AVIATRIX

Reachable Value at Risk

Price the exposure your architecture controls



Security teams report open vulnerabilities, patch times, and control coverage, but none of those numbers says what a compromised system can reach. That reach decides whether an incident stays small or becomes a breach. Reachable Value at Risk is a metric that gives the board a dollar figure for it.

The Formula: Reachable Value at Risk (RVaR)

RVaR = V × R × P × T

- **V** is the value of a business system: what it produces and what an outage or data loss would cost. Finance builds it with the CFO.
- **R** is the share of that value an attacker can reach at runtime from an assumed point of compromise. It comes from observed paths instead of a diagram.
- **P** is the probability of compromise in the planning period, stated openly as an assumption.
- **T** is how much the loss grows while unauthorized access lasts, calibrated from exercises and incident data.

The result is the expected annual loss from what an adversary can reach, ranked per business system rather than one company score.

Why Value and Probability Drop Out

Compare the same system before and after a containment project and take the ratio. Value and probability appear on both sides, so they cancel. What remains is reachability and containment time, the two terms architecture controls and the two you can measure in your own environment. The CISO no longer has to win a debate about breach odds to justify the work.

Why Reachable Value at Risk Matters Now

The incident clock runs faster than response. CrowdStrike puts average eCrime breakout at 29 minutes. IBM and the Ponemon Institute put the average time to identify and contain a breach at 247 days. Threats that operate at machine speed are too fast for the last era's security paradigm.

Instead of trying to patch faster and detect sooner, security teams need to use architecture to contain how far a compromised workload can reach. Blast Radius is set before an incident begins, so a defender can fix it in advance, not after an alert fires.

What to Report for Each Crown-Jewel System

- What it can reach and what it depends on
- The machine identities with standing access into it
- The share of outbound paths governed by explicit communication policy
- The measured time to contain a compromise
- Whether recovery infrastructure sits inside or outside the same reachable environment

Track the trend quarterly, not as a single reading.

The Companion Score: Durable Risk Reduction

Reachable Value at Risk states the exposure. Durable Risk Reduction ranks the projects that reduce it:

DRR Score = (Reduction × Durability) ÷ (Effort + 3 × (Debt + Cost))

how much reach the work removes × how long the removal holds ÷ what it costs once +three years of what it keeps costing

- → **Reduction** is how much of the Blast Radius the project removes, a single narrow path at the low end, the enterprise estate at the top.
- → **Durability** is how long the result holds before an adversary routes around it, 5 for structural controls that match no pattern, 3 for behavioral detection anchored to a validated baseline, 1 for a hash, an indicator, or a static rule.
- → **Effort** is the build cost, paid once.
- → **Debt** is the ongoing labor left behind, tuning, triage, vendor management.
- → **Cost** is the ongoing dollars, licensing, subscriptions, infrastructure.

Each input is scored 1-5. Report the result in bands rather than decimals, because five integer inputs cannot support two decimal places of meaning. Results fall into four bands: sandcastle, weak, durable, and seawall.

Score	Durable Risk Reduction Ranking
Below 0.15	Sandcastle
0.15-0.50	Weak

Score	Durable Risk Reduction Ranking
0.50–1.50	Durable
Above 1.50	Seawall

Example scoring:

Project	Rd	D	E	Dt	C	Score	Band
East-west visibility platform, detection only	1	2	4	4	5	0.06	Sandcastle
Microsegment the crown jewel production estate	4	5	5	3	2	1.00	Durable

Limits of These Equations

The output is a way to compare systems and rank investments, not actuarial truth. T is the weakest term. Containment limits how far one compromise spreads, and it doesn't prevent the first break-in. Detection is still needed.

The First 90 Days

1. Calibrate the scores on two or three projects everyone already agrees on.
2. Score everything in flight, queued or up for renewal.
3. Build V for the top crown-jewel systems with the CFO, and derive R from observed paths.
4. Report the exposure numbers and the score distribution, and fund the highest scores first.

The framework is open and requires no product. Aviatrix builds containment, and its free, read-only Containment Assessment shows what every workload your controller manages can reach.

Read the Whitepaper **Take a free Containment Assessment**

About Aviatrix

Aviatrix® is the network containment company. The Aviatrix Containment Platform sets what every cloud workload may reach before any attack, so a compromised workload does not become a company-wide breach. Built on the Cloud Native Security Fabric, it enforces that policy in the network, at every workload and in every cloud, with nothing to install and nothing to detect first, and encrypts the traffic it allows. It is simpler, safer, faster, and less costly than the firewalls and agents it replaces. The Cloud Native Security Fabric is quantum safe. Trusted by more than 500 of the world's leading enterprises. For more information, visit aviatrix.ai.

References

CrowdStrike, "2026 CrowdStrike Global Threat Report: AI Accelerates Adversaries and Reshapes the Attack Surface," Feb. 24, 2026, https://www.crowdstrike.com/en-us/press-releases/2026-crowdstrike-global-threat-report/
IBM, "Cost of a Data Breach Report 2026," July 29, 2026, https://www.ibm.com/reports/data-breach