

TECH & AI CASE STUDY - SAAS - 2026

CSPM Remediation That Drove 1,400 Cloud Misconfigurations Down to 60

Based on a delivery engagement with Cirrostream

1,400 to 60

CLOUD MISCONFIGURATIONS

zero

CRITICAL FINDINGS

14 days to 48h

CRITICAL REMEDIATION TIME

95%

PRE-MERGE POLICY PASS RATE

A fillable practice edition: the full story, 8 actions,
6 reflections and a 90-day plan - work it with your team.

Free - no email required
emersontechnology.com

MAKE THIS PRACTICE BOOK YOURS

Work it, do not just read it

This practice book turns the Cirrostream case study into a working session for your team. Read the full story first - what happened, what was built and what it changed. Then tick the 8 actions you can commit to, write short answers to the 6 reflections, and finish with a 90-day plan. Every field in this PDF is fillable: open it in Adobe Acrobat Reader, Chrome, Edge or macOS Preview, type directly into the boxes and save.

YOUR NAME	ROLE
COMPANY	TEAM / DEPARTMENT
DATE	EMAIL (OPTIONAL)

MY GOAL FOR THIS PRACTICE SESSION

- 01 The story** - What happened at Cirrostream - before, during and after the project.
- 02 The results** - The numbers that changed, plus industry benchmarks from public research.
- 03 The 8-action checklist** - Tick boxes as your organization completes each step. Owner and date fields included.
- 04 The 6 reflections** - Fillable questions that pressure-test your own roadmap.
- 05 My 90-day plan** - Three fillable phase cards that turn this case study into your roadmap.

RUN IT AS A 90-MINUTE TEAM SESSION

25 min READ Read the story together. Ask everyone to note the one number that surprised them most.	40 min PRACTICE Work the 8-action checklist and the 6 reflections. Assign an owner and a date to every action you commit to.	25 min COMMIT Fill in the 90-day plan. One goal per phase, one number that tells you it worked. Book a review date before you leave the room.
--	--	---

THE STORY

What happened, and why it worked

01 The Company

Cirrostream is a 75-engineer analytics SaaS that arrived at its current shape through acquisition rather than a single organic roadmap. Two smaller platform companies joined the core product in as many years, one built on AWS and the other on Azure, and the combined business now serves mid-market and enterprise customers out of both clouds simultaneously. Around the engineering organization sit customer success, sales and a two-person security team responsible for everything from vendor questionnaires to incident response. The product itself is data-hungry: customers connect warehouses, streams and third-party sources, which means Cirrostream holds production datasets that several of its buyers would describe as commercially sensitive.

Growth changed the risk profile faster than the security program could follow. Each acquisition brought its own account structures, its own networking conventions and its own shortcut decisions made under startup deadlines. The engineering culture was strong — deployment frequency was high, code review was disciplined — but infrastructure changes flowed through with far less ceremony than application code. When enterprise procurement teams began asking pointed questions about cloud posture during security reviews, leadership realized the company had no single, defensible answer to a very basic question: how secure is our cloud configuration right now, and can you prove it?

02 Where Things Stood

The scanners already knew the answer, and it was uncomfortable. Cirrostream's cloud security tools carried 1,400 open misconfigurations across the two environments: public object storage buckets, over-permissive IAM roles, unencrypted data stores and exposed management ports. Roughly 180 of those findings were rated critical. The backlog had become a permanent fixture of the security team's dashboards — everyone agreed it was too large, nobody agreed on the order in which it should be attacked, and no finding had a named owner outside the security team itself.

The most damaging evidence came from an outside penetration test contracted during the renewal cycle for a major enterprise account. The tester chained a sequence of IAM privileges that no single severity score had flagged as urgent and reached production customer data in under four hours. None of the individual findings on that path looked dramatic in isolation; together they were a straight line from the internet to customer records. The test report landed the same quarter that the customer's procurement team made remediation of the sample findings an explicit condition of renewal — a contract worth \$2.1M in annual value.

Meanwhile the fix process itself was eroding trust on both sides. Engineers treated scanner output as background noise because severity scores bore little relationship to actual exploitability, and genuinely dangerous findings sat in the same undifferentiated queue as hundreds of informational items. Security, in turn, could not tell whether remediated findings stayed remediated, because fixes were applied by hand in cloud consoles and quietly drifted back within weeks. There was a scan backlog, but no agreed prioritization method, no ownership model and no definition of done that anyone trusted.

03 The Challenge

The challenge was not a shortage of visibility — the scanners were producing plenty of it. The challenge was that raw findings are not decisions. Cirrostream needed a way to rank 1,400 items by realistic attack path rather than vendor severity, assign each critical cluster to a team with the authority and time to fix it, and then prevent the same classes of misconfiguration from reappearing after every remediation push. Without those three mechanisms, any cleanup effort would be a treadmill: burn down the queue for a quarter, watch it refill, and repeat.

Commercial pressure compressed the timeline further. Enterprise buyers had begun demanding cloud security evidence during procurement as a standard step, and the \$2.1M renewal was contingent on remediating the specific findings documented in the customer's report. The Gartner prediction that through 2025 at least 99% of cloud security failures would be the customer's fault rather than the provider's was not an abstraction to Cirrostream — it was a description of their exact exposure, since IBM Security's 2024 breach research has repeatedly identified cloud misconfiguration among the leading initial attack vectors in multi-cloud environments. Any credible program had to produce both a safer environment and auditable proof of the improvement, on a schedule set by the customer's renewal calendar rather than the security team's backlog.

04 Discovery and Diagnosis

Emerson Technology opened with a two-week discovery sprint across both clouds, combining scanner exports, identity graph analysis and interviews with the platform teams who actually administered each environment. The audit confirmed that the scanners were technically correct — all 1,400 findings were real — but it also demonstrated why the backlog had never translated into risk reduction. Sorting by severity buried the ten findings that mattered most under hundreds that did not, and the identity analysis showed that a handful of privilege chains crossed account boundaries the scanner never connected.

Three structural findings shaped the program design. First, exploitability was a property of combinations, not items: internet exposure combined with privileged data access was what turned a moderate finding into a breach path, so prioritization had to be graph-based rather than list-based. Second, remediation regressed because the secure configuration was harder than the insecure one — engineers rebuilt infrastructure from console clicks and old examples, so every fix was a one-time event rather than a durable default. Third, the alert queue had lost credibility with engineering, which meant even accurate findings were being dismissed on sight. NSA and CISA's joint cloud security guidance attributes most cloud incidents to customer-side identity gaps and misconfigurations rather than provider failures, and Cirrostream's diagnosis was a textbook confirmation: the problems were fixable, but only through workflow changes, not another scanning tool.

05 The Solution

Emerson Technology deployed a cloud security posture management program with graph-based attack-path analysis at its center, so that every finding was ranked by how it combined with others — internet exposure joined to privileged data access — rather than by its raw severity score. Around that engine the team rebuilt the operating model in three layers.

Prioritization and ownership

The 200 highest-risk findings, selected by attack-path analysis rather than severity, went to named fix squads drawn from the platform teams that owned each environment. Each squad worked in two-week sprints with a clear definition of done: finding closed, root cause documented, and a regression guard in place. At the same time, low-impact and compensated findings were deliberately tuned out of the queue — marked as accepted with expiry dates and written rationale — so that the remaining alerts were ones engineers would take seriously. The 48-hour

SLA for anything critical forced the organization to fix root causes instead of clicking through alerts, and critical remediation time fell from 14 days to 48 hours as a result.

Guardrails in the delivery pipeline

The durable fix was architectural. Terraform modules wrapped the approved patterns for storage, IAM and networking, making the secure configuration the easiest path available — engineers copy existing patterns, so the defaults quietly decide the future posture. Open Policy Agent checks ran in CI on every infrastructure change, blocking non-compliant configurations before merge rather than discovering them in production weeks later. Auto-remediation handled the recurring classes outright: public storage buckets and wildcard IAM policies were reverted automatically, with notifications routed to the owning squad. Within a quarter, pre-merge policy checks passed on 95% of infrastructure changes on first attempt, which meant the guardrails were shaping behavior rather than blocking it.

The leadership cadence

A weekly risk scorecard went to engineering leadership tracking findings burn-down, open exception counts and pre-merge policy pass rates across both clouds. The scorecard did three jobs at once: it kept fix squads staffed after the initial urgency faded, it made the tradeoff when a team requested an exception visible to everyone, and it gave the security team a shared number with engineering instead of a private one. Procurement responses started drawing from the same source of truth, so the evidence sold to enterprise buyers was the same evidence engineering lived with daily.

06 The First 90 Days

The first month was spent almost entirely on prioritization and trust repair. Week one stood up the attack-path analysis across AWS and Azure and produced the ranked top-200 list, which the security lead walked through with each platform team in working sessions rather than shipping as a mandate. Weeks two through four launched the first four fix squads, deliberately staffed with the engineers who had built the affected systems, and retired or accepted-with-rationale more than 600 low-impact findings so that the queue engineers saw each morning was finally one they believed.

The second month concentrated on the delivery pipeline. Terraform modules for the ten most common infrastructure patterns went into the internal registry with documentation and worked examples, and the Open Policy Agent checks moved from audit mode to blocking mode after a two-week warning period. Auto-remediation went live for the two noisiest finding classes, and the first weekly scorecard reached engineering leadership in week six. The program hit its first real test that month: a squad's change to a data pipeline tripped a policy check that revealed a previously unknown privilege path, which was closed inside the SLA window and added to the module library so the class of problem could not return.

The third month was about proving the trend. Critical remediation time, tracked from SLA start to verified closure, dropped from 14 days to 48 hours; findings fell past the 1,000 mark on their way to 60; and the penetration-testing retest was scheduled for the end of the quarter. By day 90 the security team's weekly triage meeting had shrunk from an hour to fifteen minutes, because the queue it met to discuss had become short, trusted and owned.

07 The Results

Within six months, findings fell from 1,400 to 60, every one of the remainder low severity, and the environment has held zero critical findings since. Critical remediation time dropped from 14 days to 48 hours, and pre-merge policy checks now pass on 95% of infrastructure changes on first attempt. The penetration-testing retest could not reach customer data — the IAM chain that worked in four hours no longer existed as a path — and the \$2.1M renewal was signed with the security evidence attached. Procurement reviews that once stalled now start from a clean posture report instead of a defensive conversation.

METRIC	BEFORE	AFTER
Cloud misconfigurations	1,400	60
Critical findings	-	zero
Critical remediation time	14 days	48h
Pre-merge policy pass rate	-	95%

The operational changes compounded the numbers. Engineers stop worrying about a queue that no longer cries wolf, and the security team spends its limited headcount on novel risk instead of bucket number 412. New infrastructure inherits compliant patterns by default, so the findings count that once grew with every release now stays flat as the platform scales. The weekly scorecard outlived the remediation program itself and became the standing instrument leadership uses to judge whether cloud risk is being managed or merely scanned.

08 What Your Business Should Do

The pattern behind Cirrostream's turnaround is portable to any multi-cloud engineering organization, and none of it requires headcount the company did not already have. Start by ranking findings by attack path rather than severity: combine internet exposure, identity privilege and data sensitivity into exploitability scores, because raw severity rankings bury the ten findings that actually matter under hundreds that do not. Assign every critical finding to a named fix squad with a two-week sprint and a definition of done — named ownership is what converts scanner output into merged infrastructure changes. Wrap your approved patterns in Terraform or CloudFormation modules so the secure configuration is the easiest path available, and remember that engineers copy existing patterns, so your defaults quietly decide the entire future posture.

Block regressions where they start, in CI before merge, using policy-as-code checks such as Open Policy Agent or Checkov on every infrastructure change; preventing one bad merge is cheaper than remediating it across three environments. Auto-remediate the repetitive classes — public storage buckets and wildcard IAM policies head most lists — so human attention goes to novel risk rather than to bucket number 412. Tune out the noise deliberately by marking low-impact or compensated findings as accepted with expiry dates and rationale, because a queue engineers trust is worth more than a queue that is complete. Set a 48-hour SLA for criticals and staff for it; speed targets force teams to fix root causes instead of clicking through alerts. Finally, publish a weekly burn-down scorecard showing findings trend, exception counts and pre-merge pass rates — visible momentum is what keeps fix squads staffed after the first sprint ends. Run this sequence against your own cloud using the action checklist in this practice book, and let the reflection questions reopen the review every quarter: how many misconfigurations sit in your scanners right now, how many could an attacker chain together, and when an enterprise buyer asks for cloud security evidence, will your team scramble or attach a report?

REAL-WORLD PROOF & BENCHMARKS

Gartner has famously predicted that through 2025, at least 99% of cloud security failures will be the customer's fault rather than the provider's. - Gartner

IBM's Cost of a Data Breach research has repeatedly identified cloud misconfiguration among the leading initial attack vectors in multi-cloud environments. - IBM Security, 2024

Joint NSA and CISA cloud security guidance reportedly attributes most cloud incidents to customer-side identity gaps and misconfigurations rather than provider failures. - NSA/CISA joint guidance

THE PRACTICE PAGES

The 8-action checklist

Work through the list with your team. Tick each box as your organization completes the step, and fill in an owner and a target date so every action has a name and a deadline.

☐

1. Rank findings by attack path

Combine internet exposure, identity privilege and data sensitivity into exploitability scores. Raw severity rankings bury the ten findings that actually matter under hundreds that do not.

OWNER

TARGET DATE

STATUS

--	--	--

☐

2. Assign critical findings to fix squads

Give each critical cluster a named owner and a two-week sprint rather than a backlog ticket. Named ownership is what converts scanner output into merged infrastructure changes.

OWNER

TARGET DATE

STATUS

--	--	--

☐

3. Wrap approved patterns in modules

Publish Terraform or CloudFormation modules that make the secure configuration the easiest path available. Engineers copy existing patterns, so your defaults quietly decide the entire future posture.

OWNER

TARGET DATE

STATUS

--	--	--

☐

4. Block regressions in CI pre-merge

Run policy-as-code checks like Open Policy Agent or Checkov on every infrastructure change. Preventing one bad merge is cheaper than remediating it across three environments.

OWNER

TARGET DATE

STATUS

--	--	--

☐

5. Auto-remediate the repetitive classes

Automate fixes for recurring finding classes such as public storage buckets and wildcard IAM policies. Human attention should go to novel risk, not to bucket #412.

OWNER

TARGET DATE

STATUS

--	--	--



6. Tune out the noise deliberately

Mark low-impact or compensated findings as accepted with expiry dates and rationale. A queue engineers trust is worth more than a queue that is complete.

OWNER

TARGET DATE

STATUS

--	--	--



7. Set a 48-hour SLA for criticals

Commit to closing critical cloud findings within two days and staff for it. Speed targets force teams to fix root causes instead of clicking through alerts.

OWNER

TARGET DATE

STATUS

--	--	--



8. Publish a weekly burn-down scorecard

Show leadership findings trend, exception counts and pre-merge pass rates every week. Visible momentum is what keeps fix squads staffed after the first sprint ends.

OWNER

TARGET DATE

STATUS

--	--	--

AFTER THE CHECKLIST: OUR TOP 3 PRIORITIES

From the eight actions above, write down the three you will start first - and the single number you expect each one to move. Three priorities with owners beat eight without any.

PRIORITY 1 NUMBER IT SHOULD MOVE	PRIORITY 2 NUMBER IT SHOULD MOVE	PRIORITY 3 NUMBER IT SHOULD MOVE
--	--	--

THE PRACTICE PAGES

Reflections for your team

Use these questions in your next planning session and type short answers into the boxes. The gaps you find are usually the fastest wins.

Q1. How many cloud misconfigurations are sitting in your scanners right now — and how many could an attacker chain together?

Q2. If a penetration tester reached your production data in four hours, which finding would they thank you for?

Q3. Can you name the owner of every critical cloud finding in your queue today?

Q4. What percentage of your infrastructure changes pass security checks on first attempt — and is that number even measured?

Q5. Which recurring finding classes could automation retire this quarter, freeing engineers for real risk work?

Q6. When an enterprise buyer asks for cloud security evidence, does your team scramble or attach a report?

THE PRACTICE PAGES

My 90-day plan

Finish the session by committing to a plan. Three phases, one goal each, one number that tells you it worked. Bring this page to your next leadership review - or to a free consultation with Emerson Technology, and we will pressure-test it with you.

Days 1-30 Focus: audit and alignment

PRIMARY GOAL**KEY ACTIONS****HOW WE MEASURE SUCCESS****OWNER**

Days 31-60 Focus: build and prove

PRIMARY GOAL**KEY ACTIONS****HOW WE MEASURE SUCCESS****OWNER**

Days 61-90 Focus: scale and measure

PRIMARY GOAL

KEY ACTIONS

HOW WE MEASURE SUCCESS

OWNER

Tip: save a copy per team so each group keeps its own answers. Revisit the reflections every quarter - the questions stay the same even as the numbers move.

BOOK THE REVIEW BEFORE YOU CLOSE THE BOOK

Plans without a review date drift. Before you close this practice book, agree on when you will come back to these pages, who will run that session, and when you will check the numbers again. If you want an outside pair of eyes, bring this page to a free consultation with Emerson Technology and we will pressure-test the plan with you.

REVIEW DATE	REVIEWED BY	NEXT CHECK-IN
------------------------------------	------------------------------------	--------------------------------------

Ready for a transformation like Cirrostream's?

Emerson Technology designs and builds the data, AI, cloud and automation systems behind results like these. On a free consultation call we will map this exact playbook to your business - your data, your constraints, your numbers.

Book a free consultation

support@emersontechnology.com

or start online: emersontechnology.com/contact