

365 DAYS OF ZERO TRUST FAILURES

— AND STRATEGIC TRUST SOLUTIONS

Everyday we explore a new breach and bring the Zero Trust failures into light so we can learn from them, consider them for our environments and then we see the Strategic Trust solutions that circumvent the failure completely and commonly would have prevented catastrophic loss to the business.

365 > ZERO TRUST FAILURES

DAY 1

AUTHENTICATED, BUT MALICIOUS

The Uber Breach,
Sept 2022



SECURITYBYSTRATEGY

JUNE 17, 2025

Attack Overview:

🚨 UBER 2022 BREACH TIMELINE



🧠 1. Recon & Target Selection (Pre-September 2022)

Lapsus\$ or affiliated attacker scans for soft targets — likely identifying contractors with VPN access and weaker MFA habits.

Recon includes public employee data, social engineering prep, and knowledge of Uber's internal structure/tools (e.g., Slack, Thycotic, AWS, etc.).

👤 2. Initial Access via Social Engineering

Method: MFA fatigue attack on an Uber contractor.

Attacker floods them with 2FA requests (push notifications).

After repeated attempts, contacts the target via WhatsApp, impersonating IT support.

Result: Contractor approves one MFA prompt, granting VPN access to internal systems.

🔑 3. Privilege Escalation & Lateral Movement

Attacker scans intranet and tools once inside.

Finds a PowerShell script containing admin credentials (hardcoded) for Thycotic PAM.

Uses those credentials to escalate access to:

- AWS
- Google Workspace (GSuite)
- Slack
- Duo, OneLogin, and more.

Gains wide-reaching admin control — described as having the "keys to the kingdom."

📁 4. System Breach & Data Access

Attacker posts a message in Uber's internal Slack, declaring the breach.

Views or accesses:

Internal dashboards

Bug bounty reports (HackerOne)

Source code repositories

Admin panels

No hard evidence of customer or driver PII exfiltration, but systems were clearly browsed.

5. Data Exfiltration Potential

While Uber claims no sensitive user data stolen, access level suggests:

Viewing of internal documentation and code.

Possible exfiltration of security-related reports (e.g., HackerOne bug bounty entries).

Screenshots shared publicly confirm sensitive systems were visible.

6. Detection, Lockdown & Response

Breach becomes public on September 15, 2022.

Uber:

Disables Slack and internal tools.

Revokes VPN sessions and privileged credentials.

Resets passwords, rotates secrets and keys.

Brings in Mandiant and other security partners for forensics.

Law enforcement notified.

7. Cleanup, Containment, & Aftermath

Internal audit confirms:

Breach was limited to internal tools.

No long-term persistent access detected.

December 2022: separate vendor breach (Teqativity) exposes 77,000 employee records, unrelated to September event.

Uber updates policies to:


Harden MFA workflows.

Eliminate hardcoded secrets.

Monitor abnormal push behavior.

Increase contractor security training.

Zero Trust Failures:

 Zero Trust Failures in the Uber 2022 Breach

Zero Trust Principle	Control Expected	What Failed or Was Breached	Category
Verify Explicitly	Strong identity verification with MFA enforcement and behavioral analysis	✅ MFA used, but attacker used MFA fatigue + social engineering to bypass it	Design failure (MFA abuse)
Use Least Privilege	Limited access for contractors; role-based access controls (RBAC)	❌ Contractor had VPN access to internal systems , enabling lateral movement	Access overprovision
Assume Breach	Continuous monitoring, microsegmentation , alerting on anomalous behavior	❌ No immediate alert on lateral movement or access escalation	Detection/control gap
Microsegmentation	Internal tools and systems should be isolated by trust zones	❌ Attacker moved freely from VPN to PowerShell scripts, Thycotic, Slack, and GSuite	Architecture flaw
Prevent Credential Theft	Secrets management tools (e.g., vaults), no hardcoded secrets	❌ PowerShell scripts contained hardcoded admin credentials	DevSecOps failure
Just-In-Time (JIT) Access	Temporary elevation of privileges when needed, not permanent admin access	❌ Static credentials allowed persistent admin-level access once discovered	Privilege mismanagement
Visibility & Analytics	Centralized logging and real-time monitoring of sensitive actions	❌ Attacker posted in Slack without triggering immediate alert	Detection lag
Secure Workloads	PAM (Privileged Access Mgmt), EDR on endpoints, segmentation of systems	❌ PAM system (Thycotic) was accessible through initial intrusion path	Inadequate isolation

Zero Trust Principle	Control Expected	What Failed or Was Breached	Category
Third-party Risk	Tightly controlled third-party access; contractor segmentation	✗ Contractor VPN access allowed full corporate network exposure	Third-party exposure

ZERO TRUST FAILURES IN THE UBER 2022 BREACH



Verify Explicitly

MFA bypassed via social engineering



Use Least Privilege

Contractor had VPN network access



Assume Breach

No alert on lateral movement or escalation



Microsegmentation

Inadequate segregation of systems



Prevent Credential Theft

Hard-coded admin credentials stored



Just-In-Time (JIT) Access

Persistent admin-level access granted



Visibility & Analytics

Attacker posted in Slack undetected



Third-party Risk

Full exposure from contractor access



Strategic Trust would have prevented this breach in its entirety

1. Recon & Target Selection

What Happened in Uber:

Attacker targeted a third-party contractor with weak MFA habits and wide network access.

Strategic Trust Response:




-  **Third-Party Signal Scoring:** Contractors would carry a *lower baseline trust score* by default, requiring enhanced verification or limited session scope.
-  **Pre-execution Threat Detection:** Behavioral analytics would detect unusual reconnaissance probes or new device types even before login attempts.

2. MFA Fatigue Attack (Social Engineering)

What Happened in Uber:

Attacker bombarded user with push notifications, then impersonated IT via WhatsApp.

Strategic Trust Response:




-  **MFA Saturation Defense:** Alerts and rate-limiting stop repeated failed push attempts; *no more than 3 per session*.
-  **Adaptive Challenge Escalation:** If signals show fatigue pattern, system upgrades challenge to **biometric or out-of-band call**.
-  **Live Trust Scoring Drop:** The PIP would flag behavioral anomalies (e.g., multiple MFA attempts + foreign IP + social app open) and immediately lower trust score → deny access.

3. Initial Access via VPN

What Happened in Uber:

VPN access granted full lateral movement to internal network.

Strategic Trust Response:




-  **Micro-perimeter Enforcement:** VPN access would land in a *containment zone*, not the flat network.
-  **Contextual Access Policy:** New login → restricted to contractor resources only, pending live trust revalidation.
-  **Live PDP Check:** PDP would evaluate session state, MFA method, device ID, geo-velocity → and deny lateral movement unless all signals aligned.

4. Credential Discovery & Privilege Escalation

What Happened in Uber:

PowerShell script had hardcoded Thycotic admin credentials.

Strategic Trust Response:




-  **Secrets Governance Enforcement:** PIP scans would flag hardcoded secrets during dev pipeline or runtime and **auto-revoke credentials**.
-  **Privilege Use Justification:** Admin elevation must come with a **justification message**, and is time-boxed, scoped, and human-reviewed.
-  **Automated Session Isolation:** Lateral movement to PAM system triggers a new **trust checkpoint**, requiring fresh validation or isolation.

5. Full Internal Access & Slack Breach

What Happened in Uber:

Attacker posted in Slack, accessed dashboards, cloud services, bug reports.

Strategic Trust Response:




-  **In-App Activity Scoring:** System monitors **user behavior inside apps**. Unexpected Slack channel posting by new/contractor user → alerts + lockdown.
-  **Internal Control Mesh:** Slack, AWS, GSuite each have **per-app adaptive policies**. Access across environments without known role correlation → auto-block.
-  **Session Disposition Review:** Strategic Trust enforces live session scoring. A new spike in activity (e.g., multiple system accesses in seconds) downgrades trust and restricts activity.

6. Data Exfiltration Potential

What Happened in Uber:

Attacker may have accessed source code, bug bounty entries.

Strategic Trust Response:




-  **Content-Aware Policy Enforcement:** Data tagged with sensitivity labels (e.g., “Confidential–Security Research”) triggers export denial unless session is high-trust.
-  **Intent Validation Engine:** If user tries to download >X MB of sensitive data in a short span, a PDP/human checkpoint blocks or requires elevated authorization.
-  **Exfil Pattern Detection:** PIP observes unusual behavior (e.g., repo cloning, batch downloads) → initiates automatic session lockdown and SOC alert.

7. Detection, Lockdown & Forensics

What Happened in Uber:

Attacker self-disclosed, and Uber responded manually.

Strategic Trust Response:

-  **Autonomous Containment:** Risk scoring and behavioral thresholds would **auto-expire** the session once violations reached a threshold.
-  **Retrospective Signal Chaining:** System records chain-of-events per session → feeds into forensic replay, root cause mapping, and policy improvement.
-  **Trust Recovery Framework:** Strategic Trust guides cleanup by revoking session credentials, issuing per-app trust resets, and updating policy weights across the mesh.

Strategic Trust Outcome Summary

Attack Phase	What Uber Had	What Strategic Trust Does
Recon	No deterrence	Risk scoring of signal anomalies pre-login
MFA Fatigue	Static push MFA	Behavioral MFA, escalation, abuse defense
VPN Access	Flat network access	Microsegmented, contextual zone access
Lateral Movement	No checkpoint	PDP-enforced transitions w/ trust decay
Privilege Escalation	No JIT or context control	Just-in-time, just-enough access w/ intent verification
Data Access	Broad system reach	Per-app trust boundaries, real-time behavior scoring
Data Exfiltration	No content-aware defense	Label-aware, intent-enforced download control
Detection & Lockdown	Human detection via Slack	Autonomous lockdown, forensic reassembly, session memory in trust mesh


The Uber 2022 breach wasn't just a security failure—it was a case study in the real-world collapse of static Zero Trust implementations under pressure. By dissecting each phase of the attack and mapping it against Strategic Trust's adaptive defenses, we reveal the difference between simply checking compliance boxes and truly securing a modern enterprise. Strategic Trust doesn't rely on hope that controls will hold—it responds in real time, layering context, behavior, and intent into every access decision. The insights uncovered in this breakdown are not hypothetical—they are actionable, scalable, and ready to deploy.

If this kind of tactical clarity and next-generation security thinking resonates with you, the full Strategic Trust book dives even deeper. From architecture to enforcement logic, real-world vignettes to design playbooks, it's the definitive guide for security leaders ready to move beyond Zero Trust's limitations. Get your copy today and join the forward edge of cybersecurity thinking—because staying ahead of threats means thinking beyond them.

What Comes Next – Continue Your Strategic Trust Journey

Tiered Access – Learn at Your Level

Tier	What You Get	Access Duration	Price
Tier 3 – Leader Access	365 Days of Deep Dives + PDF Copy of <i>Strategic Trust: Rescuing Zero Trust from Stagnation</i> + 60-Minute Consultation with Abraham	1 Year	\$197

 [Unlock a Tier Now](https://www.securitybystrategy.com/365ZTF): www.securitybystrategy.com/365ZTF

Get the Full Book

Strategic Trust: Rescuing Zero Trust from Stagnation

Available now on Amazon and in direct PDF format


 [Read the Book](#): (Amazon: <https://a.co/d/10fAX0f>,

Direct: <https://buy.stripe.com/cNi28r7zi6F829A7Cc2oE07>)

 Includes actionable frameworks, visual models, and Zero Trust fixes that *actually work*.

Book Consulting & Design Services

Service	Price
Strategic Trust Session (20 min)	\$99.00 (https://calendly.com/abraham-andresen/20-min-strategy-consult)
Strategic Architecture Session (90 min+)	\$847.00 (https://calendly.com/abraham-andresen/new-meeting-1)
Strategic Trust Alignment Engagement	\$1,500.00 (https://calendly.com/abraham-andresen/strategic-trust-advisory-roadmap-advisory)

 Whether you're fixing a failed Zero Trust rollout or building from the ground up, these sessions deliver clarity, architecture guidance, and mission-aligned security evolution.

Coming Soon: Volume 2

Strategic Trust Vol. 2: AI-Driven Policy & Mission-Critical Defense

Early reviewers are forming now. Be among the first to shape the next stage of cyber resilience.

Stay Connected

 SecurityByStrategy.com  [LinkedIn](#) • Ask Abraham Anything

“Clarity at the edge, Confidence at the Core.”