

# Cybersecurity Case Studies: Patterns and Tradeoffs



Turn incidents into reusable patterns,  
not memorized war stories



Cases build judgment; control  
catalogs don't



One evidence base, multiple depths:  
leads, analysts, architects, defenders, educators



Structure: read a case, pattern library,  
tradeoff matrix, exercises



Ground rules: cases as falsifiable evidence,  
not hindsight moralizing



Anchors: exploitation leads initial access (31%),  
third parties in 48%, ransomware in 48%



# How to Read a Case Study Like a Defensive Practitioner

Reading cybersecurity case studies for evidence, not war stories

EVIDENCE  
CONTEXT  
JUDGMENT  
STRONGER DEFENSES

## ANATOMY OF A CASE STUDY

## WHAT WAS KNOWABLE AT EACH MOMENT



## KEY TAKEAWAYS

- Case anatomy: trigger, discovery path, response sequence, root cause, systemic lessons
- Timeline discipline: separate what was knowable then from what is obvious now
- Split proximate causes from contributing and governance causes
- NIST SP 800-61 Rev. 3: prepare via Govern, Identify, Protect; execute via Detect, Respond, Recover
- Guard against hindsight bias, blame substitution, and outcome bias in debriefs

# Pattern: Initial Access and Attack Surface Concentration

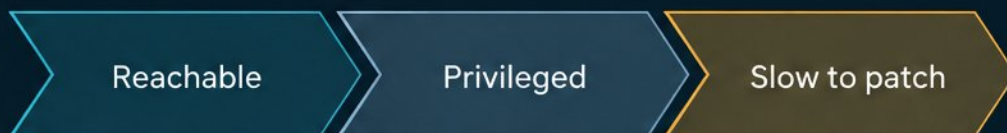
- Exploitation of vulnerabilities now leads initial access at 31% of breaches, up 55% year over year
- Edge devices and VPNs jumped from 3% to 22% of exploitation-driven breaches
- Inbound listeners are reachable, privileged, and slow to patch by design
- Only 26% of CISA KEV criticals fully remediated; median resolution rose to 43 days
- 42.5% of exploited 2025 edge vulnerabilities hit end-of-life devices
- Levers: inventory every internet-facing listener, sub-14-day KEV SLA, outbound-only access

## Initial Access Vectors in Breaches



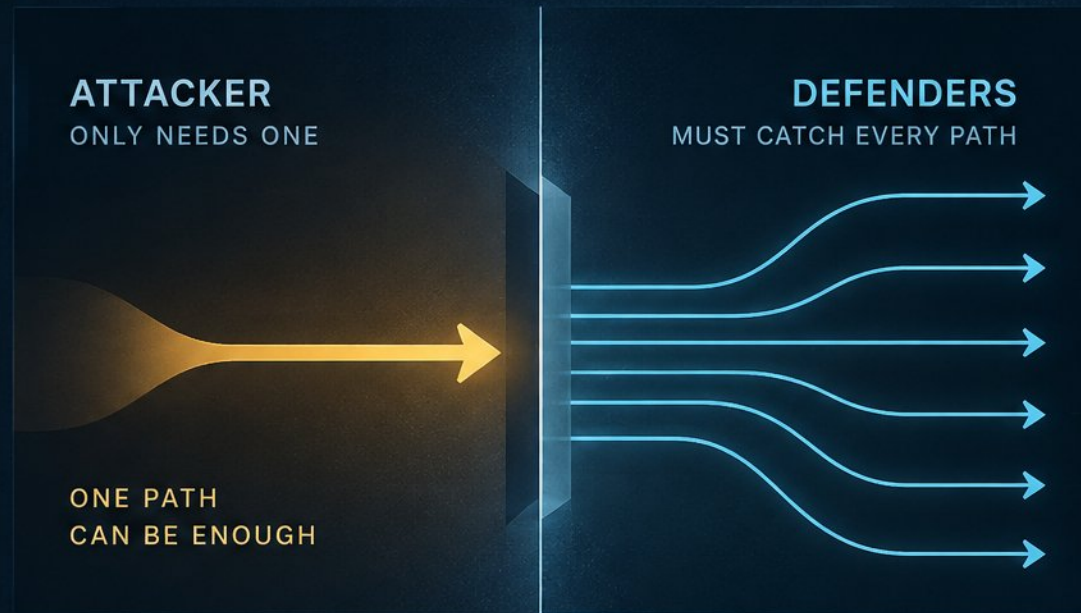
Edge devices and VPNs in exploitation-driven breaches 3% → 22%

## Inbound Listeners by Design



# Pattern: Detection Gaps and Visibility Tradeoffs

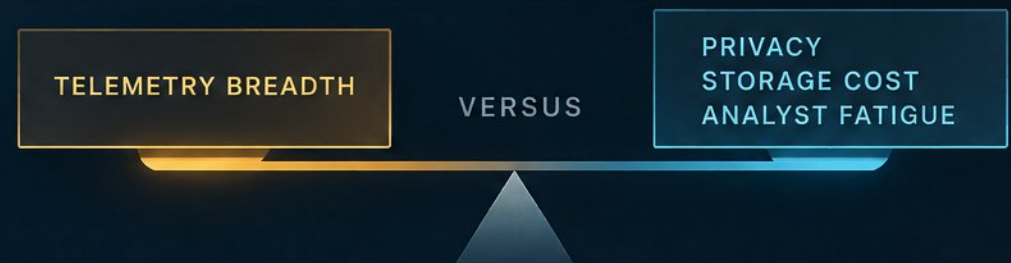
- Defenders must catch every path; attackers only need one
- Alerts fire on roughly 1 in 7 simulated attacks
- Median dwell time rose to 14 days, up from 11
- External notification stretches dwell to 25 days; internal holds near 9
- Espionage and insider cases show 122-day medians, some exceeding a year
- Tradeoff: telemetry breadth versus privacy, storage cost, analyst fatigue
- Metrics: dwell time by detection source, coverage on identity/endpoint/lateral paths



## DWELL TIME BY DETECTION SOURCE

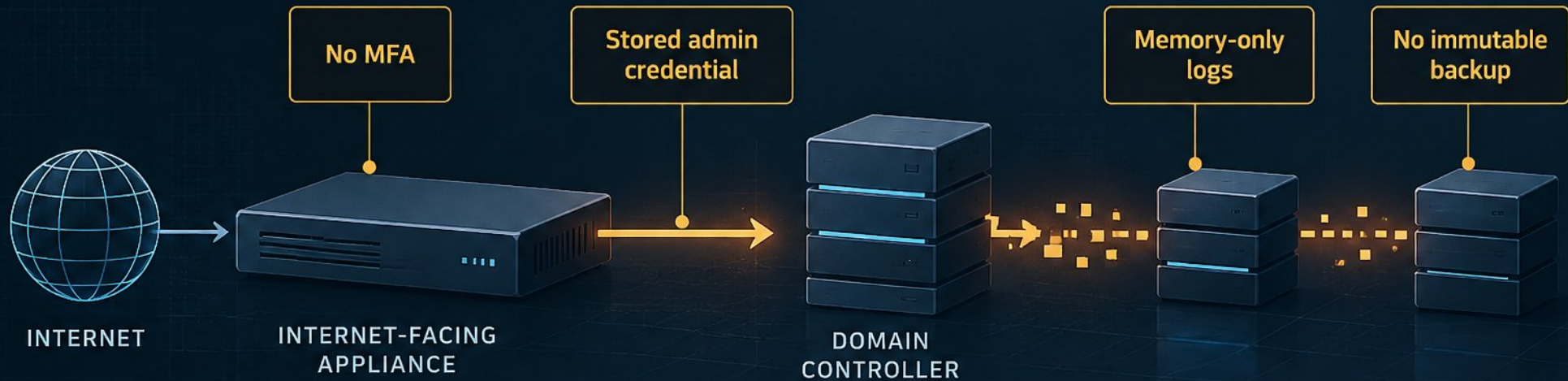


## THE VISIBILITY TRADEOFF



# Case: A Single Edge Appliance to Domain Control

A SINGLE GAP CAN BREAK THE CHAIN

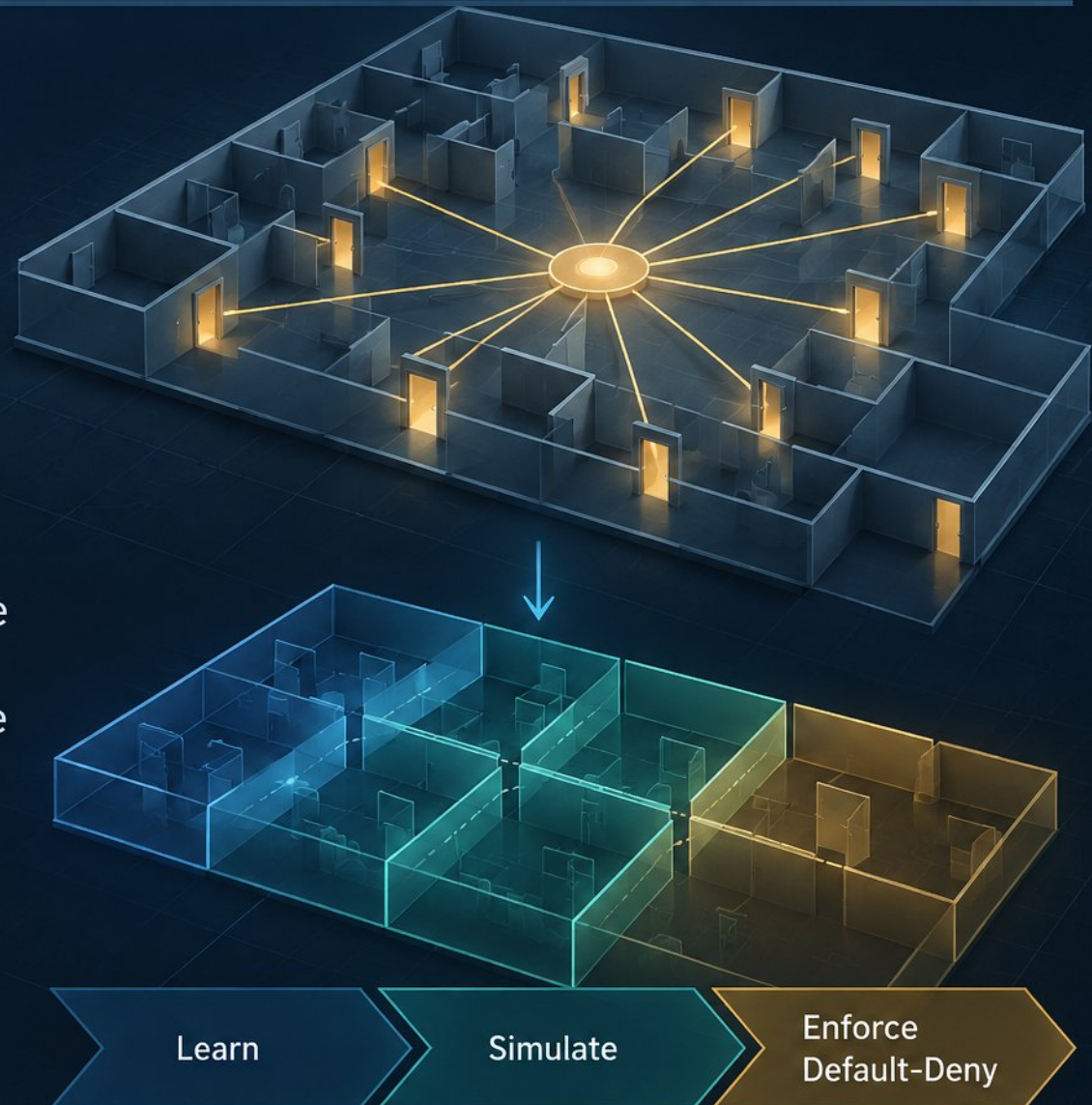


- Singapore F&B group: internet-facing appliance 4 years past support, no MFA
- Domain-admin credential stored in appliance config — perimeter equals domain control
- Attacker staged 30GB in seven archives, then encrypted ~15M files in three days
- Backups and backup-agent certificates encrypted; no clean restore inside the environment
- Workstation absent from victim's own scope list held persistence, tooling, stolen credentials
- Appliance logs memory-only: exposure reported as upper bound, not asserted
- Four cheap controls would each have broken the chain



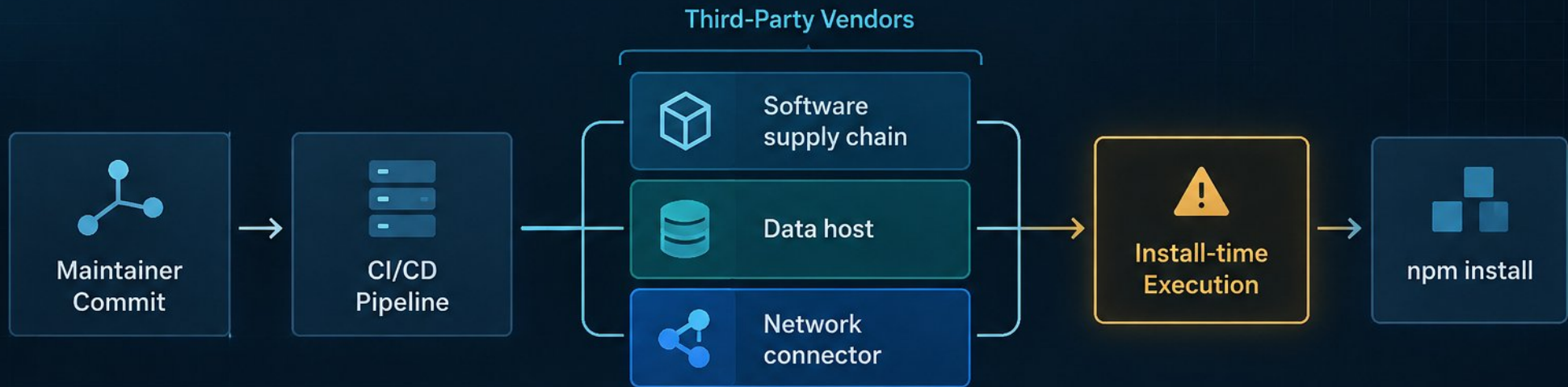
# Pattern: Lateral Movement, Identity, and Segmentation Tradeoffs

- Flat networks plus over-privileged identity turn one foothold into domain dominance
- Attackers prefer service accounts: privileged and rarely monitored
- Real cases: credentials stored on edge appliances, rogue admin accounts on the management plane
- VLAN segmentation stalls on device sprawl and re-IP: 85,000 devices, 46 days identity-based
- Learn, simulate, then enforce default-deny — blast radius, not prevention



# Pattern: Supply Chain and Third-Party Trust Amplification

HIGHER  
TRUST  
STRONGER  
SYSTEMS



- Third-party breaches up 60% YoY to 48% of incidents
- Supply chain compromise: \$4.91M average cost, 267 days to contain
- Three vendor archetypes: software supply chain, data host, network connector
- 2026 npm worms spread via OIDC token hijacking and preinstall hooks
- SLSA provenance verifies the build, not whether source was compromised
- SBOMs inventory the tree, not what executes at install
- Controls: scope OIDC to branches, allowlist install scripts, treat CI/CD as Tier-0

## EVIDENCE LEDGER

### PROVENANCE



TRACE | VERIFY | REDUCE RISK

# Case: When the Recovery Plan Becomes the Attack Surface

- Fairlife, July 2026: 11-day US production halt; Canadian operations continued
- Constraint was documentation, not safety — ISA-95 Level 3 recipe and batch systems
- Finished-goods inventory, a supply-chain choice, absorbed the outage
- Attribution discipline: no filing confirms CitrixBleed 2 as entry point
- Asahi: VPN entry, weak passwords, EDR and NIST alignment still bypassed
- Segmentation saved the factory floor; order systems down for months

WHAT WE KNEW THEN

WHAT WE KNOW NOW

# Pattern: Resilience, Recovery, and Backup Tradeoffs

LESSONS FOR A MORE RESILIENT TOMORROW

- Recovery capability is a security control: attackers delete backups before encrypting
- Real immutability means storage-enforced Object Lock in compliance mode, or disconnected media
- Retention must exceed plausible dwell time, or you restore the attacker's access
- Restoration is a rebuild: fresh hosts, rotated credentials, forensic snapshots, isolated recovery
- One hospital restored clinical systems in under four hours from an air-gapped vault
- Tradeoff: recovery time and immutability cost versus operational complexity and locked retention

### IMMUTABILITY



Storage-enforced Object Lock in compliance mode  
or  
disconnected media

### RETENTION



Retention must exceed plausible dwell time, or you restore the attacker's access

### REBUILD, NOT RESTORE



Fresh hosts      Rotated credentials      Forensic snapshots      Isolated recovery

### REAL-WORLD EXAMPLE



One hospital restored clinical systems in under four hours from an air-gapped vault

### TRADEOFF



Recovery time and immutability cost versus operational complexity and locked retention

# Case: Manufacturing Downtime as Economic Weapon

- Jaguar Land Rover, August 2025: voice-phishing credentials led to a **five-week global production halt**
- Estimated **£1.9–2.5 billion** impact and roughly **5,000** downstream organizations affected
- Manufacturer ransomware up **40%** in early 2026; new groups drive the surge
- Just-in-time inventory turns a **48-hour** network freeze into **empty shelves**
- Nichirei, Stryker, and Asahi show the same cascade across national supply
- One compromised operator can disrupt customers, hospitals, and distribution



**£1.9–2.5 billion**  
impact

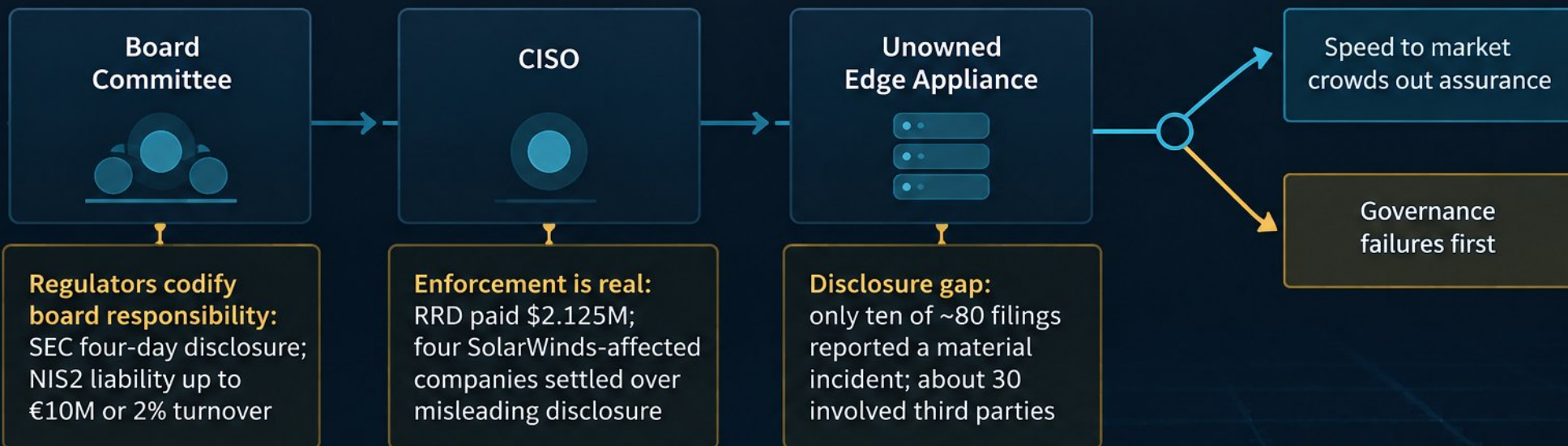


**5,000**  
downstream  
organizations affected



# Pattern: Governance, Incentives, and Accountability Failure

ALIGN OVERSIGHT. CLOSE DISCLOSURE GAPS. ASSURE WHAT SHIPS.



- 1 | Regulators codify board responsibility: SEC four-day disclosure; NIS2 liability up to €10M or 2% turnover
- 2 | Enforcement is real: RRD paid \$2.125M; four SolarWinds-affected companies settled over misleading disclosure
- 3 | Disclosure gap: only ten of ~80 filings reported a material incident; about 30 involved third parties
- 4 | Oversight professionalized: 96% disclose a board cyber committee; 58% run tabletop exercises, up from 3% in 2019
- 5 | Speed to market crowds out assurance; unowned edge appliances are governance failures first
- 6 | Levers: named ownership, formal risk acceptance, unfiltered CISO reporting, rehearsed materiality procedures

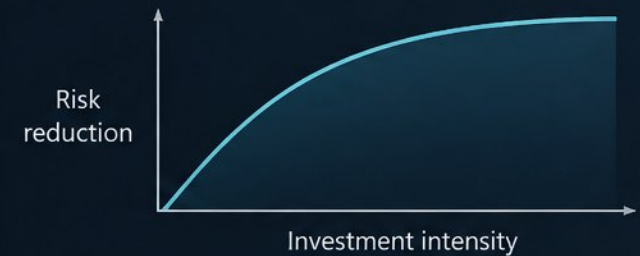
# Tradeoff Matrix: Choosing Under Uncertainty

TRADEOFFS  
LEAD TO  
STRONGER DECISIONS

BALANCE COMPETING GOALS. MAKE RISK-AWARE CHOICES.

| Tradeoff Family | Tradeoff (Two Sides)                                                                                          | Reversibility |
|-----------------|---------------------------------------------------------------------------------------------------------------|---------------|
| usability       | Security ←  → Usability      | Reversibility |
| assurance speed | Speed ←  → Assurance         | Reversibility |
| privacy         | Detection ←  → Privacy       | Reversibility |
| autonomy        | Centralization ←  → Autonomy | Reversibility |
| coverage        | Cost ←  → Coverage           | Reversibility |

- Five recurring tradeoff families: usability, assurance speed, privacy, autonomy, coverage
- Criteria: risk reduction, direct/indirect cost, circumvention risk, reversibility, evidence quality
- Curve shape: risk reduction decelerates beyond a certain investment intensity



- Prevention-heavy portfolios should shift toward detection and containment over time
- Frame with value, breach probability, and investment productivity (Gordon–Loeb)
- Document assumptions, residual risk owner, and the revisit date



# Mapping Your Own Case to the Pattern Library

ANALYZE  
CONNECT  
APPLY

- 1 **Exercise 1:** map your incident to the six patterns
- 2 **Exercise 2:** map same case onto NIST SP 800-61 Rev. 3 functions
- 3 **Exercise 3:** apply tradeoff matrix; name the reversing assumption
- 4 **Pitfall:** transplanting lessons without matching local constraints
- 5 **Facilitation:** 90-minute mixed-role session with timed injects
- 6 **Output:** one-page pattern entry with evidence and risk owner



# From Patterns to Practice: Takeaways and Action List



## Analysts

- Analysts: measure dwell time by detection source; close log gaps before adding tooling



## Architects

- Architects: inventory internet-facing listeners; broker remote access outbound-only; simulate before enforcing segmentation



## Defenders

- Defenders: prove one backup copy survives domain-admin compromise; rehearse restore, not backup



## Leaders

- Leaders: name device owners, formalize risk acceptance, brief the board with examiner numbers



## Educators

- Educators: teach pattern recognition with evidence trails and a claim that later proved wrong

# PersonWise.

PersonWise • AI digital-human course platform



Scan the code or click anywhere to watch this course live, with voice Q&A

[personwise.ai/t/1f728a94/public](https://personwise.ai/t/1f728a94/public)