CleanStart

BEYOND SPEED

securing the software supply chain in 2026

Dec 2025

Executive Summary

2025 was the year software supply chain risk became measurable. The increase in upstream attacks, CI/CD compromises and container image manipulation revealed how modern software is assembled and where it can be disrupted. Trust was often assumed. That assumption was exploited.

This report brings together signals from 2025 and outlines what enterprises must prepare for in 2026. It is designed for leaders across technology, security and business domains who need to convert supply chain awareness into operational capability.

"As we close 2025, one thing is unmistakable. Speed is no longer the differentiator. Proof is. In 2026, enterprises will be judged not by how fast they ship software, but by how clearly they can demonstrate what their software is built on..."

> **Supply chain security has become a business capability , not a security function.**

NJ

Nilesh Jain

CEO & FOUNDER, CLEANSTART

THE REPORT IS STRUCTURED IN THREE PARTS:

Part 1 What changed in 2025 and how risk shifted upstream

Part 2 Where the impact will be felt most across industries

Part 3 What readiness must look like in 2026

2026 will reward the teams that can see risk early, trace it fast and prove software integrity with evidence. The shift has already begun. This report is intended to help enterprises prepare before it becomes a requirement.

INTRODUCTION

THE STATE OF CYBER SECURITY

2025

1

Part 1: The State of Software Supply Chain Security

A Year Defined by Supply Chain Escalation

2025 marked a decisive shift in how software risk entered organizations. Supply chain attacks became active, upstream and scalable. Attackers no longer targeted the network perimeter. They entered through dependencies, build pipelines, maintainer accounts and container images. Trust was assumed. That assumption was exploited.

Key Attack Trends Observed in 2025

Upstream focus

Attacks originated during build and package inclusion rather than at runtime

Dependency poisoning

Compromised libraries entered CI pipelines without detection

Maintainer account takeover

Credential theft used to publish trojanized versions

Container reuse amplification

Malicious code scaled instantly across environments

AI-enabled variants

Automated scripts increased attack speed and volume

Shift in Attack Vectors

Supply chain attacks did not enter through networks in 2025. They entered through dependencies, CI/CD agents, unverified container images and maintainer accounts. The most frequently targeted entry points are captured below.

> “Security failures increasingly originate outside organizational boundaries. When software pipelines, third-party code and automated infrastructure become the foundation of delivery, they also become the dominant source of operational risk.”
>
> Dominant source of operational risk.
>
> WN **Wendy Nather**
> IDC RESEARCH FELLOW

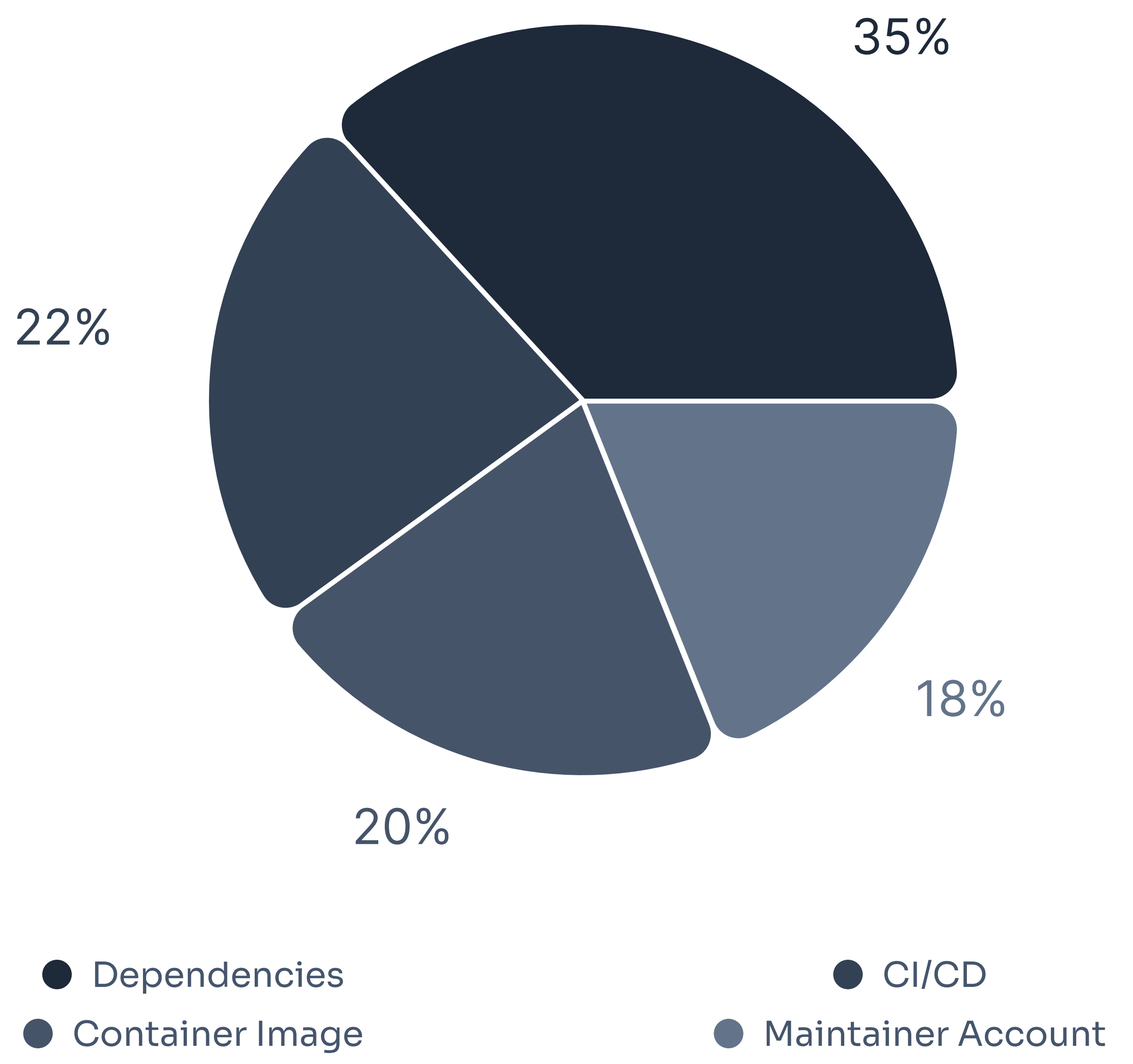
What this indicates

Attack vectors increasingly focused on dependencies and build pipelines. This marked a strategic shift in 2025 where attackers preferred to enter earlier in the lifecycle before traditional security controls could detect them.

- Dependencies have become the "new perimeter"
- CI/CD and build containers emerged as strategic targets
- Maintainer health became a real risk factor
- Containers amplified impact due to reuse and automated promotion

Attack Vector Distribution

2025 DATA

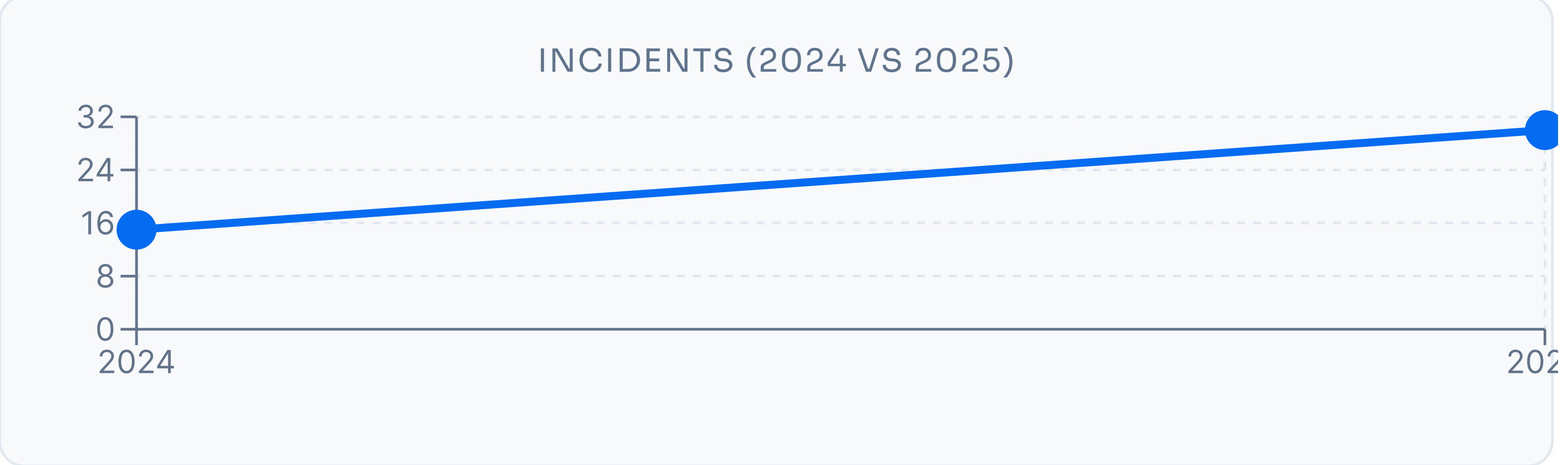


Notable Supply Chain Incidents of 2025

Incident	What Happened	Why It Matters
Shai-Hulud npm campaign	Self-propagating worm across JavaScript ecosystem	Install-time attacks bypass runtime defenses
Docker Hub image poisoning	Official-looking containers contained malicious code	Verified and trusted are not the same
CI/CD credential leaks	Secrets leaked during build stage	Pipelines became direct targets
Unmaintained repos exploited	Attackers watched for inactivity to take over libraries	Maintainer health must be treated as risk

Attack Frequency Increased Sharply

Reports showed a sustained rise in supply chain attacks. These were not isolated incidents but recurring patterns.



Attack frequency more than doubled, indicating supply chain compromise is a consistently exploitable surface.

> “Attackers are no longer just targeting users or endpoints. They are targeting the entire digital supply chain, from identities to code to infrastructure.”
>
> **Targeting the entire digital supply chain.**

AJ

Ann Johnson
CVP SECURITY, COMPLIANCE & IDENTITY
MICROSOFT

> “What were once isolated supply chain attacks are now recurring at scale. October 2025 marked the highest sustained activity we have observed across npm, open-source ecosystems and cloud infrastructure.”

Combined research findings

- Supply chain attacks more than doubled compared to 2024
- October 2025 recorded the highest number of known incidents
- Over 70 percent of surveyed organizations experienced at least one supplier-related incident
- Fewer than half monitored more than 50 percent of their extended supply chain
- Global economic loss is projected to reach 60 billion dollars by end of year

Containers Multiplied the Blast Radius

Container adoption accelerated across industries. That acceleration also amplified risk because once a malicious component entered a base image, it propagated rapidly across microservices and environments.

Regulatory Attention Accelerated

Observation

Observation	Implication
Public base images widely used	Trust established by convention not verification
Dependency bloat increased	SBOMs often missing or incomplete
Runtime security detected threats too late	Build-time trust became essential
CI/CD tokens often exposed	Build environments became high-value targets

> “Third-party and software supply chain risk has moved from an operational issue to a board-level governance concern due to the scale and systemic nature of recent attacks.”
>
> From operational issue to board-level governance concern
>
> G **Gartner**
> 2025 SUPPLY CHAIN CYBERSECURITY OUTLOOK

CleanStart Observed Insight

Across enterprise environments, provenance and build attestations remain inconsistent, even where container security tooling is mature. This gap between assumed trust and verifiable proof is one of the defining software supply chain risks enterprises will need to address in 2026.

Conclusion

2025 proved that supply chain security can no longer begin at runtime. It must be established before the first build, before the first deployment, and before trust is assumed. That shift is not optional in 2026. It will define which organizations are prepared and which become case studies.

Sector Exposure Became More Noticeable

Sector	Why the Risk Increased	Common Impact
BFSI	Compliance obligations and API integrations	Transaction risk and regulatory penalties
E-Commerce	Rapid deployments and open-source reliance	Checkout failures and customer trust erosion
Media & Entertainment	AI-driven pipelines and high-value content	IP loss or content manipulation

Procurement, insurance and audit frameworks began shifting toward requiring evidence of software origins, SBOM and provenance inquiries surfaced in compliance reviews. Supply chain security is no longer an operational conversation. It has become part of commercial eligibility.

The impact will not be uniform.

The same vulnerability will land differently in BFSI, E-Commerce and Media and Entertainment. To understand where risk becomes disruption, review the supply chain dynamics and sector-specific sector dynamics.

SECTOR IMPACT

2

PART 2 : Sector Impact and Threat Maps

How Risks Translate into Business Impact Across Industries

While supply chain and container risks are universal, their **business impact is highly uneven** . The same vulnerability can produce different outcomes depending on:

- Deployment speed
- Integration density
- Compliance pressure
- Exposure to customer data
- Operational traceability

2025 showed that exposure is shaped more by **how a business operates** than by **what technology it uses**.

To understand how technical issues become financial and reputational risk, it is necessary to view the software supply chain **through sector dynamics rather than technical categories**.

The sections that follow illustrate how **one attack pattern can produce three very different consequences** across three industries that define the digital economy in 2026:

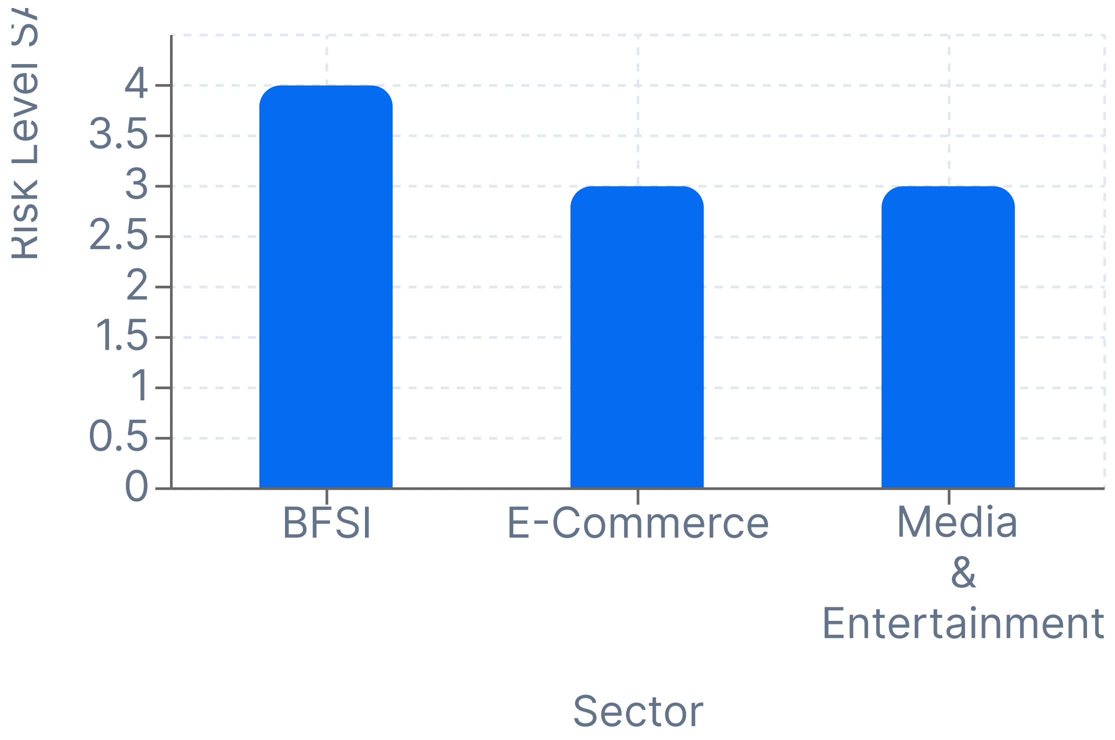
Sector	Primary Business Dependency
BFSI	Trust and compliance as operating licenses
E-Commerce	Revenue at risk with every deployment
Media & Ent.	Integrity, licensing and IP protection

What follows is not only threat modeling. It is **a view into how risk becomes cost, how compromise becomes public, and how lack of traceability becomes operational drift**.

> “Financial institutions are facing growing supervisory scrutiny around software provenance, third-party dependency validation, and build integrity as part of operational resilience.”
>
> F **FS-ISAC**
> 2025 REPORT

> “Dependency sprawl and microservice complexity are now among the leading contributors to large-scale checkout outages and failed rollbacks during peak traffic events.”
>
> E **Ecommerce Europe**
> 2025 REPORT

Sector Risk Exposure (Illustrative)



Illustrative model based on publicly reported incidents, regulatory pressure, deployment velocity, and dependency complexity. Not a statistical risk score.

Interpretation

- BFSI faces regulatory and systemic impact
- E-Commerce faces high deployment velocity and customer trust risk
- Media and Entertainment faces intellectual property and AI-driven integrity challenges

BFSI (Banking, Financial Services and Insurance)

High integration density. High compliance burden. High consequence of failure.

Public Registry → Package → CI/CD → Container → Production Cluster

- **Maintainer Hack**
- **Credential Leakage**
- **Data Exfiltration / Transaction Risk**
- **Install-Time Script Theft**
- **Unsigned Image**

Business Impact

- Unauthorized access to customer data
- Transaction manipulation or fraud
- Loss of regulatory clearance
- Audit failure due to lack of traceability

LEADERSHIP FOCUS FOR 2026

- Can provenance be demonstrated for all production containers?
- Can all affected workloads be found and rebuilt in less than one day?
- Is supply chain security part of compliance and procurement policy?

E-Commerce

High-speed deployments. Frequent dependence on open-source frameworks. Customer trust is directly linked to application stability.

Open Source → Feature Build → Container → Microservices → User Session

- **Trojan UI Lib Risk**
- **Missing SBOMs**
- **Outdated Package**
- **Lateral Movement**

Business Impact

- Checkout abandonment
- Revenue loss downtime
- Credential theft
- Difficult rollback

LEADERSHIP FOCUS FOR 2026

- Can compromised components be traced across microservices
- Is rollback automated and repeatable
- Can supply chain security become a guardrail rather than a bottleneck

> “Digital content pipelines now depend on complex chains of third-party software, build systems, and distribution platforms. When those software supply chains are compromised, the result is not just a security breach. It is piracy, content manipulation, and direct revenue loss.”
>
> **Motion Picture Association**
> SECURITY ADVISORY 2025

Media and Entertainment

High-volume content processing. Growing AI usage. High legal and IP impact if content integrity is compromised.

Threat Path

AI Model → Encoding Pipeline → Container Cluster → CDN → End User

- **Compromised Model**
- **Tampered Metadata**
- **IP Leakage or Legal Dispute**
- **Image Drift**
- **Content Distribution**

Business Impact

- IP loss or piracy
- AI-generated content manipulation
- Licensing disputes and liability risk
- Brand and distribution disruption

LEADERSHIP FOCUS FOR 2026

- Can provenance be proven for content transformation
- Can compromised workloads be isolated instantly
- Can threat detection correlate content with its source code lineage

Conclusion

The same vulnerability does not create the same outcome in every sector. Business models determine blast radius. Velocity, integration and compliance pressure shape exposure. The difference between inconvenience and disruption will depend on how quickly each sector can trace and rebuild. But while risk varies across industries, **the path to resilience requires the same foundation.** Whether the priority is regulatory clearance, operational continuity or customer trust, the ability to govern the supply chain must move from awareness to operational control.

STRATEGIC READINESS

3

PART 3 : Strategic Readiness Framework for 2026

From Awareness to Operational Control

Supply chain and container security cannot be treated as isolated technical initiatives. To operate safely in 2026, enterprises will need **end-to-end lifecycle control** across ingestion, build, image management, deployment and recovery.

This requires more than tools. It requires **operational discipline**, **governance as code**, and **evidence that can travel with the artifact**.

Five Pillars of Readiness

VISIBILITY

Know what is running and where it came from

CONTROL

Reject untrusted code before deployment

PROVENANCE

Record origin and maintain lineage

RESILIENCE

Rebuild and redeploy quickly

TRUST AS CAPABILITY

Demonstrate security with evidence

> These pillars form the foundation of enterprise readiness. Each one must evolve from practice to proof.

Life Cycle based operational Blueprint

- **Ingestion**
  Mirror packages and monitor maintainers
- **Build**
  Harden CI/CD agents and remove static credentials
- **Image Creation**
  Use signed base images and attach SBOMs

- **Registry & Promotion**
  Approve only verified images
- **Deployment**
  Enforce policy & block unverified components
- **Response**
  Maintain Searchable component inventory for rapid rebuild

> Security must begin at ingestion, not only at runtime. The build stage will become the new trust boundary in 2026.

Maturity Model for Enterprises in 2026

01 **NO VISIBILITY**
HIGH EXPOSURE

02 **SCANNING ONLY**
FALSE CONFIDENCE

03 **SBOM AVAILABLE BUT NOT ACTIONABLE**
AUDIT RISK

04 **SIGNED AND VERIFIED BUILDS**
REDUCED EXPOSURE

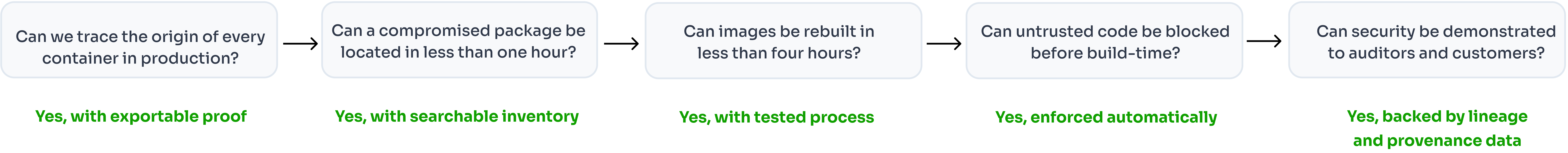
05 **PROVENANCE AND TRACEABLE LINEAGE**
FAST RECOVERY

06 **CONTINUOUS ATTESTATION WITH AI GUIDANCE**
SCALABLE TRUST AS A COMPETITIVE ADVANTAGE

The industry baseline in 2025 sits between Level 1 and Level 2. Competitive advantage will emerge atLevel 4 and above.

Executive Readiness Scorecard

To be considered resilient in 2026, enterprises should be able to answer these questions with data:



Can we trace the origin of every container in production? → Can a compromised package be located in less than one hour? → Can images be rebuilt in less than four hours? → Can untrusted code be blocked before build-time? → Can security be demonstrated to auditors and customers?

Yes, with exportable proof

Yes, with searchable inventory

Yes, with tested process

Yes, enforced automatically

Yes, backed by lineage and provenance data

These are no longer aspirational. They are becoming contractual.

Strategic Advantage for Enterprises That Adapt

Organizations that embed supply chain and container security early will:

- Reduce audit and insurance costs
- Qualify for regulated markets
- Recover faster from failures
- Gain customer preference based on trust
- Shift security from overhead to differentiator

> **Speed will continue to matter. Trust will become currency.**

Conclusion

Awareness is no longer the problem.

Operational control is now the mandate.

Provenance, rebuild speed and traceability must become measurable capabilities.

In 2026, leadership will be judged less by what they knew and more by how fast they could act.

> "
>
> Trust will need proof. Proof will need process. Process must be built into the lifecycle.

Where CleanStart Fits in the 2026 Shift

Supply chain security should not be a late-stage inspection. It must be built into how software is ingested, assembled and trusted. The industry is moving toward **evidence-driven security** and every enterprise will need a way to prove what their software is built on.

That is where CleanStart aligns with the shift ahead.

CleanStart enables teams to:

Build from verified sources with provenance that travels with the artifact

Use hardened base images built from source and aligned with compliance benchmarks

Generate SBOM and lineage automatically as part of the build process

Rebuild workloads quickly when upstream components are compromised

Treat rust as a build property rather than as a post-deployment inspection

CleanStart was built on the belief that **speed should not sacrifice integrity** and that **trust must be measurable** to become operational.

2026 will reward the teams that can prove what they deploy.

CleanStart exists to make that possible at scale.

The Imperative for 2026

2026 will not only test software security. It will test the credibility of how software is built.

The enterprises that will lead the next phase of digital transformation will not be the fastest. They will be the ones who can **prove integrity at scale** and treat trust as a capability rather than an assumption.

> **The era of assumed safety is over. The era of measurable trust has begun.**

Reference List

Supply Chain Attack Trends

01 Cyble – Supply Chain Attacks Have Doubled in 2025

02 Verizon DBIR – Third Party & Supply Chain Breaches

03 SecurityScorecard – Supply Chain Cybersecurity Trends

04 RevenueLabs – 2025 Software Supply Chain Security Report

itusa.org

Business and Economic Impact

05 Cybersecurity Ventures – Global Supply Chain Breach Cost Forecast

06 IBM – Cost of a Data Breach Report 2025

07 Allianz Risk Barometer 2025 – Top Business Risks

08 Marsh McLennan – 2025 Cyber Risk Index

AI in Attack and Defense

09 ENISA – AI Threat Landscape 2025

10 MITRE – Secure AI with Threat-Informed Defense

11 Gartner – 2025 Security Operations Hype Cycle