RAPID7

CUSTOMER STORY

Industry
Manufacturing

Region
Americas

Company Size
Large Market

Products
InsightIDR,
InsightVM, and
InsightConnect

BUILDING A FORTRESS: HOW ACME BRICK STRENGTHENS CYBERSECURITY WITH RAPID7

ACME BRICK
brick.com

OVERVIEW

Acme Brick has been laying the foundation for American homes and businesses since 1891. But as their operations grew, so did the complexity of their cybersecurity needs. With just two team members securing 1,200 workstations, servers, and active users, efficiency wasn't just a goal—it was a necessity.

Enter Dusty Zook, Acme Brick's Security Lead. With seven years at the company and two years at the helm of the security team, Zook knows the challenges of safeguarding a lean yet expansive digital ecosystem. "Back when I joined the security team, it was me and the manager. I was the analyst at the time. When he left, I took over and then hired another analyst," he recalls. The team needed a solution that would provide broad visibility, streamline investigations, and offer 24/7 monitoring—without adding complexity. Rapid7 was the answer.

A Growing Security Stack for a Small Team

When Zook first joined Acme Brick in 2016, the security team barely existed. There was just one person responsible for securing the entire company, and the only Rapid7 product in place was Nexpose, now known as InsightVM. As cyber threats grew more sophisticated, it became clear that vulnerability management alone wasn't enough. Over the years, Acme Brick steadily expanded its security stack, adding InsightIDR for detection and response, InsightConnect for automation, and Metasploit for penetration testing.

Managing this growing security footprint with just two team members was daunting. "For a relatively small company, I mean, we have roughly 1,200 workstation servers and about 1,200 actual active users. The two of us, it gets pretty overwhelming at times," says Zook. The need for efficiency became paramount. "Having a tool that makes our life easier was very critical for our day-to-day."

FROM CHAOS TO CLARITY: INSIGHTIDR BRINGS EVERYTHING INTO ONE VIEW

Before Rapid7, Acme Brick relied on IBM's QRadar. But managing it was overwhelming. "I would spend my entire day in that one platform and not look at any other tool because none of our other tools really fed into it," Zook explains. Investigations took too long, alerts were scattered across different platforms, and keeping up with threats felt impossible.

When Rapid7 introduced InsightIDR, it was a game changer. "Being able to log in just to Rapid7 to see all the other security tools that I have, feeding into Rapid7, makes my day-to-day go way faster," says Zook. "My analyst logs into one tool, and if we see an alert, then we can log into the other tools. Otherwise, we don't because there's no need. It's all feeding into you guys, and we're using you as a simple single pane of glass to make our day just go smoother."

> **Being able to log in just to Rapid7 to see all the other security tools that I have, feeding into Rapid7, makes my day-to-day go way faster,"**
>
> Dusty Zook, Acme Brick's Security Lead

InsightVM: Vulnerability Management That Works Smarter, Not Harder

Zook has relied on Rapid7's InsightVM for nearly a decade to identify and prioritize vulnerabilities. "Vulnerability management is a job in and of itself," he notes. "InsightVM helps us understand where our weak points are, what workstations or servers are missing critical patches, and gives us visibility into what's still exposed—like old Java libraries with Log4j vulnerabilities."

What sets InsightVM apart? Integration with InsightIDR. "We could use other vulnerability management tools, but they're not going to integrate the way you guys do."

Speeding Up Response Time with InsightConnect

Acme Brick's small team doesn't have time to waste on manual security tasks. That's why they turned to InsightConnect for automation. "We're using it for a lot of alerting and some vulnerability lookups," Zook explains. "But the fact that you can use it to lock accounts, unlock accounts, and do AD query lookups through Slack or Teams—it just really makes the tool worth having."

That automation has already paid off. Zook recalls a critical moment when Rapid7's tools prevented a security breach in real-time. "We got an alert that a user's account was being accessed from a foreign country where we don't do business. The alert was so critical it was sent to our Slack notifications. Within minutes, we shut down the account, reset the password, and confirmed there was no compromise. How fast does it take for a bad actor to compromise an account? Minutes. This tool let us act just as fast."

> **"But the fact that you can use it to lock accounts, unlock accounts, and do AD query lookups through Slack or Teams—it just really makes the tool worth having."**
>
> Dusty Zook, Acme Brick's Security Lead

One Platform, One Agent, One Solution

Managing multiple tools with a tiny team isn't just frustrating—it's inefficient. That's why the seamless integration of Rapid7's platform stood out. "Not having to install multiple agents for different things makes the platform shine even more," says Zook. "I'm not going back to the infrastructure team saying, 'Hey, I need you to put this agent on, but I also need this one for this tool.' Nope, I just need this one. This gives me everything I need."

Beyond efficiency, the real-time visibility of Rapid7's platform makes security monitoring proactive rather than reactive. "One of the things we look at in our daily checks is where people are logging in from. Seeing that global map on IDR's homepage helps us spot anomalies immediately. If we see a successful login in Brazil, we investigate—because we don't do business outside the U.S."

Advice for Security Teams Looking to Simplify

For teams considering Rapid7, Zook has a simple piece of advice: start with the Insight Agent. "The Insight Agent is absolutely critical. It's lightweight, doesn't interfere, and gives us incredible data. When we moved to IDR, our work was already 90% done because the agent was already in place."

Looking to the future, Zook hopes to see Rapid7 expand its capabilities into operational technology (OT) security. But for now, he's confident that Acme Brick's security posture is stronger than ever. "Rapid7 is the highlight of our security strategy. When I go to my executives and show them our tools, Rapid7 is the name they see the most. And the fact that we haven't had an incident? That tells them it's worth every penny."

RAPID7 IS HERE FOR THAT.

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/trial/insight