RAPID7

CUSTOMER STORY

Industry
Healthcare

Region
Americas

Company Size
Small Market

Products
InsightVM,
Managed Detection
& Response

Package
Managed Threat
Complete

HOW A HELP DESK TOOK ON A $5.6 BILLION PROBLEM AND WON

THE OREGON CLINIC

OVERVIEW

Think about it: medical records are worth 10 times more than credit card numbers in the internet's darkest corners and black marketplaces.[1] Purchase electronic health records, and you have everything: social security numbers, addresses, everybody's jobs, their kids, all of it.

Now, rewind to 2014 and meet Kenny George and Eric Bachelder. Along with seven help desk associates and four network administrators, they took over security at the Oregon Clinic a decade ago and started figuring stuff out.

The Oregon Clinic is the largest private multispecialty physician practice in the state. Like most organizations in 2014 — a time Kenny George calls their cybersecurity "infancy" — they used a lot of manual processes as well as a couple of smaller, specific security solutions for log management. And they knew they needed something proactive to handle logging and vulnerability management.

+

550,000 PATIENTS VISIT EACH YEAR.

DATA BREACHES COST THE INDUSTRY A CRUSHING $5.6 BILLION PER YEAR.[2]

1 Experian global information service
2 PBS News, "Has health care hacking become an epidemic?" 3/23/16

CONSOLIDATION, AND MAKING THE WORLD'S HARDEST JOB EASIER

Leave it to help desk guys to know instinctively: tools that are easy for humans to work with are always the best idea.

"Rapid7 was really the one that stood out to us as being easy to use as well as easy to set up," said George, who rose to become Information Security Analyst for the Oregon Clinic. "And the support was also really thorough."

The Oregon Clinic uses Rapid7's next-gen SIEM InsightIDR, vulnerability management solution InsightVM, and 24/7 monitoring with Rapid7 Managed Detection and Response (MDR). "Rapid7 has helped us automate things and find those alerts that we really need," George explained.

George says his team loves the ability of Rapid7 to integrate with other platforms that they also need. "We still have a few different vendors and manufacturers, and getting it all in one pane of glass is beneficial," he said.

> **"We love that it's cloud-hosted, we don't have to stand anything up on-premise. It was a huge selling point to not have to manage that in our own environment. And the cost for that benefit is great."**
>
> Kenny George, Oregon Clinic Security

TODAY, VISIBILITY IS UP 10X ON THAT LONGED-FOR SINGLE PANE OF GLASS

Rapid7's ability to easily integrate matters. The team can see logins from the VPN, logins to Active Directory and workstations, even executables that may have been launched on an endpoint. It's all correlated within Rapid7's InsightIDR.

The result? According to Eric Bachelder – another long-termer who rose to IT Operations Manager – it's alerts that are meaningful. "Alert fatigue is a real thing! The tuning we have been able to do with Rapid7, filtering out the alerts that we know are benign, gives us the ability to know that when we see an alert, it's something we should be looking at. We can rely on Rapid7 for that. We're confident in them."

Oregon Clinic's cybersecurity insurance company asked over and over: *do you guys have 24/7 security operations center coverage?* The answer was no. "We didn't have eyes on those alerts at three in the morning," said Bachelder. Now, with Rapid7 MDR, the environment is watched around the clock.

Like all healthcare organizations, Oregon Clinic is bound by HIPAA regulation. Bachelder also says his support team and account managers have been wonderful to work with: “They’re a trusted extension of our team.”

Q: ANY ADVICE FOR THOSE MAKING THEIR WAY INTO CYBERSECURITY LEADERSHIP NOW?

When asked how IT managers and analysts can get off to a strong start, Bachelder had a quick answer: “Ingest as much data as possible to the platform. Send everything to Rapid7 and then fine-tune what you actually do or don’t care about over time.”

The Oregon Clinic, for example, has set up their Rapid7 preferences to send logs to InsightIDR about every single attempt to try to log on to any device on their network.

“We’re able to tell if somebody fails to login to a network device, and I have that as a custom alert added on,” he said. “We were curious if somebody’s trying to brute force a network switch or something like that. We never had that visibility before until we had Rapid7. We get that email alert saying, Hey, this is suspicious. It was noisy, but we’ve fine-tuned it. You have to go big and just ingest everything. Then tailor it to your environment.”

Data breaches aren’t just catastrophically expensive, they also grind things to a halt – which you cannot have in the provision of health care services to patients. It’s a serious mission. Rapid7 is here for that.

> **If somebody, anybody, is trying to drop data into a third-party storage service like Dropbox or Box.com, any place like that, it’s not allowed, Batchelder explained. “Rapid7 identifies that traffic and puts a stop to it.”**
>
> Kenny George, Oregon Clinic Security

View more success stories.

CUSTOMER STORIES

RAPID7

PRODUCTS

Cloud Security
XDR & SIEM
Threat Intelligence
Vulnerability Risk Management
Application Security
Orchestration & Automation
Managed Services

CONTACT US

rapid7.com/contact

To learn more or start a free trial, visit:
rapid7.com/try/insight