Test Your Real Systems. Break Nothing.

A plain guide to security testing for IT leaders who have never run one.

What security testing is, what it produces, and why testing a copy beats testing the real thing.

Rediacc | 2026

What a pentest is, and why it costs $4.88 million if you skip it

A pentest is when security professionals try to hack into your systems on purpose to find weaknesses. The goal is to find the holes before a real attacker does.

The average data breach now costs $4.88 million worldwide (IBM 2024). In the United States it is $10.22 million; healthcare runs $9.77 million per incident.

Slow detection makes it worse. Breaches that take more than 200 days to spot cost $1.26 million more than ones caught sooner (IBM 2024). Only 12% of hit companies fully recover.

Companies that test often find and fix problems early. **Structured testing cuts critical weaknesses by over 60% in the first year** (SANS). Fixing one weakness before a breach costs 30 to 100 times less than fixing it after.

Yet **43% of companies run only 1 or 2 pentests a year** (Core Security). That gives them about 14 days of security visibility out of 365.

> Ask your IT team: when was our last pentest, and what did it find?

"AI pentesting" is the board buzzword. Here is what it actually means.

AI red teaming is using AI software to run hacking attempts on your own systems. A human pentester tries 50 to 100 attack moves over a week. An AI tool can try thousands in an hour. What changes is the speed and breadth of testing, not the kind of attacks.

In a recent survey, **97% of companies said they would consider AI pentesting** (Aikido 2026). 90% think AI will take over pentesting one day.

Gartner has flagged real problems with these tools. They make stuff up. They cannot judge business risk. When one breaks your live system, nobody knows who is on the hook.

The catch: AI tools that test fast also break things fast if given full access. That is why most are sold with strict approval gates. A cautious test misses what an attacker would not miss.

> Ask your IT team: if we used an AI pentester, would we let it run on our live systems or somewhere safer?

The trap: test the real thing and risk an outage, or test a fake and miss the real holes

Every security testing tool forces the same choice.

Option A: test your actual live systems. Most accurate but risky. Tools that hack your real systems can cause outages, expose customer data, and trigger your firewall in ways nobody planned.

Option B: test a model or a copy. Safer but less accurate. Over 40% of companies say their pentest results are already out of date the day they get them (Horizon3.ai). Their systems change faster than the test finishes.

The two leading tools sit on opposite ends. One runs real attacks on your live systems and promises to play nice. The other builds a math model and never actually attacks anything. Either way, it can guess wrong.

Neither solves the trap. You either accept risk or accept blind spots. **And none of the tools on the market today test your real systems against real attacks.**

> Ask your IT team: which option are we picking today, and what are we missing because of it?

Most breaches start with a setting that is wrong

A setting that is wrong is **the #1 cloud security threat** in the Cloud Security Alliance 2024 report. It beats out brand-new, never-seen-before attacks (what the industry calls zero-day).

15% of all data breaches start with a wrong setting (IBM 2024). 23% of cloud incidents come from these settings (SentinelOne). 82% are caused by humans, not bugs. Azure storage accounts show a 60.75% rate across 504,421 checks (Trend Micro), and these attacks rose 47% year over year in 2024.

AT&T paid $1.2 billion in reserves because one misconfigured storage bucket exposed 110 million customer records. The bucket was a setting wrong, not a hack.

Test systems do not catch this either. New Relic's test side was breached in November 2023 because it had weaker security than the real side.

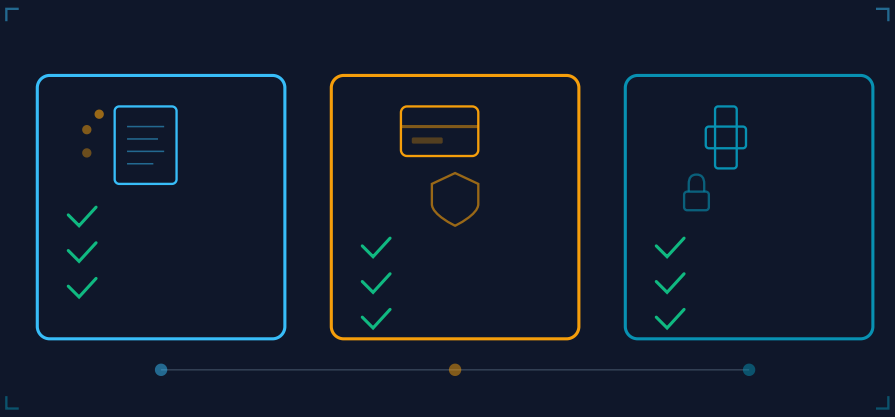
Harness, an industry tool maker, put it well.

> "The more your test environment differs from real life, the less you can trust the test."

Like fire-drilling in a model house. The real fire is in the actual building, with different exits and blocked hallways.

> Ask your IT team: how close is our test environment to our real one?

The rules are changing. You will be required to test.



If you handle EU customer data, take card payments, or process health data, two or three of these touch you. Most mid-market companies hit at least one.

The EU's DORA rule, in force January 17, 2025, makes financial firms prove they can recover from cyberattacks. It covers **22,000+ EU financial firms**. It requires advanced testing every three years. Fines reach 1% of daily worldwide revenue for up to six months.

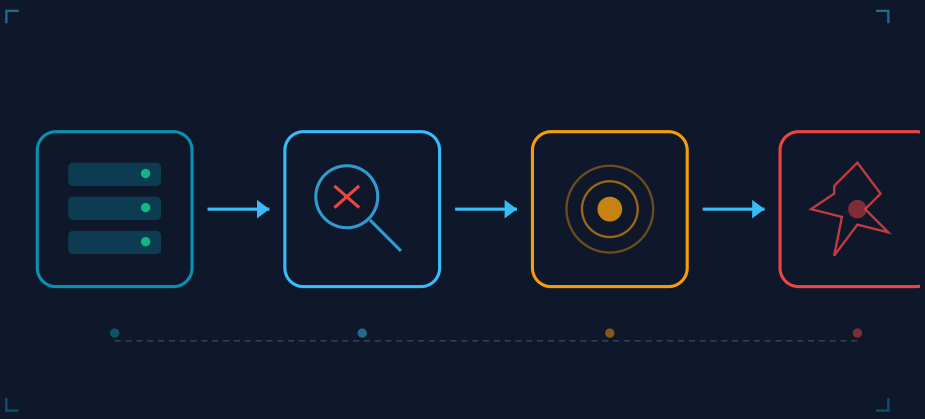
The payment-card rule (PCI DSS 4.0), mandatory March 31, 2025, sets four hard requirements. Yearly pentests. Scans every three months. A fresh test after any big change. Penalties run $5,000 to $100,000 per month. **Only 14.3% of companies were fully compliant in 2023**, down from 43.4% in 2020 (Verizon 2024).

The proposed 2025 HIPAA update would require yearly pentests for the first time. Fines run $100 to $2 million a year, with up to 10 years in prison for willful neglect.

The audit bar is rising on top of the rules. **34% of companies lost business for missing a security certification** (A-Lign 2024). 91% plan constant checking, not once-a-year audits (Drata). A once-a-year pentest cannot prove your security worked last Tuesday. Auditors want weekly proof, dated and stamped.

> Ask your compliance officer: which of these apply to us, and when is our next deadline?

A copy of your systems that is safe to attack



Until now, only the US Cyber Command and a few Fortune 500 firms could do this. SimSpace and similar vendors built custom replicas of client systems at consulting cost, taking months to stand up. Now any team can do it on demand.

There is a way out. Make an identical, separate copy of your live systems, attack the copy as hard as you want, then throw it away.

Step 1. Copy. A storage shortcut makes an instant, exact copy of your live systems, whether your data is one terabyte or one hundred.

Step 2. Test. Point the AI pentester at the copy with no limits needed. The copy is disposable, so the tool can try every move it knows.

Step 3. Find. The copy matches your real systems exactly. The holes the tool finds are real.

Step 4. Destroy. When the test ends, throw away the copy. The next test starts fresh from your current live state.

Like having a stunt double for your production systems. The stunt double takes all the dangerous hits.

> Ask your IT team: can we test a copy of our real systems on demand?

Test your real systems. Break nothing.

See how a copy-based pentest works on your infrastructure. We will walk you through what it finds and what it costs.

Book a 30-minute call. We will show you the workflow and answer the questions your board is asking.

Request a Demo | Schedule a Security Assessment | Download the Technical Brief

rediacc.com

One platform. Real systems. Zero risk.