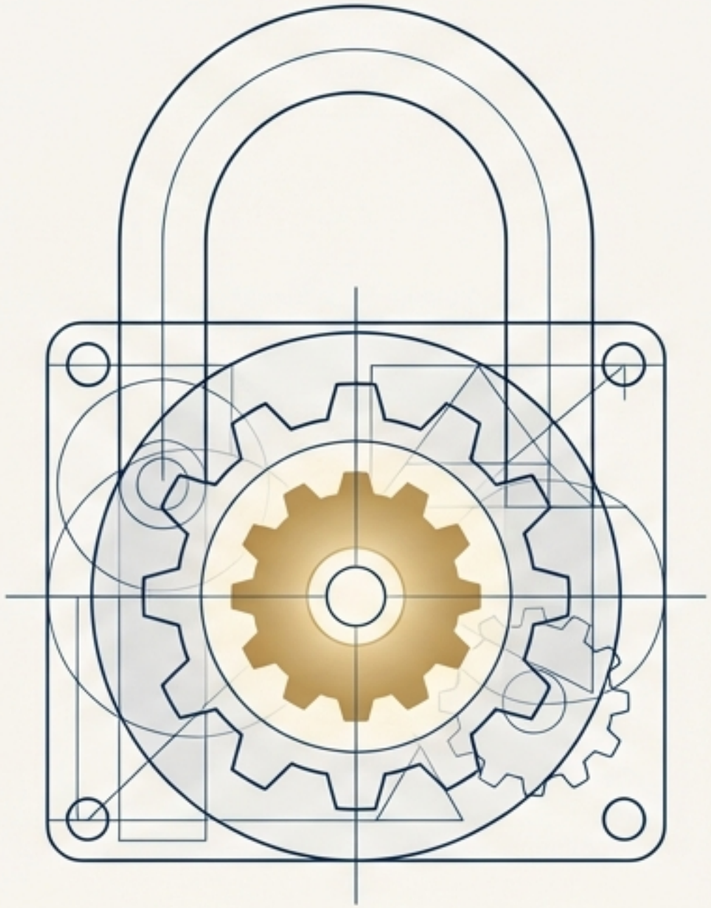


# The Visibility Principle

## How Radical Transparency Transforms Vulnerability Management

# The Real Challenge Isn’t Finding Vulnerabilities. It’s Getting Them Fixed.


## How do we bridge the gap between detection and action?

*“어떻게 조치를 이끌어낼 것인가” (How to drive action).

# The Solution Isn’t Technological. It’s Psychological.

Organizations that successfully accelerate patching leverage three powerful psychological drivers through internal transparency.

### 1. Perceived Accountability

The expectation of being evaluated for one’s actions.

### 2. Perceived Surveillance

The awareness of being observed by others.

### 3. Behavioral Deterrence

The motivation to avoid negative social consequences.

---

*“What gets measured gets improved.”* - Peter Drucker

# Principle 1: Perceived Accountability

The state of perceiving that one's actions are identifiable and will be evaluated by others. It transforms a task from a private chore into a public responsibility.

**“내가 무엇을 (안)했는지를 모두가 안다”**
**(Everyone knows what I have (or haven’t) done).**

## Case Study in Failure: The 2017 Equifax Breach

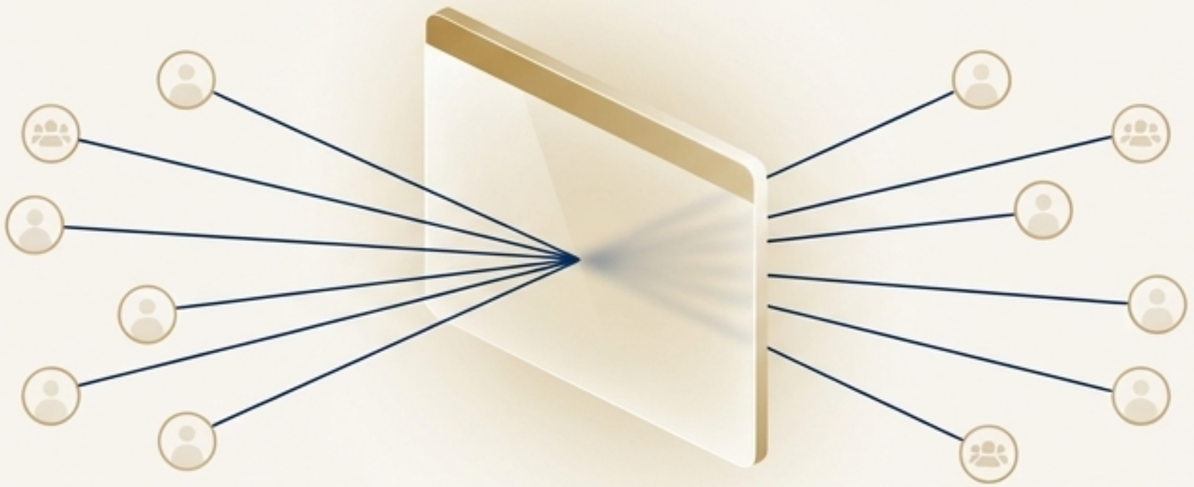
**Root Cause:** A critical vulnerability was left unpatched.

**The Finding (U.S. House report):** Equifax's process “failed to establish a clear line of responsibility for the implementation of security updates.”

**The Takeaway:** When no single person or team is clearly responsible, critical tasks fall through the cracks. Transparency forces clear ownership.

# Principle 2: Perceived Surveillance

The feeling that one's actions are being observed by others. This awareness inherently encourages compliance with established norms.



**Mechanism**

A transparent, shared dashboard creates this effect constantly and passively. The simple awareness that “Security, leadership, and my peers can see this” drives teams to manage their own posture proactively.

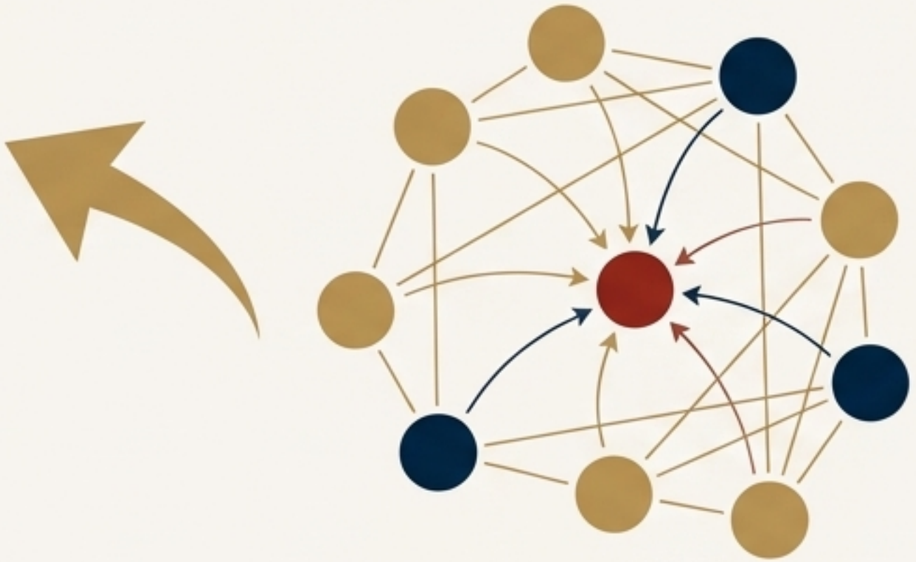
**Source Insight**

Research shows that UI elements signaling that user activity is being monitored (e.g., activity logs, access notifications) significantly increase compliance with security policies.

# Principle 3: Behavioral Deterrence

Deterrence isn’t just about formal punishment. It’s about the desire to **avoid negative social outcomes like shame or loss of reputation.**

**Formal Deterrents**
(e.g., penalties)



**Informal Deterrents**
(e.g., peer evaluation, shame)

## Evidence from Research

A meta-analysis on security compliance found that **informal deterrents (like peer evaluation and shame) have a stronger influence on behavior than formal deterrents (like penalties).**

## How It Works in Practice

No team wants to be last on the dashboard or be seen as the “team with the most unpatched vulnerabilities.” This social pressure creates a powerful incentive to act, protecting both the system and the team's reputation.

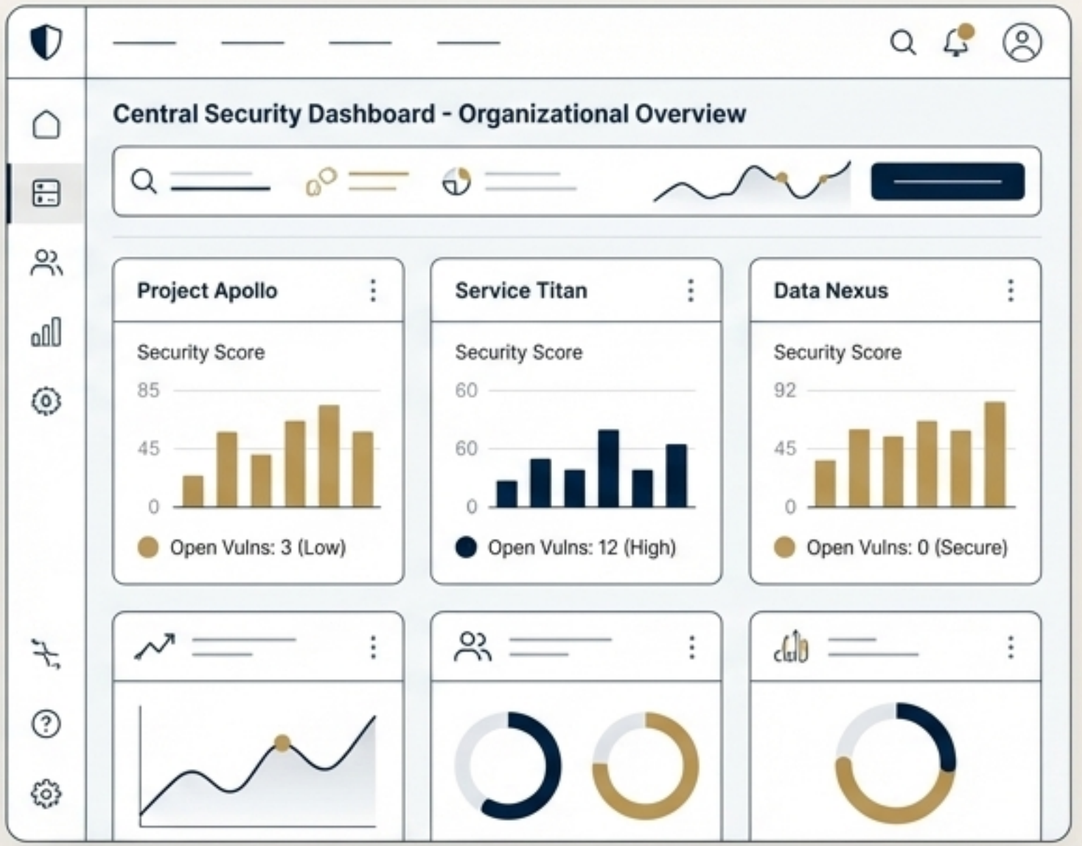
# The Proof in Practice: The Central Security Dashboard

**The Tool:** Top-performing organizations create a single source of truth—a central dashboard displaying vulnerability status across all teams and services.

**The Strategy:** This dashboard is not firewalled within the security team. It is shared openly with all engineering, development, and operations teams.

**Example:** Companies like **Netflix** provide engineers with real-time dashboards showing vulnerability scan results and security scores for their services, maximizing visibility.

**The Outcome:** This eliminates information silos, prevents "responsibility dispersion," and empowers teams to own and manage their security posture directly.



# From Conflict to Collaboration: A Case Study

**The Scenario:**


At a software company (“TechCo”), inter-departmental conflict and blame-shifting led to severe delays in vulnerability patching.

**The Intervention:**

They implemented a bi-weekly, cross-functional meeting where representatives from Security, Dev, Ops, and Compliance reviewed all unresolved vulnerabilities **together and in the open**.

Within **one year**, the mean time to remediate vulnerabilities was reduced by over 50%.

**The Lesson:** Shared information and a collaborative forum transform a contentious process into a shared mission.

# An Unassailable Proof Point: Lessons from Google's Project Zero

## The Policy:

Google's Project Zero publicly discloses vulnerabilities 90 days after reporting them to the vendor, whether they are patched or not.

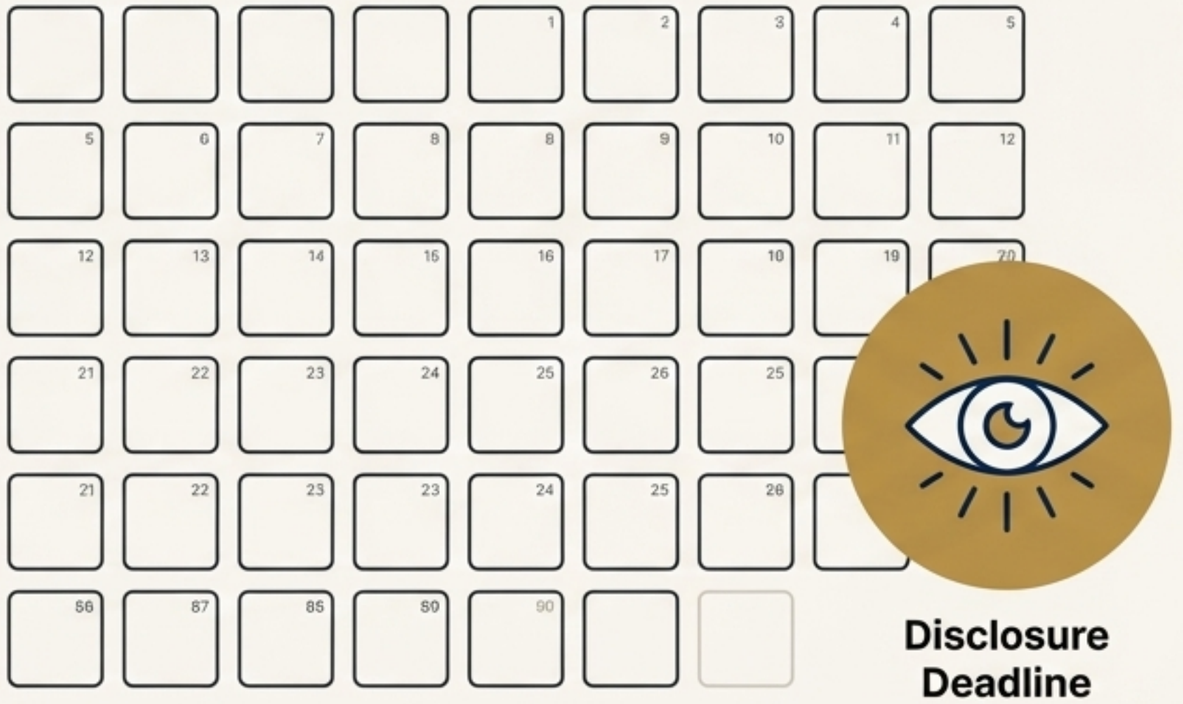
## The Impact

**Before**

Some vulnerabilities took over 6 months to patch.

**After**

Over 97% of vulnerabilities are fixed within the 90-day deadline.




**Transparency + a Deadline = An Undeniable Forcing Function**

# The Critical Caveat: Transparency is a Tool, Not a Weapon

**The Risk:**

If transparency is implemented poorly, it can lead to a culture of blame, fear, and metric-gaming. Teams may start hiding problems or focusing only on what's measured, ignoring other risks.

**A Worst Practice:**

Using vulnerability metrics for the sole purpose of **"문제 부서 낙인찍기 (naming and shaming problem departments)"** is counter-productive and will backfire.

So, how do we leverage the power of transparency without creating a toxic environment?

# The Solution: Practice “Soft Transparency”

The goal is to make vulnerabilities visible without making it feel like an accusation.

## A Tale of Two Dashboards

### ❌ The Blaming Approach

**VULNERABILITY LEADERBOARD!**

| | |
|---|---|
| **Team X** 15 Critical Vulnerabilities! | ⚠ |
| Team Y | 1.0 |
| Team Z | 3.1 |

### ✅ The Displaying Approach

**Live System Vulnerability Status**

| | |
|---|---|
| **Service Alpha** 2 Issues | **Service Beta** 0 Issues |
| **Service Gamma** 1 Critical Issue | **Service Delta** 1 Issue |

Frame the data not as a list of who has failed, but simply as **“the current state of the system.”**

# The Goal: Build a Culture of “Blameless Accountabiity”

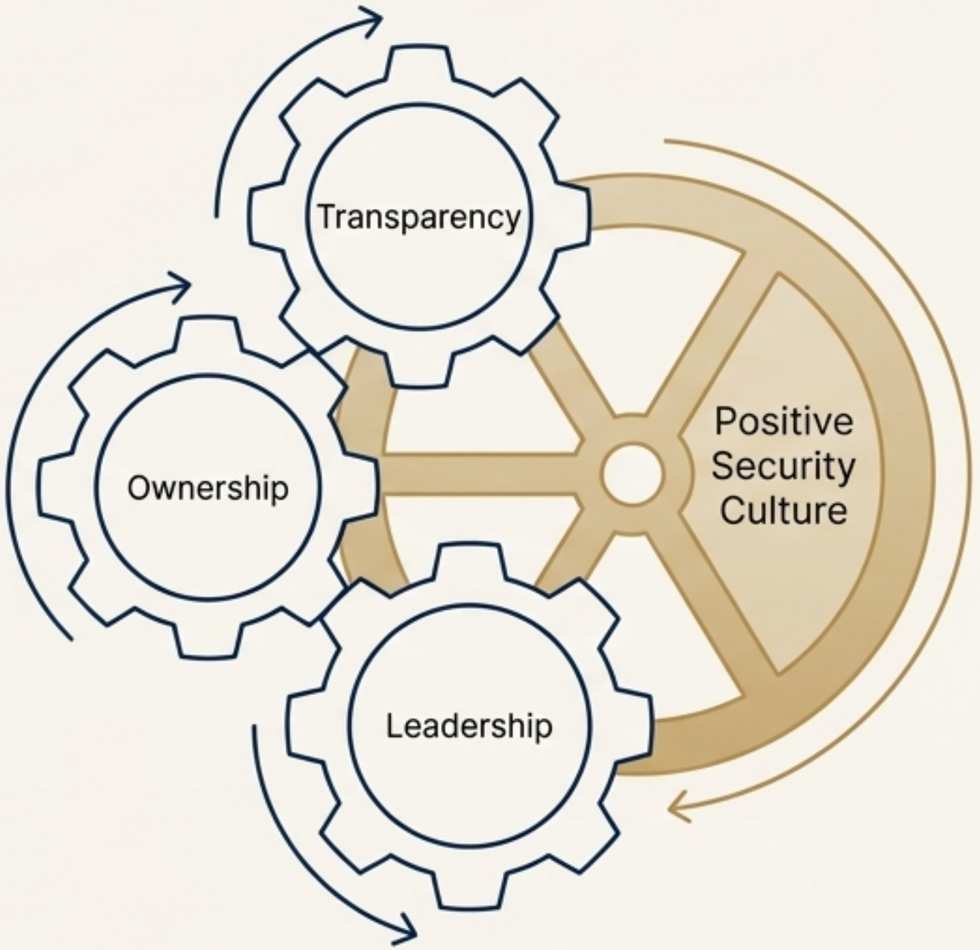
## The Objective

The purpose of transparency is to foster a culture where security is a **shared responsibility**, not a source of blame.

## Leadership in Action

**Meta (Facebook):** Fosters a culture where "security is everyone's responsibility," encouraging developers to surface issues openly and collaboratively.

**Microsoft:** Integrated security metrics directly into team and leadership evaluations, making security a core part of performance, not an external mandate.




## The Role of Leadership

Frame transparency as a tool for **collective improvement**, not individual punishment.

# The Visibility Principle: See. Solve. Secure.

## THE WHY: Leverage Human Psychology

Activate the powerful drivers of **Accountability**, **Surveillance**, and **Deterrence**. Make responsibilities clear and actions visible.

## THE HOW: Implement Shared Systems

Use central **Dashboards** as a single source of truth and **collaborative Forums** to align teams and solve problems together.

## THE MASTERY: Practice Soft Transparency

Focus on
Focus on **objective visibility**, not blame. Build a culture of **shared responsibility** to drive sustainable improvement.

# In your organization, are vulnerabilities a private accusation or a shared reality?