// SECURITY MATTERS ROUNDTABLE

How far does it get before it stops?

Beyond Prevention: Strengthening Operational Resilience Against Ransomware

// WHO WE ARE

A Danish-founded company with one focus: stopping ransomware in the act.

Since 2016, BullWall has focused on a single problem — what happens in the moments a ransomware attack is actually encrypting data.

2016

FOUNDED

1,000+ customers

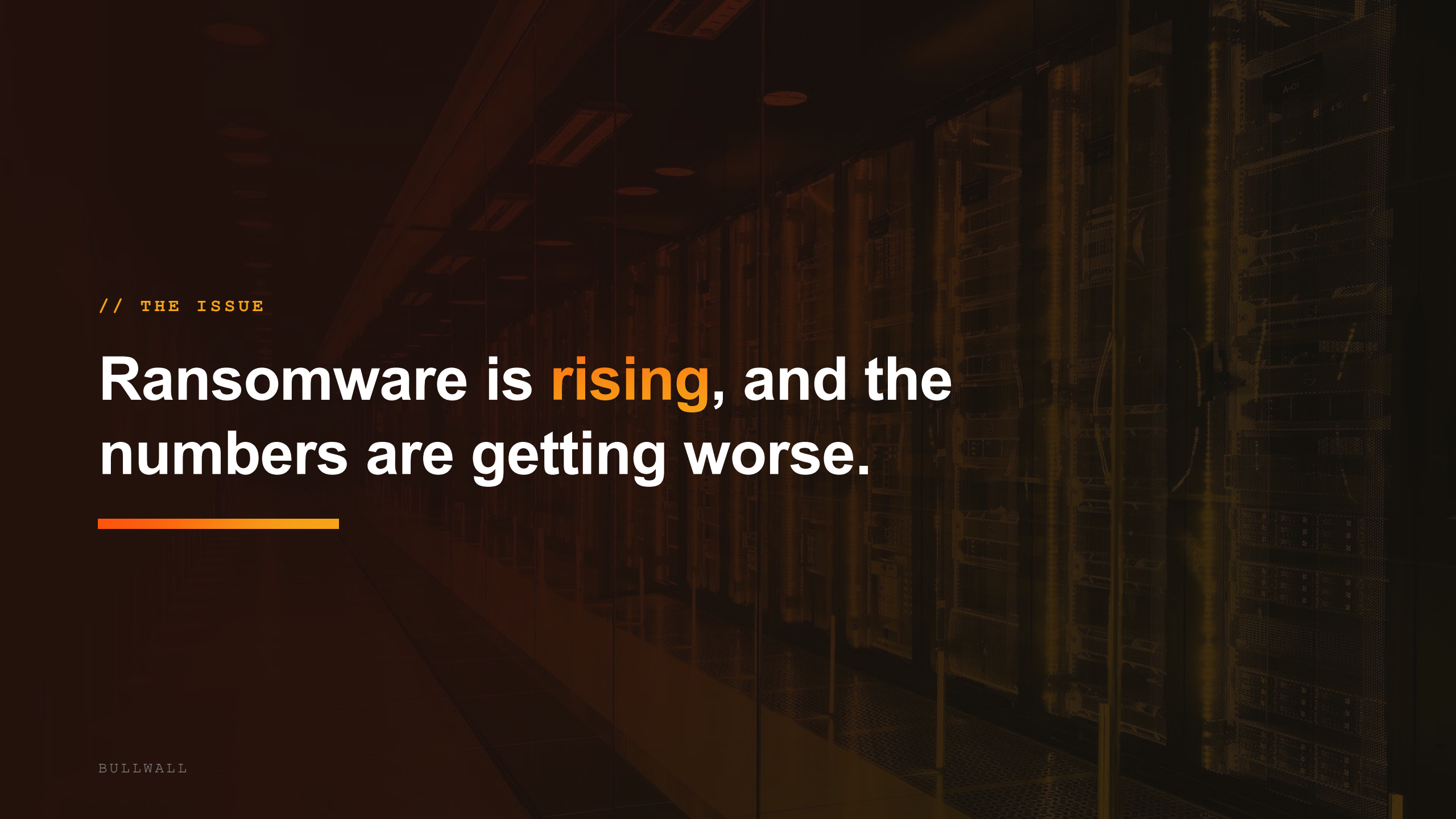
Across 19 countries, spanning critical-infrastructure sectors.

Single focus

Ransomware containment — not a broader security suite.

Headquartered in Denmark

With offices in the UK and US.



// THE ISSUE

Ransomware is rising, and the numbers are getting worse.

// THE NUMBERS

The gap between access and encryption has nearly closed.

Speed and stealth have compressed the response window to almost nothing.

22 seconds

Median 2025 handoff time from initial access broker to ransomware operator, down from over 8 hours in 2022 (Mandiant M-Trends 2026).

79%

Of initial access attacks are now malware-free (CrowdStrike 2025 Global Threat Report).

$2.5m

Highest median ransom demand of any country, 2025 (Sophos).

// WHY 22 SECONDS

It's not just AI that closed the gap — crime got organised.

None of these three is new on its own. Together, they're why access-to-encryption time keeps collapsing.

8 hours

2022 (Mandiant M-Trends 2026)

22 seconds

2025 (Mandiant M-Trends 2026)

Access brokers

Pre-verified access sold outright — no reconnaissance needed (biggest factor).

Automated playbooks

Scripted, repeatable operations — a process, not improvisation (major factor).

AI, at the edges

Sharper phishing and scripting upstream of the breach (growing factor).

// NOT ALL ATTACKS LOOK THE SAME

Ransomware doesn't arrive one way anymore.

Each style is built to slip past a different layer of the stack — which is exactly why no single control catches all of them.

Commodity RaaS	Ransomware-as-a-service kits let low-skill actors rent sophisticated attacks — constant new variants outpace signature-based tools.
Identity-based intrusion	Stolen credentials and legitimate admin tools leave nothing for antivirus or EDR to flag until encryption actually starts.
Double extortion	Data theft happens alongside encryption, so a clean recovery doesn't undo the exposure — prevention has to stop two actions, not one.

// THIS ISN'T HYPOTHETICAL

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

£300m

LOST OPERATING PROFIT

The call

A phone-based social-engineering attempt — no malware, no exploit.

The spread

The ransomware reached the VMware estate behind stores and online orders.

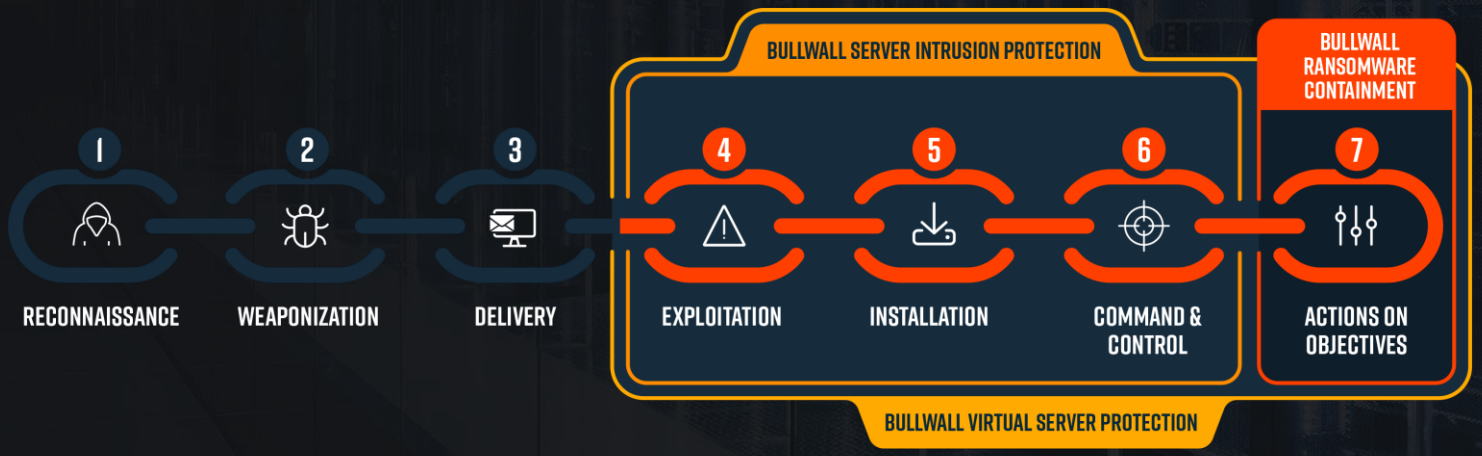
The source

M&S trading statement; Reuters, May 2025.

// WHERE WE SIT

We act at the final stage, when everything before it has already failed.

Reconnaissance, delivery and installation can all happen unnoticed. The attack still has to reach its final stage to do damage.



BullWall Ransomware Containment acts at the final stage

// THE THREE LEGS OF RESILIENCE

Prevention and backup both have a gap only containment closes.

Resilience isn't one control — it's three, and each one covers what the others miss.

Prevention

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

Containment

Built for the exact moment prevention and backup have already fallen short.

Backup & recovery

The safety net when everything else fails — but backups are targeted too, and there's always a gap between the last backup and the moment of attack.

// AFTER AN ATTACK

NIS2 and DORA both assume you can prove what happened, not just that you tried to stop it.

Regulators increasingly 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.
Built-in evidence	Automated, per-incident reporting mapped to GDPR, NIS2 and DORA — generated as part of containment, not bolted on afterwards.

// A METRIC WORTH KNOWING

Mean Time to Containment is the metric most incident reports skip.

MTTD tells you when you noticed. MTTR tells you when you recovered. MTTC tells you how long the damage kept spreading in between.

IBM: 181 days average to detect, then a further 60 days to fully contain — the gap real-time containment is built to shrink to seconds.

// TAKE THIS BACK TO YOUR TEAM

Four questions worth asking on Monday morning.

Not a pitch — just what's worth taking back to your own environment this week.

01	If ransomware bypassed every preventative control tomorrow, what would actually stop it?
02	How many minutes would your organisation have before a security incident became a business crisis?
03	Which part of your security strategy is designed to contain an attacker, rather than simply detect one?
04	What is your mean time to containment — not just mean time to detection?

// WHERE TO GO FROM HERE

Three ways to take this further.

Not a hard sell — just the paths people usually find useful after a session like this.

See it live

A short live demo of containment stopping an encryption event in real time.

Get assessed

Tests your exposure and shows where containment fits in your environment.

Just talk

Contact details are on the next slide — no product conversation required.

// LET'S CONTINUE THE CONVERSATION

Let's talk about what happens after prevention fails.

Andrew Grant, SVP EMEA, BullWall | ag@bullwall.com | bullwall.com