

# MEMORANDUM

**TO:** Executive Leadership Team, hypothetical mid-sized B2B software vendor  
**FROM:** Cole Blahut  
**DATE:** July 11, 2026  
**RE:** Lessons from the SolarWinds SUNBURST breach and a 90-day remediation roadmap

*Independent case study built from public sources (SEC filings, court and government reports, press). The client is hypothetical, and the roadmap cost ranges are the author’s planning assumptions, not vendor quotes.*

## BOTTOM LINE

Like SolarWinds, we ship software into customer networks through an update channel. In 2020, attackers turned SolarWinds’ channel into a delivery route for malware. We recommend a \$1.2M–\$2.8M program, starting with four quick wins in the first 30 days, to harden our build pipeline, identity controls, and detection. That is roughly 2–5% of the \$52.6M in gross incident expenses SolarWinds disclosed for 2020–2021.

## WHAT HAPPENED

- Attackers compromised SolarWinds’ internal environment and software build process. SolarWinds said they had access for at least nine months before an October 2019 test run; trojanized Orion updates then shipped between March and June 2020.
- The breach surfaced on December 13, 2020, when FireEye detected it. SolarWinds notified about 33,000 Orion customers, and fewer than 18,000 were believed to have installed the tainted update.
- The U.S. government identified 9 federal agencies and about 100 private companies as compromised. Attackers chose targets selectively rather than exploiting every installation.

## BUSINESS IMPACT

| Measure                 | Disclosed figure and context                                                                                                           |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| 2020 incident expenses  | \$3.5M pretax (SolarWinds FY2021 Form 10-K)                                                                                            |
| 2021 incident expenses  | \$49.1M gross, offset by \$15.0M of insurance receipts and expected proceeds (FY2021 Form 10-K)                                        |
| Securities class action | \$26M settlement, paid March 2023; the company expected its D&O insurers to reimburse it in full                                       |
| Stock price             | Fell about 17% on December 14, 2020 (to \$19.62); the SEC cites roughly a 35% decline by month-end                                     |
| Regulatory              | SEC sued in October 2023; most claims dismissed July 2024; case dismissed with prejudice November 2025 with no admission of wrongdoing |

Gross disclosed expenses for 2020–2021 total \$52.6M (\$78.6M including the settlement). This excludes lost sales and defense costs not itemized in the filings.

## ROOT CAUSES

- Technology:** a build pipeline without independent integrity checks, so malicious code could be inserted before signing. The SEC alleged a known VPN weakness that allowed access from unmanaged devices.
- Process:** the SEC alleged SolarWinds did not follow its own password policy or a secure development lifecycle as publicly described, and granted excessive admin rights.
- People and governance:** the SEC cited a 2019 internal assessment showing a program or practice for only 21 of 325 NIST 800-53 controls (about 6%) while public statements described strong practices. These are allegations; the court dismissed most of them and the case ended without admission.

## RECOMMENDATIONS, PRIORITIZED

| #  | Action                                                                      | CIS v8 | Impact | Est. cost     | Timing          |
|----|-----------------------------------------------------------------------------|--------|--------|---------------|-----------------|
| R1 | Harden build pipeline: ephemeral, parallel builds; signed build steps; SBOM | 16     | 5 of 5 | \$600K–\$1.2M | Pilot by day 90 |
| R2 | MFA and privileged-access controls on VPN, admin, and build systems         | 5, 6   | 5 of 5 | \$80K–\$200K  | Days 0–30       |
| R3 | Secrets vaulting, credential rotation, enforced password policy             | 5      | 4 of 5 | \$40K–\$120K  | Days 0–30       |
| R4 | Remote access only from managed, compliant devices                          | 12, 13 | 4 of 5 | \$100K–\$300K | Days 31–60      |
| R5 | Central logging and detection across dev, build, and release systems        | 8, 13  | 5 of 5 | \$250K–\$600K | Days 31–90      |
| R6 | Framework baseline, independent testing, board-level reporting              | 18     | 4 of 5 | \$75K–\$200K  | Days 31–60      |
| R7 | Incident-response plan, tabletop exercise, security-to-disclosure process   | 17     | 4 of 5 | \$50K–\$150K  | Days 0–30       |
| R8 | Review cyber and D&O insurance limits against realistic loss                | n/a    | 3 of 5 | \$10K–\$30K   | Days 0–30       |

## COST VERSUS RISK

The full program costs an estimated \$1.2M–\$2.8M. SolarWinds carried \$15M of cyber insurance, which covered less than a third of its 2021 gross expenses alone, so insurance limits are not a substitute for prevention. The comparison is illustrative, not a probability estimate: the point is that the program’s cost is small next to the scale of a single supply-chain incident.

## DECISION REQUESTED

- Approve the four 30-day quick wins (R2, R3, R7, R8).
- Fund a pilot of parallel, signed builds on one product line (R1).
- Adopt quarterly security reporting to the board so public statements match internal assessments.

## SOURCES

SolarWinds Form 10-K FY2021 (sec.gov); SolarWinds securities class action settlement notice (blbglaw.com/cases/solarwinds); Hunton Andrews Kurth, “Judge Dismisses Most of SEC Case Against SolarWinds and Its CISO” (July 2024); Winston Taylor, “SEC and SolarWinds Litigation Dismissed Following Joint Stipulation” (Dec. 2025); WilmerHale and BCLP analyses of the SEC complaint (Nov. 2023); SecurityWeek, “SolarWinds Shares More Information on Cyberattack Impact”; TechTarget, “White House: SolarWinds Hack Impacted 9 Fed Agencies, 100 Entities”; Reuters via Business Insurance, “Hacked IT firm says fewer than 18K customers compromised”; SolarWinds, “Setting the New Standard in Secure Software Development” (2022).