

EXECUTIVE BRIEF



The Missing Layer in Cybersecurity

Why governance alone is no longer enough,
and what comes next.

EXECUTIVE SUMMARY

The Missing Layer in Cybersecurity

Key finding

Organizations have spent decades building security controls: firewalls, identity platforms, cloud security, fraud prevention, threat detection, compliance programs.

These investments have made a real difference. And yet cybercrime, fraud, financial crime, and AI-related risk keep growing.

The problem is not a lack of controls. It is that organizations continue to perform increasingly risky work inside environments designed for trusted work.

GOVERNANCE

Manages behavior. Reduces the probability of a bad outcome.

SEPARATION

Manages consequences. Limits what a bad outcome can reach.

The cybersecurity industry spent thirty years building the protection layer. The next decade belongs to the containment layer.

01. THE EVIDENCE

The Data Is Moving in the Wrong Direction

Organizations are spending more than ever on security, compliance, and fraud prevention. The trend lines are not improving.

\$15T

Projected annual cybercrime cost by end of decade

\$4T+

Global financial crime losses annually

\$190B

Annual financial crime compliance spend by institutions

+33%

Increase in U.S. cybercrime losses in 2024

+25%

Increase in U.S. consumer fraud losses in 2024

5.75×

Total downstream cost for every \$1 of fraud loss

The traditional response has been more policy, more monitoring, more approvals, more detection, more response. These investments are valuable. But the trends are not reversing.

This is not a failure of governance. It is a limitation. Governance can influence behavior. It cannot eliminate uncertainty

02.THE CORE PROBLEM

The Industry's Founding Assumption

Most cybersecurity investments rest on a single premise: **risky activities will occur on trusted infrastructure.**

Organizations expect their people to evaluate AI models, execute unfamiliar code, investigate malware, research threat actors, visit hostile websites, assess third-party software, and conduct fraud investigations — all from the same environment used for normal business operations.

The industry's answer has been governance: policies, approvals, access controls, monitoring, detection, logging.

All of these controls share a common characteristic: the risky activity still occurs inside the environment being protected.

The activity remains. The controls attempt to manage the risk. That is a structural problem, not a configuration problem.

03.THE DISTINCTION THAT MATTERS

Governance versus Separation

APPROACH ONE

Governance

Attempts to reduce the probability of a bad outcome by controlling behavior.

- Acceptable use policies
- AI governance frameworks
- Access controls
- Approval workflows
- User training

How do we reduce the chance something bad happens?

APPROACH TWO

Separation

Attempts to reduce the impact of a bad outcome by controlling what it can reach.

- Network segmentation
- Tenant isolation
- Air-gapped systems
- Dedicated containment environments
- Disaster recovery zones

If something bad happens, what can it reach?

That is a fundamentally different risk model. Governance and separation are not alternatives — they operate on different dimensions. Most organizations have invested heavily in one and almost nothing in the other.

04.PRECEDENT

Why Separation Works

Every mature industry that handles inherently dangerous processes understands the value of separation. This is not a new idea.



Nuclear

Reactors are separated from personnel and administrative operations.



Manufacturing

Hazardous processes are isolated from the broader facility.



Finance

Duty separation and vault security contain insider and external risk.



Maritime

Watertight compartments prevent a single breach from sinking the ship.



Cloud

Tenant isolation ensures one customer's compromise cannot reach another's.



Critical Infrastructure

Operational systems are separated from business networks by design.

The principle is consistent: when an activity is inherently risky, separate it from the assets you cannot afford to lose.

No policy can make unknown code trustworthy. No approval process can make hostile infrastructure safe. No governance framework can make uncertainty disappear.
The only reliable control is containment.

05.THE EMERGING CHALLENGE

The Growth of Untrusted Work

The most consequential trend in cybersecurity is not the sophistication of attacks. It is the volume of intentionally risky work that organizations now perform as routine business.

SECURITY TEAMS

- Malware analysis
- Threat hunting
- Incident response
- Digital forensics

THREAT INTELLIGENCE

- Adversary research
- Infrastructure analysis
- Persona operations
- Dark web investigations

FRAUD & FINANCIAL CRIME

- Scam investigations
- AML investigations
- Cryptocurrency tracing
- Account investigations

TECHNOLOGY TEAMS

- AI model evaluation
- AI agent testing
- Third-party software assessment
- Code experimentation

These are no longer edge cases. They are core business processes — and as AI adoption accelerates, the volume of untrusted work will grow faster than any governance program can track. Most organizations still perform this work from environments designed for trusted operations. That is the architectural gap.

06.THE ANSWER

The Rise of the Containment Layer

The next phase of cybersecurity will not be defined by better detection, better prevention, or better governance alone. It will be defined by the creation of dedicated containment environments which is a place where uncertainty can exist without directly exposing trusted systems.

WHAT A CONTAINMENT LAYER PROVIDES

A purpose-built execution environment for untrusted work

Isolation

Containment

Observability

Governance

Auditability

Recovery

This does not replace existing security investments. It amplifies them. Identity still governs access. Security tools still provide visibility. Policies still define acceptable behavior. The difference is where the work occurs.

Governance asks how to reduce the chance of failure. Separation asks what happens if it does. Both questions deserve an answer. Most organizations have only built infrastructure for one of them.

CONCLUSION

A Different Way to Think About Risk

"For decades, cybersecurity has tried to make dangerous activities safer. The better question is whether those activities belong on trusted infrastructure in the first place."

As cybercrime, fraud, AI adoption, and digital investigations continue to grow, the volume of work involving uncertainty will increase. The question organizations need to be asking is not how to govern this work — it is where this work should occur.

The future of risk reduction will not be defined by controlling every interaction with untrusted content. It will be defined by containing those interactions before they can affect what matters most.

THE CONTAINMENT LAYER IS THE NEXT DECADE OF CYBERSECURITY

Supporting Data & Sources

- **\$15T** – Cybercrime projected to exceed \$15 trillion annually by end of decade.
(cybersecurityventures.com)
 - **\$4T+** – Global financial crime exceeds \$4 trillion annually.
(nasdaq.com – Global Financial Crime Report)
 - **+33%** – Reported U.S. cybercrime losses increased 33% in 2024.
(ic3.gov – 2024 IC3 Annual Report)
 - **+25%** – Reported U.S. consumer fraud losses increased 25% in 2024.
(ftc.gov – FTC 2024 Consumer Fraud Data)
 - **\$190B** – Financial institutions spend approximately \$190 billion annually on financial crime compliance and operations
(celent.com)
 - **5.75×** – Every \$1 of fraud loss creates approximately \$5.75 in total downstream costs.
(risk.lexisnexis.com – True Cost of Fraud Study)
 - **2–5%** – Money laundering accounts for approximately 2–5% of global GDP annually.
(unodc.org)
 - **\$4.4M** – Average global cost of a data breach.
(ibm.com – Cost of a Data Breach Report)
-