PITWALL

Competitive Battlecard Set

Version 1.0 | Internal Sales Use Only | 2026

Four battlecards: Reach Security, Panaseer, Tidal Cyber, Nagomi

Competitive Landscape Overview

The security stack effectiveness market is real and growing, but it is not yet a defined category with a single vendor owning the space. Four companies are the primary threats in competitive deals. None of them own the same white space Pitwall owns.

Pitwall's Defensible Position

The core claim: Pitwall is the only platform that tracks every alert from generation to resolution, identifies which controls are producing noise, and delivers specific configuration recommendations. That is the white space.

The Competitive Map

COMPETITOR	WHAT THEY OWN	PRIMARY BUYER	THREAT LEVEL
Reach Security	Misconfiguration and configuration drift detection	Security architect, SecOps engineer	HIGH — closest functional overlap
Panaseer	Compliance and GRC control reporting	CISO, GRC team, audit	MEDIUM — different buyer, different budget
Tidal Cyber	Threat-informed coverage mapping (MITRE ATT&CK)	Threat intel team, security architect	MEDIUM — strategic vs. operational
Nagomi	CISO board reporting and security effectiveness storytelling	CISO for executive communication	LOW — no SOC Manager story

The One-Line Summary for Every Deal

Reach fixes misconfigurations. Tidal maps coverage gaps. Panaseer reports on compliance. Nagomi builds board presentations. Pitwall fixes the alert problem none of them address.

When a prospect says they are already using one of these tools, the response is always the same: ask them what their false positive rate is on their top five controls right now. None of the above can answer that question. Pitwall can, in 14 days, with no infrastructure changes.

THEME 3

- Founded 2023 with limited production deployments. Pitwall's 45 percent result comes from live customer data. In a deal where credibility matters, proof beats positioning.

Objection Handling

PROSPECT SAYS	PITWALL RESPONSE
Our CISO just started using Nagomi for board reporting.	Nagomi tells a story about your security program. Pitwall generates the numbers that make the story credible. The Shakedown data integrates directly into the narrative your CISO is already building.
We need better board communication, not another monitoring tool.	The Shakedown delivers a boardroom-ready report in 14 days with no infrastructure changes. That report is board communication. The difference is it is built on actual performance data from your controls.
Nagomi already shows our security effectiveness.	Ask Nagomi which specific control in your stack reduced false positives by the most last quarter. They cannot answer that. We can, in 14 days, with zero infrastructure changes.

Proof point: The CISO needs the story. The SOC Manager needs the fix. Pitwall delivers both in 14 days. Nagomi delivers the story without the fix. In a deal where both buyers have a voice, Pitwall wins.

Standing Rules for Competitive Conversations

- Never disparage a competitor directly. Name the difference, not the deficiency.
- Lead with the Shakedown. It is the structural advantage none of them can match for speed and zero obligation.
- The 45 percent false positive reduction in 30 days is the proof point. Use it specifically, not generally.
- In multi-vendor environments, position Pitwall as the operational layer underneath whatever they already have.
- If a prospect has Panaseer or Nagomi, frame Pitwall as complementary, not competitive. Different budget, different buyer.

PITWALL vs. **REACH SECURITY**

They fix misconfigurations. We fix alert performance.

REACH SECURITY IS	REACH SECURITY IS NOT
Configuration posture management	Alert performance monitoring
Drift detection and remediation	Resolution tracking from generation to close
Focuses on how tools are configured	Identifies why alerts are firing
Addresses underutilized features	Addresses what controls are generating noise
AI-assisted remediation workflows	No-infrastructure-change assessment

Head-to-Head

DIMENSION	PITWALL	REACH SECURITY
Primary question	Are your controls configured correctly?	Are your controls configured correctly?
Entry point	Configuration audit and drift detection	Configuration audit and drift detection
Alert visibility	Flags misconfig that could cause noisy alerts	Does not track alert volume, FP rate, or resolution
SOC Manager value	Reduces rework from configuration drift	Does not give time back on active alert triage
Assessment offer	No equivalent free assessment	14-day Shakedown, 20 controls, boardroom report
Deployment	Requires integration with security tools	No infrastructure changes, runs in 14 days
Funding stage	Series A	Series A

Why Pitwall Wins This Deal

THEME 1

- Reach is a misconfiguration tool. Pitwall is an alert performance tool. A control can be perfectly configured and still generate 500 false positives a day. Reach does not see that. Pitwall does.

THEME 2

- The Shakedown closes deals Reach cannot open. No infrastructure changes, 14 days, boardroom-ready report. Reach has no equivalent offer. Our prospect can start Pitwall today and see results before their next board meeting.

THEME 3

- The SOC Manager story is ours. Reach talks to security architects who own configuration. Pitwall talks to SOC Managers who own the alert queue. Different buyer, different pain, different champion.

Objection Handling

PROSPECT SAYS	PITWALL RESPONSE
We already use Reach.	Reach solves misconfiguration. Pitwall solves alert performance. A control can be perfectly tuned and still flood your queue with false positives. Run the Shakedown and see what Reach is not showing you.
Reach covers the same problem.	Ask Reach what the false positive rate is on your CrowdStrike deployment. They cannot tell you. We can, in 14 days, with no infrastructure changes.
We do not have budget for another tool.	The Shakedown has no cost and no obligation. You get a boardroom-ready report at the end. If the data does not justify the investment, you walk away with better visibility than you had before.

Proof point: Early adopters reduced false positive volume by 45 percent in 30 days. No infrastructure changes. No additional headcount. That result is not available from a misconfiguration tool.

PITWALL vs. **PANASEER**

They report on controls. We fix them.

PANASEER IS	PANASEER IS NOT
Continuous controls monitoring (CCM)	SOC Manager operational tool
Compliance and GRC reporting platform	Alert performance diagnostics
250+ framework-mapped metrics	Configuration recommendation engine
Audit and regulatory evidence generation	14-day hands-on assessment
CISO and board reporting focus	Built for daily SOC workflows

Head-to-Head

DIMENSION	PITWALL	PANASEER
Primary question	How are your controls performing against frameworks?	Are my controls compliant with our chosen framework?
Primary user	CISO, GRC team, audit function	CISO, compliance, audit teams
SOC Manager relevance	High — daily operational tool for alert management	Low — a reporting layer, not an operational one
Output	Specific configuration fix recommendations	Compliance scores and framework gap reports
Assessment offer	14-day Shakedown, zero obligation	Enterprise implementation project
Time to value	14 days to first insight	Weeks to months for full onboarding
Deployment complexity	No infrastructure changes required	Agentless but requires extensive data connector setup

Why Pitwall Wins This Deal

THEME 1

- Panaseer is a compliance reporting platform. The CISO uses it to answer audit questions. The SOC Manager never sees it. Pitwall lives in the SOC Manager's daily workflow. We are operational, not ornamental.

THEME 2

- Panaseer tells you how you score. Pitwall tells you what to fix. A CISO who already uses Panaseer for board reporting is still flying blind on which controls are generating the alert flood. Those are not the same product.

THEME 3

- Speed is the differentiator in competitive deals. Panaseer is a months-long implementation. The Shakedown delivers a boardroom-ready report in 14 days with no infrastructure changes. No Panaseer deal closes that fast.

Objection Handling

PROSPECT SAYS	PITWALL RESPONSE
Our CISO uses Panaseer for board reporting.	Panaseer answers the compliance question. Pitwall answers the operations question. The SOC Manager who runs your alert queue is not looking at Panaseer dashboards. They need Pitwall.
Panaseer already gives us control visibility.	Ask Panaseer which specific control generated the most false positives in the last 30 days. Ask them what configuration change would fix it. Pitwall answers both questions.
We need compliance reporting, not another monitoring tool.	Pitwall and Panaseer solve different problems for different buyers. The data from the Shakedown actually improves your Panaseer compliance scores by fixing the underperforming controls.

Proof point: Pitwall and Panaseer are not competing for the same budget. Pitwall is a SOC Manager tool. Panaseer is a CISO reporting tool. In accounts where Panaseer is already live, Pitwall is the missing operational layer underneath it.

PITWALL vs. **TIDAL CYBER**

They map coverage gaps. We fix alert noise.

TIDAL CYBER IS	TIDAL CYBER IS NOT
Threat-informed defense platform	Alert performance monitoring
MITRE ATT&CK-aligned coverage mapping	False positive reduction
Built by former MITRE leadership	SOC operations tool
Identifies gaps vs. known adversary techniques	Configuration recommendation engine
Strategic threat coverage analysis	Quick-turn assessment offer

Head-to-Head

DIMENSION	PITWALL	TIDAL CYBER
Primary question	Are your controls covering the threats targeting you?	Does your defense coverage map to known adversary techniques?
Framework anchor	Alert performance data from live controls	MITRE ATT&CK adversary behavior mapping
Primary user	SOC Manager, security operations team	Threat intel team, security architect, CISO strategy
Output	Configuration fixes and alert reduction	Coverage gap analysis and adversary mapping
Assessment offer	14-day Shakedown, 20 controls, boardroom report	Platform evaluation, no equivalent free assessment
Time to value	14 days to first insight	Ongoing strategic analysis tool
Deployment	No infrastructure changes	Platform integration with existing tools

Why Pitwall Wins This Deal

THEME 1

- Tidal answers a strategic question: are we covered against the right threats? Pitwall answers an operational question: are our controls actually working? A control can cover the right ATT&CK techniques and still generate 300 false positives a day. Tidal does not see that.

THEME 2

- Different buyers. Tidal sells to threat intelligence teams and security architects thinking about long-term coverage strategy. Pitwall sells to SOC Managers who need the alert queue under control this quarter. In a deal, they are rarely competing for the same budget.

THEME 3

- The Shakedown is a structural advantage. No infrastructure changes, 14 days, boardroom-ready report. Tidal has no equivalent entry point that moves at that speed.

Objection Handling

PROSPECT SAYS	PITWALL RESPONSE
We use Tidal to manage our ATT&CK coverage.	Tidal tells you if you have coverage. Pitwall tells you if that coverage is working. A control mapped to the right techniques still fires false positives if it is misconfigured. Run the Shakedown alongside Tidal.
Our threat intel team drives tool decisions here.	The Shakedown is designed for the SOC Manager, not the threat intel team. Different buyer, different champion. We are not asking the threat intel team to replace Tidal.
We are focused on coverage gaps, not alert volume.	Coverage gaps and alert volume are different problems. Your coverage map can look complete while your analysts are drowning in noise. The 45 percent false positive reduction in 30 days came from accounts where the coverage map showed no gaps.

Proof point: In accounts where Tidal Cyber is already deployed, Pitwall is the missing operational layer. Tidal shows the map. Pitwall shows whether the territory is actually held.

PITWALL vs. **NAGOMI**

They tell the story to the board. We fix the controls.

NAGOMI IS	NAGOMI IS NOT
Security effectiveness measurement	SOC Manager operations tool
Automated CISO board reporting	Alert queue management
Defense and threat data integration	Configuration fix recommendations
Security program ROI storytelling	Hands-on 14-day assessment
Stakeholder communication platform	False positive reduction engine

Head-to-Head

DIMENSION	PITWALL	NAGOMI
Primary question	How do we demonstrate security program value to stakeholders?	How do we show the board our security program is effective?
Primary user	CISO, VP Security for board and exec communication	CISO for board reporting and exec communication
SOC Manager value	High — direct operational improvement for the analyst team	None — SOC Managers do not use Nagomi
Output	Configuration fixes and measurable alert reduction	Executive dashboards and security program narratives
Assessment offer	14-day Shakedown, 20 controls, zero obligation	No equivalent rapid assessment offer
Time to value	14 days	Tool setup and data integration required
Funding stage	Series A (founded 2023)	Series A (founded 2023)

Why Pitwall Wins This Deal

THEME 1

- Nagomi builds the story for the boardroom. Pitwall generates the data that makes the story true. A CISO presenting security program effectiveness to the board needs actual performance data, not just a well-designed dashboard. The 45 percent false positive reduction from the Shakedown is boardroom-ready content.

THEME 2

- Nagomi has no SOC Manager story. Their product does not live in the analyst's daily workflow. Pitwall does. In a competitive deal, the SOC Manager champion runs the Shakedown and presents the results upward. Nagomi needs the CISO to champion it from the top down.