BISHOPFOX

CASE STUDY

SECURING SMART HOME TECHNOLOGY IN DECENTRALIZED GLOBAL ENTERPRISE

CUSTOMER SNAPSHOT

INDUSTRY	Technology – Software & Services
CUSTOMER	Global provider of smart locks, alarms, and connected home devices
SERVICES PROVIDED	Continuous Threat Exposure Management, Application Penetration Testing & Network Penetration Testing

"Cybersecurity is our number one priority. A single breach could damage both our products and our brand."

— VICE PRESIDENT, SMART RESIDENTIAL SOLUTIONS

CUSTOMER OVERVIEW

This Bishop Fox customer designs and delivers smart residential security solutions, including connected locks, alarms, and other digital-first products supported by cloud platforms and mobile applications. With millions of households relying on their products to keep them safe, the stakes were high. The customer turned to Bishop Fox to meet their needs, combining internal accountability with external expertise to strengthen security at scale.

THE CHALLENGE

When a business unit within the customer organization inherited ownership for smart residential security products after restructuring, its team faced steep challenges. Operating in a decentralized IT model, the unit had to quickly adapt to full accountability for its own applications, cloud platforms, and customer-facing services, all without a dedicated cybersecurity function.

SECURITY CHALLENGES

- Full responsibility for cybersecurity without in-house expertise
- Decentralized accountability across regions, each with unique compliance obligations
- Pressure to meet stringent data protection and resilience requirements
- Resource constraints that limit the ability to manage noisy alerts or conduct continuous testing

The team approached these challenges with urgency and seriousness, elevating cybersecurity to a top business priority.

THE SOLUTION

Having previous experience with Bishop Fox's offensive security services through its North American counterparts, the business unit valued a proactive approach to cybersecurity and continued the partnership when it assumed full responsibility for its smart residential security products.

Bishop Fox engaged in collaborative scoping sessions to understand the organization's products, priorities, and threat exposure. Together, they agreed on a two-pronged approach:

- **Continuous threat exposure management** to identify and validate exposures and emerging threats in real time, so internal teams can fix prioritized issues before they're exploited.
- **Targeted penetration testing** of mobile applications, web applications, and internal networks to provide deeper visibility, validate remediation efforts, and strengthen security processes.

From the start, Bishop Fox stood out for its professionalism, technical expertise, and consultative approach, and the customer matched that with a high level of engagement. Their team leaned into scoping discussions, prioritized high-risk systems, and committed to address findings quickly, making the collaboration highly effective.

"With Bishop Fox's attack surface management service, we know every alert is real. That saves us countless hours and ensures our small team focuses only on what matters."

— **VICE PRESIDENT, SMART RESIDENTIAL SOLUTIONS**

THE OUTCOME

The engagement delivered tangible improvements and lasting confidence in the customer's ability to protect its smart residential platforms.

KEY RESULTS

- **Critical risks surfaced and resolved** – Penetration testing identified systemic weaknesses that could have led to significant access or data exposure. Bishop Fox guided remediation and validation, while the customer acted quickly to resolve issues, driving architectural and process changes that strengthened their overall posture.
- **Continuous coverage** – Bishop Fox ran millions of tests each month across the customer's environment, covering hundreds of discovered services. Every finding was validated by Bishop Fox experts, ensuring the lean team focused only on real issues, not noise.
- **Emerging threat monitoring** – Bishop Fox actively monitored the threat landscape for new vulnerabilities, exposures, and TTPs, alerting the customer if they were at risk or in the clear.
- **Stable and secure attack surface** – Quarterly reviews confirmed no high-risk exposures, strong DNS hygiene, and seamless migration to the latest AWS connectors, reinforcing confidence that the business unit was operating with a strong baseline of security.
- **Executive validation** – Bishop Fox's clear, detailed reports not only guided immediate fixes but also impressed group-level security leaders across the parent company, helping the business unit demonstrate progress and accountability.

"Our network test uncovered issues that were honestly scary. Fixing them changed how we manage our infrastructure."

— **VICE PRESIDENT, SMART RESIDENTIAL SOLUTIONS**

CONCLUSION

This organization's experience shows what's possible when customer ownership and expert partnership align. Bishop Fox provided the expertise, scale, and validation to uncover risks and strengthen defenses, while the customer brought urgency, accountability, and fast remediation to the table.

The results spoke for themselves: critical issues addressed, operations streamlined, and validation from senior leadership across the parent company. Most importantly, the customer demonstrated that security isn't just an external service, it's a shared responsibility that, when embraced fully, protects the millions of households that rely on their products every day.

Looking ahead, the business unit is building on this foundation by exploring advanced testing and adversarial simulations and continuing its partnership with Bishop Fox to evolve alongside an ever-changing threat landscape.

OUTPACE MODERN ADVERSARIES.

STOP CHASING ALERTS. START MANAGING RISK.

External attack surfaces are constantly expanding and becoming harder to manage, as cloud services, SaaS adoption, remote work, and third-party integrations expose assets far beyond the firewall. These internet-facing systems are what attackers see first, making them prime targets for exploitation. The challenge goes beyond visibility – it's knowing exactly where your attack surface is exposed, which exposures truly pose a threat, which have the highest potential business impact, and how to prioritize them in a way that drives timely, effective action.

Adopting a Continuous Threat Exposure Management (CTEM) program addresses these challenges by combining continuous discovery, business-aligned prioritization, real-world validation, and coordinated action across security and non-security teams. This enables you to focus on the exposures that matter most and fix them faster.

Bishop Fox's managed services give you the continuous visibility, expert validation, and real-time threat intelligence needed to run an effective CTEM program across your external attack surface—without building a massive program in-house. We help you identify, prioritize, and remediate business-impacting exposures so you can strengthen resilience and stay ahead of attackers.

ABOUT BISHOP FOX

Bishop Fox is the leading authority in offensive security, providing solutions ranging from continuous penetration testing, red teaming, and attack surface management to hardware, cloud, application, and AI/LLM security assessments. As a trusted partner to the world's most recognizable brands, Bishop Fox protects 25% of the Fortune 100, eight of the top 10 global tech companies, all of the top five global media companies, 50% of the top 20 retailers, and seven of the top 10 manufacturers.

LEARN MORE AT BISHOPFOX.COM