

Acme Brick

Rapid7 Brings Peace of Mind and
Newfound Time for Lean Teams.

Products

InsightVM

InsightIDR

InsightConnect

Industry

Manufacturing

Size

Enterprise (Mid-Size)



Overview

The Company

Since its founding in 1891, Acme Brick has continually advanced the art and science of brickmaking, to make brick an affordable, sustainable, enduring, and beautiful choice for America's homeowners, builders, contractors, institutions, and businesses.

The Challenge

Dusty Zook has been with Acme Brick for seven years. In his earliest days, there was no "security team" – just a single employee. Today, there are just two team members (Zook and an analyst) responsible for the security posture of 1200 workstation and servers as well as 1200 actual active users. Naturally, life can get overwhelming for this team of two. Acme Brick needed a tool that could streamline the day-to-day operations of a very lean team – in fact, Zook called the need for efficiency "critical" from day one.

The Solution

“InsightVM was the only Rapid7 product that we had purchased at first,” recalled Zook, whose team has since brought on InsightIDR, InsightConnect, and Metasploit. “Before we transitioned to InsightIDR, I would spend my entire day on another platform and not look at any other tool because none of our other tools really fed into it. I couldn’t keep up with everything. And, when we looked at trying to streamline and bring everything into one pane of glass, Rapid7 showed us the simplicity of the InsightIDR user interface. And I’m telling you, being able to log in and to see all of our other security tools feeding into Rapid7 makes my day-to-day go way faster.”

According to Zook, that efficiency extends to his analyst colleagues as well. “He logs into one tool, and if we see an alert, then we can log into the other tools in one pane of glass. It’s all feeding into Rapid7, and we’re using it as a simple single pane of glass to make our day go smoother.”

Peace of Mind Beyond the 9 to 5

One key thing Zook’s firm needs in a security solution is a 24/7 partnership, since his team doesn’t work the graveyard shift. “I’m not going to say we’re eight to five people, but we were looking for something that happens after hours,” he recalled. “If it’s critical, Rapid7 reaches out to us. Rapid7 gave us the opportunity to give them access to our platform to co-manage it with us without going through extra hoops like creating local accounts on our network and granting VPN access. We’ve basically just created accounts for Rapid7 and they took over and could manage it with us.”

Vulnerability Management Made Easy

“Vulnerability management is a complex job,” mused Zook, referencing the fact that he has one analyst who is responsible for much more. Zook and his analyst are both happy that Rapid7 allows them to efficiently learn as much as they want about different aspects of their security posture. “InsightVM helps us understand where our weak points are... which workstations or servers are missing critical patches, for example. It helps us find those weak links in the system or in the network. And, the fact that it feeds back into IDR just makes it an even better tool. We could use other vulnerability management tools, but they’re not going to integrate like Rapid7.”



InsightVM helps us understand where our weak points are... which workstations or servers are missing critical patches, for example.

Dusty Zook, Security Team, Acme Brick

Furthermore, Zook waxes poetic about InsightVM's ability to find an asset and filter down with ease. "Let's say I'm going to try to find every workstation that has a specific CVE. With InsightVM, it's super easy, and it doesn't take very long. I can export a list within just a few minutes. I don't have to write a complex query that says, If this, not that, but this. It's pretty straightforward. And it's critical for us that we're not spending hours to find and investigate assets."

ICON: A Critical Addition

Zook is also very happy that his organization elected to utilize InsightConnect with InsightIDR in recent years. "There have been instances where we got an alert when access to a user's account was being attempted in a foreign country – not a country that we would do business in, nor a country that the user was vacationing in," he explained.

"It was such a critical alert that it was actually sent to our Slack notifications. Because we had InsightConnect set up for Slack notifications, we were able to see that really quickly," continued Zook. "Within just minutes, we're able to get the user's account shut down with password reset and then start the investigation. There was no compromise. It was remediated within ten minutes."

"How fast does it take for a bad actor to compromise an account, use that account, send out thousands of emails, or start utilizing it in a negative way?" he asked, rhetorically. "I mean, within minutes, they're going to cause some damage. We've seen it before. But because of ICON, we were notified very quickly. That helped us. It saved us from an incident."

A Cut Above the Rest

When asked for a bottom line about Rapid7, Zook barely hesitated to offer a strong endorsement.. "It's such a good platform. It's just one pane of glass. That is the most critical part about all this – you log into one website, one interface, and you see it all. You have access to all the integrations, your tools, and everything else; it's just impressive. And Rapid7 is constantly evolving and improving, which helps them stand out above other similar vendors."



Within just minutes, we're able to get the user's account shut down with password reset and then start the investigation. There was no compromise. It was remediated within ten minutes.

Dusty Zook, Security Team, Acme Brick



About Rapid7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open source communities and cutting-edge research—using these insights to optimize our products and arm the global security community with the latest in attacker methodology. Trusted by more than 11,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.



RAPID7

PRODUCTS

Cloud Security

XDR & SIEM

Threat Intelligence

Vulnerability Risk Management

Application Security

Orchestration & Automation

Managed Services

CUSTOMER SUPPORT

Call +1.866.380.8113

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