SafeBreach

CASE STUDY

Husch Blackwell Quantifies Real Risk & Drives Real Remediation with SafeBreach

Learn how Husch Blackwell's security team discovered the power of the SafeBreach platform to continuously validate the law firm's security controls and optimize its cyber stack.

HUSCH BLACKWELL

Industry Legal

Challenge Loss of trust in endpoint-protection vendor promises with no easy way to independently validate the security controls for their designated EDRs.

Solution Implemented SafeBreach to execute safe, automated attack scenarios to continuously validate efficacy of security controls for endpoint devices.

Results With SafeBreach, Husch Blackwell achieved:

- Comprehensive security-control validation
- Tech-stack optimization to improve cybersecurity ROI
- Improved and more efficient workflows
- Greater peace of mind

“Data leak could be a business disaster for any number of law firms, both from an operational and reputational perspective, and often, companies are just one small executable away from a major incident.”

The Endpoint-Protection Delusion

With 25 offices and more than 1,850 employees across the U.S., Husch Blackwell is a fast-growing, full-service corporate and litigation law practice. Faulkingham joined the firm in 2013 as its dedicated security leader, focusing first on IT-based concerns, but quickly branching out to cover all vulnerable areas across the nationwide organization.

Ian Faulkingham got his start in IT before cybersecurity departments even existed. Today, he is a Certified Information Systems Security Professional (CISSP) with more than 20 years of leadership experience in information technology security, and he proudly serves as Husch Blackwell’s director of information security.

“We had a minor incident walk right past our previous endpoint-protection platform,” said Faulkingham. “I immediately hired an independent expert to run a script matching my endpoint settings to thousands of ransomware variants. Even against known, older threats, our EDR failed miserably. From that point on, I lost all trust in the word of ransomware-protection vendors.”

Faulkingham found himself in the market for a new detection-and-protection system, but first he needed a way to independently verify the capabilities of his short list. He knew this evaluation would require a focused task force and a significant time commitment. He was close to outsourcing the job to a ransomware penetration tester when he discovered a simpler, more streamlined solution in SafeBreach’s industry-pioneering breach and attack simulation (BAS) platform.

“All the old endpoint-protection comparative testing methods have gone out the window,” said Faulkingham. “They’re only testing known signatures—which don’t even matter anymore. There wasn’t an effective way for us to test it for ourselves prior to BAS.”

"It couldn't be simpler to use the tool. We had SafeBreach up and running our first test in minutes, and boom — we could tell instantly if our control was validated."

Continuous Security Validation

SafeBreach quickly verified Faulkingham's assumptions, proving what he had thought to be a top endpoint product had a number of previously undetectable weaknesses. He used SafeBreach to run the same tests across all the security tools he was considering to see how they did on pre-execution detection and understand what they were really stopping—versus just detecting—in order to determine a clear leader.

"SafeBreach was instrumental in helping narrow down our decision and highlight any deficiencies in the products, no matter what a vendor's marketing might have us believe otherwise," said Faulkingham. "We changed our endpoint product based on the data SafeBreach gave us—backed up by our third-party's initial findings—and we used SafeBreach to validate our new solution. The difference since then has been night and day."

But that was just the beginning for Faulkingham. Once he got a taste for what SafeBreach could do, he realized he had the power at his fingertips to validate all of Husch Blackwell's security controls. And not just for ransomware against his endpoint controls—he could now quantifiably measure and validate the risk associated with all his designated security controls, including web, cloud, and email.

> "We're using SafeBreach as our red-team in a box, running simulations, then examining the forensic information the system delivers to see how well our endpoint solutions performed and look for ways to build better detections."
>
> **Ian Faulkingham**
> **Director of Information Security, Husch Blackwell**

Faulkingham and his team have eagerly adopted SafeBreach as a cornerstone of their security program, using the tool to continuously identify gaps, build more effective red- and purple-team exercises, and map their controls to the MITRE ATT&CK framework to help find and fix blindspots.

"Now when my boss asks, 'How safe are we?' SafeBreach gives us a clear answer," said Faulkingham. "We can quickly run the simulation against any new attack, and I can send the clear results—with quantitative data analysis—right to senior management and the executive board to show we've tested against it and we're safe."

"I couldn't imagine running a security program without a BAS tool now. There's too much at stake to count on someone's sales pitch or opinion. I rely on the hard data SafeBreach provides."

Worrying About the Known vs. the Unknown

Faulkingham hadn't heard of the BAS category prior to his SafeBreach experience, but now he considers himself a full convert and advocate for the power of continuous attack simulation.

"Worrying about the unknown is what keeps me up at night," said Faulkingham. "I would obsessively wonder if we were doing enough to protect ourselves, but now I can just go into the SafeBreach platform and three buttons later, even if we didn't do well, at least I know where we have an issue. SafeBreach has given me the peace of mind so I can go to bed and not wonder where we stand against the latest threat that just showed up on the evening news."

SafeBreach has also proven its worth as more than just a platform for Husch Blackwell. Faulkingham has appreciated the continuous engagement he's received from SafeBreach's trusted security experts and researchers tirelessly working on his behalf to provide rapid threat intelligence and verified tactics, techniques, and procedures with actionable attack plans.

"SafeBreach organizes the threat intelligence landscape into nice, neat buckets for us versus us flying by the seat of our pants," said Faulkingham. "The MITRE framework can be pretty intimidating, but SafeBreach helps us figure out where to focus our efforts and how to best operationalize that information."

Next up, Faulkingham's team will work to better operationalize their use of the SafeBreach solution and create repeatable workflows around it to run attacks, visualize data, and keep them pointed in the right direction. It's a tool he sees becoming even more valuable as they're able to leverage even more of its capabilities beyond security control validation.

"The threat landscape never stops changing," said Faulkingham. "So we have to keep up with it and be running tests and improving our defenses all the time. SafeBreach helps us do that, and the proof's in the pudding—we've had zero incidents."