Closing the ServiceNow shared responsibility gap

CIO servicenow Rezilient

The undo button for the AI enterprise: enterprise-class backup for ServiceNow

ServiceNow is far more than a ticketing tool. It's a Tier-1 business-critical platform, orchestrating IT operations, HR, customer service, security response, finance, and agentic AI. This creates data-related risk that slows the pace of innovation. Regulators have taken note. Compliance mandates have shifted from "best effort" to "provable control."

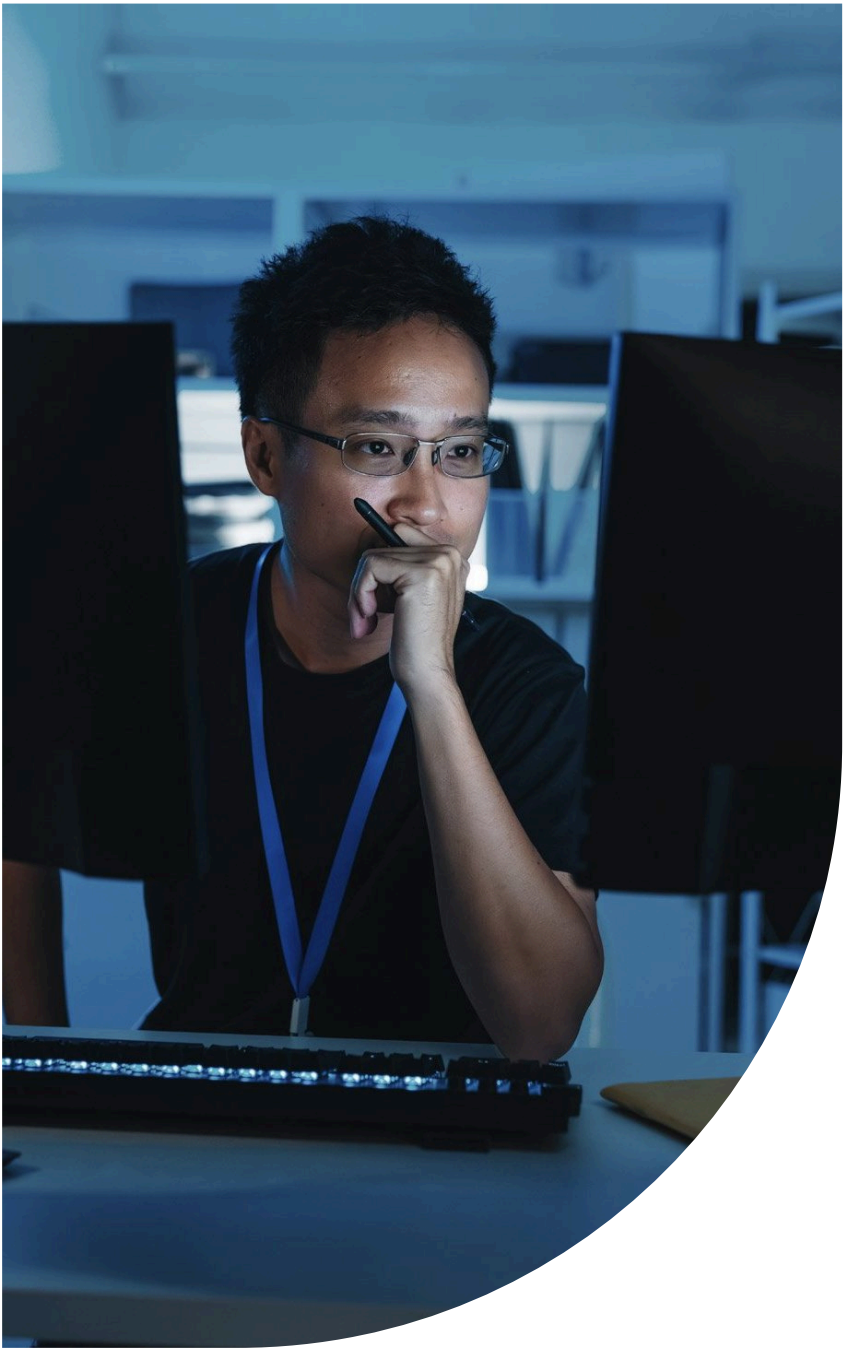
Data powering the SaaS engine room of the business must be recoverable, immutable, and auditable. Yet many customers aren't aware of ServiceNow's shared responsibility model, or the limitations of its native backup capabilities.

To help them manage these risks and unleash innovation, customers need a trusted partner to step up. One that offers continuous, enterprise-class backup and restore — a controlled, reliable undo — designed for the AI enterprise.

A risky business

Risks to SaaS data are proliferating. Data loss might stem from human error and misconfigured integrations, malicious activity, or even AI agents. Three-quarters of organizations suffered a SaaS-related breach last year, with the average cost per incident now at nearly $5m.

Against this backdrop, most users believe SaaS platforms include backup and recovery by default, but this isn't true. ServiceNow natively retains weekly full backups for just 14 days and daily differential backups for seven. It's designed for infrastructure-level disaster recovery, not the surgical recovery that regulators expect, and engineering teams require, to innovate safely. Under ServiceNow's shared responsibility model, its users are expected to take on the backup burden beyond that 14-day window.



So, what are the options? Many existing solutions fall short because they're optimized for replicating and using data, not protection or recovery. Copies are mutable and don't provide verifiable restore capabilities. Custom solutions that export to a data lake or warehouse are another option; however, they require a significant engineering effort, and every successful restore feels like a lucky roll of the dice.

This is where Rezilient Restore has an advantage, as the only purpose-built backup and recovery layer for ServiceNow that reduces the risk of a problem becoming an incident. No dice required.

Backup to rely on

Rezilient stores enterprise data encrypted and off platform, captures every change immutably, and gives operational and compliance teams a way to prove and undo changes inside the instance. Unlimited retention eliminates the 14-day ceiling. Precision recovery reduces the need for full instance restores. And Rezilient is schema-aware to remove manual remapping requirements after every upgrade or customization.

This means always-on protection, targeted recovery, and audit-ready retention. Off-platform storage meets the strictest regulatory and ransomware-resilience requirements, from Europe's Digital Operational Resiliance Act (DORA) to New York's Department of Financial Services Part 500. Additionally, AI governance records the pre- and post-state of every automated change, supporting rigorous oversight expectations.

Managing AI risk

These capabilities will become more critical as AI agents change the enterprise risk landscape. In April 2026, an AI coding agent wiped the entire production database of a SaaS company in under 10 seconds, including all on-platform backups. Customers lost three months of data.

The same risk lives inside ServiceNow via Now Assist and agentic AI workflows. The blast radius is significant. Only off-platform backups, continuous capture, surgical recovery, and reversible AI governance can mitigate these risks.

Embracing AI

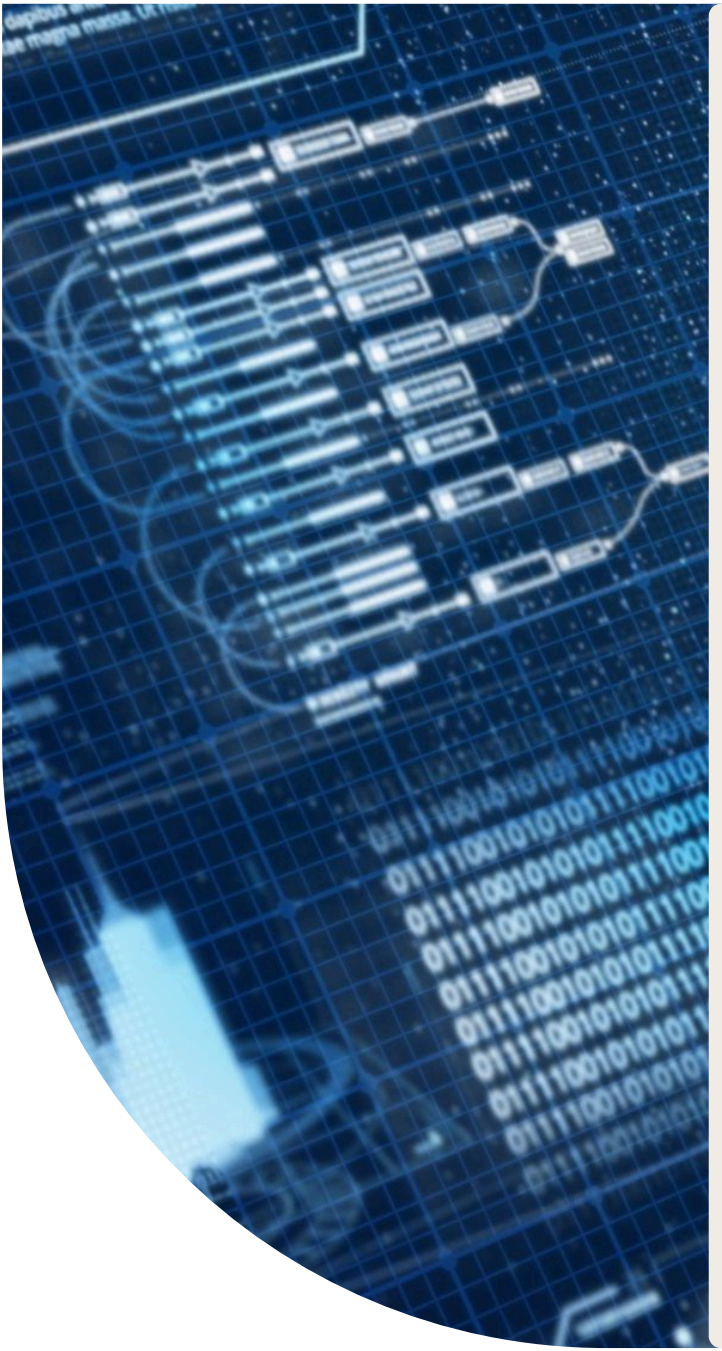
Fear of permanent data loss makes ServiceNow platform teams cautious and slows innovation. Regulators demand businesses remain in control of their data. But full-instance restores are disruptive to the business.

Rezilient provides the control and confidence to unleash AI-driven innovation. Customers know that if something goes wrong, they can hit “undo.” It’s about continuous backup and precision recovery. Because in the ServiceNow world, the integrity of your data is the integrity of your business.

Book a Demo

CIO servicenow Rezilient

Rethinking security for the AI era



How many AI agents are in play throughout the enterprise? What is their level of data access and what kind of actions can they take? These deceptively simple questions may be a challenge to answer, even for the most AI-savvy organizations — a failing that has major consequences for businesses.

AI is expanding faster than human capacity can manage, let alone track. The typical IT environment has exploded beyond the usual employees, endpoints, and networks to encompass cloud apps, factory equipment, and IoT devices. As the number of identities skyrockets, there's often no centralized view of who — or what — has access to which data and systems. This lack of visibility puts sensitive data at risk, while overprivileged agents can be unleashed without proper controls.

Legacy tools may address pieces of the security and governance challenge, but they aren't architected to mitigate risk at the pace of today's shifting AI landscape. These tools are limited by:

The inability to recognize machine identities and AI agents

Insufficient business context, which hampers insights into what's at stake until too late in the game

Sporadic AI agent compliance

Unifying security, IT, and cyber risk operations with identity and cyber asset intelligence in a single platform will help prevent breaches well before they happen. Instead of agents surfacing problems without closing the loop on resolution, end-to-end agentic workflows are executed with embedded guardrails. Every AI agent, identity, device, and data flow becomes visible at the moment of action, not after the fact. Remediation draws from identity-enriched incident playbooks to ensure optimal resolution.

With this new paradigm, security, IT, and risk and compliance teams can execute a cohesive defense strategy at the pace of AI. **The benefits: stronger operational resilience, sustained compliance, and the ability to mitigate security threats in real-time — all while enabling AI transformation at scale.**

"As AI becomes more autonomous, **governance can no longer be an afterthought**," notes Jeffrey DiMuro, Deputy Chief Information Security Officer at ServiceNow. "CISOs must shift from securing systems to establishing trust, control, and accountability across the entire AI lifecycle through a partnership with the business."

> **As AI becomes more autonomous, governance can no longer be an afterthought.**

Jeffrey DiMuro,
Deputy Chief Information Security Officer, ServiceNow

CIO servicenow Rezilient

What's not working and what's at stake

Security and risk organizations face a wide array of challenges as they modernize defense strategies for the AI era. Changing dynamics impacting risk and security strategies include:

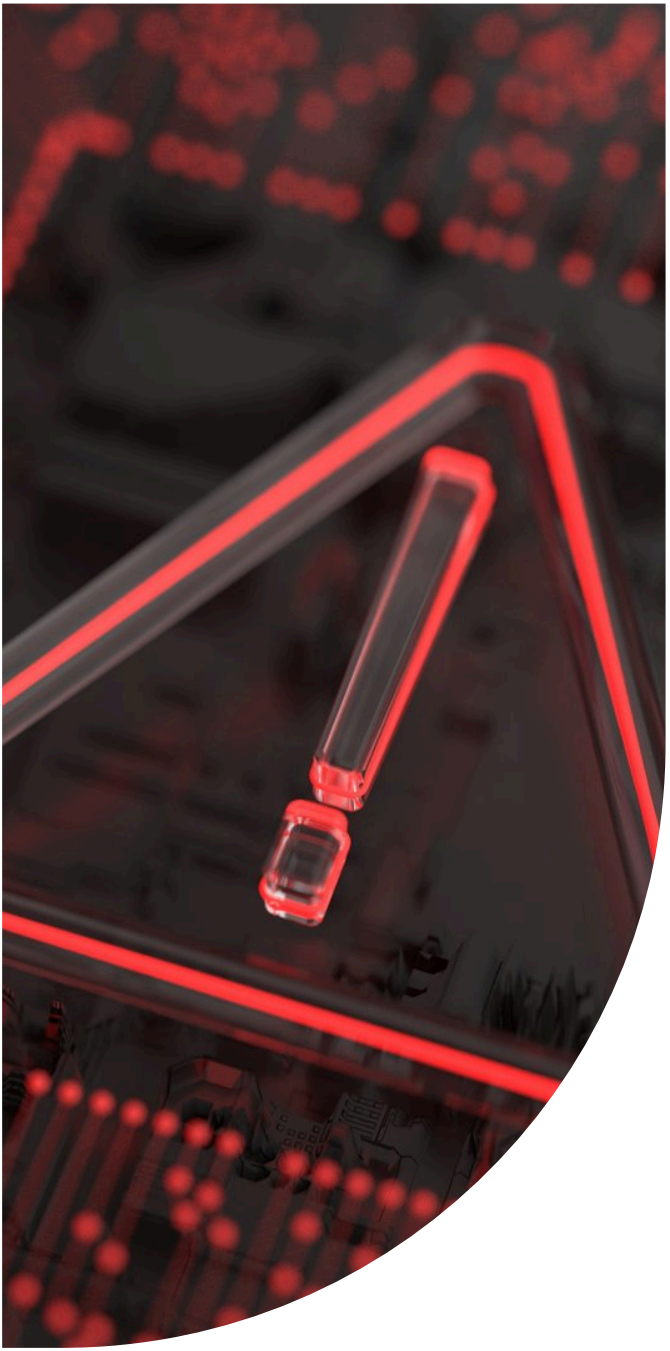
An invisible AI workforce that answers to no one.

An invisible workforce is emerging as AI agents are spun up across third-party tools, platforms, and disparate business units without central oversight. Provisioning is programmatic, and agents are rarely deprovisioned when work is complete. Agents execute decisions, access systems, and accumulate permissions at machine speed without the same fixed identity lifecycle applied to human employees.

The rise of a broad class of non-human identities, including service accounts, API keys, bots, and machine credentials, compounds the problem. These entities fall off the radar of legacy identity tools, leading to a swarm of ungoverned identities, dormant accounts, and permissions creep.

Without clear accounting for what agents are in play or what sensitive data is at risk, agents that spring to life as productivity assets can quickly become enterprise liabilities. These authorized, active, and unmonitored agents are ripe for potential data exposure, IP leaks, or compliance violations.

"**Organizations that can't see where AI is being used, what data it's touching, or who authorized it aren't just exposed, they're unable to scale responsibly,**" says Bryce Schroeder, Vice President Customer Security and Trust at ServiceNow. "Security and risk leaders need real-time inventory of AI assets mapped directly to business services, continuous risk scoring, and policy enforcement that acts on what it finds — not just reports on it. **Governance isn't a foundation you declare; it's one you demonstrate through discovery, control, and auditability.**"



Point solutions cloud visibility.

Dozens of endpoint, identity, vulnerability scanning, and Governance Risk Compliance (GRC) solutions are deployed across the enterprise but rarely operate in a cohesive way. Sensitive data flows through prompts, integrations, and AI workflows that traditional protection tools were never designed to recognize. One misconfigured integration quietly exposes dozens of systems to the whims of a connected agent when no one is watching and can rein it in. **Security and risk teams often end up flying blind because data remains buried in disconnected tools without a common lexicon or shared understanding.**

Most security tools stop at the IT boundary.

Years of investment in security tools hardened the perimeter — endpoints, detection, and edge controls — but the estate has expanded far beyond what those tools were built to see. OT devices, medical equipment, industrial control systems, and physical infrastructure are active participants in the mix, operating out of view of most identity systems and inventory frameworks. A breach that starts with an unmanaged device moves quietly following paths that haven't been mapped. Endpoint alerts aren't triggered and they don't surface in the identity record or vulnerability scanner. **That leaves organizations adept at governing human credentials still highly vulnerable.**

Fragmented systems impede work.

Security teams are drowning in signals, but there's no real guidance on where to focus or how to determine what problem has the widest impact. The fragmented tool portfolio leaves teams dependent on manual processes to stitch together data from disparate systems, a practice that is highly ineffective against an active threat landscape. Without a cohesive workflow that automates and executes tasks, it's hard to connect the dots from detection to prioritization all the way through remediation and proof of controls.

There's no clear cross-process ownership that ensures proper resolution once a problem is detected and specific remediation chosen. **As identities explode across humans, machines, and AI agents, the delta between workflows that detect and act only widens.**

"The industry is drowning in signals and starving for orchestration," says Diana David, Futures Director for ServiceNow. "**The problem was never a shortage of data; it's the absence of a governed workflow**. Without that connective tissue, every new tool just adds noise to an already overwhelmed security operations center."

Threats are moving at lightning speed.

Off-the-shelf AI has created opportunity for anyone to launch sophisticated cyberattacks, which are coming fast and furiously. Fragmented systems make it difficult to triage alerts at scale, leaving teams burnt out and perpetually behind.

The regulatory landscape is intensifying.

Regulatory frameworks are multiplying across every region with real penalties and business risks. For example, the EU AI Act, which expands GDPR enhancement, is changing the landscape overseas; at the same time, in the United States, California and Colorado are leading the way with laws imposing safety and security frameworks on AI systems. There are dozens of other AI and data regulations in the works, many surfacing each year.

> **Organizations that can't see where AI is being used, what data it's touching, or who authorized it aren't just exposed, they're unable to scale responsibly.**

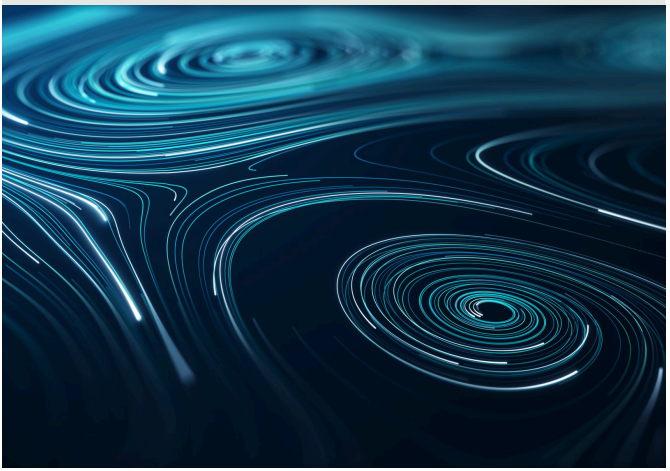
Bryce Schroeder,
Vice President Customer Security and Trust, ServiceNow

CIO servicenow Rezilient

ServiceNow key capabilities at work

> **Unlike human employees who maintain relatively stable behavioral patterns, AI agents can be modified rapidly and subtly, making the old castle and moat model of identity obsolete.**

Diana David,
Futures Director, ServiceNow



Purpose-built for the AI era, ServiceNow's Security & Risk platform brings together identity intelligence with enterprise asset data to close exposures before they become a breach while leveraging AI agents to autonomously complete work. **Key benefits include:**

Control over identity sprawl:

ServiceNow pulls signals from hundreds of tools into a single operational model, transforming scattered security and risk efforts into one cohesive defense. Identity and access intelligence layers in permissions across human, machine, and AI identities at the authorization layer, not just users and groups, with everything framed with the proper business context. The system continuously detects overprivileged accounts, dormant permissions, toxic permission combinations, and access drift, closing gaps automatically at machine speed.

With ServiceNow, identity is no longer just about authentication, but also ownership, authorization, and accountability for autonomous decision making. "**Security is going from a one-time credential check at the gate to continuous monitoring based on identity**," says David. "Unlike human employees who maintain relatively stable behavioral patterns, AI agents can be modified rapidly and subtly, making the old castle and moat model of identity obsolete."

Bring order to ungoverned AI agents:

AI without governance is a liability, not an asset. Every agent, model, and workflow needs guardrails at the moment of action, not after the fact, with direct mapping to relevant business services across its entire lifecycle. ServiceNow ensures every system, cyber asset, and identity (human or AI) is compliant, policy aligned, and auditable. Continuous least privilege is enforced across all identity types, and built-in risk and compliance scoring keeps regulators, auditors, and the board confident in controls and risk strategy.

Replace fragmented efforts with autonomous workflows.

AI agents built directly into the ServiceNow platform use identity and asset intelligence to prioritize tasks that matter while also surfacing relevant business risks and recommending actions. ServiceNow's AI agents autonomously remediate exposures, respond to incidents, and enforce governance without the need for manual handoffs. Human experts remain in the loop to provide additional judgment, resulting in faster, more informed decisions. "The future isn't fewer tools, it's intelligent orchestration and execution," DiMuro says. "**Platforms that can operationalize response through workflow, not just visibility, will be the ones that keep pace with an increasingly autonomous threat landscape.**"

Reduce alert chaos.

ServiceNow manages cyber risk across the full attack surface. This creates a unified, end-to-end security exposure and operations stack that handles real-time asset discovery, threat intelligence, and risk prioritization with automated remediation and response workflows. AI agents proactively monitor identities and system activity for potential threats. When threats are detected, incidents are automatically enriched with context while response workflows are immediately triggered to contain risk. This way, analysts no longer make triage decisions in the dark.

Make governance and compliance a continuous process.

In today's fast-paced environment, governance and compliance no longer follow routine schedules with regular reviews and risk assessments. The evolving regulatory landscape, coupled with rampant cloud and AI system changes, requires more than static snapshots, but rather ongoing, real-time monitoring of controls. ServiceNow aligns AI system activity with established policy, **automatically detecting deviations and addressing issues well before regulatory violations occur**.

Sallie Mae transforms identity operations with Veza from ServiceNow

Problem:
Education solutions company Sallie Mae wanted to shift from on-premises solutions to a full cloud infrastructure, including SaaS solutions. It needed to ensure data was fully protected while convincing regulators that governance standards were met.

Results:
Using Veza from ServiceNow Access Intelligence, **Sallie Mae achieved a 96% reduction in dormant non-human identities while streamlining regulatory compliance** during the move to a cloud-based organization.

ServiceNow's 4 critical architecture pillars

Sense: Most organizations don't have the full picture of the attack surface, including what exists, where it lives, and what it's actually connected to. Yet everything that happens downstream depends on getting this right. **ServiceNow delivers continuous, agentless discovery across every connected cyber asset** — IT, OT, IoT, medical devices, physical infrastructure, and cloud. Every asset is classified by business criticality and mapped to the services and teams that depend on it. AI agents are inventoried the moment they're activated. But discovery alone isn't the differentiator. What makes the picture complete is enterprise context. Every discovered cyber asset flows into the CMDB (Configuration Management Database) mapped to the services, processes, and teams that depend on it. A device isn't just known, it's understood in terms of business impact. That context is what makes every downstream decision grounded in reality, not assumptions.

Decide: Security teams are drowning in signals that lack business context. The ServiceNow Veza Access Intelligence layers 30 billion-plus permissions across human, machine, and AI agent identities. These are not assigned roles, but actual access paths that are resolved and risk-scored continuously on top of that cyber asset foundation. Every decision is grounded in operational reality to reflect which asset is affected, what business service is supported, and what the blast radius is. **Exposures are prioritized by what matters most, not by raw severity scores or probabilistic guesswork.**

Act: Detection is only the beginning of the process. ServiceNow connects the dots from finding a problem to fixing a problem with AI agents autonomously remediating across the full security lifecycle from exposure to patch orchestration to incident containment — all without manual handoffs. **Most security platforms stop at the alert, but ServiceNow closes the loop, automating and connecting risk directly to the resolution without waiting for work to be assigned.**

Secure: Governance is not a late stage checkpoint but rather must be embedded throughout the process. ServiceNow enforces least privilege continuously and governs every agent, model, and workflow at the moment of action. In addition, every decision, exception, and remediation action is automatically captured as evidence. **When the board asks for proof of compliance, the answer is already there.**

Thank you for reading

Closing the ServiceNow shared responsibility gap

POWERED BY TURTL