than two-fold increase since 2018

Background

The healthcare industry has seen sweeping changes over the past several years, with technical innovations that have brought the doctor's office and advanced diagnostic services directly to the patient—24 hours a day, seven days a week, from any Internet-connected location in the world.

These innovations have made healthcare more accessible than ever before: self-service web portals enable rapid access to test results; video-based remote appointments facilitate physician access to fragile and non-ambulatory patients; continuous monitoring of patients with potentially life-threatening medical conditions immediately informs the attending physician the moment a critical change occurs; and these are just a few examples.

While some of these services provide overwhelming convenience that can dramatically improve patient satisfaction and loyalty, others significantly improve critical patient outcomes and survival rates. In addition, most of these innovations have enabled healthcare providers to dramatically reduce their operating costs due to a reduced number of office appointments, expensive diagnostic tests and inpatient stays that may not be reimbursed by third-party payors.

But despite its many benefits, this level of innovation has also exposed healthcare providers to a wide range of cybersecurity threats. And in many cases, the innovation has been fast-tracked by the business to keep pace with competitors, leaving IT and security teams scrambling to determine how to support it without sacrificing the organization's security posture.

[1] Verizon, "*2020 Data Brief Investigations Report.*" https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

Key Challenges

- Myriad connected health devices located inside and outside the network, and built on a wide range of platforms frequently controlled directly by patients, expose the network to attack
- The requirement for continuous availability of critical patient data makes it difficult to take the system down for updates and maintenance needs
- An abundance of high-value data makes healthcare providers highly attractive targets for financially-motivated attackers
- 24/7 patient care requires always-on devices and IT systems that are often at odds with sound security practices

Healthcare Cyberattacks: A Clear and Present Danger

Most experts identify healthcare as one of the most frequently targeted industries by cyberattackers. Phishing, brute force attacks and ransomware are all common cyberattacks levied against the healthcare industry, due primarily to the sheer volume of high-value patient data healthcare providers rely on to maintain a high standard of care.

Financially motivated cybercriminals have surmised that locking providers out from their sensitive patient data can lead to particularly lucrative payouts. As a result, ransomware has become the top attack method in recent years, outpacing all forms of account credential compromise.

Whereas electronic health records (EHR) once represented the boldest technology move to advance patient care at the potential expense of cybersecurity, every new innovation in the past few years represents a new, and far more exploitable, potential path of entry for adversaries. This is fueled by the fact that many of those innovations leverage devices that are operated and maintained by patients, and can be accessed from any network, while others such as connected health devices are built on myriad internet-of-things (IoT) platforms that can lack proper security protocols. As a result, the organization is exposed to a multitude of new vulnerabilities.

Legacy Vulnerability Management Doesn't Help

Legacy vulnerability management (VM) tools weren't designed to handle the modern attack surface and its growing number of threats. Instead, their visibility is limited to traditional IT environments, so they completely miss any vulnerabilities that are present in the most dynamic aspects of the modern attack surface, including cloud, operational technology (OT) and container environments. In healthcare, these vulnerable entry points include assets such as remote patient monitoring devices, bedside connected devices such as PCA machines, and portable EKG machines.

Legacy VM tools are also risk-unaware, relying exclusively on Common Vulnerability Scoring System (CVSS) base scores to determine which vulnerabilities to remediate. Since CVSS base scores are static and lack any degree of business context or threat intelligence, they can lead security teams to waste the majority of their time chasing after the wrong issues while missing many of the most critical vulnerabilities that pose the greatest risk to the business.

The most common method among businesses is to prioritize every vulnerability with a CVSS base score of 7.0 and above. But according to Tenable Research, more than half of all vulnerabilities fall into this category. Since this reduction isn't nearly enough, your workload quickly spirals out of control. And while that's problematic in every organization, it's particularly concerning in a healthcare setting where a backlog could cause delays in remediating a critical vulnerability affecting assets that are directly involved in patient care.

Compliance Doesn't Equal Security

Whether your organization falls under HIPAA or any other regulatory agency, it's important to understand the difference between passing an audit and maintaining a high level of security. First, most compliance regulations are written to protect patient confidentiality, not to safeguard your business. As a result, you can pass every audit easily, yet still not be secure. However, if you achieve and maintain a high level of security, you're highly likely to pass the cybersecurity portion of your audit as well.

Regulatory audits also only consider a subset of your assets to be in-scope, so focusing exclusively on those can lead you to ignore other business-critical assets and the vulnerabilities that reside on them. In addition, focusing on regulatory compliance often leads to point-in-time assessments at irregular intervals.

To be secure, you must continuously assess every asset across your entire attack surface and employ analytics that dynamically assess changes in vulnerability, threat and asset criticality data. Without a clear understanding of what is affecting your network at every moment, security teams are incapable of determining which vulnerabilities pose the most risk, requiring you to react every time a new exploit is discovered in your network or a zero-day exploit gains media attention.

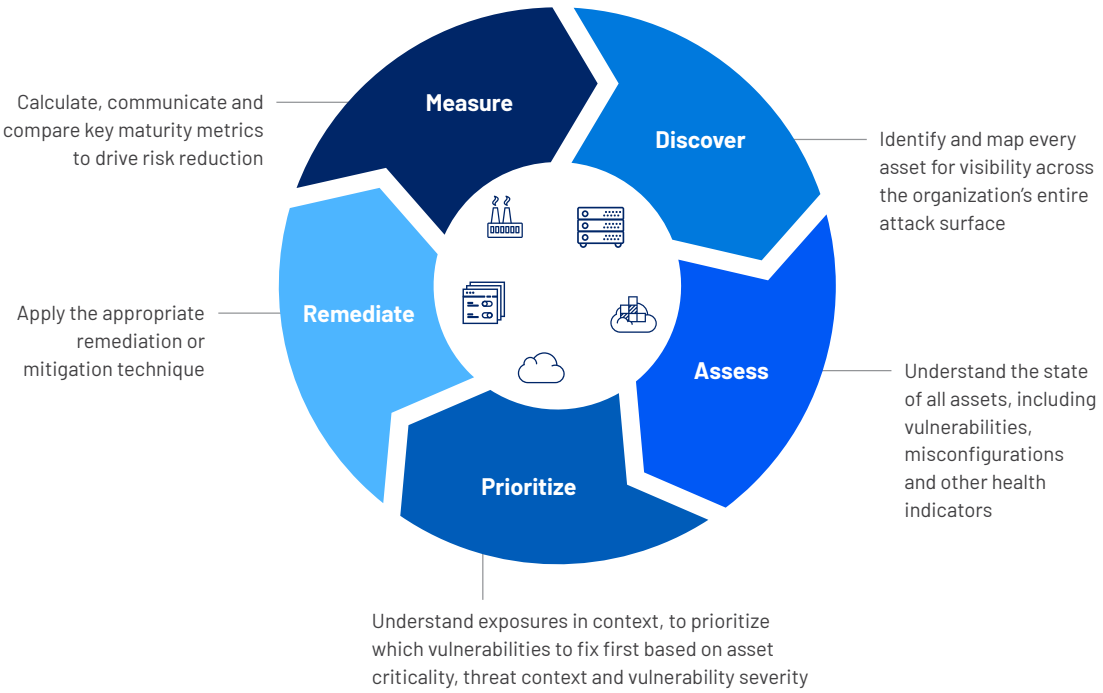
Prioritize What Matters Most

Between your expansive, dynamic networks and the growing number of vulnerabilities from patient-focused innovations, you have more vulnerabilities than your security and IT teams can possibly be expected to manage. And with a well-funded, highly-skilled, motivated group of adversaries, you can't afford to waste time on vulnerabilities that don't pose real business risk.

Evolving to a risk-based VM strategy will help you evolve from a highly reactive approach, which is interrupt-driven and error-prone, to one that is more proactive and strategic, so you can maximize your efficiency and effectiveness.

The first thing to understand about evolving to a risk-based VM strategy is that it's a far more comprehensive solution than you can get while using legacy VM tools. Rather than just discovering and assessing vulnerabilities, you'll be able to effectively prioritize them, determine the appropriate action to take, and calculate key metrics as well as compare against industry standards. This approach not only helps you determine when and where to make adjustments to optimize your strategy, but it enables you to build and maintain management's confidence and keep them out of panic mode when high profile exploits occur.

Lifecycle for Risk-Based Vulnerability Management



With risk-based VM, security teams can focus on the 3% of vulnerabilities that pose the most risk, so you can address the organization's true business risk instead of wasting valuable time on vulnerabilities that have a low likelihood of being exploited. By understanding the full context of each vulnerability – including severity, threat actor activity and the criticality of affected assets – and employing machine learning to predict which vulnerabilities attackers are most likely to exploit in the next 28 days, you can take decisive action to reduce the greatest amount of business risk with the least amount of effort.

Summary

As a cybersecurity professional in the healthcare industry, you know that sensitive patient data is a big draw for financially motivated cybercriminals. Not only is that data valuable to your organization, but quality patient care – and, frequently, lives – depend on it remaining secure and available at all times. Continuous innovation creates an endless stream of attack vectors for these adversaries. You need to cut through the noise and focus on the vulnerabilities that pose the most risk. Risk-based VM enables you to focus on what matters most, so you can make the best use of your limited resources and stay ahead of adversaries.

About Tenable

Tenable®, Inc. is the Cyber Exposure company. Over 30,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, more than 30 percent of the Global 2000 and large government agencies. Learn more at www.tenable.com.

082020 v1