



The Vulnerability Flood.

Why point-in-time pen tests can't keep up in 2026.

What happens left of boom, and what it costs right of boom: a practical look at why the vulnerability count keeps climbing, why annual and quarterly testing can't track it, and what running security as a continuous process looks like instead.

Presented by

James Miente, Chief Systems Architect | **George Just**, Head of Channel



What We'll Cover

01

Where we are, and why testing can't keep pace

George on the flood, the buying model, and the left of boom / right of boom framework

02

Three stories from the field

George opens with one from the field; James takes over from there, on both sides of boom

03

What to do Monday

Questions for any provider you work with, regardless of who you call

THE SETUP

You bought the right tools.
It's still not enough.



Endpoint from the market leader. Firewall from the thirty-year veteran. MDR from whoever won the bake-off. Every decision made sense at the time. The stack was assembled carefully, one smart decision at a time, over several years.

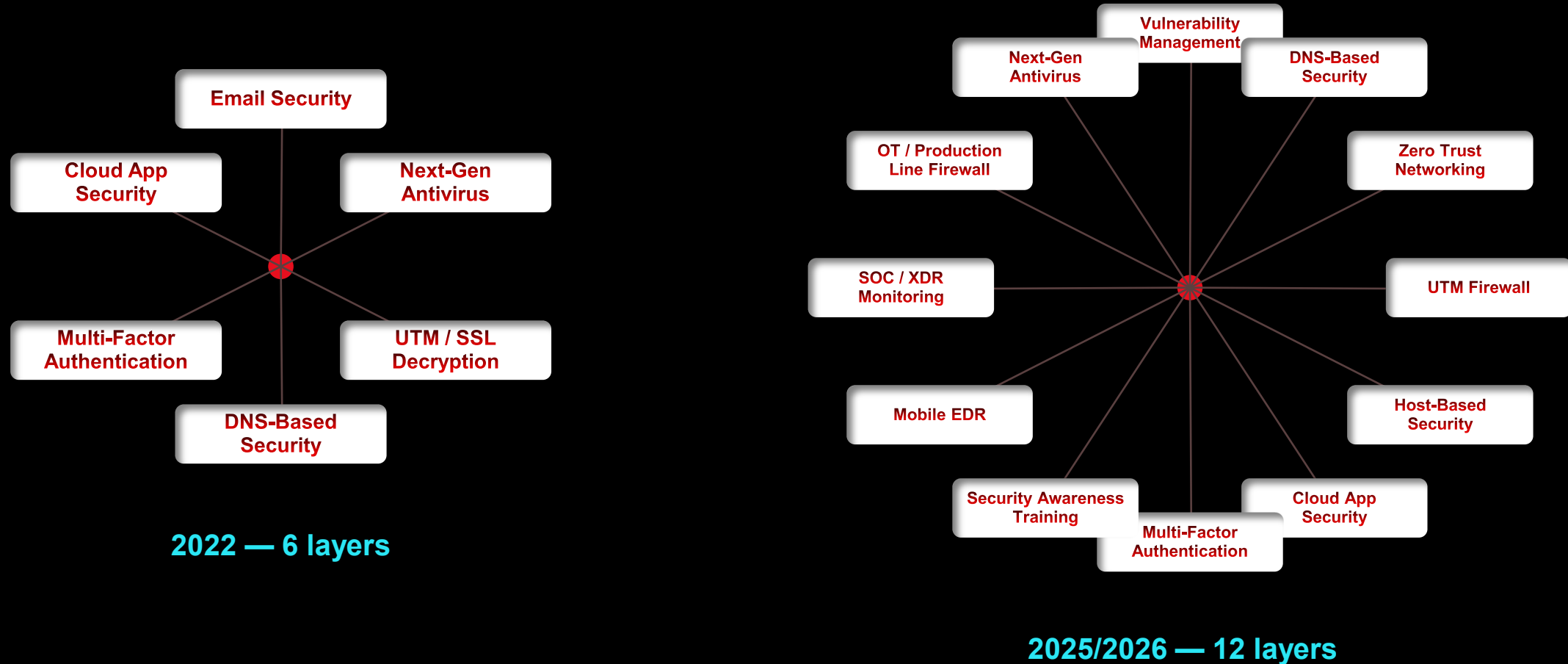


But every vendor brought its own SLA, its own escalation path, its own definition of where responsibility ends and yours begins. Nobody owns the space between the tools. And when something breaks, you're not solving a security problem. You're refereeing a blame tournament.

It's not a tools problem. It's an operating model problem.

The Stack Keeps Growing

One real account, three years. Same problem, twice the layers.



131 New Ways In. Every Day.

48,185

CVEs published in 2025, up 21% year over year. About 131 a day. The volume alone outpaces manual triage.

1

5 days

median time from disclosure to mass exploitation, industry-wide. The average fix still takes 54.8 days.

2

15–20%

of incoming CVEs NIST now has capacity to fully enrich, after moving its own database to a triage model in April 2026.

3

31%

of breaches now start with vulnerability exploitation, the number one initial access vector for the first time.

4

THE FLOOD

More findings isn't **more risk.**

A scan that turns up 40 findings can be a safer environment than one that turns up 2. What matters is exploitability, exposure, and whether anyone's actually watching the gap between scans. **Counting vulnerabilities and managing risk are two different jobs.**

Left of boom. Right of boom.



LEFT OF BOOM

Prevention. Detection. Preparation. Everything that happens before an incident that changes whether it happens at all, or how bad it gets when it does.

RIGHT OF BOOM

Response. Recovery. Cost. Everything that happens after an incident that determines how fast you get back, and what it costs to get there.

Term borrowed from military and EOD risk planning, now common vocabulary in business continuity and cyber resilience.

Yes, Test on a Cadence.

“You got the pen test. You fixed what it found. Then what?”

A regular test is table stakes, and you should have one. But cadence only tells you where you stood on the day it ran. It doesn't run the remediation plan after. That's continuous security operations, and it's what actually closes the gap.

54.8 days

average time to patch a high or critical vulnerability once it's found, industry-wide.

~95%

reduction in exposure window with continuous remediation vs. annual testing.

38%

of CISA's Known Exploited Vulnerabilities are ever fully remediated. About one in three on network edge devices are never fixed at all.

THE THESIS

Security is a process. Not a product.

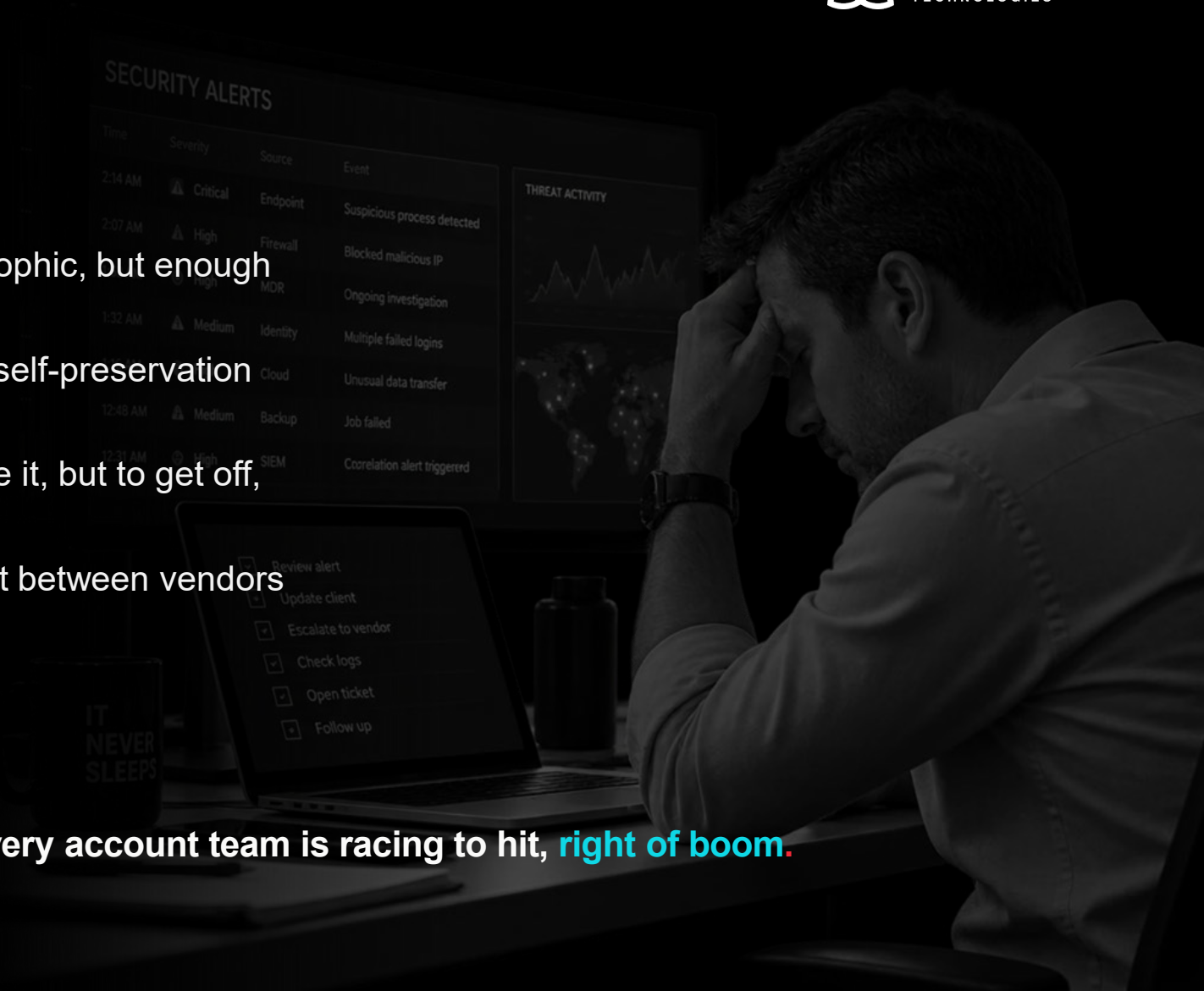
No single tool, however good, secures an organization by itself. Security is what happens continuously between the tools, left of boom and right of boom, and whoever is running that space, day after day.

Mean time to innocence.

What actually happens inside an account during an incident.

- Something goes sideways at 3am. Nothing catastrophic, but enough to start a chain of uncomfortable conversations.
- Every vendor on the account goes into immediate self-preservation mode. Not fix-it mode.
- Every one of them working the problem not to solve it, but to get off, or stay off, the hook.
- The customer is left refereeing a blame tournament between vendors who are each racing to prove it wasn't them.

The metric nobody puts on a dashboard, but every account team is racing to hit, **right of boom**.



STORY ONE, CONTINUED

Where Threats Actually Hide

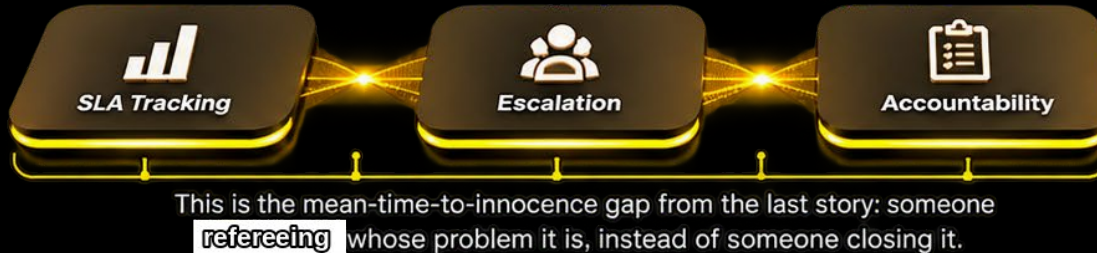
GAP ONE — BETWEEN THE TOOLS



GAP TWO — IN THE PROCESS THAT RUNS THEM

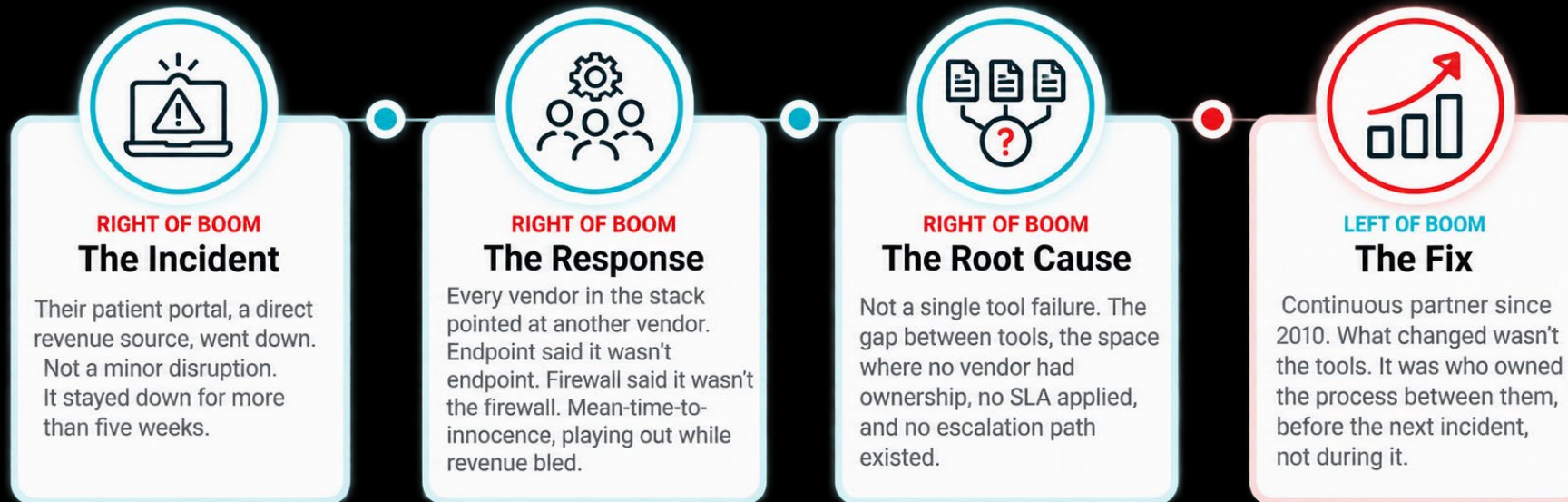


GAP THREE — MANAGING THE VENDORS THEMSELVES



When right of boom goes wrong.

170 locations. Multiple security vendors. A revenue-generating patient portal.



Anonymized by industry and scale. Customer details available under NDA.

How We Actually Score It

Not every finding earns a 9. That's the point.

9–10

Reserved for unusual PCI, audit, or regulatory mandates. Without one, investing here is overinvestment.

8

About as optimized as current technology and a reasonable budget allow.

6–7

A real gap, but a decent place to be. Worth a prioritization conversation before pushing further.

4–5

Progress has been made. A solid investment still separates current state from the target.

1–3

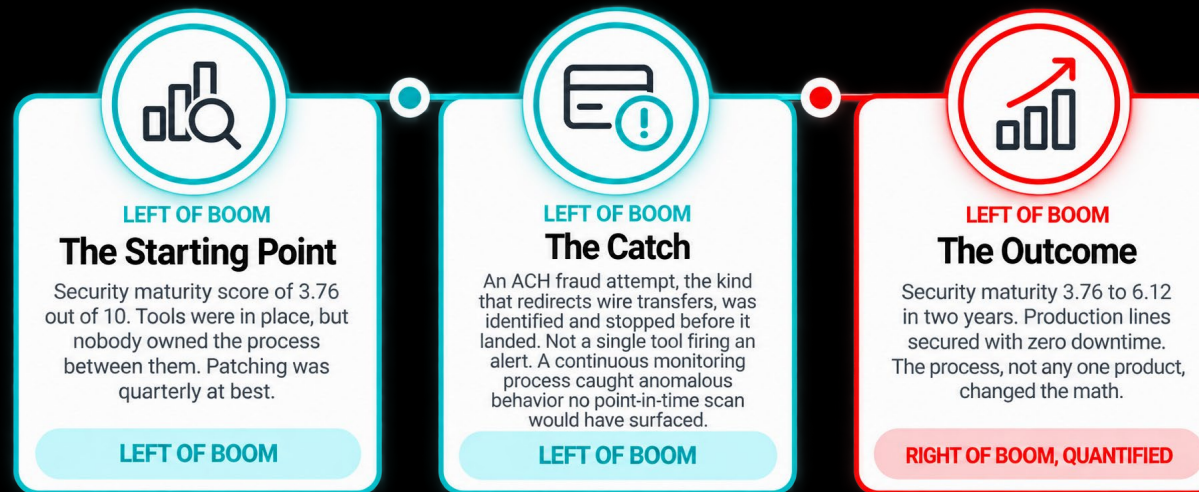
A significant gap between where you are and where you need to be.

0

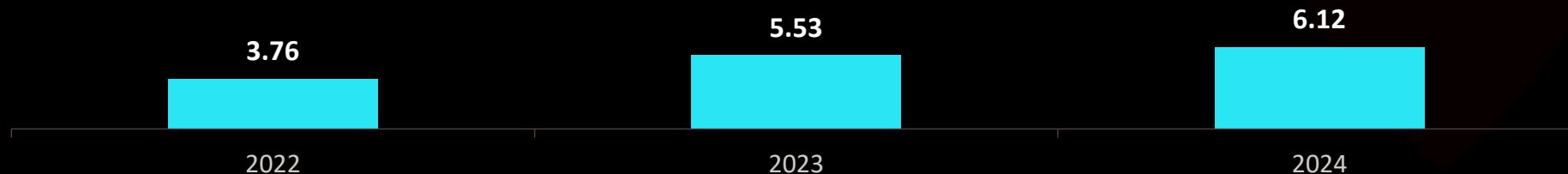
No safeguards in place at all.

When left of boom works.

Multi-site operation. Production lines running 24/7. OT and IT converging.



Critical-severity score, RedZone's 0–10 scale — higher means more mature.



There's no case study for the disaster that got caught in time. **Only the numbers that didn't happen.**

The pattern across clients.

Four verticals, same starting condition, same outcome. The common thread isn't the industry. It's that somebody took ownership of the process.



Healthcare

170 locations

Continuous partner since 2010



Credit Union

NCUA-regulated

Continuous partner since 2010



Manufacturing

Multi-site, 24/7 OT

Continuous partner since 2021



Legal

140 offices

Long-term managed program

Anonymized by industry and scale. Customer names and program details available under NDA on request.

Ask Your Current Provider This

01 Are you testing us, or watching us?

Once a year or once a quarter is a snapshot. Continuous monitoring is a different thing entirely.

02 How do we learn we're exposed?

When a new critical vulnerability drops, do we hear it from you, or find out the hard way?

03 Who owns a finding until it's actually closed?

Not who reports it. Who's accountable for the fix landing.

04 What's our exposure right now, today?

Not on the day of the last report. Right now.

None of this requires buying anything. It just requires asking better questions.

If any of this landed on your environment.

You don't need to decide anything today. If today raised a real question about where your own gaps might be, give us 30 minutes. We don't sell products. We help you build the process that closes the gap.

No pitch. No obligation. **Just 30 minutes on your exact situation.**



James Miente

Chief Systems Architect

jmiente@redzonetech.net



George Just

Head of Channel

partner@redzonetech.net

Thank You.

Thanks for spending your hour with us.

If you want a second set of eyes on any of this, we're glad to help. But today was about better questions, not a pitch.

Sources & Citations

1. Sophos, "The State of Ransomware 2025," n=3,400 respondents across 14 countries. 32% exploited-vulnerability root cause figure.
2. Verizon, "2025 Data Breach Investigations Report (DBIR)," 22,000+ incidents analyzed. 34% YoY exploit-breach increase, 32-day median patch time, 54% patch rate.
3. IBM X-Force, "Threat Intelligence Index 2026." 44% surge in public-facing app exploitation, 56% no-authentication exploitation rate.
4. Rapid7, "2025 Threat Intelligence Report." 105% YoY increase in exploited high/critical vulnerabilities.
5. CrowdStrike, "2025 Global Threat Report." 79% of detected intrusions were malware-free.
6. IBM Security, "Cost of a Data Breach Report 2024." \$4.88M average total breach cost. \$5.36M without security AI/automation vs. \$3.84M with full deployment.
7. NIST National Vulnerability Database, daily publication tracking. 133/day figure reflects trailing average.
8. "Left of boom / right of boom" is established terminology from military and EOD (explosive ordnance disposal) risk planning, widely adopted in business continuity and cyber resilience contexts.
9. Exposure reduction (~95%) and case study details reflect RedZone Technologies program data. Customer names available under NDA.

Sources & Citations, Continued

10. NIST NVD / Mondoo, “2026 CVE Analysis.” 48,185 CVEs published in 2025, up 21% year over year, approximately 131 per day.
11. Edgescan, “2026 Vulnerability Statistics Report.” 54.8-day average patch time for high/critical flaws; 5-day median time to mass exploitation; 38% of CISA KEVs ever fully remediated.
12. NIST, National Vulnerability Database triage-model transition, announced April 2026. Roughly 29,000 backlog CVEs reclassified as Not Scheduled; enrichment now focused on 15–20% of incoming CVEs.
13. Verizon, “2026 Data Breach Investigations Report (DBIR).” Vulnerability exploitation is the leading initial-access vector at 31% of breaches, up from 20%.
14. Mandiant, “M-Trends 2026.” Mean time-to-exploit estimated at -7 days for 2025, meaning exploitation now often precedes patch availability.
15. CrowdStrike, “2026 Global Threat Report.” 42% of exploited vulnerabilities were attacked before public disclosure; eCrime breakout time averaged 29 minutes.
16. Security layer count (6 in 2022, 12 in 2025/2026) and average score by severity quartile (2022–2024): RedZone Technologies program data, anonymized single-account history. Customer identity available under NDA.