NOPSEC

FINANCIAL SERVICES CASE STUDY

When Cyber Risk Is Financial Risk

How a North American proprietary trading firm turned scattered vulnerability data into decisive, audit-ready action with NopSec CTEM.

EXECUTIVE SUMMARY

In proprietary trading, decisions get made on clear signals, not noise. The security team at this North American proprietary trading firm wanted its vulnerability management practice to work the same way. The hardest part of the job was never finding vulnerabilities. It was prioritizing the ones that actually mattered and proving that remediation was reducing risk.

The team chose NopSec's Continuous Threat Exposure Management (CTEM) platform to prioritize what matters and to report on remediation with a single, clear view of risk. The result is a repeatable operating rhythm that turns raw scanner output into decisive action, and into the reporting the firm's regulators expect.

CHALLENGES

Plenty of data. No clear way to act on it.

A proprietary trading firm runs on speed and uptime. Its security team is responsible for reducing risk across that environment without slowing the business, and for proving to auditors and regulators that the work is getting done.

A mountain of findings, no way to prioritize

The problem was never a shortage of findings. Scanners surfaced far more than the team could realistically act on, with no reliable way to tell which of them actually mattered to this environment. Harder still, the team had no way to know whether its remediation work was reducing risk or only keeping pace with the backlog. Effort was going in, but its effect on the firm's real exposure was impossible to see.

Action without the evidence to prove it

Even where the team knew what to fix, getting it done and proving it was done were separate problems. Remediation was not orchestrated across the people who owned it, and with vulnerability data split between a commercial scanner and a separate third-party tool, there was no single view of where an item stood or whether a fix had actually closed the risk. Confirming that came down to manually lining up scanner results before and after patching, one reconciliation at a time. For a regulated firm, that is the costly gap: action without evidence does not satisfy an auditor, who needs to see not only that the work was done, but that it worked.

Company Profile

INDUSTRY
Financial services (proprietary trading)

REGION
North America

REGULATORY ENVIRONMENT
NYDFS and other financial-sector regulators

TEAMS USING NOPSEC
Security, GRC, and business unit stakeholders

SOLUTION
NopSec CTEM Platform

ABOUT NOPSEC

NopSec's Continuous Threat Exposure Management platform unifies vulnerability data with prioritization and remediation workflow. Security teams use it to move from scattered findings to verified, reportable action.

> "Data is useless if you can't do anything with it. NopSec lets us actually act on the information we have, because it offers clarity."

SECURITY PROGRAM MANAGER · PROPRIETARY TRADING FIRM

SOLUTION

From scanner output to a repeatable operating rhythm

The firm adopted the NopSec CTEM platform to bring prioritization, reporting, remediation workflow, and assignment into one place. For this team, the platform's value is not that it produces more data. It is that it makes the data actionable, and that the people who depend on it find it clear and easy to use.

One repeatable operating rhythm

NopSec is built into how the security team works each cycle. What used to be manual reconciliation is now a defined process the team runs the same way every time.

1

Filter the dashboard

Surface open critical and high-severity vulnerabilities not yet in a plan, by team.

2

Triage by detection date

Separate what predates the last quarterly patch cycle from what came after it.

3

Plan and ticket

Review the fix, add it to a remediation plan, and open a ticket to the infrastructure team.

4

Track to closure

Work open plans, confirm remediation, and roll items into new plans as projects evolve.

From data to decisive action

The platform's core value to the team is action. NopSec helps them act on the data, and because the interface is clear and easy to use, the team understands not just what to do but how to do it. That clarity is the difference between a list of findings and a plan the business can execute.

> "NopSec helps us take action on the data."
>
> SECURITY PROGRAM MANAGER · PROPRIETARY TRADING FIRM

Built for every team that touches risk

NopSec is not only a security tool at the firm. Security, GRC, and business unit stakeholders work from the same platform, with the goal of bringing infrastructure and IT teams onto it as well. Each group uses it for vulnerability management and for clear visibility into its own security posture. The team points to a set of needs it treats as equally important, and refuses to rank:

- **Compliance for auditors and regulators, including NYDFS**
- **Collaboration across remediation teams**
- **Visibility into risk**

RESULTS

A defined process, and reporting that stands up to a regulator

Centralizing vulnerability management on NopSec replaced manual, one-off reconciliation with a process the team runs the same way every cycle. The security team can now see which vulnerabilities are outstanding and confirm that remediation has actually closed them. Reporting on that progress, for leadership and for regulators, comes from the same place. The Security Program Manager describes NopSec simply, as the firm's vulnerability management reporting platform: one intuitive source for prioritizing remediation and demonstrating progress across Security, GRC, and the business.

- Manual reconciliation replaced with a repeatable workflow
- Clear confirmation that remediation closed the risk
- Outstanding vulnerabilities surfaced and prioritized
- Reporting ready for auditors and regulators, including NYDFS
- One shared view across Security, GRC, and business teams

BY THE NUMBERS

60+ hrs/mo
Reduction in reconciliation time

50%
Improvement in mean time to remediation

2 days/mo
Reporting effort saved

Ready to take a clearer position on risk?

NopSec works with the security stack you already run, turning scattered vulnerability data into prioritized, verifiable action and reporting your stakeholders can trust.

Schedule a Demo