VERIFIED THREAT

Customer Case Study

Case Study September 2025

SaaS / Technology Consulting / 50-100 Employees | Location: UK

SaaS Technology Consulting Client.

This SaaS technology Consulting client develops and delivers SaaS platforms to global customers and the channel. With sensitive commercial data at the heart of its business model, maintaining a strong and provable security posture is essential to protect clients, compliance requirements, and preserve brand trust.

In particular, as more of its partners were auditing 3rd party supplier risk, it needed to have demonstrable proof that the company was proactively guarding against future threats and weaknesses to protect the customer's sensitive data.

The company had invested in skilled internal IT security staff and engaged third-party penetration testers on a regular basis. However, the Senior Leadership Team (SLT) remained concerned about blind spots and the limitations of a cycle-based testing approach. Penetration tests were costly, infrequent, and by design limited in scope. The business sought a faster, more cost-efficient, and continuous method of validating its external security posture to give the SLT and customers the confidence needed.

Challenges

- **Blind Spots**: Internal audits and pen tests left uncertainty around unmanaged domains, legacy systems, API microservices, and shadow IT.

- **High Cost**: Traditional third-party penetration testing consumed tens of thousands of pounds annually.
- **Limited Frequency**: Security validation was point-in-time rather than continuous.
- **False Positives**: Although the vulnerability reports were comprehensive, they also delivered many potential vulnerabilities that needed investigation, which sucked time from the security leadership team. Many of these 'vulnerabilities' when investigated, proved to be false positives, erroneous or were not high impact.
- **Board Assurance:** Leadership requires a clear and independent view to report confidently on risk exposure, as it seeks additional investment.

Deployment and Approach

Rapid Setup: The system was live and delivering results very quickly, requiring minimal internal resources and training.

Comprehensive Coverage:

Verified Threat scanned across domains, IPs, cloud assets,& API's surfacing exposures not previously identified.

Actionable Reporting:

Delivered technical detail for engineers, but also clear executive summaries that were aligned to business impact.

Prioritisation:

Risks were ranked by exploitability and relevance, enabling the security team to focus on what mattered most.

Zero False Alerts

Every alert was verified with evidence. A full vulnerability exposure and log details are available to deep dive.

Always on Coverage

24/7 Red Team virtual monitoring at enterprise scale ensures continual assessment is active constantly.

Realtime AI Remediation

VerifiedThreat layers across existing defence setups, scales out autonomously and combines verified vulnerability testing with instant AI remediation.

Security Standards

Support for ISO 270001, SOC 2 & NIST Frameworks takes the pain out of manually recording incident and logging risk data, and automatically maps to each relevant control.

Attack Vector Chaining

Attackers can exploit weakly segmented domains to move laterally and escalate privileges. VerifiedThreat stops the attacks at the reconnaissance stage - before they can cause damage. This dramatically reduces the reconnaissance stage attacks by 70-90% and prevents more serious attack escalation in the future based on exploiting the weak defences.

Benefits

Typically customers see an immediate decrease in reconnaissance activity which leads to 30-40% decrease in unexpected server maintenance and overhead. Benefits can be measured by setting up custom tags for each major risk area, department or risk owner, and can be reported on an enterprise-wide basis to give complete 360° visibility.

Why Verified Threat?

The company selected Verified Threat to provide an **outside-in, attacker-perspective assessment** of its digital footprint. The platform's approach was attractive because it required no heavy internal deployment, delivered verified results quickly, and provided a continuous line of sight into the actual business areas with the sensitive data. This helped us to focus on the core risk areas for the business, concentrating on our sensitive partner data, and align our security testing with our business needs for maximum, continuous security.

Results

- **Previously Unseen Risks Identified**: Legacy system exposures and misconfigurations missed by pen testers were uncovered in a range of API services that hosted sensitive client data.
- **Significant Cost Savings:** VerifiedThreat picked up a large volume of significant data mining of our APIs, which resulted in a £200,000 annual saving on data hosting, CPU and data costs from our partners.
- **Improved Confidence:** Board and leadership gained an independent, transparent view of the organisation's external posture.
- **Operational Efficiency**: Internal security staff shifted effort from discovery to remediation and strategic improvement. The threat intelligence provided the team with actual proven vulnerabilities which they could then look to harden, re-test and benefit from the continuous improvement cycle.
- **Scalable Assurance:** The model can be repeated easily as the business grows, providing ongoing resilience.

Impact

By using Verified Threat, the organisation achieved both technical depth and business value:

- **Technical**: Continuous visibility, faster identification of real-world vulnerabilities, and structured prioritisation for remediation.
- **Business:** Reduced costs, better use of resources across the new cloud microservices and legacy infrastructure, and stronger assurance to clients and the board.

> ***"Verified Threat uncovered risks and hidden data mining abuse that neither our internal team nor external auditors had identified. It gave us speed, clarity, and more than paid for itself by reducing operating costs, as well as providing ongoing threat testing against our core impact areas, and the board now has greater confidence in our security posture."***

SaaS Consultancy Board Member

Please reach out to our sales team and book in a demo to see the platform in action.

www.verifiedthreat.com