THE CHALLENGE

Targeted cyberattacks in the healthcare industry have been a problem for years and are now being thrust into the spotlight as a result of COVID-19.

Network-connected medical devices are exposing significant vulnerabilities that could be exploited to cause significant harm to patients or impact a hospital's ability to deliver care. While targeted attacks on these devices are certainly possible, attacks on back-end infrastructure and third-party technology ecosystems in order to gain access to these devices and sensitive medical information at scale offer attackers a better return on investment than compromising a single device. These targets include web application servers and back-end servers for remote medical devices. They also include vendor provided services (clinical or technical) for hospital-based devices.

Amid the many challenges for healthcare is managing escalating costs without compromising quality of care and risks to patient safety and privacy.

For med-tech companies, this presents a major opportunity to support healthcare providers with advanced digital services, often via mobile connected devices that process and transmit critical patient-related health information. This service infrastructure must be secure and compliant with the HIPAA security standards.

Further, the *FDA's guidance for cybersecurity of connected medical devices* states that medical device manufacturers are responsible for remaining vigilant about identifying risks and hazards associated with their medical devices, including risks related to cybersecurity.

They are responsible for putting appropriate mitigations in place to address patient safety risks and share responsibility with healthcare delivery organizations to ensure proper device performance.

As connected medical devices often involve sending telemetry data into the provider's cloud infrastructure, it is critical to gain real-time insights into the vulnerabilities which pose the greatest risk of attack and mitigate those first.

THE SOLUTION

Rezilion helps connected healthcare device companies prioritize mitigation of the risks that pose the greatest threat to their cloud-based service infrastructure.

By doing so, we ensure connected device manufacturers are meeting the required Security Management Process standards defined by HIPAA which *"form the foundation upon which an entity's necessary security activities are built"*. The two leading and key requirements revolve around risk analysis and risk management processes that become the baseline for security processes within covered entities.

RISK ANALYSIS:
Rezilion provides accurate assessment of the potential risks and vulnerabilities associated with applications developed for use by medical professionals to more efficiently collect and process patient monitoring data. Rezilion determines which vulnerabilities associated with the application and its infrastructure present a legitimate risk based on their exploitability. Rezilion highlights which vulnerabilities are exploitable and which are not.

RISK MANAGEMENT:
Rezilion helps to minimize attack surface by prioritizing which vulnerabilities need to be addressed to make the biggest impact on risk reduction and identifying which resources that present risk, can be removed without impact to the underlying service functionality. Creating a smaller attack surface and prioritizing mitigation efforts based on risk helps IT resources efficiently and securely deliver healthcare services to their customers.

BUSINESS BENEFITS

Rezilion enables effortlessly secure delivery of healthcare service applications – improving organizational security posture while allowing product teams to release faster. With Rezilion, the volume and associated cost of vulnerabilities that must be mitigated prior to release are dramatically reduced.

A vulnerability is only as dangerous as the threat exploiting it. The cyber security industry has been unnecessarily exaggerating the number of vulnerabilities security teams must address, which has significant ramifications to the cloud security landscape.

A continuous adaptive risk and trust assessment (CARTA) based approach reduces friction and overhead by identifying vulnerabilities running in memory and then prioritizing treatment to those that don't have a mitigation or compensating control.

It is crucial to first validate that critical applications have minimum necessary resources installed to minimize its attack surface, and then measure the exploitable attack surface used by critical applications so that associated vulnerabilities that are not exploitable can be de-prioritised, therefore, delivering significant gains in operational efficiency.

7-10%

According to analyst firm IDC, organizations are spending 7-10% of their security budget on vulnerability management as daily operations become increasingly more dependent on cloud services.

Vulnerability scanners overload and confuse security teams with mountainous results that would be impossible to patch all at once. The existing prioritization practices such as CVSS provide no notable reduction of breaches in organizations with mature vulnerability management programs. Firms with good security posture are equally breached by known vulnerabilities as those with poor security posture. Gartner recommends in their Implement a Risk-Based Approach to Vulnerability Management report that "security and risk management leaders should rate vulnerabilities on the basis of risk in order to improve vulnerability management program effectiveness".

Gartner also predicts that "by 2022, approximately 30% of enterprises will adopt a risk-based approach to vulnerability management" and "by 2022, organizations that use the risk-based vulnerability management method will suffer 80% fewer breaches."

Rezilion has published research that found 85% of known vulnerabilities identified by vulnerability scanners were never loaded to memory. Our platform identifies artifacts such as code, files and packages loaded to memory analyzing host, container and application resources in production.

We then integrate our telemetry with vulnerability scanners at different stages of the Software Development Lifecycle to correlate vulnerabilities from the scanner results to our mapping of memory in stage or production. If vulnerable code is not loaded in memory — if it's not "running" — it's not exploitable, thus it can either be removed or its patching can be deprioritized.

This visibility helps siloed teams improve their interactions to attest actual risk vs spending time and effort on phony risks, which tends to create mistrust between teams over time. This leads more efficient prioritization with 67% less to patch.

On average, network-connected medical device manufacturers and healthcare delivery organizations are spending $1.4 million annually based on vulnerability management activities. Next year, the spend is expected to grow by 17%.

Reducing that spend by over 60% is significant not only to the bottom line, but to the agility of the organization.