CASE STUDY

Heavy-equipment dealer fights ransomware attack – and wins – with Tanium

After an attack, Ring Power, a Florida-based dealer of Cat® equipment, used Tanium to avoid paying ransom while restoring its data center and endpoints to full operation.

Industry
Heavy-equipment dealer

Headquarters
St. Augustine, Florida, USA

Endpoints under management
2,300

Tanium solutions

- XEM Core
- Endpoint Management
- Risk & Compliance
- Incident Response

If and when ransomware strikes, Tanium can help organizations recover quickly and efficiently.

How Ring Power recovered from ransomware with Tanium

In September 2019, Kevin Bush was awakened one early morning by a phone call informing him that Ring Power was the victim of a ransomware attack. He subsequently discovered that the company's entire data center was disconnected from the outside world. In addition, some unknown number of the company's 2,300 endpoints was dangerously infected.

With help from Tanium, Bush and his 10-person IT team were able to completely disinfect and restore Ring Power's IT infrastructure in a matter of weeks. And he did so without paying the ransom – in fact, without ever communicating with the attackers.

Challenge

A ransomware attack left Ring Power with its data center completely cut off and an unknown number of endpoints infected.

Solution

With help from Tanium, Ring Power recovered fully from the attack and without paying the ransom.

Result

With Tanium's help, Ring Power didn't need to pay the ransom or even communicate with its attackers.

Challenge

It was at 4:30 in the morning when Kevin Bush, VP of IT for heavy-equipment dealer Ring Power Corp., was awakened by a phone call he'd hoped to never get. The predawn caller, a representative from Ring Power's MSP, had bad news. Sometime during the previous evening, one of Ring Power's managers had unknowingly clicked on a phishing email. In the hours that followed, the company's IT infrastructure was attacked by ransomware. And now, with an unknown number of endpoints infected, Ring Power's data center had been taken hostage. All that, and it was only Bush's 11th day working for Ring Power. "Ransomware's like a terrible disease" he says today. "You know about it. But you hope it'll never happen to you."

> Sometime during the previous evening, one of Ring Power's managers had unknowingly clicked on a phishing email.

Solution

With help from Tanium, Bush and his team restored the IT infrastructure in a matter of weeks. And they did so while not only refusing to pay the ransom, but also refusing to contact the attackers at all.

“Tanium made it so much easier to recover,” says Brian Hall, Ring Power’s MIS operations manager and a member of Bush’s IT team.

> “Tanium really helped us recover.”
>
> **Brian Hall**
> MIS Operations Manager,
> Ring Power Corp.

Achieving all that took Bush and his 10-person IT team about three weeks. That morning in September 2019, their first action after receiving the phone call was to rush to the office and assess the damage. What they found wasn’t good. Ring Power’s entire data center, including all 150 servers, had been completely disconnected from the outside world.

> “Tanium brings visibility to one screen for our whole team. If you don’t have that kind of visibility, you’re not going to be able to sleep at night.”
>
> **Kevin Bush**
> VP of IT, Ring Power Corp.

To limit the damage, Bush and his team took quick action. They powered down all the servers. They protected their backup systems by taking them offline. And they made phone calls to the company’s 26 locations, telling people to test their computers for infection. If they could open Word or Excel, their machine was clean. But if they instead saw the “Ryuk” icon on the screen — that’s the name of a ransomware type — their machine was infected. In those cases, employees were instructed to turn off their computer, pack it in a box, and ship it to Ring Power headquarters, where the machine could be cleaned.

Once that was completed, the next agenda item was restoring systems. It was a big job involving restarting those 150 servers, redeploying some 200 applications, and bringing back up roughly 2,300 endpoint devices. With so much to do, Bush and his team worked exhausting 80-hour weeks for two long months.

Bush’s next step was to get Tanium installed on all clean endpoints. Ring Power had recently signed on with Tanium, but so recently, the installations hadn’t started yet. The IT team loaded Tanium tools onto many portable USB drives and shipped them to the branch offices with instructions.

Says Bush: “We spread Tanium like butter.”

> “I love Tanium right now. You configure it the way you want, and it just runs. Tanium is truly set it and forget it.”

Brian Hall
MIS operations manager,
Ring Power Corp.

Result

Once all Ring Power users had Tanium on their computers, they could redeploy their applications themselves. That meant Bush and his team didn’t need to do the job manually – a big savings given Ring Power’s large number of locations, users, and systems.

It also meant that Ring Power paid no ransom whatsoever. In fact, the company never even communicated with its attackers. Instead, Bush simply shared the attackers’ email address with the FBI. Later, the agent assigned to their case said Ring Power was already in better shape than 90% of the companies he deals with. Given that the agent is assigned to an average of four new cases a day, that’s one authoritative assessment.

With Tanium, Ring Power also greatly improved its visibility into and control of endpoints on its network. Ring Power found Tanium to be extremely simple to manage with modules and capabilities that other endpoint management tools do not have.

“I love Tanium right now. You configure it the way you want, and it just runs. Tanium is truly set it and forget it,” says Hall.

Using Tanium has also allowed Ring Power to automate patches and updates. Previously, the MIS team had to manually install software, a time-consuming process. Now, with Tanium doing that work, the team is saving an estimated hour and a half a day.