CASE STUDY
Healthcare

Healthcare Services Provider

Easily Measure and Manage Cyber Risk with RiskSense

CUSTOMER PROFILE

Healthcare Services Provider that is a private, not-for-profit healthcare insurer and provider in the Southwest. They own and operate hospitals in many different communities, and also administer different health plans.

"I don't know how we would manage cyber risk in our organization without RiskSense. It's simple to use, highly intuitive, and quite frankly, I'm not sure why everybody hasn't bought it by now.

– Chief Information Security Officer

THE CHALLENGE

This healthcare services provider takes IT system and patient data security very seriously. But analyzing cyber risk was an inefficient and time-consuming process for the provider's internal IT security team. "It was impossible to accurately manage and measure our overall level of cyber risk before RiskSense," explained Chief Information Security Officer. "We had to look at each individual security report, match it up against multiple other reports, do a lot of our own internet research, and then keep our fingers crossed that we had the situation in hand. We clearly needed a way to automate these processes to improve our overall security understanding and defensive posture."

THE SOLUTION

This healthcare services provider started using the RiskSense platform in 2016. RiskSense's innovative approach to cybersecurity leverages intelligence-driven analytics to reveal cyber risk across a growing attack surface, quickly guide remediation, and monitor the results. The platform provides complete threat and vulnerability data for all asset classes, including the network, endpoints, applications, databases, and Internet of Things (IoT) devices. RiskSense also includes support for industry-leading scanners and threat data sources, providing additional rich context. "Rather than doing pure malware research, RiskSense has taken more of a risk-based approach, something that resonates very well with our security team as well as our board members and executives," explained the CISO.

THE RESULTS

Mitigating a Security Event Even with the diligent efforts of the provider's hard-working IT security team, This healthcare services provider experienced a very impactful security event a few years ago. "We struggled through the event, even though we had engaged some of the best known names in the information security sector to help us work our way out," reported the CISO. "Luckily, RiskSense came to the rescue and helped us deal with the system-wide event that had brought all of our IT systems to a screeching halt. With RiskSense by our side, we were able to quickly identify and mitigate the attack before it caused any harm to our systems or private patient data."

A Comprehensive View of Risk "I think the dream of every security manager in a medium to large enterprise is the concept of a single pane of glass, or one-stop shop for vulnerability management," noted the CISO. "But when your infrastructure consists of hundreds of applications and thousands of devices, it's very difficult to gain any level

of clarity when you're digging through six pages of metrics to make sense of the overall threat landscape."

RiskSense has greatly improved cyber risk management for this healthcare provider by providing all security metrics and information in one centralized console. "Many tools will tell you about all of the separate 'potholes in your street', but RiskSense combines it all together for greater insight. Being able to understand the risks revealed from a pen test within the greater landscape of our overall posture has led to improved security and greater efficiency for our organization," reported the CISO. "With all relevant information in one place, we can immediately see what kind of remediation is needed, not just what our current problems are. RiskSense enables us to ask, 'Is this risk theoretical, like the Intel flaw that was recently shared again? Is it theoretical and would take a PhD to cause a problem? Or is it well-known and everybody's getting hit with it?' We get a pragmatic view with RiskSense, rather than a theoretical view. It has given us the ability to accurately identify the risks that are most germane to our environment and quickly work on closing those gaps to seal off the exposure."

An Accurate Assessment Using RiskSense Scores

Much like a credit score for articulating financial health, RiskSense continuously reports on this healthcare provider's cyber risk profile by asset, department, organization, and user-defined categories, and then calculates an overall security score. "Our board of directors always asks us, 'What's our overall risk?' In security we joke, 'What time of day is it?' It's not like the stock market, where there's an opening bell and a closing bell—vulnerabilities get released around the clock," explained the CISO. "We had a fairly good handle on our 'traditional' risk level in terms of security policies, processes, and standards, but we lacked a single, holistic metric of our overall risk. The RiskSense score is a great way to quickly tell the story at the executive level, and track all of the improvements we're making to security over time. It makes our infrastructure more secure and our Board of Directors much happier!"

NEXT STEPS

This healthcare provider is now focused on reducing risk for all of its IoT devices. "Up until now, we've focused on our virtual and physical system infrastructure – worrying about those vulnerabilities and getting them patched quickly," said the CISO. "But when we look at our entire environment, there are over 40,000 things that 'talk' on our network and less than 30% of those are traditional desktops, laptops, and servers. We also have smart thermostats, wireless IV pumps, pacemakers, surgical robots, surveillance cameras, and hundreds of other IoT devices. In a world where the IT perimeter is rapidly eroding, it's those things that keep me up at night. It's not a malicious attack to an individual IoT device that I'm worried about, it's the unintended consequence if malware gets into our environment and those devices sustain collateral damage. RiskSense is enabling us to get a better handle on our entire attack surface—including all of our IoT devices—reducing overall risk to our infrastructure."

When asked if he had any advice for other IT organizations seeking to improve cybersecurity, the CISO replied, "In my opinion, RiskSense should be part of your 'quiver'. If it's not, you're flying blind. RiskSense is providing the level of clarity I sought in our vulnerability management processes. I don't know how we would manage cyber risk in our organization without RiskSense. It's simple to use, highly intuitive, and quite frankly, I'm not sure why everybody hasn't bought it by now."

WHY RISKSENSE

- Single pane of glass console provides better visibility into expanding attack surface, reducing cyber risk to IT infrastructure and IoT devices
- Quantitative risk scores provide an easy-to-understand measure of overall vulnerability, enabling the IT team to measure security improvements over time
- Comprehensive security reports and metrics enable IT analysts to quickly understand risk and prioritize activities to acheive specific risk goals