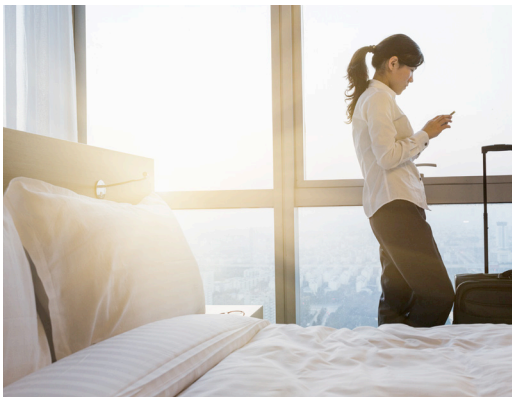
ThreatINSIGHT Keeps Vigil at a Global Hotel Chain

Gigamon Network Detection and Response Quickly Replaces Cumbersome Old-School Network Forensic Tool



UNEXPECTED SAVINGS

One unexpected area the Gigamon solution saved the hotel change money was in acquisitions. When assimilating a newly acquired company's IT infrastructure, or preparing an acquired site for eventual closure, it turned out to be much less expensive and easier to install Gigamon solutions in the interim instead of continuing to use legacy security solutions. And when a temporary site eventually closes, Roger and team deploy the Gigamon solutions to the next appropriate site. The CapEx savings have been substantial.

Roger Smith leads a team within the Security Operations Center (SOC) of one of the largest hotel chains in the world. As you'd imagine, being in the hospitality business adds some interesting wrinkles to his job.

Amid the coming and going of hundreds of thousands of people from all over the world, safeguarding point-of-sale installations is important, certainly. As is guarding against attacks from advanced persistent threat (APT) groups. But the number-one daily threat faced by Roger and his team is surprisingly mundane.

"It's phishing," says Roger. "Our biggest pain point, quite honestly, is still just people clicking on stuff in emails that they shouldn't. We see that every day, and it's a tough battle that we still fight."

Given the seemingly infinite human capacity for folly, Roger and team needed a solution to afford the business as much proactive, real-time protection as possible. They found it in Gigamon ThreatINSIGHT cloud-native, high-velocity network detection and response.

Out with the Old: Revamping an Entire Network

That addition didn't happen overnight. Prior to finding Gigamon ThreatINSIGHT, Roger and team suffered with a series of legacy tools. They adopted one key solution in 2015, but after taking weeks to deploy, it didn't fully cover all the bases the SOC needed covered. Other important tools were difficult to use and didn't mesh well together.

"It was a poor experience," says Roger. "This was an old-school network forensic tool, so it was cumbersome to use and sometimes searches never finished. It threw a lot of unnecessary stuff at the user that would confuse them, create analysis paralysis or lead them down pointless rabbit holes."

As the larger company embarked on a massive reorganization, Roger's group had the rare opportunity to design a new network infrastructure from scratch.

"Everything is net new and carefully planned," says Roger. "We barely have any of the legacy, security and IT problems that a lot of organizations face."

The Worst Laptop Ever

Gigamon: Tell us the laptop story.

Roger: Hoo boy. Okay. We had a contractor come in. It was his first day on the job, and he was waiting for an imaged machine from IT. He decided to plug his personal laptop into the network where the contractors sit, and ThreatINSIGHT immediately went crazy.

I'm a malware reverse engineer by trade. This was probably, across my decade-plus career in cybersecurity, the single most infected machine I'd ever seen. This thing was ringing all the bells. If there was a detection available in Gigamon ThreatINSIGHT, this laptop was tripping it.

It was both funny and horrifying. We traced its location and sent over a mini raiding party because everyone just had to see this thing. And the… artifact we found sitting on this guy's desk looked just as scary in real life as it did on the network. It was bad.

But yeah, we got it contained and told him he might want to throw the thing out. Funnily enough, the next day we had our official ThreatINSIGHT training, so that gave us a nice dataset to go through. And the incident also helped make our case for changes in how we handle contractors.

One for Two

ThreatINSIGHT replaced a network forensic suite and a tactical detection platform the SOC had used in the old network. In contrast to their fragmented and clunky user experience, ThreatINSIGHT provided the hotel chain a complete network-intrusion response platform that was easy to use, showing all relevant data in on solution

"We went from proof of concept to production in about a month," says Roger. "And when we deployed the first ThreatINSIGHT sensor in a regional datacenter, it was up and running that same day. They simply received it, plugged it in and it was working."

He likens it to a tripwire on the network, able to quickly detect all manner of threats and malware via its built-in detection logic.

The Teams Loves Using ThreatINSIGHT, Too

"As a daily user I appreciate the consistency among all the screens, the clean user interfacet, how easy it is to pivot. Just the fact there's a right-click menu is huge; you just don't see that enough," says Roger.

"The shortcuts save us a ton of time. I don't have to manually open a tag, log into the console, rebuild my search. It's just one right click and another left click: done. I can now pivot on that data and move on."

Gigamon: What are your five favorite things about ThreatINSIGHT? (We're fishin' for compliments here.)

Roger: Earlier I think I mentioned the right-click menu, and having everything on a single pane of glass. So that's two.

Three, our team trusts the data coming out of ThreatINSIGHT as reliable. And that's coming from a place where, yeah, I'm not sure we always had full trust in the old products. I'm super-confident in ThreatINSIGHT. Since we've switched it's been night and day.

Four, I love that the default detection rules cover a lot of our threats in the background. That's refreshing because that's less time we have to worry about the tool and more time we can focus on advanced threats.

Five? It's so easy to use. We waste much less time figuring things out, and we love all the thoughtful touches like documentation and training material embedded right in the tool. That all's helped get our SOC guys up to speed on the product quickly.

Gigamon: We're blushing. You really rattled those off!

Word Gets Around

As Roger put ThreatINSIGHT through its paces this last year, he discovered one more thing it's good at: Making the case for IT's business value to his C-level management, who don't necessarily respond to technical talk of network TAPs and packet sniffers.

"My high-level explanation is that ThreatINSIGHT is watching what's coming and going between our most critical infrastructure and the internet," says Roger. "When ThreatINSIGHT captures something anomalous, identifies and bubbles it up for us to investigate and remediate, that immediately shows value to our senior leadership: Gigamon picked up on something important that would have been missed by all of our other tools."

He concludes, "With Gigamon deployed there's a sense, I don't want to call it relief, but a better sense that we've got this than not."

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | www.gigamon.com