Healthcare Organizations: What You Don't See Will Hurt You – Stop The Threat Now

Every Network Has a Security Vulnerability – Where is Yours?

One of the top questions on the minds of network security personnel is "how do I reduce my security risk?" This is because there has been a 500% increase in healthcare ransomware attacks and a 55% increase in healthcare breaches since the pandemic started. So, do you know where you are the most vulnerable? Wouldn't you like to fix any problems now, before a hacker exploits them?

Here is a three-point plan that works to expose intrusions and decrease network security risk:

1. Reduce as many vulnerabilities within the network as possible
2. Find and quickly remediate intrusions that are discovered in the network
3. Periodically test your defenses to make sure they are actually detecting and blocking threats

Network Security – It All Starts With Prevention

Inline security solutions are a high impact technique that businesses can deploy to address security threats, especially ransomware targeting healthcare networks. These solutions can eliminate 90% or more of incoming security threats before they even enter your network. While an inline security architecture will not create a foolproof defense against all incoming threats, it provides the crucial data access that security operations (SecOps) teams need to make the real-world security threat load manageable.

It is important to note that an inline security solution is more than just adding a security appliance, like an intrusion prevention system (IPS) or a web application firewall (WAF). The solution requires external bypass switches and network packet brokers (NPBs) to access and deliver complete data visibility. This allows for the examination of ALL suspect data coming into the network.

Hunt Down Intrusions

While inline security solutions are absolutely necessary to lowering your risk for a security intrusion, the truth is that something bad will make it into your network for whatever reason. This is why you need a second level of defense that helps you actively search for threats. To accomplish this task, you need complete visibility into all segments of your network.

At the same time, not all visibility equipment is created equal. For instance, are your security tools seeing everything they need to? You could be missing more than 60% of your security threats and not even know it. This is because some of the vendors that make visibility equipment (like NPBs) drop data packets (without alerting you) before the data reaches critical security tools, like an intrusion detection system (IDS). This missing data contributes significantly to the success of security threats.

Keysight Technologies has the solution to this problem. Our taps, bypass switches and NPBs provide the visibility and confidence you need that you are seeing EVERYTHING in your network – every bit, byte and packet. Once you have this level of visibility, threat hunting tools can proactively look for indicators of compromise (IOC) for network components and Internet of Medical Things (IoMT) devices.

Stay Vigilant and Constantly Validate Your Security Architecture

The third level of defense is to periodically validate that your security architecture is working as designed. This means using a breach and attack simulation (BAS) solution to safely check your defenses against real-world threats. Routine patch maintenance and annual penetration testing are good security techniques; but they don't replace weekly or monthly BAS-type functions. For instance, maybe a patch wasn't applied (or applied incorrectly) and penetration tests are only good for a specific point in time. Once a few weeks or months have passed, new weaknesses will probably exist. And crucially, were the right fixes applied if a vulnerability was found? For these reasons and more, you need to use a BAS solution to determine the current strength of your defenses.

Keysight NPBs, taps, bypass switches, and BAS solutions offer businesses the following benefits:

- Increased network reliability with better inline security fail-over techniques.
- Improved security appliance survivability with a self-healing architecture.
- Integrated transport layer security (TLS) decryption to expose hidden security threats.
- Zero packet loss for data transfers to your threat detection tools, like an IDS.
- Ability to deploy measures to capture indicators of compromise.
- A BAS solution that enables you to safely test against real-world threats.

Keysight Technologies and our technology partners can show you how to fortify your network against multiple threat vectors.

Remember, you're not anonymous to hackers – find your weakness before they do it for you.

Learn more at: www.getnetworkvisibility.com/FindItBeforeTheyDo

Keysight sponsors GetNetworkVisibility.com, a thought leadership website dedicated to the importance of packet-based visibility to power security, performance, and network monitoring tools. For more information, contact us at:

www.getnetworkvisibility.com/contact-us/