AGILEBLUE

Automation. Visibility. Confidence.

Healthcare Organizations

Whitepaper

AgileBlue, 2021

Securing the future of connected healthcare for patient safety

Institutions such as hospitals, clinics, physician offices, medical device manufacturers, and healthcare technology providers all hold extremely valuable and critical patient data. The implications of a cyberattack on these systems can not only cost institutions millions of dollars but, they can often be a life-and-death matter for patients.

Social engineering, malware, and ransomware attacks are all methods that cyber criminals are increasingly using against healthcare providers. With an increase in connected medical devices, cloud networks and remote workers, there is a greater surface for cybercriminals to attack. The number of systems and devices that IT staff must account for is vast making it hard for teams to secure their systems. Cybersecurity in this environment is critical for the safety of patients, their data and efficacy of healthcare institutions.

At a Glance

- In the next 10 years, medical IoT devices will increase from 10 billion to 50 billion.
- During the first three quarters of 2020, there was a 64% increase in threat detections for the healthcare sector.
- 82% of healthcare organizations had their cloud or IoT devices targeted by a cyberattack within the last year.
- 67% of manufacturers believe attacks on their devices are likely to occur in the near future.
- McKinsey research states, "As more healthcare providers move to the cloud, permit remote workers and increase tele-health the attack surface will expand greatly."

Types of Targeted Attacks

While manufacturers try to produce medical devices to make them as secure as possible, many still have doubts about how they will hold up in light of a cyberattack. There are various explanations for why these medical devices and their networks are so vulnerable. Firstly, end-point security is irrelevant because of regulation limitations on software, operating systems, and warranty concerns. In addition, many of these medical devices were not designed to be connected on a collective network, which makes them even more susceptible to attackers. Along with design limitations, manufacturers withhold information about software and firmware making it challenging for security researchers to inspect the software. Lastly, regular patching for software and devices is a complex process, which in turn affects the continuity of healthcare services.

Devices and Data at Risk

The most private patient data is stored on hospital devices and networks making cyberattacks extremely harmful not only for hospitals but for patients as well. These devices are vital to patient care and safety but, their networks are not as secure as they should be. If not properly monitored, these vulnerable devices and networks can harm patients more than they help them.

Devices

Secure medical devices are essential to patients and healthcare professionals. The Internet of Things (IoT Devices) like infusion pumps, MRI machines, x-ray machines, heart monitors, etc. all operate on a network that can be susceptible to cyberattacks. While these devices help professionals stay connected with patients, breaches in the systems can cause long-term harm to both parties. There are multiple reasons for why IoT devices pose a risk to being compromised. For example, when some of these devices were produced, they were not intended to be connected on a collective network meaning that the proper security measures were not implemented in their production.

Data Risk and compliance

Cyberattacks on healthcare organizations are on the rise making patient data even more vulnerable. These attacks are not only are large monetary setbacks for hospitals but also detrimental to patients whose data is exposed. Healthcare organizations must follow strict protocols and HIPAA rules in order to maintain patient privacy. But, even when hospitals and healthcare companies store patient data on their own network, they are still at a great risk for ransomware attacks and stolen data. Before the end of this year alone, millions of patients across the country have had their data stolen due to ransomware attacks on hospitals and healthcare businesses.

Phishing schemes and ransomware attacks are just a few of the methods hackers use to steal patient data and private information. It is crucial that healthcare organizations review their policies and procedures when it comes to patient data so that it can remain as secure as possible. Implementing 24x7 SOC-as-a-Service technology into your network's security plan is an important first step in securing your organization and patient data.

Device End Point Issues:

- Microsoft Windows 10 Server Block 3.1.1
- Low Bluetooth Energy (LBE) in IoT medical devices
- Ripple20 Flaw in IoT medical devices
- VPN Vulnerabilities
- IoT Device flaws from Baxter, BD Alaris, Biotronik

SOC-as-a-service: Securing the Future of Healthcare

Our Solution

AgileBlue SOC-as-a-Service employs powerful Machine Learning + User Behavior Analytics to create an advanced threat detection and auto-response platform. This technology alerts our team about critical cyber threats in real-time and provides an immediate actionable response. While other IT security solutions can generate tons of false positives when detecting cyber threats, our proprietary Silencer technology learns your behaviors and reduces false positives by 78%.

Along with 24x7 monitoring, detection and response, our platform analyzes millions of log events in order to determine anything that could potentially be a threat. With the AgileBlue SOC your organization will remain secure and compliant with mandates.

About AgileBlue

AgileBlue is a managed breach detection company with an Autonomous SOC-as-a-Service for 24x7 monitoring, detection, and guided response for cloud, digital infrastructures, and applications. AgileBlue provides their clients with enhanced visibility regarding cyber risk via the AgileBlue analytics reporting dashboard. The company offers a proprietary risk scoring algorithm including industry comparisons and risk analysis trends. AgileBlue's silencer technology significantly reduces false positives with a 95% confidence score on incident alerts based on their proprietary machine learning and user behavior analytics.

Ready to protect your company? Contact Us.