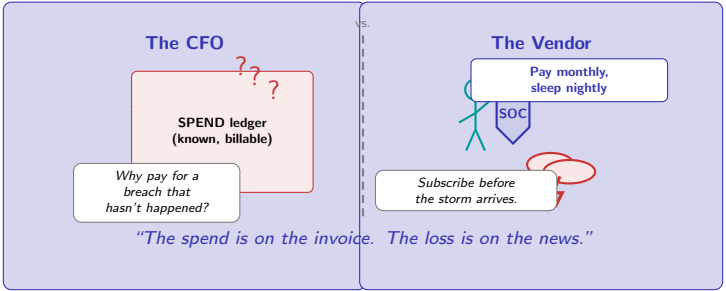
Cybersecurity Business Models

Selling certainty against probabilistic loss — the spend is provable, the breach is not

Digital Finance


The CFO
? ? ?
SPEND ledger
(known, billable)
Why pay for a breach that hasn't happened?
vs.
The Vendor
Pay monthly, sleep nightly
SOC
Subscribe before the storm arrives.
"The spend is on the invoice. The loss is on the news."

Why Do Financial Firms Pay Vendors for Threats That Have Not Yet Materialised?

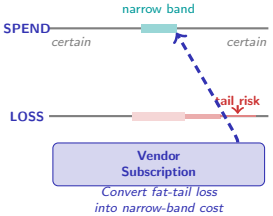
The Spend-vs-Loss Asymmetry
A line item in a budget is concrete — the invoice arrives, the controller signs, the cost flows through the income statement. A breach loss is hypothetical until it happens, then catastrophic. Cybersecurity vendors monetise this asymmetry: they convert an uncertain liability into a predictable subscription.

Three line items the CFO can defend: the **SOC** contract (security operations centre — the round-the-clock monitoring team), the **EDR** licence (endpoint detection and response — agent software watching every laptop and server for malicious behaviour), and the **threat-intel feed** (a subscription stream of malicious IP addresses, file hashes, and attacker infrastructure pushed into the defender's tools).

- **Probabilistic loss:** the breach distribution has a fat tail; the expected value is small, the variance is enormous.
- **Asymmetric outcome:** skipping the spend looks rational ex ante and reckless ex post. Vendors price exactly that gap.

Regulatory arbitrage = a firm earns profit specifically because it faces a lighter rulebook than its competitors, not because it is better at the underlying business. The advantage lasts only as long as the rulebook gap does.

The friction the cyber BM exploits is not technical — the tools themselves are commoditising. The friction is **anxiety arbitrage**: the buyer purchases the absence of a tail event.



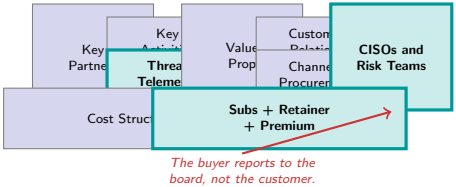
The cyber BM monetises the difference between provable spend and probabilistic loss — the BMC Value Proposition is converting tail risk into subscription expense.

Which Canvas Blocks Make a Cyber-Defence Vendor Look Nothing Like a Bank?

The B2B Cyber Canvas
Osterwalder's Business Model Canvas frames nine interlocking blocks: value proposition, customer segments, channels, revenue streams, key resources, key activities, key partners, cost structure, customer relationships. For cyber-defence vendors, three blocks reshape away from the consumer-FinTech template.

- **Customer Segments:** chief information security officers and enterprise risk teams — procurement contracts, not app-store installs. The buyer signs because of board-level liability, not product joy.
- **Key Resources:** threat-intel telemetry, validated detection content, and incident-response playbooks — evidence inventories, not interface polish.
- **Revenue Streams:** subscription tiers per endpoint or per gigabyte, plus per-incident retainers, plus underwriting premia for the insurance variant.

The canvas reveals that cyber-defence is a B2B-evidence business adjacent to enterprise software and reinsurance — not a consumer finance product at all.

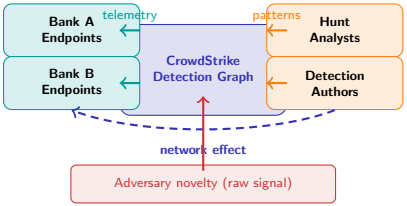


Osterwalder's Business Model Canvas adapted to cyber-defence: three blocks (Customer Segments, Key Resources, Revenue Streams) sit closer to enterprise software than to consumer banking.

How Does CrowdStrike Turn Endpoint Telemetry into a Two-Sided Defence Platform?

The CrowdStrike Case
CrowdStrike (US-listed endpoint-security vendor, headquartered in Austin, Texas) sits between two populations: the agents installed on client endpoints (which stream telemetry inward) and the threat-intel analysts (who push detection content outward). Each side raises the value of the other.

- **Multi-sided platform:** more endpoints feed the global detection graph; richer detection content draws more endpoints.
- **Cross-side network effect:** every novel intrusion seen at one client becomes a signature deployed instantly to every other client; defence improves before the next attacker arrives.
- **Chicken-and-egg solution:** the vendor seeded the data side first — ingesting open-source intel and operating its own hunt team — before charging clients for a richer corpus than any single firm could assemble alone.
- Invisible to the end-user customer of the bank, indispensable to the SOC analyst who watches the bank's perimeter.



Platform economics in cyber-defence: every fresh client telemetry stream improves the detection graph, which raises the vendor's appeal to the next client. Winner-take-most dynamics emerge.

How Does a Threat-Intel Feed Vendor End Up Selling a Cyber-Insurance Policy?

Unbundling = pulling one service out of a historical bundle and offering it alone; *rebundling* = stacking adjacent services onto that foothold once trust is established. Clayton Christensen (Harvard Business School) argued disruptors start narrow and cheap, earn trust, then expand upward — the *unbundling* phase followed by the *rebundling* phase.

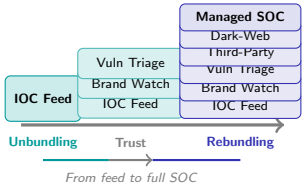
Christensen's Disruption Cycle Applied

Phase One — Unbundling: Recorded Future (US-headquartered threat-intelligence firm in Somerville, Massachusetts) entered with one proposition: a curated stream of *indicators-of-compromise* (IOCs — malicious IP addresses, domains, or file hashes whose presence in a defender's own logs signals an intrusion in progress) delivered as an API. No agents, no consoles, no incident-response contract.

Phase Two — Trust Earned: SOC teams integrated the feed into existing tooling, then trusted the vendor with broader analytic workflows. Switching cost accumulated through embedded queries and tuned rule packs, not contractual lock-in.

Phase Three — Rebundling: Brand monitoring, vulnerability prioritisation, third-party-risk scoring, dark-web surveillance, and managed analyst services. The single-feed vendor became a portfolio of intelligence products covering most of the SOC backlog.

The endpoint of disruption looks remarkably like a re-created Big-Four managed-security practice — the survivor resembles the firms it originally undercut.



Christensen's disruption theory predicts this cycle: the vendor enters narrow, trust accumulates through embedded usage, and rebundling re-creates the very managed-services bundle the wedge was undercutting.

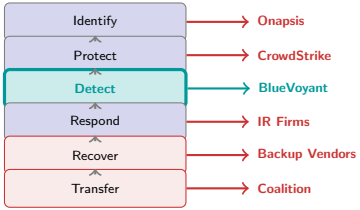
Where in the Defence Lifecycle Does BlueVoyant Place Itself — and What Does It Capture?

Value chain = the ordered activity sequence a service passes through. Evans and Wurster (BCG) argued that when information is cheap, each link can be split off to a specialist — the chain *deconstructs* into independent layers.

The Defence Value Chain

BlueVoyant (US-headquartered managed-detection-and-response provider based in New York) lives inside exactly such a deconstructed chain. Every link is now contestable by a specialist vendor:

- **Identify** — attack-surface mapping (Onapsis on ERP)
- **Protect** — preventive controls (CrowdStrike on endpoint)
- **Detect** — monitoring and hunting (BlueVoyant managed SOC)
- **Respond** — triage and containment (Mandiant-style retainers)
- **Recover** — restoration and lessons learned
- **Transfer** — insurance and risk financing (Coalition policies)



Vendors that own the **detection link** capture the most repeat revenue, because Detect runs continuously while Identify and Recover are episodic. BlueVoyant sells managed detection as a subscription wrapper around third-party tooling the bank already paid for.

Evans and Wurster argued that information-rich value chains deconstruct. The defence lifecycle is no exception: each link is now a separate vendor category competing on continuous revenue capture.

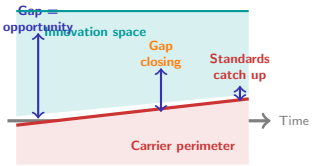
Is Coalition's Underwriting Edge a Lasting Moat or a Time-Bombed Arbitrage?

The Cyber-Insurance Arbitrage
Coalition (US-headquartered cyber-insurance MGA — managing general agent — based in San Francisco) combined two regulated industries — insurance underwriting and cyber-defence services — in a way neither incumbent could easily copy. Underwriters lacked the technical telemetry to price risk; security vendors lacked the licences to write policies. Coalition straddles both perimeters.

- **Underwriting arbitrage:** the firm priced policies using continuous scanning data that traditional carriers could not collect, capturing the lowest-risk segment of the market.
- **Active-defence arbitrage:** bundled monitoring let Coalition intervene before a claim crystallised — a cost structure no pure carrier could match.
- **Regulatory arbitrage:** insurance regulation evolved more slowly than the threat landscape; Coalition operated under surplus-lines rules that gave it pricing flexibility incumbents lacked.

(In business-model language, a *moat* = a competitive advantage that rivals cannot easily copy.)

The tension: as carriers wake up and adopt similar telemetry, and as regulators push standardised cyber-policy forms, the arbitrage narrows. Coalition's bet is to convert today's edge into a permanent data-and-distribution moat before the perimeter catches up.

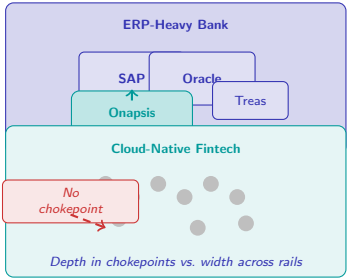


The best cyber vendors convert temporary regulatory and informational arbitrage into permanent data-and-distribution moats — before standardised cyber-policy forms equalise the playing field.

Why Does Onapsis Earn Its Best Returns Inside ERP-Heavy Banks Rather than Cloud-Native Ones?

The Onapsis Lesson
Onapsis (US-headquartered ERP-security specialist based in Boston, Massachusetts, with research roots in Buenos Aires) protects mission-critical *ERP* (enterprise resource planning — integrated software suites that run a bank's general ledger, payroll, and treasury on a single data model) platforms such as SAP and Oracle EBS. The firm thrives where regulated banks have decades of encrusted ERP investment that cannot be replatformed without breaking audit trails.

- In ERP-heavy estates the protected asset is concentrated, business-critical, and replacement-resistant — the vendor's willingness-to-pay is high and renewal sticky.
- In cloud-native fintechs the same firm faces fragmented stacks, shorter half-lives and built-in security telemetry from the cloud provider — the wedge product matters less and the vendor's willingness-to-pay drops sharply.
- Fundamentally different from CrowdStrike or BlueVoyant: Onapsis built deep in one chokepoint rather than wide across many.
- The lesson: cyber-defence value creation depends on where the protected asset sits. Concentrated, replacement-resistant assets reward depth specialists; commoditising assets reward platform generalists.



Onapsis's insight: where the protected asset is concentrated and replacement-resistant, depth wins. Where assets are fragmented and commoditising, only platform breadth survives.

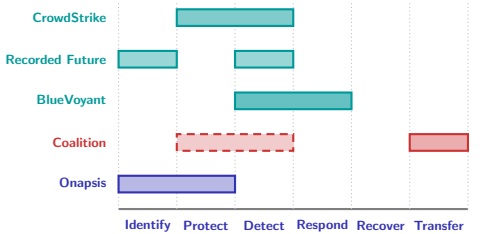
Mapping the Defence Lifecycle: Where Does Each Vendor Earn Its Continuous Revenue?

The Gantt Synthesis

The five worked vendors each occupy a different band in the defence lifecycle. The Gantt-style chart on the right shows where each one earns its continuous subscription or premium revenue — and where the gaps lie.

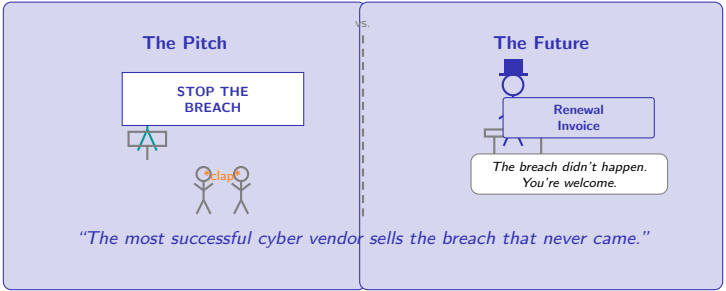
- **CrowdStrike:** broad band across Protect and Detect — the platform play.
- **Recorded Future:** concentrated upstream in Identify and Detect — the intel layer.
- **BlueVoyant:** the deepest band in Detect and Respond — managed services.
- **Coalition:** the only vendor that owns Transfer — the insurance carve-out — with active-defence reach into earlier phases.
- **Onapsis:** a narrow, deep band in Identify-and-Protect for ERP estates only.

The lesson: the vendor who owns the longest continuous band captures the most renewal revenue. Episodic phases (Recover) reward incident-by-incident pricing instead.



Solid bar = primary revenue band; dashed = active-defence reach

The Gantt view makes vendor positioning legible: the longer the continuous band, the more renewal revenue; episodic phases reward retainer pricing instead of subscription pricing.


The Pitch
STOP THE BREACH
clap
vs.
The Future
Renewal Invoice
The breach didn't happen. You're welcome.
"The most successful cyber vendor sells the breach that never came."