RAPID7

CASE STUDY

EMW Law Relies on Rapid7 Insight Platform to Meet Evolving Security Requirements

InsightConnect, InsightIDR, InsightVM, InsightAppSec

Customer Overview

EMW is a law firm with a refreshing approach, advising UK based and global businesses and individuals on legal matters from corporate and banking, commercial, technology & data, real estate, employment law and dispute resolution to personal legal services for individuals. They have offices in Gatwick, London, and Milton Keynes. Since 1992, their strong commercial sense and proactive manner has helped transform their clients' legal challenges into business solutions.

Challenge

As a law firm entrusted with confidential client business data, EMW takes cybersecurity extremely seriously. "There is a requirement, not only from our clients but also from the Solicitors Regulation Authority (SRA), that we exceed certain criteria when it comes to being secure and handling confidential data," explains Lee Killner, IT Director at EMW. This commitment to security shows: EMW has achieved National Cyber Security Centre (NCSC) Cyber Essentials certification every year since 2017.

Despite the success, Killner says the firm's established on-premises security solutions were struggling to keep up with an evolving threat landscape and work environment.

"Our detection and response product mostly did what we needed it to do, but also generated a lot of false positive alerts. That caused significant inefficiencies, as each alert could lead to two or three hours of research getting to the bottom of it. Time spent investigating false positives is time I'd rather devote to tasks that really matter."
Killner adds that the firm's vulnerability management solution had a patch management system that wasn't meeting the needs of the business and was too resource intensive. "That's why we looked to find something that would give us the confidence that we're tracking the vulnerabilities."

Meanwhile, a shift in user behavior prompted Killner and his team to add another requirement to any new solution: it had to be cloud-based. "I wanted to have access to this information anywhere." states Killner. "During the course of the pandemic, users were taking devices and working at home, so there's a significant flaw in having a system that is purely based on-prem and only looks at equipment based on-prem."

When selecting the law firm's new threat detection and vulnerability management solutions, Killner didn't just want to eliminate noise and move to the cloud. "The solutions needed to be intuitive to use, but also had to be backed by expert support. If I've got security experts I can go to and ask, 'What does this mean?' and they're willing to assist with that, that's half the battle."

After weighing the available options and speaking with trusted third-party consultants, Killner and EMW landed on InsightIDR and InsightVM from Rapid7.

InsightIDR is Rapid7's cloud-based threat detection and response SIEM, enabling organizations to respond with speed and confidence to attacks by spotting the behavior behind security breaches. With machine learning, advanced analysis, and out-of-the box detections curated by Rapid7's global SOC team, it allows security professionals to quickly sift through data to identify and respond to real threats, all within one interface.

"Having a solution that can filter through that noise, and just give you the alerts that are more concerning – that's a godsend because it makes sure that I'm actually focused on the things that really matter," explains Killner. "I can honestly say that for me, Rapid7 has ticked that box."

"Rapid7 is an intuitive tool that gives you the results you need, without all the noise in the background."
InsightVM from Rapid7 uses the same underlying agent to provide real-time insight into vulnerabilities. Risk-based attacker analytics help firms to automatically prioritize threats and remediate with speed.

> ***"Having a solution that can filter through the noise, and just give you the alerts that are more concerning – that's a godsend because it enables me to focus on the things that really matter. Rapid7 has ticked that box.***
>
> ***- Lee Killner, IT Director at EMW***

Immediate Deployment

InsightIDR and InsightVM are built in the cloud to get up and running quickly, while continuously up-leveling an organization's capabilities as they grow into the platform. For EMW, this has made the transition a painless one.

"Agent deployment is literally click, click, next, done. And suddenly it appears in the portal," according to Killner. "Life is wonderful, as they say. From a tech perspective, this is the ideal."

"I installed agents on all servers and we are rolling it out on endpoints as well to give us visibility," continues Killner. "Particularly in the current climate, where everybody's working from home, we can actually see what's going on with the endpoint as well."

Alerts That Matter

Since switching to InsightIDR, Killner and the IT team at EMW have experienced “so much less noise,” with a 93% reduction in false positive alerts. And thanks to the Insight Platform’s powerful endpoint visibility, analytics, and automation, this reduction in time-consuming alerts is coupled with the “confidence that we’re gathering the right set of data.” “I particularly like this because it’s actually highlighted an issue for us,” explains Killner. “It has the ability to recognize that people are logging in from different countries at the same time. I am confident that the solution we have in place now will enable me to go back and look to see what occurred and when it occurred, then provide me with the detail I need in a timely fashion.”

Expert Insights

EMW has already started to leverage Rapid7’s threat intel network, research, and SOC experts to help them make the most of their resources. From relevant blog posts to responsive support, Killner appreciates the access to industry-leading insights. “I rely on my partners and vendors to provide me with as much information as possible, so I can make informed decisions for our organization.”

Seamless Integration

The next step for EMW? Integration between the Insight Platform and their existing technology stack to get even faster analysis, prioritization, and remediation. “With all of these technologies working together, we’ll have a fuller picture of where we are and where we’re going,” says Killner.

In other words, “as the security environment evolves, EMW will be looking to Rapid7 to help us evolve with it.”