CASE STUDY

ULTRARED

HOW HALOCK DELIVERS TRUSTED SECURITY OUTCOMES WITH ULTRA RED

HALOCK®

Head Office: Schaumburg, Illinois, USA
Founded: 2001
Industry: Cybersecurity Consulting & Professional Services
Website: www.halock.com

Background

HALOCK is a leading cybersecurity consulting firm based in Illinois, US specializing in human-led offensive security, risk management, compliance, and security engineering services.

As client environments expanded across cloud, shadow IT, and AI-powered services and APIs, traditional point-in-time testing alone could not maintain visibility between engagements. Clients needed continuous awareness of changes to their external attack surface, paired with expert guidance on exploitation techniques and accelerated remediation strategies.

To meet this need, HALOCK looked for a technology partner that could deliver accurate EASM and CTEM that strengthened and extended offensive security programs, with minimal false positives and defensible evidence of real risk for penetration testers and security leaders alike.

Customer Challenges

As HALOCK's clients faced growing cyber risk from evolving threats and expanding digital ecosystems, several key challenges emerged:

Limited visibility across complex environments

Clients struggled to maintain an accurate inventory of all internet-facing assets, including cloud resources, forgotten subdomains, M&A assets, and shadow IT introduced by business units — often outside the scope of scheduled testing windows.

Difficulty prioritizing remediation

Without proof of exploitability, clients' security teams couldn't confidently determine which vulnerabilities posed actual risk versus theoretical concerns, leading to decision paralysis and inefficient resource allocation.

Alert fatigue from false positives

Traditional vulnerability scanners generated overwhelming volumes of findings, many of which were false positives or unexploitable in real-world scenarios. This eroded trust and distracted teams from meaningful remediation and deeper testing.

Need for continuous monitoring between assessments

Point-in-time assessments provided only a snapshot view. As attack surfaces changed daily, clients needed ongoing monitoring to inform and guide future penetration testing and validation efforts.

The HALOCK Approach: Why ULTRA RED

After evaluating multiple external attack surface management solutions, HALOCK selected ULTRA RED for its validation-first approach and exceptional accuracy. Unlike traditional tools that rely solely on CVE scores or software version detection, ULTRA RED focuses on actual attack vectors — providing evidence that HALOCK's offensive security consultants can trust, review, and expand upon.

ULTRA RED was selected not as a replacement for penetration testing, but as a force multiplier that accelerates time-to-remediation and enhances offensive security outcomes through continuous discovery and automated validation.

Key Selection Criteria:

Exceptional detection accuracy

ULTRA RED uncovers real, exploitable weaknesses others miss, including complex application-layer issues and misconfigurations — helping HALOCK testers focus where it matters most.

Automated, real-world validation

Every exposure is tested and proven exploitable — giving Halock consultants verified attack vectors they can immediately use for targeted and accelerated remediation.

<1 false positives

Security teams and consultants avoid noise and focus only on issues that truly matter.

Actionable proof for remediation

Detailed PoCs with request/response evidence support tester findings and eliminate debate during remediation discussions.

Faster outcomes, less noise

Customers see a 75–90% reduction in alerts and resolve issues 2–3× faster, allowing teams to spend more time on advanced testing and strategic improvements.

Continuous, agentless visibility

Real-time insight into the evolving attack surface, enhancing penetration test scoping and reducing blind spots between engagements, with no deployment or whitelisting required.

> **ULTRA RED's validation-first approach was a game-changer for our clients. Instead of overwhelming security teams with thousands of theoretical vulnerabilities, we deliver a focused list of exposures attackers can actually exploit — enabling our consultants to immediately focus on sophisticated exploitation techniques and fast-track remediation with precise, expert guidance."**
>
> ***Terry Kurzynski, HALOCK Founder and Partner.***

Implementation & Results

Delivering Continuous Value to Clients

HALOCK integrated ULTRA RED into its External Attack Surface Management (EASM) service offering, alongside penetration testing and offensive security services, delivering both baseline assessments and ongoing managed services to clients across industries.

Discovery & Asset Management

ULTRA RED continuously discovers all internet-facing assets, including cloud storage, admin portals, development environments, and forgotten subdomains — ensuring HALOCK's offensive teams are testing the full, current attack surface.

Validated Risk Prioritization

Rather than generating lengthy lists of CVEs, ULTRA RED validates which vulnerabilities are actually exploitable. This enables HALOCK consultants to provide targeted offensive guidance and remediation strategies based on real business risk, not theoretical scores.

Executive Reporting & Compliance

HALOCK translates ULTRA RED findings into executive-ready reports that align technical vulnerabilities with business impact, reinforcing the value of expert interpretation and strategic guidance, and demonstrating continuous monitoring to auditors.

Early Success: Uncovering Hidden Exposures

In one engagement, ULTRA RED flagged an exposed internal subdomain for a client that had been overlooked by existing scanning tools. The vulnerability was in an exploitable state, representing a critical entry point for attackers. HALOCK's team immediately assessed the exposure, provided offensive guidance on potential attack scenarios, and worked with the client's security team to remediate the issue within hours — preventing a potential breach.

This incident demonstrated how continuous discovery paired with specialist remediation guidance accelerates response from days to hours.

> **ULTRA RED didn't just surface an issue — it provided verified evidence our team leveraged to immediately guide remediation. That certainty allowed our clients to act with urgency and confidence."**
>
> ***Terry Kurzynski, HALOCK Founder and Partner.***

Looking Ahead: Expanding EASM Services

HALOCK continues to expand its EASM service offerings powered by ULTRA RED, integrated tightly with offensive security and penetration testing programs, providing flexible engagement options to meet diverse client needs:

- Baseline assessments for one-time discovery and prioritization
- Continuous managed services to support ongoing monitoring between penetration tests
- Scalable resale options for clients who want direct access to the platform with HALOCK expertise available as needed

> **As our clients' attack surfaces grow more complex, HALOCK focuses on what matters most: evidence-based security outcomes teams can trust. By combining continuous validation with offensive testing expertise and guidance, we help organizations stay ahead of attackers and reduce real risk."**
>
> ***Terry Kurzynski, HALOCK Founder and Partner.***

HALOCK®

About HALOCK

HALOCK is a leading cybersecurity consulting firm providing human-led offensive security, risk management, compliance, and security engineering services. With deep expertise across regulated industries, HALOCK helps organizations reduce cyber risk through evidence-based assessments and strategic guidance. Learn more at www.halock.com.

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.