

SolarWinds SUNBURST: Impact and Remediation Strategy

Independent consulting case study built from public sources

Cole Blahut | July 2026



A trusted update channel became the attack path

<18,000

customers believed to have
installed the tainted update

\$52.6M

gross incident expenses
disclosed for 2020–2021

\$26M

securities class action
settlement

Recommendation Invest an estimated \$1.2M–\$2.8M in build integrity, identity controls, and detection, starting with four quick wins in 30 days. That is roughly 2–5% of SolarWinds' disclosed gross incident expenses.

The attackers were inside for months before anyone noticed



Almost nine months passed while the tainted updates went unnoticed, according to Reuters reporting.

Few were targeted, but thousands were exposed

300,000

SolarWinds customers
overall

~33,000

Orion customers
notified

<18,000

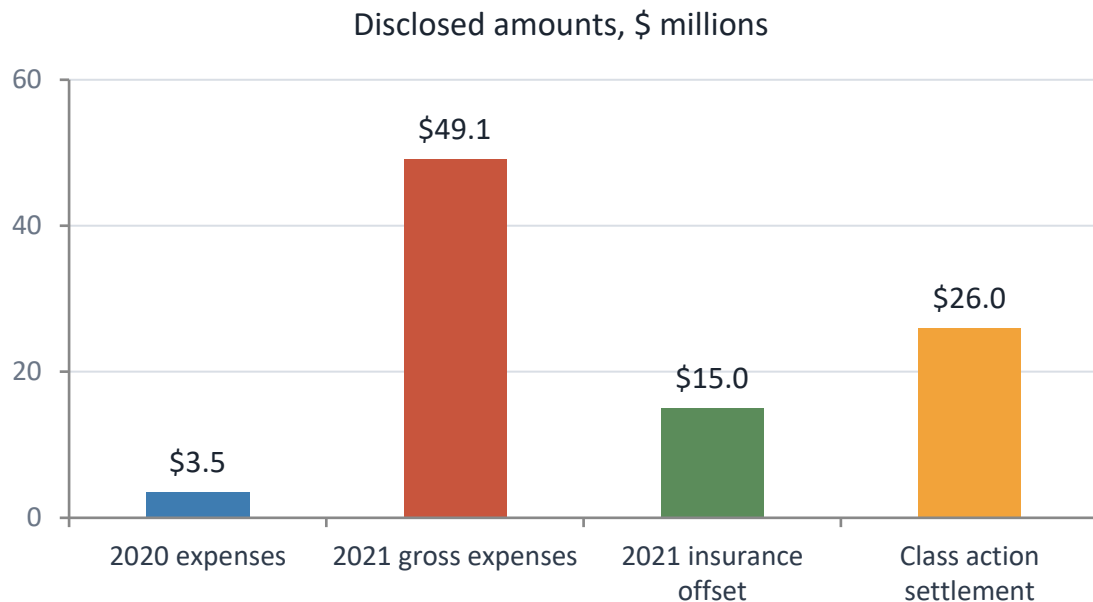
believed to have
installed the tainted
update

9 + ~100

federal agencies and
private companies
compromised

The attackers were selective. A trusted update channel gave them a foothold on thousands of networks, and they chose which ones to exploit.

Direct costs ran to tens of millions, and the stock fell about 35%



Settlement was expected to be reimbursed by D&O insurers.

-17%

stock drop on Dec 14, 2020 (to \$19.62)

-35%

approximate decline by end of Dec 2020, per the SEC

Root causes span technology, process, people, and governance

Technology

No independent integrity checks on the build, so tainted code shipped in signed updates. The SEC also alleged a VPN gap.

Process

The SEC alleged password policy, secure development, and access controls fell short of public claims.

People

Internal slides cited by the SEC described thin security expertise and inappropriate access to critical systems.

Governance

A 2019 assessment showed practices for 21 of 325 NIST 800-53 controls, while public statements claimed more (alleged).

SEC claims were mostly dismissed in July 2024 and the case ended without admission in November 2025.

Quick wins in identity first, then pipeline and detection



A 90-day roadmap sequences quick wins ahead of big builds

Days 0–30

- R2 MFA and privileged access
- R3 Secrets vault and rotation
- R7 Incident-response plan and tabletop
- R8 Insurance limits review

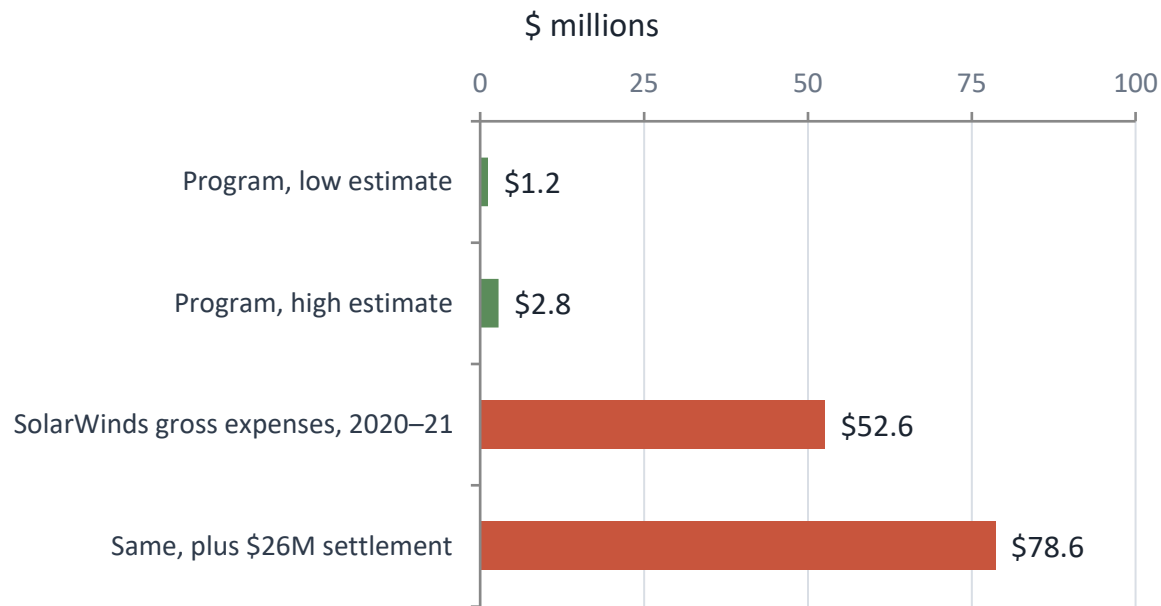
Days 31–60

- R4 Managed devices only for remote access
- R6 Framework baseline and testing
- R5 Start logging on dev and build

Days 61–90

- R5 Detection live across build and release
- R1 Pilot parallel, signed builds on one product
- Report results to the board

The program costs a small share of one incident



2-5%

program cost versus
SolarWinds' \$52.6M gross
expenses

Program costs are planning assumptions, not vendor quotes. The comparison is illustrative, not a probability estimate.

Decision requested and lessons for leadership

Decision requested

1. Approve the 30-day quick wins (R2, R3, R7, R8)
2. Fund a parallel-build pilot on one product (R1)
3. Report security to the board quarterly

What the case teaches

- Update channels are attack paths
- Public claims must match internal reality
- Insurance covered under a third of 2021 expenses