

Aikido Attack: Deployment Benchmark

One autonomous methodology. Two deployment options. Both outperform a senior human pentester.

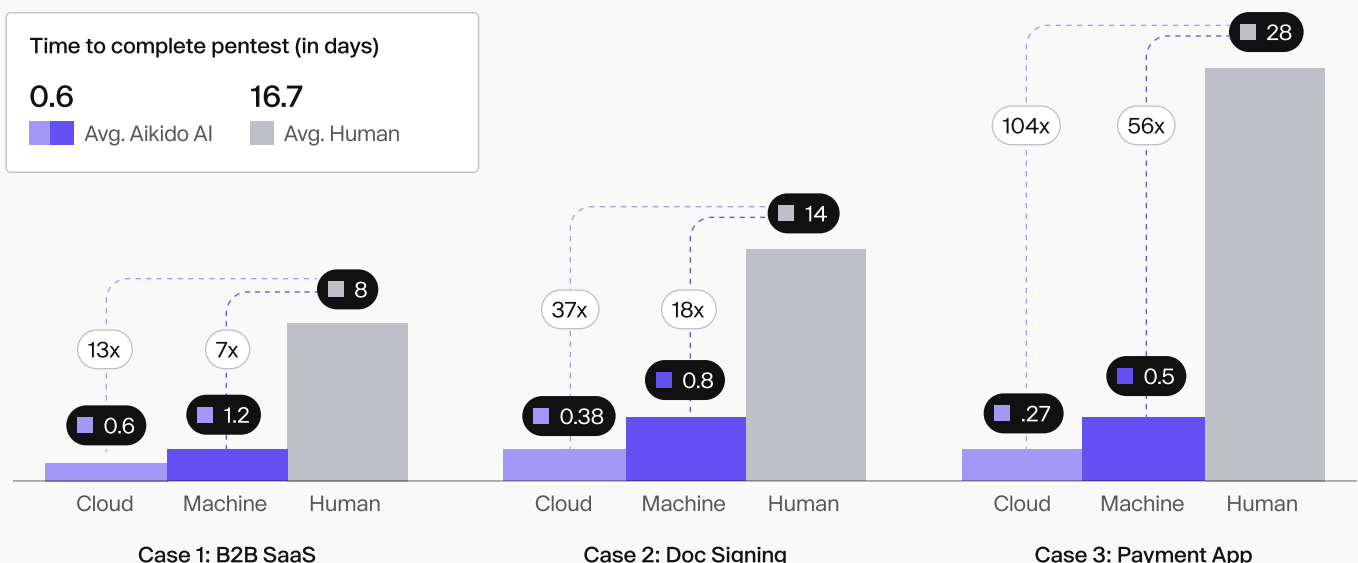
Traditional pentests arrive long after code is in production and quickly go stale. You wait 2 to 4 weeks for a senior tester to hand over a PDF. By the time you've read it, code has shipped twice. Aikido Attack replaces that cadence with an autonomous engine that runs in hours and re-runs on every release.

AI Cloud is the managed service. Aikido Machine is a self-contained on-prem server with dedicated GPU and local inference, for teams whose source code and findings cannot leave their network. Both were run against the same three production applications, head-to-head with a senior human pentester.

Speed Advantage

Autonomous: Completed test in hours (approx. 6.5 to 14.5 hours)

Manual: Took weeks (up to 4 weeks) for testing and reporting

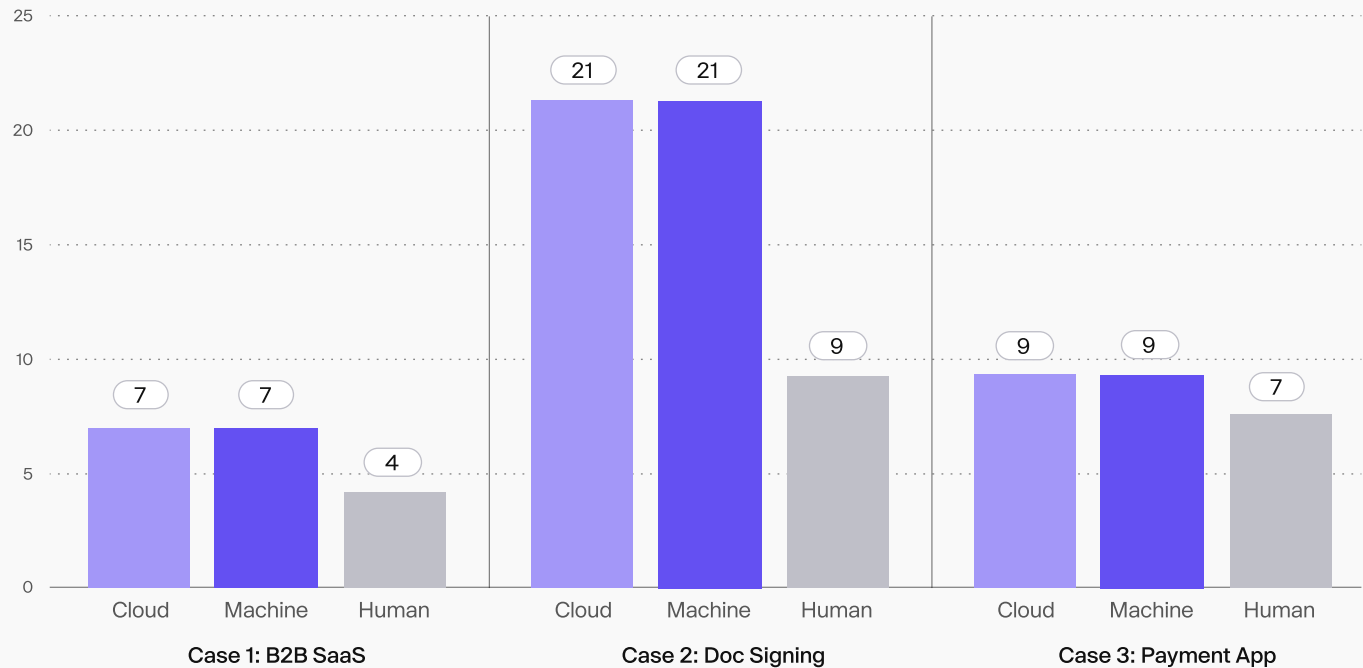


Depth vs Compliance

AI strengths: Found deep logic flaws like IDORs, Authentication bypasses, and e-signature forgery that humans missed

Human strengths: Focused heavily on compliance, configuration hardening, and general security hygiene

Number of findings per case



Takeaways



Speed

Cloud and Aikido Machine finish in hours. A manual engagement takes two to four weeks and runs once or twice a year.



Volume

Cloud and Aikido Machine surface the same amount of findings. Manual trails behind both.



Severity

Aikido Machine and Cloud identified the same Critical and High findings.

The bottom line

Cloud is faster than Aikido Machine, which trades off some performance for an air-gapped setup so code and findings never leave your premises. Either way, you're significantly ahead of manual pentests.

Deployment

Aikido Machine is a single rack-mounted hardware appliance with dedicated GPU compute. The model runs locally. Source code, pentest results, and prompts never leave your network. No runtime callback to Aikido. Fully air-gap capable.

Zero data egress. Dedicated GPU compute. Local model inference.

The Verdict

AI Cloud

The most capable pentest we ship. Highest finding volume in every case, fastest time to result, and more deep logic flaws than a senior human found.

→ ***Run Cloud when source code has no residency constraint.***

AI Machine

The same autonomous methodology, inside your network. Total issue and High/Critical issue parity with Cloud and zero data egress.

→ ***Run Aikido Machine when source code can't leave your environment.***

Conclusion

Autonomous pentesting now finds more issues and faster than the senior humans it is measured against. With local inference on dedicated GPUs, it does so without your code and findings leaving the premises. Manual pentesting is no longer the benchmark, rather it's the floor.

Sources: Cloud and Human figures: Aikido Q4 2025 "Autonomous vs. Manual Pentesting" whitepaper, measured. AI Machine figures: Aikido internal benchmarking, estimated (~100% of Cloud finding volume; 100% Critical/High retention).