CASE STUDY

ULTRARED

HOW LEAF HOME GAINED AN ATTACKER'S VIEW OF ITS EXTERNAL ATTACK SURFACE

How North America's Largest Home Improvement Company Validates External Risk with ULTRA RED

LeafHome

Customer Profile

Founded: 2005
Head Office: Ohio, US
Annual Revenue: $2.5 billion
Workforce: 10,000
Locations: 290+ offices
Customers Served: 2+ million
Industry: Home Improvement & Home Services
Website: www.leafhome.com

Background

Leaf Home is the world's largest direct-to-consumer home improvement company, serving more than 2 million homeowners across the U.S. and Canada. The company delivers end-to-end home solutions, including gutter protection, water filtration, accessibility, bath, and home enhancement services, through a nationwide network of in-house teams.

As Leaf Home scaled rapidly through organic growth and frequent acquisitions, its digital footprint expanded just as quickly. With hundreds of locations, thousands of employees, and a constantly evolving external presence, maintaining confidence in what was exposed to the internet became a critical security priority.

KEY BENEFITS

- True External Attack Surface Visibility
- Trustworthy, Validated Findings
- Zero Setup and Operational Efficiency
- Security Team Force Multiplier
- M&A Security Acceleration

Key Challenges: Security at the Pace of Growth

As Leaf Home expanded, its external attack surface grew broader, deeper, and harder to track. New brands, new applications, and new acquisitions meant that assets were constantly being introduced - sometimes faster than security teams could fully account for them.

Traditional security approaches, such as annual penetration tests and point-in-time vulnerability scans, provided value but relied heavily on known assets and predefined scope. Anything unknown, forgotten, or inherited through acquisition could easily remain invisible.

For a small cybersecurity team supporting a large, distributed enterprise, this created a fundamental challenge: how to continuously understand what attackers could see - and confidently prioritize what actually posed risk.

- **Blind Spots in External Visibility**
- **A Growing Attack Surface**
- **Inherited Risk from Acquisitions**
- **Limited Security Resources**

> **Your tooling is only as good as what you can actually see. If something exists outside of that view, it might as well not exist to your security program but attackers will still be able to see it."**
>
> *Todd Eldredge, Head of Cybersecurity, IAM & GRC*

The Goal: A True Attacker's View

Leaf Home's security team set out to answer a deceptively simple question:

"What does our organization look like from the outside?"

To do that, they needed to move beyond point-in-time assessments and gain:

- Continuous visibility into all external assets, including unknown or forgotten ones
- Clear identification of real, exploitable exposures, not theoretical findings
- Confidence in findings without spending time on manual validation
- A scalable way to evaluate inherited risk during M&A activity

Why ULTRA RED

Leaf Home already had digital risk and monitoring tools in place, but those tools depended heavily on manually fed data – domains and assets the team already knew about. ULTRA RED offered a fundamentally different approach.

TRADITIONAL TOOLS	ULTRA RED
○ Rely on manual data feeds	☑ Autonomous discovery beyond known assets
○ Point-in-time assessments	☑ Continuous, automated monitoring
○ High false positive rates	☑ Fully validated, verified findings
○ Requires constant maintenance	☑ Set-it-and-forget-it operation
○ Limited depth	☑ Deep connection mapping and analysis

By autonomously discovering the external attack surface and validating exposures under real-world conditions, ULTRA RED revealed risks that other tools couldn't see and removed the burden of manual verification.

> **"We already had a digital risk platform, but those tools only work with the data you give them. With ULTRA RED, we provided some initial domains and then it went out and found far more than we expected. That was eye-opening."**

Just as important, the platform was fast to deploy and low-touch to operate, making it a practical fit for a lean security team managing a large environment.

First Results: Critical Vulnerability in an Internal App

ULTRA RED was deployed as part of a proof of value (POV), and results appeared within days.
Early on, ULTRA RED identified a significant vulnerability in an internally developed application, an exposure other tools had missed entirely. The finding wasn't just flagged; it was fully validated, complete with technical evidence and remediation context.

> **"ULTRA RED didn't just send us alerts and ask us to investigate. They handed us verified, actionable findings with evidence, ready to give straight to our web development team. Our involvement was minimal."**

At the same time, ULTRA RED uncovered unknown external websites and suspicious redirects associated with the organization – assets that no one internally recognized or could explain. "That's exactly the kind of thing we need to see because if we don't see it, we can't act on it."

Impact

By delivering validated findings, ULTRA RED fundamentally changed how the Leaf Home security team operated.

Instead of spending time validating alerts, re-testing vulnerabilities, or debating false positives, the team could move directly to remediation and risk reduction.

> **“ULTRA RED acts as a force multiplier for our team. We don’t have to validate, double-check, or chase false alerts. Everything is fully vetted out, which is huge for a small team supporting a growing organization.”**

Results at a Glance

- **Critical exposure identified within days of deployment**
- **Zero manual validation required**
- **Previously unknown external asset discovered and remediated**
- **Faster remediation with higher confidence**
- **Significant reduction in alert fatigue and noise**

Looking Ahead

Leaf Home is now fully onboarding ULTRA RED across its environment, with plans to expand usage across brands and future acquisitions.

> **“We already see a lot of value and clearly understand the vision. As we continue to scale, having validated visibility into our external risk is only going to become more important.”**

ULTRA RED will continue to support:

- Continuous external exposure monitoring
- Ongoing M&A security assessments
- Integration of validated findings into existing security workflows

> **“I have a small team and a very large attack surface. We don’t have time to validate every alert manually. Being able to trust the data and immediately act on it saves enormous time and effort and removes a massive burden from our workload.”**

About ULTRA RED

ULTRA RED is a pioneer and leading provider of Continuous Threat Exposure Management (CTEM) solutions, built on a validation-first approach. Our CTEM platform helps security teams confidently reduce threat exposure by continuously identifying, validating, and prioritizing gaps across the entire attack surface. Learn more at www.ultrared.ai.