Build Environment Risk Governance

A Zero-Trust Framework for Software Supply Chain Visibility

Amina Emenena

George Washington University | School of Engineering & Applied Science

BUILDFLOWLABS

// THE_PROBLEM

Software Supply Chain Under Attack

742%
increase in supply chain attacks since 2019

$4.45M
average cost of a data breach

66%
of consumers won't trust a breached company

Key Incidents

2020	**SolarWinds**	Build system compromised; 18,000+ organizations affected
2021	**Codecov**	CI tool breach exposed secrets across thousands of repos
2025	**tj-actions**	GitHub Action compromise leaked secrets from 23,000+ repos

// THE_GAP

SBOMs Are Not Enough

What SBOMs Cover

- Component inventory
- Known vulnerabilities (CVEs)
- Dependency relationships
- License compliance

The "WHAT"

What's Missing

- Build tool integrity
- Pipeline access controls
- Credential exposure risks
- Workflow configuration security

The "HOW"

Regulatory mandates (EO 14028, SEC 2023) focus on component transparency but leave build environments ungoverned.

// LITERATURE_REVIEW

Four Research Streams

// 01

Business Impact of Breaches

Stock declines of 2.1% within two days (Cavusoglu et al., 2004). Sales growth drops for 3+ years post-incident (Kamiya et al., 2021). 66% of consumers lose trust after breach (Ponemon, 2022).

// 02

Supply Chain Risk Management

Rising dependency attacks (Ohm et al., 2020). Build system compromise among most severe vectors (Ladisa et al., 2023). 22% of attacks now target CI/CD pipelines (ReversingLabs, 2025).

// 03

SBOM Limitations

SBOMs document the "what" not the "how" (Koishybayev et al., 2022). Improved CVE response (Xia et al., 2023) but blind to build tool compromise, credential leaks, and workflow misconfiguration.

// 04

Security Friction Problem

Developers bypass controls that impede productivity (Braz et al., 2022). Alert fatigue causes systematic under response (Thomas et al., 2021). Zero-touch design as emerging principle (Rashid et al., 2023).

// THEORETICAL_LINK

The Trust-Revenue Connection

Build Environment Security Posture → **Customer Trust** → Revenue Retention

Morgan & Hunt (1994)	Trust directly correlates with purchasing behavior, loyalty, and willingness to pay premium prices.
Sirdeshmukh et al. (2002)	Consumer trust is a leading indicator of loyalty in relational exchanges — trust erosion precedes churn.
Reichheld & Schefter (2000)	Trust erosion precedes customer departure by months or years as contracts expire and renewals approach.

A supply chain compromise weaponizes the vendor-customer relationship itself — categorically different from other breach types.

// THEORETICAL_FOUNDATION

Zero-Trust Applied to Build Environments

NIST 800-207 Core Principle

No system component should be implicitly trusted. Continuous verification is required.

Verify Everything

Every tool, config, and credential access is treated as potentially compromised

Link to Business

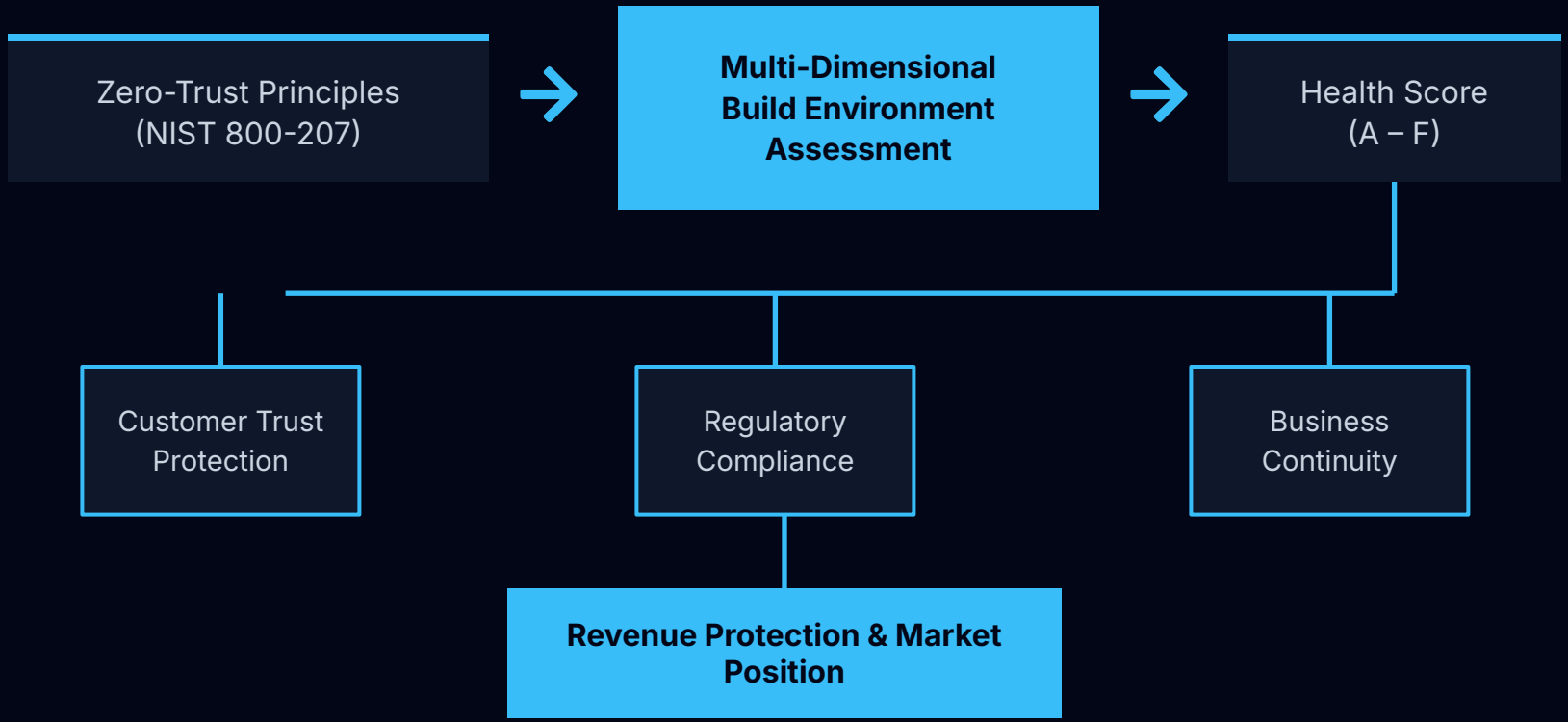
Security posture maps directly to customer trust and revenue outcomes

Measure Continuously

Multi-dimensional scoring enables trending and benchmarking over time

// FRAMEWORK_OVERVIEW

From Zero-Trust Principles to Revenue Protection



// RESEARCH_PROPOSITIONS

Research Propositions

P1 Build environment governance will identify violations undetected by SBOM-based compliance, revealing previously unquantified business risk.

P2 Zero-touch architectures that require no developer workflow changes will achieve higher organizational coverage than traditional tools.

P3 Composite health scoring will facilitate more effective stakeholder risk communication than raw technical metrics.

P4 Organizations governing build environments proactively will retain stronger customer trust after industry-wide incidents.

// METHODOLOGY

Design Science Research Approach

Design Requirements

Zero-Touch Operation

Collects metadata via organizational APIs with no changes to repos or workflows

Scalable Coverage

Evaluates all repositories through a single integration point

60-Day Pilot

Repositories	30
Platforms	Multiple
Portfolio	Customer-facing apps, internal tools, infra

Data Collected

- Initial health scores across all repos
- Policy violation frequencies by category
- Score progression over 60 days
- Qualitative feedback from security & compliance stakeholders

// RESULTS

Zero-Touch, Full Coverage

100%

Repository Coverage
on Day One

No workflow modifications required

3.2s	average scan time per repository
<2 min	full organization assessment
0	developer-facing changes required

Validates Proposition 2: Zero-touch architecture achieves comprehensive coverage without adoption friction.

// RESULTS

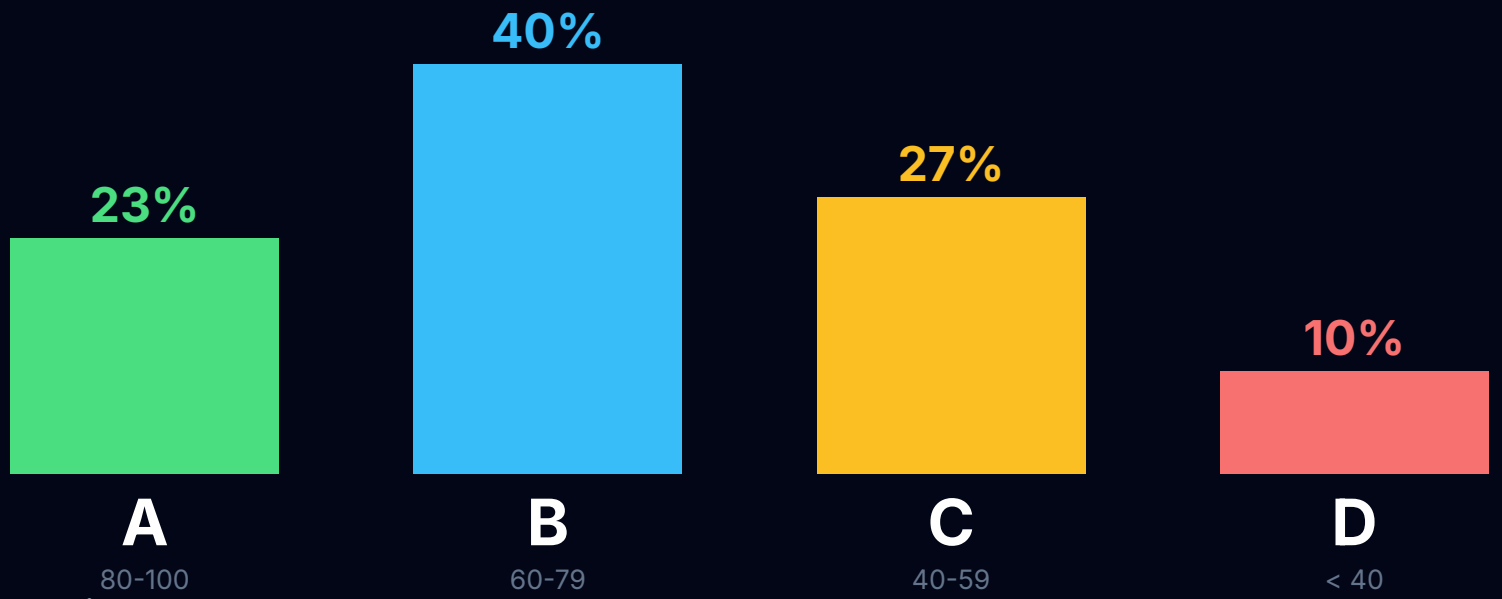
What I Found: Pervasive Misconfigurations

Violation Category	Prevalence	Traditional Detection	Business Risk
Supply chain injection vectors	67%	Not monitored	Customer compromise
Governance control gaps	45%	Partial	Audit failure
Access control deficiencies	38%	Partial	Unauthorized access
Separation of duties issues	12%	Monitored	Compliance violation

> 67% of repositories had supply chain injection vulnerabilities — yet only 12% would trigger traditional compliance alerts. That's 55% of risk completely invisible to existing governance.

// RESULTS

Health Score Distribution



Key Insights

- No repositories achieved perfect scores — universal room for improvement
- 10% of repos scored below 40 — concentrated risk requiring immediate attention
- Lowest-scoring repos shared traits: older codebases with legacy configurations

// KEY_FINDING

67%

of repositories vulnerable to supply chain compromise

12%

would trigger traditional compliance alerts

55% of supply chain risk is invisible to current governance.

Organizations relying solely on traditional compliance monitoring may believe their security posture is stronger than evidence supports.

// BUSINESS_IMPLICATIONS

Security Risk Is Revenue Risk

Revenue Impact Model

Mid-sized vendor: $50M ARR

3.9% churn increase post-breach = **~$2M** lost revenue per year

Recurring annually until trust is rebuilt + remediation + regulatory penalties + acquisition costs

Revenue Impact Channels

Customer Retention
3.9% avg churn increase compounds annually

New Acquisition
Security assessments now standard in vendor selection

Pricing Power
Weak security forces price competition over value

Contract Terms
Enterprise customers require security warranties

// STAKEHOLDER_FEEDBACK

What Practitioners Said

> *"Finally gives us something concrete to put in the board deck."*
>
> — Compliance Officer — Board Communication

> *"Turned a vague concern into an actionable backlog."*
>
> — Security Engineer — Prioritization Clarity

Additional Themes

- Customer Assurance — health scores as evidence for security questionnaires and vendor assessments
- Audit Evidence — continuous scanning documentation supports SOC 2 and regulatory inquiries

// LIMITATIONS

Honest Assessment & Next Steps

Single Organization	30 repositories in one tech org; cross-industry validation needed
No Incident Correlation	Did not measure link between scores and actual incident rates
Trust-Revenue Link	Theoretical connection not empirically tested
Platform Coverage	GitHub only; GitLab, Azure DevOps, self-hosted systems need study
Change Management	How teams negotiate remediation priorities needs further research

Most Promising Direction

// CONCLUSION

Three Takeaways

1

Build environments are a critical blind spot

67% of repos had exploitable misconfigurations invisible to traditional governance. SBOMs alone are insufficient.

2

Zero-touch governance works

100% organizational coverage on day one with zero developer friction. Comprehensive security need not conflict with velocity.

3

Security risk is revenue risk

Supply chain compromise transforms your product into an attack vector against customers. Proactive governance protects trust and revenue.

The question is not whether to invest in supply chain governance, but whether organizations will act proactively or reactively — after customers have already begun their exit.

Thank You

Questions & Discussion

Amina Emenena

George Washington University | School of Engineering & Applied Science

amina@buildflowlabs.com