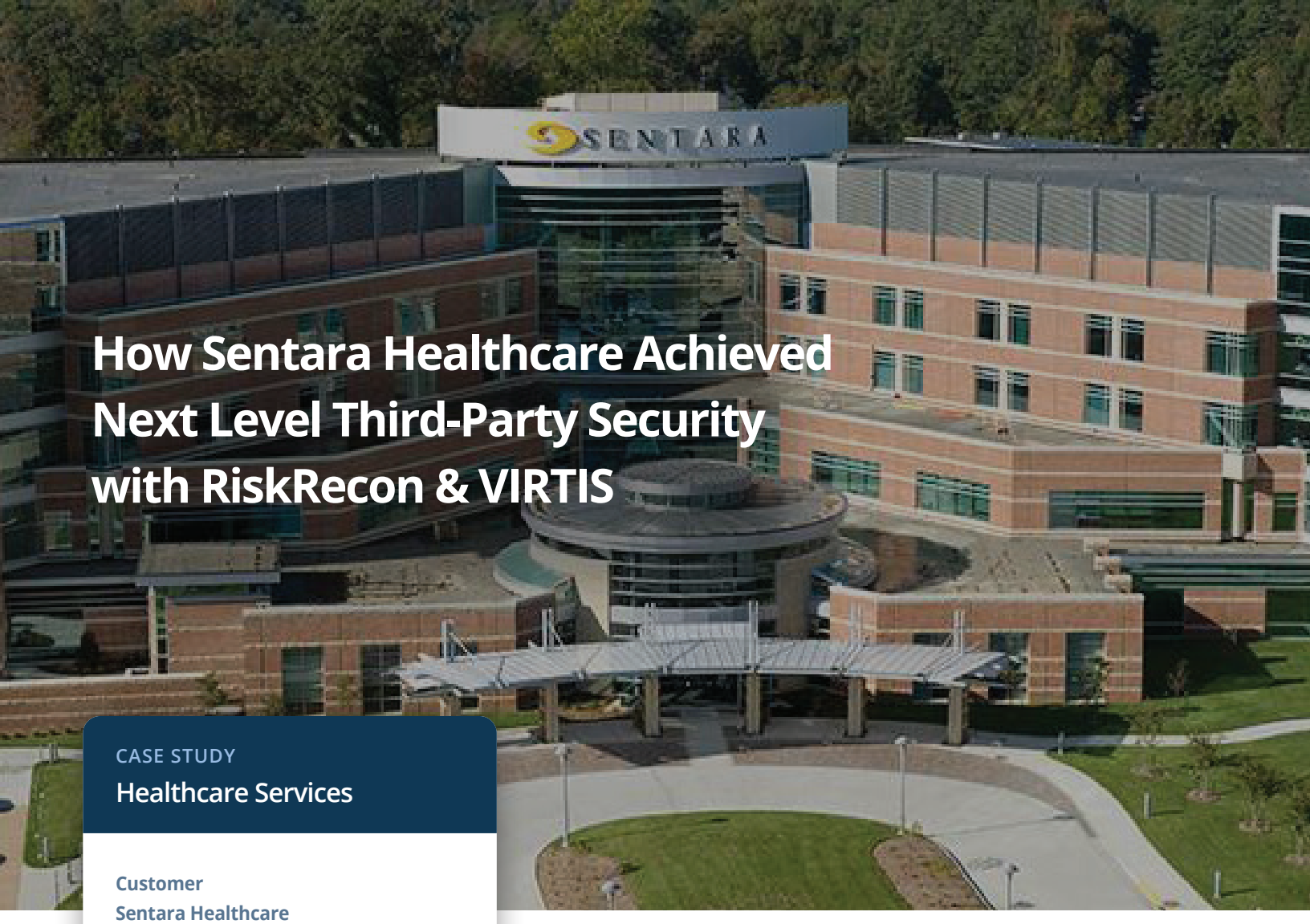

How Sentara Healthcare Achieved Next Level Third-Party Security with RiskRecon & VIRTIS

CASE STUDY

Healthcare Services

Customer
Sentara Healthcare

Industry
Healthcare

Summary
After seeing the benefits of using RiskRecon and VIRTIS for threat shielding and third-party risk monitoring, this healthcare organization found a way to use the platform to validate security controls internally as well.

Results

- Validation of the efficacy of internal application security controls
- Prioritized security vulnerabilities in internal infrastructure
- Provide a benchmark for proving security investment ROI to executive team

THE CUSTOMER

A not-for-profit healthcare system based in the US mid-Atlantic region, Sentara Healthcare is a long-running organization that serves communities with more than 300 sites of care. Its technology team supports a range of urgent care centers, advanced imaging centers, medical groups, and 12 different hospitals.

Sentara's tight-knit team of cybersecurity professionals support the organization's significant digital transformation strategy for the coming years, which includes investment and development work on a new patient portal, health plan member portals, telehealth capabilities, and mobile apps. To do this the team needs a strong set of security controls and validation mechanisms to keep track of both third-party and internal risk, without getting in the way of innovation.

VIRTIS
We Keep You Protected

riskrecon
mastercard

THE PROBLEM

As Sentara's executive leaders learned more about cyber threats posed by the organization's third party service providers, and the challenges of constant vulnerability management on web and mobile applications, they sought out solutions to provide better risk posture reporting—while protecting key web and mobile application platforms.

Bowden's immediate recommendation was to bring on RiskRecon to start continuously assessing the risk posture of vendors and partners serving Sentara. The RiskRecon platform now serves as the backbone of a maturing third-party risk program that the executive team increasingly leans upon to understand how their external relationships shape their cyber risk exposure. Additionally, VIRTIS, powered by RedShield was added to their security program to provide Sentara with advanced shielding and vulnerability remediation for their web applications.

But the process of growing that trust in third-party risk management and the visibility RiskRecon afforded brought one more thing to consider.

"If your boss has any awareness at all—which mine did—they're going to ask 'What does this score say about us?'" Bowden explains. "We sat down and I showed him that it wasn't terrible, but it wasn't comfortable either."

But as Bowden explains, he was happy and eager for that conversation because it kicked off a new initiative for cyber self-improvement that dovetailed perfectly with the strategic missions his team was tasked with supporting. When Sentara used RiskRecon to assess itself, it identified some key areas for which the business felt it was imperative to bring scores up to as close to 'perfect' as possible. Chief among them was application security and vulnerability protection, which has been growing in importance as the IT team has increasingly been called to support the business with new apps and platforms.

Like all technology teams, Sentara's security and development staff faces the common issues of dealing with too many vulnerabilities and not enough time or manpower to fix everything. It needed a better way to more quickly identify the most impactful vulnerabilities for swift development fixes, and to increase the coverage of its vulnerability protection for the flaws the dev team couldn't get to right away by using other mitigation measures.

THE SOLUTION

Now in addition to powering Sentara Healthcare's third-party risk management program, the platform sits at the heart of its own internal cybersecurity efforts. Sentara uses RiskRecon as a mechanism for both validating controls and continuously prioritizing high-profile vulnerabilities based on the impact determined by RiskRecon scoring mechanisms. Besides, the scoring capabilities help Sentara measure and communicate improvements to its internal risk posture as new security controls and processes are put into place.

Central to this internal use of RiskRecon at Sentara is the integration with VIRTIS' Web Application Security services. VIRTIS' application shielding services offers an extra level of protection beyond what a web application firewall provides and virtually 'patches' known vulnerabilities within web applications before a more permanent fix can be made to the code by the development team.

> *"What we learned was by combining what we do with RiskRecon and VIRTIS, I was able to do a proof of concept for some of our web applications... That's when we started investing more heavily into both platforms."*

"What we learned was by combining what we do with RiskRecon and VIRTIS, I was able to do a proof of concept for some of our web applications, turn on the shielding service, and then use RiskRecon to validate the efficacy of the shielding," explains Bowden. " That's when we started investing more heavily into both platforms."

Today, VIRTIS continuously checks up on Sentara's RiskRecon data to identify potential new problems in its web application infrastructure and prioritize future improvements. The attentiveness of the RiskRecon and VIRTIS solution is an end-to-end solution that has helped Sentara identify problematic assets that the team previously didn't know about, implement shielding for them, and then validate that the shielding mitigated the risk to the organization. What Bowden says Sentara appreciates most about the RiskRecon/VIRTIS solution is its ability to offer clear risk prioritization information based on the likelihood of impact specifically to Sentara's infrastructure with the ongoing peace of mind knowing that VIRTIS is acting upon them.

"I like what RiskRecon does. It gives you what I call the high and wide matrix or heat map of risk," Bowden says. "It combines a given vulnerability with things that are known to be happening in terms of campaigns and applicability to your organization." Now in addition to powering Sentara Healthcare's third-party risk management program, the platform sits at the heart of its own internal cybersecurity efforts.

THE RESULTS

Using RiskRecon's prioritization of flaws in conjunction with VIRTIS' web application security services enables Bowden's team to not only have developers fix the extremely critical vulnerabilities when they're found, but also to shield against the mediums and even highs that can't be immediately fixed due to cost or time constraints.

By leveraging the VIRTIS RedShield solution, the Sentara team was able to raise its cybersecurity risk rating significantly in a short period—truly maximizing the impact from the shielding and remediation capabilities within the platform.

"High impact vulnerabilities get put there in that upper right-hand quadrant (of the heat map) and that's what our team uses to act," he says. "Occasionally our team will see something that's down the median that, just because of internal context they'll say, 'We should get rid of that one, too.'"

More fundamentally, RiskRecon's scoring has become a very meaningful risk metric for the entire organization outside of the security team.

"A meaningful metric is one that the organization's chief operating officer remembers. When someone at that level remembers that number, that's a meaningful metric," says Bowden. "That's our RiskRecon score. You can ask him, 'Hey, what's your RiskRecon score?' He'll tell you what it is."

This level of awareness enables Bowden as a CISO to have more meaningful conversations about the costs of improving risk in certain areas and in managing incremental improvement. It also helps prove investment over the long run.

"At that point, your job is so much easier because there is shared accountability," he says. "That's where you want to be as a CISO."

riskrecon mastercard www.riskrecon.com

VIRTIS We Keep You Protected https://virtis-us.com