VERIFIED THREAT

Data Sheet 2025

Benefits Summary (SCCA)

Zero False Alerts – Every alert is verified with evidence, for Zero Trust at the Network Edge

Zero False Alerts

Every alert is verified with evidence. We provide a full vulnerability exposure and detail the risks in a full log.

Always on Coverage

24/7 Red Team virtual monitoring at enterprise scale ensures continual assessment is active throughout the entire organisation.

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.

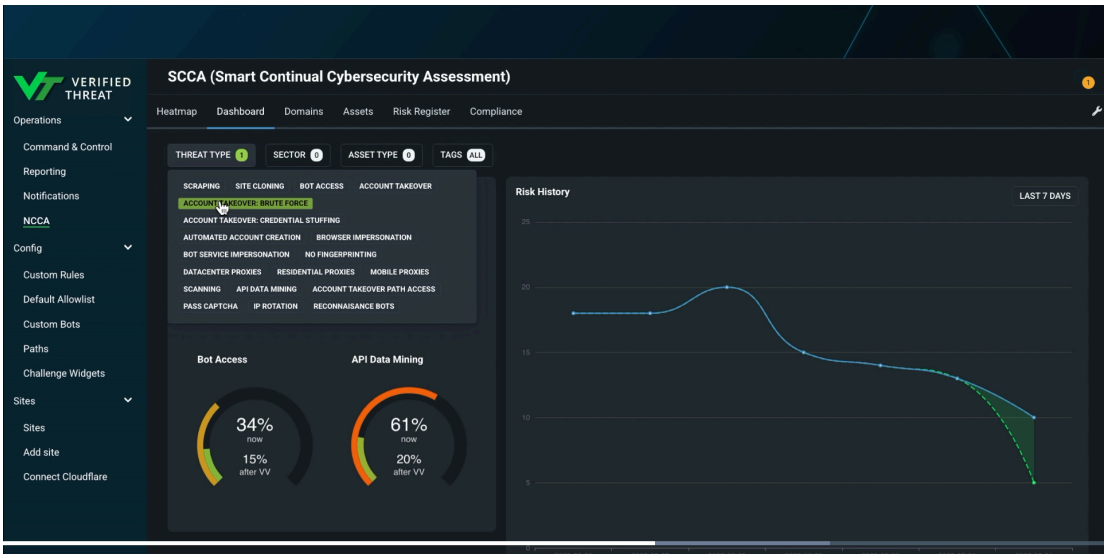
www.verifiedthreat.com/

Continual AI-Driven Red Teaming & Vulnerability Scanning

VerifiedThreat continually scans your entire digital footprint to uncover vulnerabilities and validate real risks with evidential proof.

Our scalable AI agents adapt their attack vectors—just like real adversaries—to confirm weaknesses with clear context. This eliminates wasted time on false alerts or theoretical issues. Instead, leadership and security teams see the highest risks across the estate, prioritized and proven.

Persistent Monitoring & Assessment



VerifiedThreat tracks the entire risk surface across all assets in real time. This allows organizations to:

- Align policy decisions with **verified threats**.
- Detect common misconfigurations (e.g., disabled firewalls, incorrect WAF settings).
- Replace periodic, one-off pen tests with **continuous validation**.

No security platform is stronger than its weakest link. VerifiedThreat ensures weaknesses are exposed and resolved continuously—not just once a year.

Zero Trust at the Network Edge

By focusing on **Outside-In threats**, VerifiedThreat blocks attackers at the reconnaissance stage—long before they escalate. Bots and automated AI tools that scan for weaknesses are neutralized, preventing follow-up attacks.

Stopping reconnaissance typically reduces attack attempts by **70–90%**, saving time, money, and resources.

Attack Vector Chaining

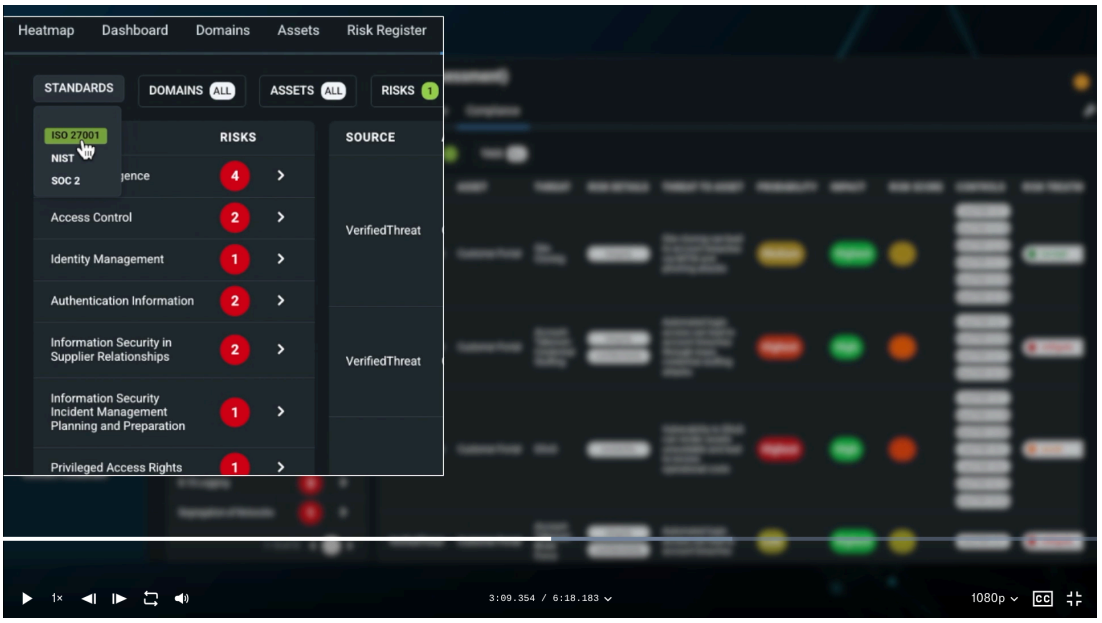
Attackers can exploit weakly segmented domains to move laterally and escalate privileges. VerifiedThreat stops the attacks at the reconnaissance stage - before they can cause damage. This dramatically reduces the reconnaissance stage attacks by 70-90% and prevents more serious attack escalation in the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

Risk Insights

Track risk with non stop AI analytics. Get real-time insights to optimize threat reduction, spot the weakest links and improve your overall security governance with clear and demonstrable risk data that is 100% verified and customized to your own internal security KPIs or OKRs.

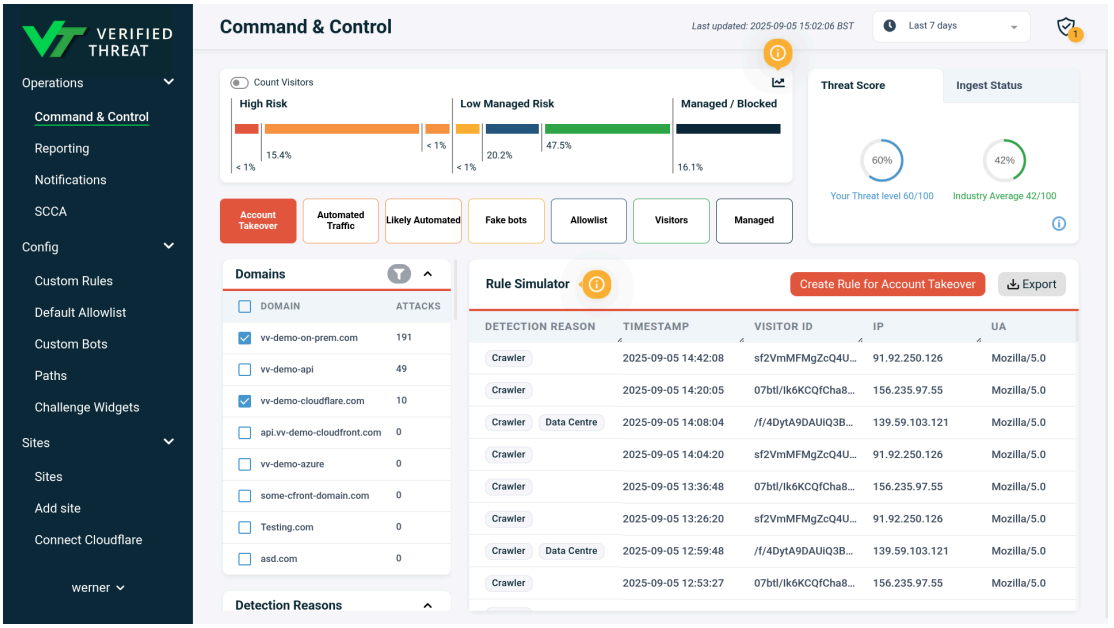
Benefits

Typically our 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.



Most attackers begin with reconnaissance, often using automated bots to scan for vulnerabilities before handing findings to specialists for exploitation. VerifiedThreat stops this process at the source—blocking reconnaissance activity and preventing attackers from ever reaching the scoping stage.

By cutting reconnaissance attempts, organizations experience far fewer follow-up attacks, reduced server maintenance, and freedom from the constant need to check logs or rewrite WAF rules as threats evolve. Better still, many of these threats can be **auto-remediated**, saving teams valuable time and resources.



Protect your enterprise with verified, continual cybersecurity assessment.
📅 Book a demo today: www.verifiedthreat.com