

// RANSOMWARE CONTAINMENT

AI vs. Ransomware: Enterprise Protection Reimagined.

Contain, verify and recover on the infrastructure you already run.

One control, built for the **moment** the files start changing.

2016

Ransomware containment since day one.

Founded in Copenhagen. The first release stopped encryption as it ran; each one since covers more.

750+

Organisations in production.

Automated containment live today, with no analyst required to act.

1,000,000+

Enterprise users protected.

On file shares, Microsoft 365, Google and ESXi hosts, with no endpoint agents.

Built for the organisations that cannot afford to be wrong: national health and emergency services, critical infrastructure, and the enterprises whose customers run on their systems. In the UK, the EU, the US and Canada.

01 **Healthcare and emergency services**

02 **Critical infrastructure**

03 **Banking and insurance**

// WHY NOW

Nearly half of all breaches now involve ransomware.

Ransomware is how it usually happens: a seven-figure bill and weeks of disruption. And it is no longer alone. Agentic attackers, and the AI inside the estate, destroy data at machine speed, on valid credentials.

48%

of confirmed breaches involve ransomware, up from 44% in the 2025 report. The highest share in the report's history, from 22,000 breaches analysed.

VERIZON 2026 DATA BREACH INVESTIGATIONS REPORT

27s

Fastest recorded breakout; average 29 minutes, with humans driving. Agentic tooling does not pause.

2026 GLOBAL THREAT REPORT

\$5.08M

Average total cost of a ransomware incident, including downtime, remediation and business interruption.

IBM COST OF A DATA BREACH 2025

94%

of ransomware incidents attacked the backups. Recovery alone averages \$1.53M, before any ransom.

SOPHOS STATE OF RANSOMWARE 2024 / 2025

Prevention lowers the odds. Nothing in the stack decides what happens once the encryption starts.

69% of victims now refuse to pay, so attackers push volume and disruption instead. Verizon 2026 DBIR.

// AI ON BOTH SIDES

Two kinds of AI can destroy your data.

01

The AI agents inside the estate hold valid credentials.

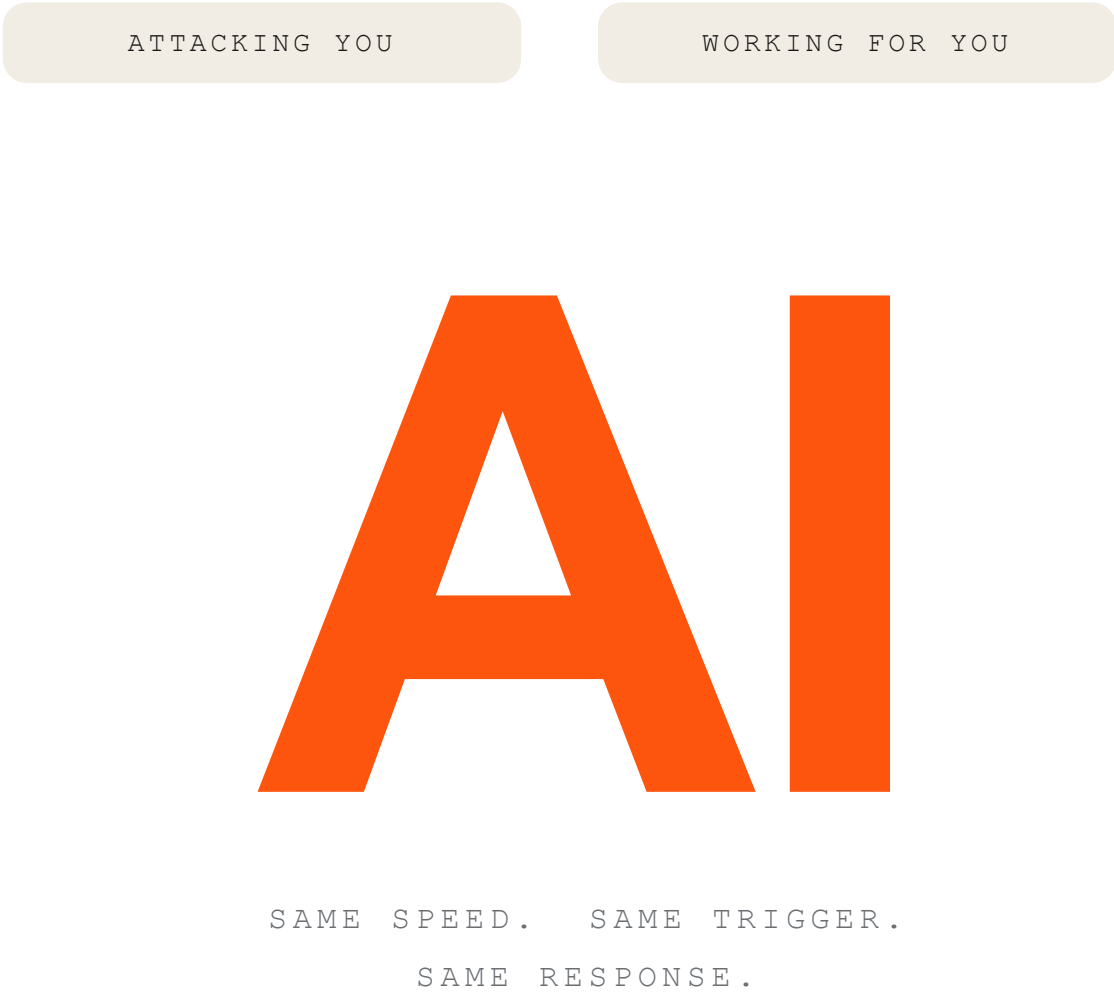
One that is hijacked, or simply wrong, rewrites and deletes at machine speed, from the inside, with permission.

02

Attack-side AI removed the pauses.

Agentic tooling does not stop to think between steps, so the run from first foothold to mass encryption keeps compressing.

We work at the speed of threat.



// THE ACTORS HAVE CHANGED

Two paths in. **One moment of impact.**

A criminal crew on agentic tooling and an AI agent the insured hired look different all the way in, until an authorised account starts destroying files at machine speed. From there, they are the same event.

01 OUTSIDE · STOLEN CREDENTIALS

The external attacker, now agentic

A valid login, the proven extortion playbook, increasingly run by software. Weeks of dwell and staging compress to minutes and the pace never drops while an operator sleeps. The encryption itself is still an authorised account writing files.

02 INSIDE · GRANTED CREDENTIALS

The AI inside the estate

An agent with credentials the organisation granted. A misfiring workflow rewriting a share, an over-permissioned copilot syncing damage at scale, an agent hijacked through its inputs. No breach, no malware, no perimeter crossed, and the same destructive writes.

// THE VERDICT

We judge the write itself.

Content is read as it is written, the verdict lands in milliseconds, the session is cut in seconds. 8.9 seconds in the latest measured incident. The record names every file touched, whoever, or whatever, was writing.

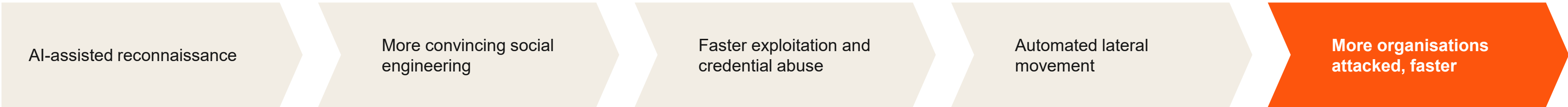
WRITES CUT IN SECONDS

MEASURED IN PRODUCTION ESTATES

The moment of impact is the layer we own. It does not ask who is acting; mass encryption at machine speed looks the same from both paths.

// THE OFFENSIVE SHIFT

AI is changing the **economics** of ransomware.



87%

of respondents identified AI-related vulnerabilities as the fastest-growing cyber risk during 2025.

WEF, GLOBAL CYBERSECURITY OUTLOOK 2026

47%

of organisations cited adversarial advances powered by generative AI as a primary cybersecurity concern.

WEF, GLOBAL CYBERSECURITY OUTLOOK 2025

42%

of organisations reported phishing or social-engineering incidents during 2024.

WEF, GLOBAL CYBERSECURITY OUTLOOK 2025

AI lowers the cost of producing credible attacks. For insurers, that increases frequency, velocity and the potential for correlated losses.

// PREMISE · LLOYD'S MARKET-WIDE SCENARIO

Lloyd's own market-wide exercise already modelled the gap. **It does not close on its own.**

Lloyd's Market Wide Scenario Exercise, published February 2026. Market systems suspended. Staff locked out of the building. Premium processing stalled for days. It was a test; the pattern we contain in production.

\$3.5tn

LLOYD'S OWN ESTIMATE OF GLOBAL ECONOMIC LOSS IN A SYSTEMIC CYBER SCENARIO

Cambridge Centre for Risk Studies; payment-system disruption alone.

\$508K

AVERAGE RANSOMWARE CLAIM SEVERITY, UP 16% YEAR ON YEAR

At-Bay 2026. Remote access was the entry point 87% of the time.

1st

FULLY AGENTIC, HUMAN-FREE RANSOMWARE ATTACK ON RECORD

JadePuffer, July 2026. Start to finish, no operator in the loop.

WHAT UNDERWRITING ALREADY PRICES FOR

Rising severity and AI-attack growth are now line items in underwriting questionnaires across the market. This is not hypothetical; it is the book.

WHAT THIS SESSION ANSWERS

One variable set all three figures: how long the writes ran before something stopped them. That is the variable we own.

// THIS ISN'T HYPOTHETICAL

One helpdesk call cost a UK high-street name £300m in profit.

£300m

LOST OPERATING PROFIT

In April 2025, attackers persuaded a service desk to reset a password, no malware, no exploit, then used that access to deploy DragonForce ransomware across Marks & Spencer's virtual server estate.

The call	A phone-based social-engineering attempt, no malware, no exploit.
The spread	The ransomware reached the virtual server estate behind stores and online orders.
The source	M&S trading statement; Reuters, May 2025.

Ransomware severity is measured in **operational impact**, not just the payment.

Fewer organisations may be paying, but refusing the ransom does not remove the loss. The cost moves into interruption, investigation and recovery.

48%

of confirmed breaches involved ransomware, up from 44% the year before.

69%

of victim organisations did not pay a ransom.

\$115K

median ransom payment, down from \$150,000.

\$5.08M

average total cost of an incident, ransom excluded.

ABOVE THE SURFACE

Ransom demand

BELOW THE SURFACE

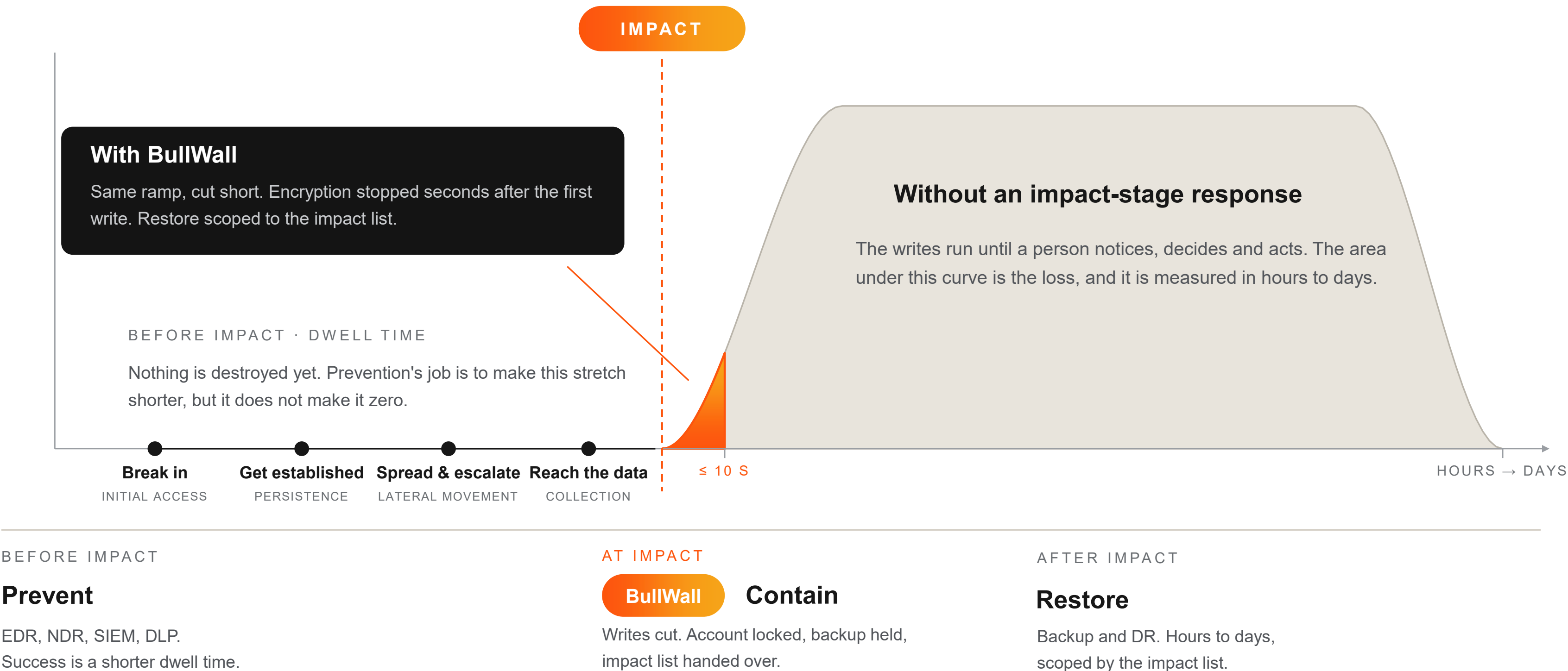
- Business interruption
- Forensic investigation
- Incident response
- Data and system restoration
- Legal and regulatory costs
- Customer notification
- Liability and reputational harm

Sources: Verizon 2026 Data Breach Investigations Report; median payment from Verizon 2025 DBIR; IBM Cost of a Data Breach 2025.

// THE DAMAGE WINDOW

The damage is in the **window** after impact.

Prevention shortens the time before. BullWall shrinks the loss after. Same attacker, same encryption rate. The only variable is how long the encryption runs.



// 'WE HAVE EDR AND MDR'

Detection on the questionnaire tells you something will be seen, **not what gets shut down.**

WHAT THE ANSWER TELLS AN UNDERWRITER

Detection is in place. The decision under pressure still sits with a person.

- The alert fires; a human has to notice, decide and act, at any hour.
- No single view of blast radius when the claim clock starts.
- No clear answer to what must be isolated now, and what can stay up.

WHAT CONTAINMENT ADDS

Detection, completed by containment.

- + Sees which systems are actually being encrypted, as it happens.
- + Contains the account and the host precisely, without a blanket shutdown.
- + Additive to EDR. It completes the response the questionnaire assumes is there.

For the file: 'EDR deployed' is a detection answer. It says nothing about scope of propagation.

// 'WE HAVE BACKUP'

Backup decides whether recovery is possible. Containment decides **how much there is to recover.**

WHAT THE ANSWER TELLS AN UNDERWRITER

Recovery is being mistaken for resilience.

- 94% of attackers went for the backups; 57% succeeded. It is attacked first, deliberately.
- With backups compromised: 26% recover within a week, 67% pay, \$3M median recovery cost.
- Everything written since the last backup is gone permanently, restore or no restore.

WHAT CONTAINMENT ADDS

Protect the recovery plan, then shrink it.

- + BullWall pauses the running backup job before damaged files overwrite the good copies.
- + With backups intact the picture flips: 46% recover within a week, \$375K median cost.
- + The affected-file list scopes the restore: thousands of files, not millions.

Sophos, The Impact of Compromised Backups (2024, 2,974 ransomware victims); Sophos State of Ransomware 2024. Not containment versus backup: whether the backups survive long enough to be used.

// THE THREE LEGS OF RESILIENCE

Prevention and backup both have a gap only containment closes.

Resilience is not one control. It is three, and each one covers what the others miss.

01

Prevention

Blocks known attacks before they reach the estate. Misconfiguration, agent failures and zero-days still get through.

02

Containment

Built for the exact moment prevention and backup have already fallen short. Cuts the writes while they run.

03

Backup and recovery

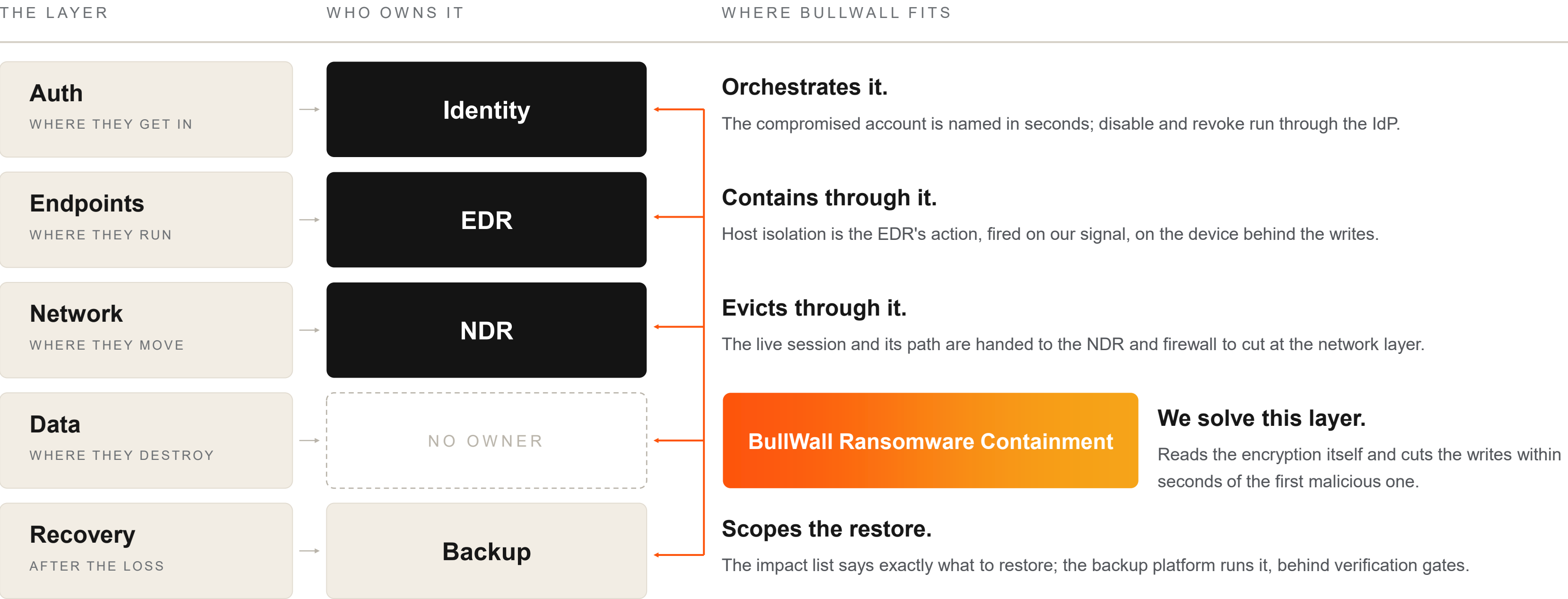
The safety net when everything else fails. Backups are targeted too, and there is always a gap between the last backup and the moment of attack.

Underwriting already asks about legs one and three. Leg two is the one that sets the size of the loss.

// HOW WE FIT THE INSURED'S STACK

Every layer has an owner. The data layer had none.

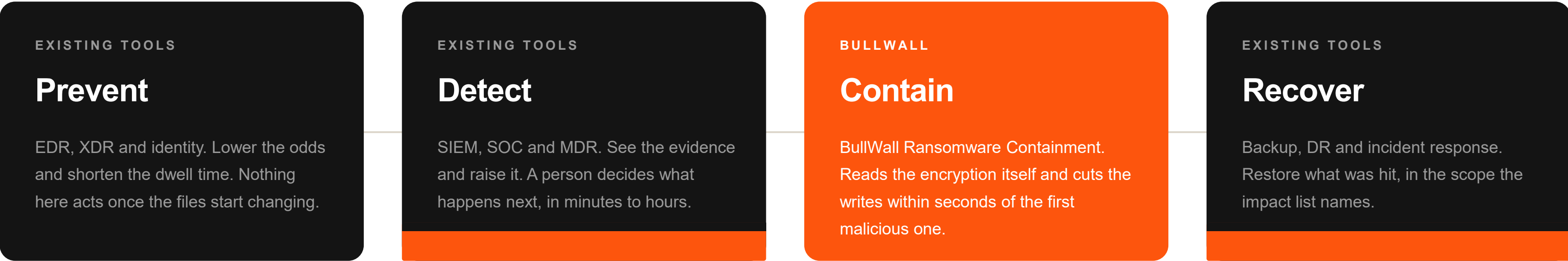
An insured's stack is well covered where the attacker comes in. BullWall Ransomware Containment takes the layer nobody owned.



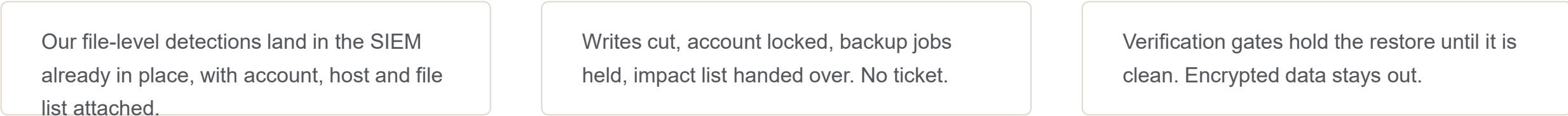
We do not replace a single one of them. We own the moment they cannot, and we use them to do it.

BullWall closes the gap between detection and recovery.

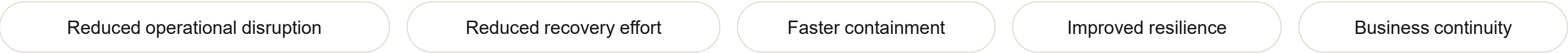
Prevention, detection and recovery stay essential, and stay where they are. BullWall takes the one stage none of them own, and feeds the two either side of it.



// BULLWALL ACTS ACROSS DETECT, CONTAIN AND RECOVER



MEASURE IT BY



BullWall reduces the business impact of ransomware by shrinking the time between detection and containment.

// AFTER AN ATTACK

Regulators increasingly assume you can **prove what happened**, not just that you tried to stop it.

Regulators want a timestamped, structured account of an incident, not a reconstruction assembled after the fact.

NIS2

Requires organisations to report significant incidents and demonstrate incident-handling capability, not only preventive controls.

DORA

Requires financial entities to evidence ICT incident response and recovery, against strict reporting timelines.

UK Cyber Security and Resilience Bill

Brings MSPs and data centres into scope, with a 24-hour initial report from awareness. In Lords committee, September 2026.

BULLWALL

Built-in incident record

A timestamped record of every affected file, account and host, generated as part of containment, not reconstructed afterwards. It supports the incident reporting these regimes require.

// THE NEXT UNDERWRITING QUESTION

The next underwriting question: **how far can an attack spread?**

TRADITIONAL UNDERWRITING QUESTIONS

- Is EDR deployed?
- Is MFA enabled?
- Are backups tested?
- Is incident response documented?
- Are vulnerabilities patched?

ADDITIONAL RESILIENCE QUESTIONS

- + How quickly can abnormal encryption or destructive behaviour be identified?
- + Can a compromised user or endpoint be isolated before it spreads widely?
- + Are file shares, servers, virtual infrastructure and cloud data included?
- + Can critical operations continue while an incident is investigated?
- + Can the organisation demonstrate and measure impact reduction?

Insurance exposure = **Probability of compromise** × **Scope of propagation** × **Duration of disruption**

Prevention changes the likelihood of an incident. Containment changes the size of the loss. For cyber insurers, resilience should not only mean restoring the business; it should mean stopping one compromise from becoming an enterprise-wide claim.

// TAKE THIS BACK TO YOUR TEAM

Three questions worth adding to the next underwriting conversation.

Not a pitch. Three questions that tell you how far an attack could spread inside an insured before anything stops it.

01 **If an AI agent, or a stolen account, started destroying data at machine speed right now, which control stops it, and how fast?**

02 **How many files are encrypted before anyone in the organisation notices?**

03 **Which controls can act without a person deciding first, at 02:00 on a Sunday?**

// WHERE TO GO FROM HERE

Three ways to take this **further**.

For carriers, brokers and the insureds they work with. No product conversation required for any of them.

01

Witness a containment test

A live encryption event stopped in seconds, on the infrastructure your insureds run.

02

Schedule a demo

See how BullWall works with a live demo and Q&A.

03

Talk about the carrier model

Talk to us about what that looks like for your book.

Andrew Grant, SVP EMEA · ag@bullwall.com

Thank you.

Built for when. Not if.

Andrew Grant, SVP EMEA, BullWall

ag@bullwall.com · bullwall.com