

servicenow®



# Deployed but Ungoverned



The State of Agentic Security



# Table of contents

- 03** What you can't see, you can't secure
- 08** Confidence outpaces control
- 12** The ungoverned AI workforce. Chaos included
- 18** Security by design, not by accident
- 22** What you track, you can prove
- 28** Five moves for defensible security posture
- 35** Appendix

**What you can't see,  
you can't secure**



# Can governance move as fast as deployment?

Agentic AI has moved quickly from experimentation into real-world use, with 59% of organizations now moving beyond pilots. These systems are making decisions, accessing systems, and accumulating permissions across the business. That creates enormous opportunity, but it also raises a basic security question: is governance keeping pace?

Our study shows why that question matters. Fifty-six percent of leaders rate their agentic security as established, yet less than half (46%) have security and governance controls in place for agentic AI. Look beyond that confidence, and the gaps become clearer. Few organizations have named a single accountable owner for agentic security governance; few can see every agent through one interface, and most can't produce evidence of their security posture on demand.

As a CISO, I have learned that security is not proven by having a policy on paper. It is proven in the structure behind it: who owns decisions, whether controls can stop a bad deployment, and whether you can show what happened when someone asks. As AI systems become more autonomous, that operational accountability matters even more.

The organizations that are further along have built governance into how their platforms operate rather than adding it after the fact. They have a clearer picture of what is running, where it has access, and how it is behaving. They can act faster when something changes and demonstrate their controls when challenged. Their confidence comes from visibility and control, not simply intent.

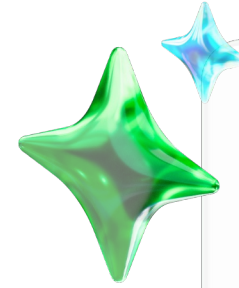
What follows in our global study is a closer look at where organizations are today, where the gaps remain, and what stronger agentic security looks like in practice. The controls you put in place today will determine how much of tomorrow you can trust to run on its own.



**Ben de Bont**

Chief Information Security Officer  
ServiceNow

# The state of agentic security



## What 3,766 security leaders revealed about agentic security

To understand how organizations are governing agentic AI, ServiceNow partnered with Phronesis Partners to conduct a global study across 20 countries and eight industries, surveying senior security and technology decision-makers, VP level and above.

### Three critical areas were explored:

- What organizations can see: which agents are operating and how much of the workforce is visible
- What they own: who is accountable for agentic security and whether security is built in early
- What they can prove: whether organizations can demonstrate their posture on demand, not just assert it

### An agentic security scale shows progress and opportunities

As part of this study, we developed an agentic security scale based on five key domains (attack surface, security by design, visibility, accountability, and audit readiness). Scale position is determined by what organizations have built, and placement is based on behavioral and structural survey responses that place each organization at one of four posture positions: Limited, Emerging, Advancing, or Defensible. See the scale methodology in the appendix.

## What the research uncovers

### Governance hasn't kept up with agentic AI

Each AI agent is a non-human identity accumulating permissions the enterprise can't fully see, and most organizations can't fully account for every AI agent running in production. That surface no longer stops at enterprise IT, as most organizations run agents in or interacting with operational technology or physical environments (such as industrial controllers, building systems, and medical devices).

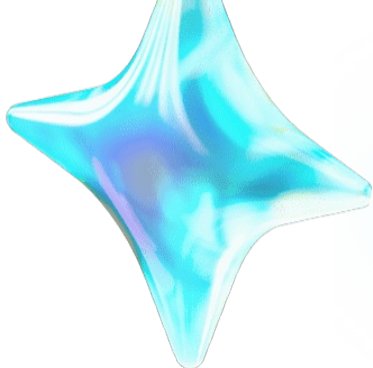
### Enterprisewide agentic security governance rarely sits with one person

Most organizations spread agentic security governance across several functions, and few can name a single individual accountable for the whole picture. That's the gap: when dispersed, ad-hoc groups own governance, accountability can prove difficult. No single individual or team is tracking how agent behavior, access, and risk connect across the enterprise.

### Few have defensible agentic security posture

The agentic security scale positions organizations by the controls they have built, not by self-assessment. On that measure, most sit short of a defensible posture. They have deployed agents faster than they have governed them, and the resulting exposure may stay hidden until something tests it.

# Agents run ungoverned, unchecked, and untraceable



## UNGOVERNED

### **Agents are deployed; governance is uneven**

In the last 12 months, 29% of security teams found AI agents running in production that were never registered or known. Governance cannot reach what it never saw arrive.

## UNCHECKED

### **A gate that isn't required is a gate that isn't there**

Only 32% have a mandatory automated gate that blocks deployment until an agent passes a defined security check, and the remainder of organizations rely on manual reviews or don't enforce reviews.

## UNTRACEABLE

### **On demand records of agent activity are lacking**

Only 39% of organizations say their governance framework explicitly covers documentation and audit trail requirements for agent activity.



# Today's agents are running on yesterday's security frameworks

## Most agentic AI is governed by legacy frameworks

Many organizations are governing agents with frameworks built for a pre-AI world, not for systems that act on their own. Existing frameworks assume a person makes each decision and can be held to it. Agents break that assumption, and few teams have rebuilt the model for how agents operate.

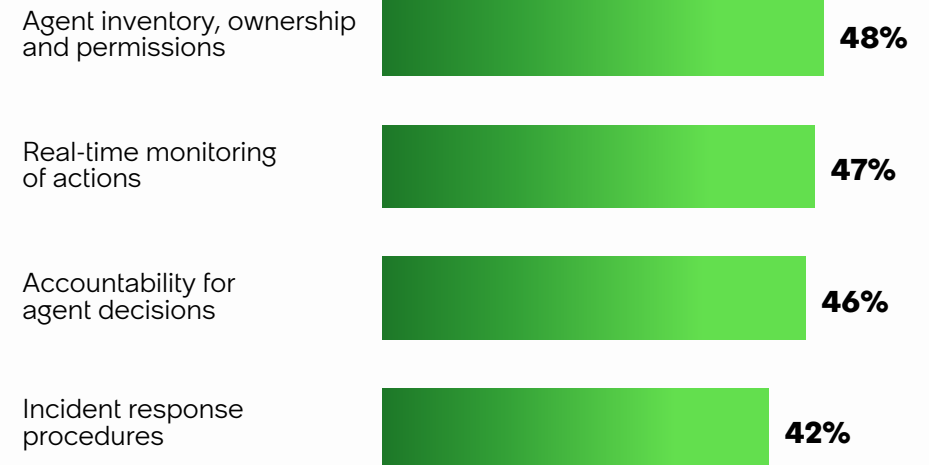


**AI agents introduce new and evolving risks organizations aren't prepared for. Addressing these emerging security challenges is critical to the secure deployment of AI-driven cyberinfrastructure."**

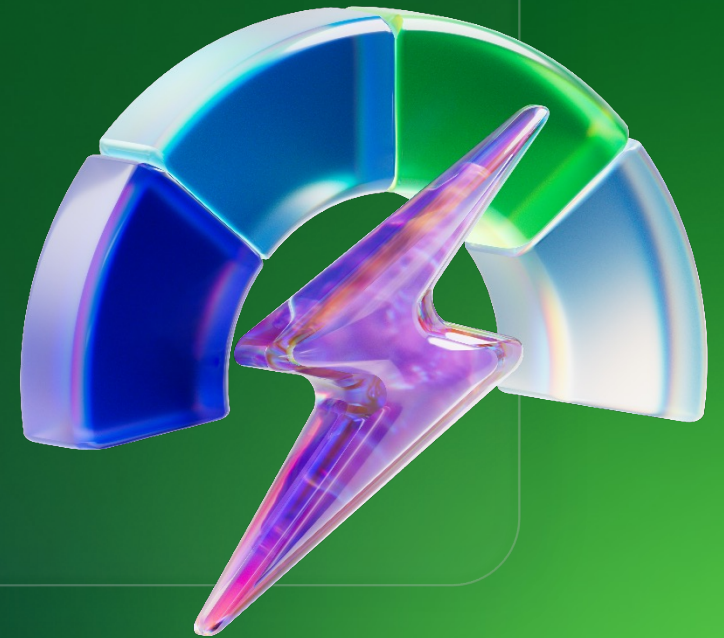
Neil Gong, Associate Professor, Duke University, Electrical and Computer Engineering

## Less than half have governance frameworks that cover key elements of AI agent deployments

*% that say framework explicitly covers the following*



# Confidence outpaces control



# Established in theory, exposed in practice

## Self-rated posture runs ahead of measured posture

Nearly six out of 10 leaders assess their agentic security as “established,” indicating they have purpose-built governance for agentic AI that is fully operational and demonstrable on demand.

But when looking past the self-assessment to the observable choices—who owns it, whether it is unified, and whether a gate can stop a bad deployment—a different picture emerges. Most organizations are running with less governance than they believe they have.

**56%**

of organizations assess their agentic security as established and purpose-built for agentic AI



## Yet only...

**20%**

have a single named, accountable owner for agentic AI governance

**21%**

have a unified single-interface visibility

**32%**

enforce an automated deployment gate

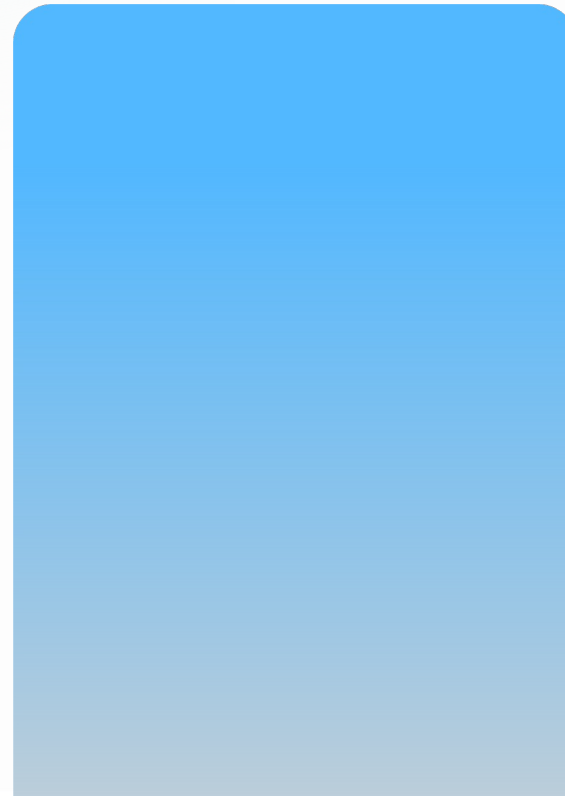
**47%**

can produce a complete evidence package on demand

**Incidents are  
common. Fast  
containment  
is not.**

**90%**

of organizations had an agentic  
security incident in the last year



ONLY

**36%**

of those organizations contained  
the incident in under 24 hours



# Few have defensible security posture

## The agentic security scale reveals progress

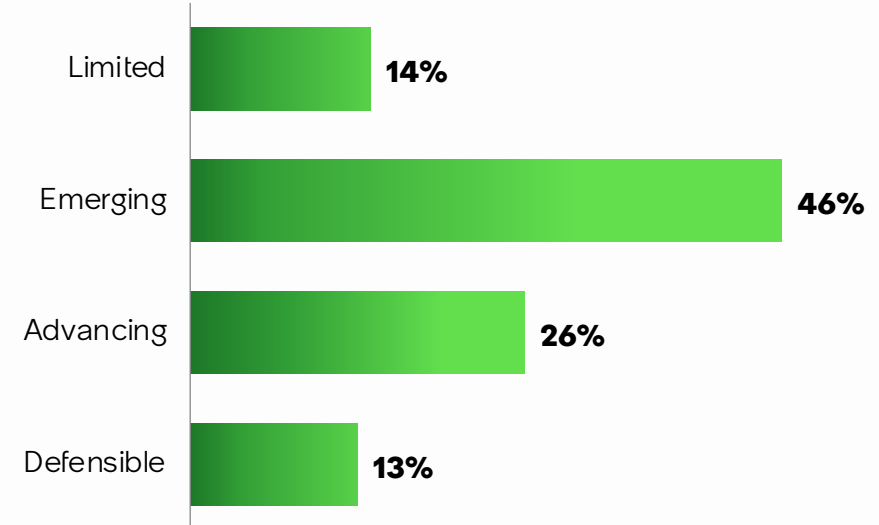
The scale places organizations into four posture bands, from limited to defensible. While many self-assess as having established agentic security posture, few hold up against a measured scale that examines how organizations are progressing across five key domains: attack surface, accountability, security by design, visibility, and audit readiness.

## Most are in early days of security posture development

While every organization in this study runs AI agents in production, only about one in eight has defensible posture. Most land in the earliest bands of the scale, still building foundations rather than operating from them. They have the agents, but what they often lack are the accountability, the visibility, and the evidence to stand behind them.

The full methodology and posture definitions appear in the appendix.

## Where organizations land on the scale



*Percentages do not sum to 100% due to rounding.*

# The ungoverned AI workforce. Chaos included



# Shift Zero starts with zero blind spots

For years, I've argued that every unsolved security problem starts with something unseen that introduces risk. Shift Zero makes that unforgiving. Zero is the only number that defeats an exponent, and you cannot zero out what you have never seen.

The organizations getting this right have full, contextual awareness of four things: what's running in their environment, what it can reach, how it's behaving against baseline, and who's accountable for it? They hold that in one shared context graph, continuously and in real time, as a condition of operating.

Most security leaders I speak with know agentic AI creates new exposure by rapidly expanding the attack surface. Far fewer have built the infrastructure to answer those four questions at machine speed, and their adversaries already operate there. Answering those fast takes governed autonomy, with the human on the loop rather than in it.

The harder version of this sits outside enterprise IT, and it's the part I see underestimated most. Push an agent, read the logs, query the API: none of that works where there is nothing to install. Teams that solved discovery in the cloud assume the approach travels with them. It doesn't, and the assumption is expensive because the agents are already there.

Shift Zero shows up differently in each domain: enforcement before the code is finished, remediation at discovery, controls before provisioning. Every one of those assumes you already know what you are governing.

Inventory isn't a project you finish. It's a precondition you maintain everywhere agents operate, by whatever method each environment allows. But seeing an agent isn't the same as controlling it. You still have to secure it, ideally before it ever ships, and manage it as conditions change. That is Shift Zero: prevention at the point of action, exposure driven toward zero rather than administered as a backlog. Zero blind spots. Zero ungoverned agents. Zero triage queue. Your ownership model, review gates, and evidence trail all rest on the ability to see, secure, and manage, which you either have or you don't. Get that right, and the rest is engineering.



**Nadir Izrael**

Global VP of Cybersecurity  
and Risk Products  
ServiceNow

# AI compounds the attack surface

## Every AI agent is a non-human identity with access

Unlike a person, an agent carries no instinct for boundaries. It executes what it is permitted to do, at machine speed, across whatever systems and data it can reach. Permissions accumulate faster than most governance frameworks can track them.

## What's running outpaces what's recorded

Forty-nine percent of organizations run between 100 and 999 agents, and 35% run over 1,000. The actual count often exceeds the known inventory because registration depends on someone remembering to do it. What gets missed may surface later as shadow AI, found only after it was already running.

### Most claim their AI agent record is complete

**57%**

say they have a full, accurate record of every AI agent in production and have processes to track changes

### Yet few register agents automatically

ONLY

**34%**

automatically register a new agent at the point of deployment through a technical control

# Access is mapped on paper but not in practice

## Mapping what exists is easier than mapping what it can reach

Context is everything an agent can reach: the data it touches, the systems it connects to, the permissions it has accumulated, and the identities that can access and act on data. Keeping the mapping up to date and complete as access roles shift in real time is where most tools give up.

WHILE

76%

say they maintain a complete, current map of every agent's access



ONLY

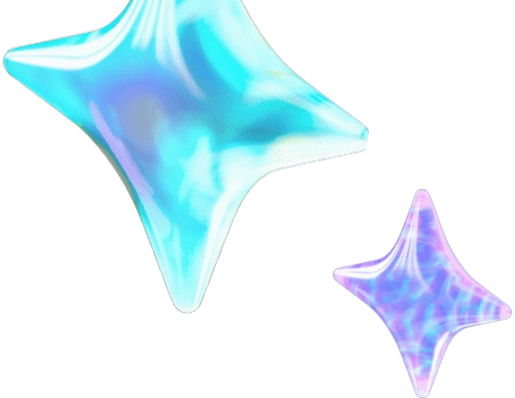
19%

say they can see more than 90% of their agents in real time



**To unlock their full potential, AI security agents need deep access to data and systems, but that power creates inherent risk. Organizations must enforce strict access controls, continuous monitoring, and mandatory human oversight for high-stakes decisions. As agent autonomy grows, so must their guardrails and security scaffolding around them—with security itself continuously and recursively improving to keep pace.**

Chaowei Xiao, Assistant Professor at Johns Hopkins University and Researcher at NVIDIA

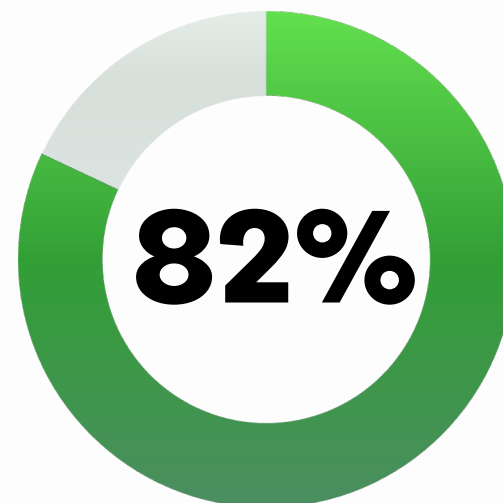


# Agentic AI extends to physical and OT

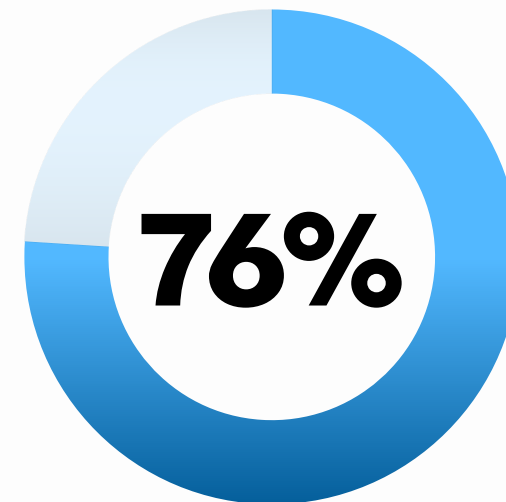
## AI agents have crossed into operational technology (OT) and physical security environments

Agents are managing industrial control systems, sensors, building access, surveillance, and connected medical devices. Where they reach, the frameworks built for enterprise IT don't always follow. The controls, the accountability, and the review gates that hold inside the data center often stop at the boundary.

Solving visibility in one environment does not always translate into solving it across the full IT, OT, and physical surface agents now occupy.



run agents in or interacting with OT or physical environments



have had an OT or physical incident involving an agent

**44%** report stronger visibility in enterprise IT than in OT or physical

**32%** have a separate governance framework specifically designed for OT or physical contexts

### Runtime, not real-time



**Runtime visibility is lacking; it persists because security tools have not much evolved to monitor agent decision making in real time.**

CIO/CTO, Australia

HEALTH

### Pace outruns policy



**AI adoption is moving faster than security and oversight can keep up.**

Chief Data Officer, U.S.

MEDTECH

### Evidence trail incomplete



**We generate massive, unstructured audit logs our traditional database can't handle efficiently. We can't store full reasoning traces for more than 30 days, so forensic analysis is always incomplete.**

SVP/VP Compliance, US

RETAIL

### Regulation shifting underfoot



**Because of changing regulations, shifting priorities, and data-privacy concerns, we are trying to provide sufficient guardrails via AI governance to ensure risks are within acceptable ranges.**

Chief AI Officer, UK

WIRELESS COMMUNICATIONS

### Change control excludes AI



**The process for system changes doesn't include sign-off on AI model iterations, and commissioning controls remain incomplete.**

SVP/VP Compliance, Germany

INSURANCE

### Ownership left undefined



**Liability frameworks are unclear...no formal documentation splits risk ownership across teams.**

SVP/VP Compliance, UK

AUTOMOTIVE

# Agentic AI governance obstacles

**Security by design,  
not by accident**



# Build in security before agents scale

As organizations move quickly to implement AI and agentic systems, the instinct is to get the use case working and deal with risk later. That's understandable, but it creates real exposure with agents because they may have access, autonomy, data context, and workflow authority before security has shaped the design.

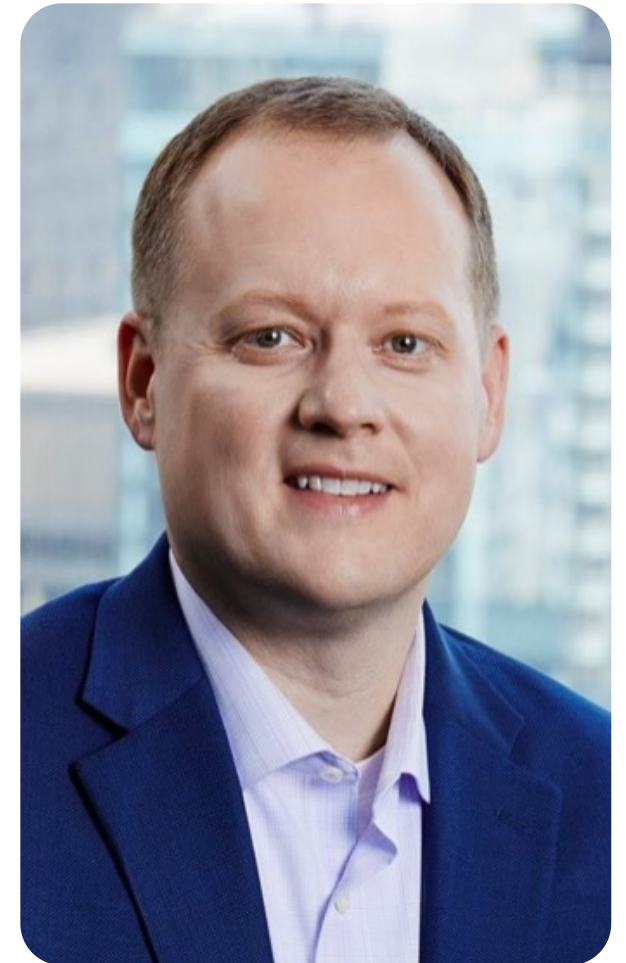
At Accenture, we see this as an operating model issue, not just a security issue. AI, data, engineering, legal, risk, and security often sit in different lanes, with different timelines and different measures of success.

The fix? Make security part of the front-door process. When security is involved before or during design, the team can make the right decisions while the solution is still flexible. They can define what the agent is allowed to do, what data it can touch, when a human must approve an action, how evidence is captured, and how the agent will be monitored once it is live.

When security comes in after the fact, the team usually has to retrofit controls around something already built. That is slower, more expensive, and often less effective.

Better outcomes from involving security early are not surprising. By building the control model into the architecture, you get faster containment, clearer evidence, and fewer surprises. If you wait until the end, you are always catching up. That's why we encourage secure by design and continuous risk operations.

A repeatable control model allows security to scale with the business instead of slowing it down. So, make the secure path the easiest path: put controls in the pipeline, connect them to provisioning and identity, capture evidence automatically, and give leaders visibility through dashboards and workflow. That's how you preserve speed without losing control.



**Paul Kunas**

Managing Director  
Accenture

# Early governance beats late detection

## The point at which security enters shapes what follows

Security can enter an agent's life at any point: before design, during design, during development, during testing, after it goes live, or not at all. Where it enters decides what it can do.

Security that arrives before the design work starts sets the permissions, defines the logging, and draws the boundaries the agent will run against. Security that arrives later inherits all three. An agent can't run without permissions, so they already exist by the time anyone reviews them. Permissions are easy to grant and hard to revoke, and a gate added later inspects an arrangement it had no hand in making.

ONLY

**44%** of organizations bring in security before agent development begins

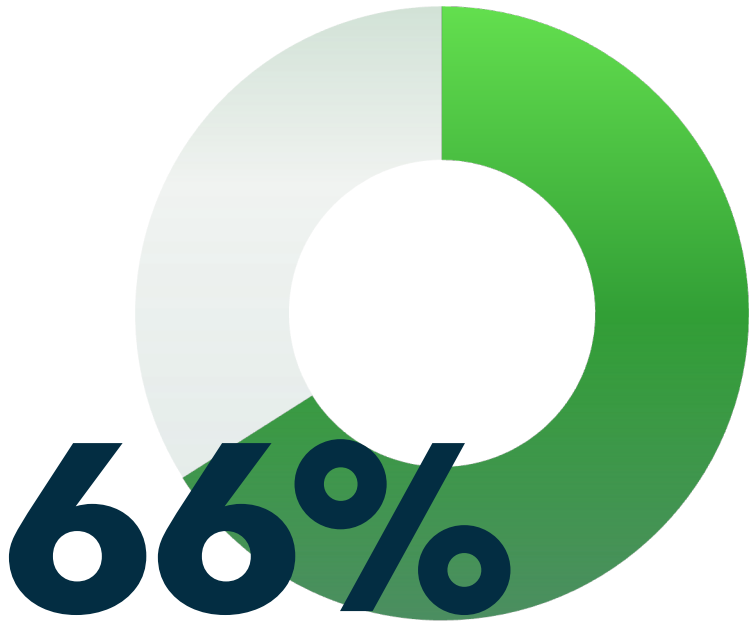


**High time pressure during rapid AI implementation prevents the creation of sufficient safety rules to mitigate risks early on.**

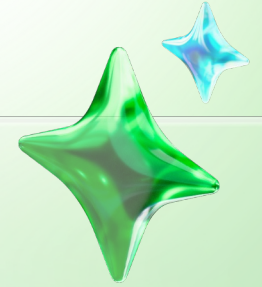
SVP/VP Security, Pharmaceutical, France



# Spotting rogue behavior isn't stopping it



cannot act automatically when an agent behaves anomalously



## Only half detect in real time

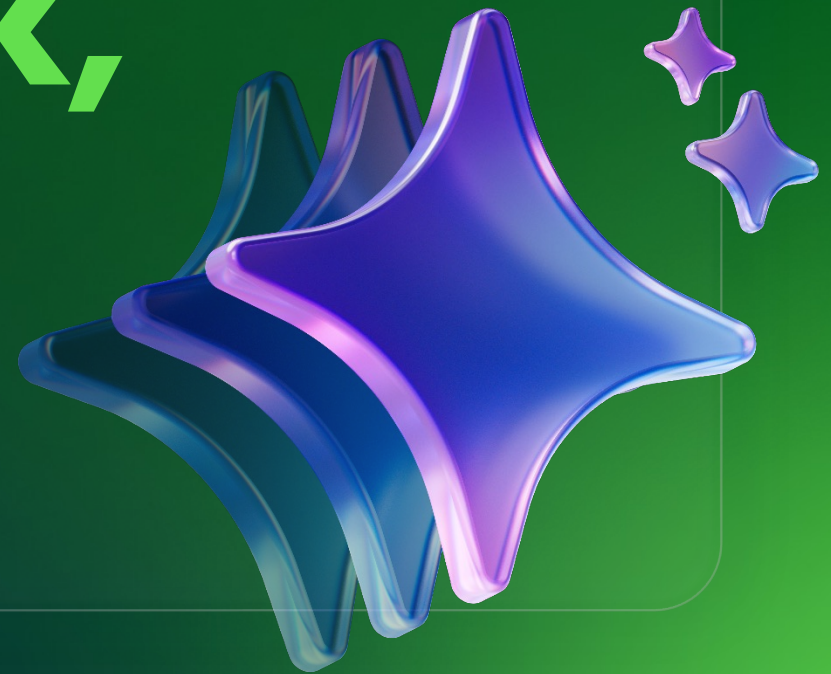
Approximately half (51%) of organizations have automated real-time detection for anomalous AI agent behavior. The rest rely on scheduled monitoring or manual review, which means the behavior surfaces on a cycle rather than as it happens.

## Detection doesn't deliver response

Many organizations do have structure after detection. Findings are routed to a named owner with a defined resolution time. But structure isn't speed, and the sequence still waits on a person before anything changes in the environment.

Real-time detection and automated response are two separate capabilities. The organizations closing the gaps didn't take people out of the decision. They moved them from approving each action to setting the rules governing those actions, which is the way review can keep pace with something operating at machine speed.

**What you track,  
you can prove**



# Tracking the agent identity crisis

I spent much of my career in identity governance and administration (IGA) and privileged access management (PAM), and the thing that always struck me about deprovisioning access is how much of it hangs on an event that has nothing to do with security. Somebody resigns, HR closes a record, and that triggers a cascading effect of tickets, disablements, access removals, and more. That one administrative moment is what causes access to end at most organizations, and everything downstream of it works reasonably well because the trigger is reliable.

An agent inherently doesn't have the same trigger. There's no resignation, no last day, no badge to turn in. It gets stood up for a migration that wraps at a point in time, and the credentials it was issued keep working indefinitely because nothing in the environment realizes the project ended.

According to our research, 76% of the leaders say they keep a complete, current map of every agent's access. Yet only 19% say they can see more than 90% of their agents in real time. They're describing what's written down, but the space in between that and what's running is where attackers start looking.

Some of this is a tooling problem that predates agents. Most identity systems are good at telling you which role got assigned to whom but bad at telling you what that role amounts to when following it through a couple of nested groups, an inherited cloud policy, and a service account somebody previously wired up.

We got away with that imprecision for humans because access reviews ran quarterly and a manager clicking approve on 400 entitlements was, if not good, at least survivable. An agent making thousands of API calls a day doesn't leave that much margin. You need what it can reach today as a computed answer, not a configuration lookup.

The hardest part is revocation, and it's where a lot of agentic security programs may eventually fail. Deciding to remove access and actually removing it are two different events. A closed ticket proves somebody agreed but doesn't prove the permission is gone from the system that grants it. When a regulator asks in 18 months whether that overprivileged agent was really cut off at a point in time, the answer should come back from the target system, not from the workflow that asked politely.

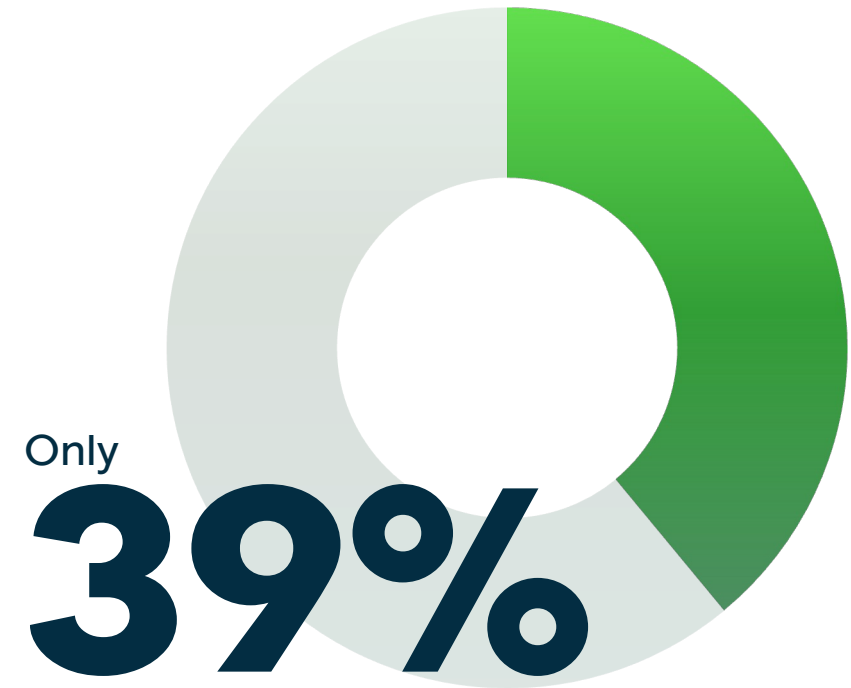
If you're standing up an agent program right now, there are two questions to answer before the count gets away: what can this agent reach today, and when you took some access away from it, did it actually go? Organizations that can answer those two questions keep working the same way at 10,000 agents as they did at 10. The ones that can't get asked eventually anyway, by an auditor, on a deadline, about an agent nobody remembers approving.



**Rahul Prakash**

VP and GM, Identity Security  
ServiceNow

**Documentation  
is the element  
governance  
frameworks most  
often leave out**



of organizations have a governance framework that explicitly covers documentation and audit trails for agent activity

# An audit trail you can't produce is a posture you can't prove

Only 47% of organizations can produce a complete evidence package on demand. For the rest, evidence is assembled under pressure from systems that were likely not designed to answer the question together.

Whether an organization can prove its posture tracks with how it runs security. Forty-seven percent manage agentic security risk on a unified platform. The rest spread it across integrated tools, point solutions, or manual work. When the system that runs security is also the system of record, the audit trail builds itself.

## A unified platform improves security outcomes

● Unified platform

● All others

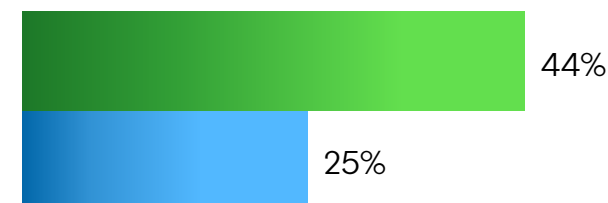
Evidence captured continuously and produced on demand



Automated real-time alerts of anomalous AI agent behavior captured



Exposure or policy violation of an AI agent auto remediated



### No kill switch



**Coding agent with legitimate credentials deleted email volumes before we could intervene. No kill switch or governance mechanism existed to prevent or detect unauthorized actions.**

SVP/VP Identity and Access Management, Singapore

RETAIL

### Static rules, live agents



**Static access rules cannot block AI's self-escalated privilege requests.**

SVP/VP Security, Japan

AUTOMOTIVE

### Unregistered, unaudited



**Endpoint tools failed to block shadow AI agents staff deployed; we had no policy to audit unapproved agent creation.**

SVP/VP Compliance, U.S.

SPECIALTY RETAIL

### Manipulated past controls



**Our traditional data-loss prevention tools completely missed a situation where a customer support agent was tricked via prompt injection into leaking internal project names, exposing an AI-output audit gap.**

SVP/VP Security, U.S.

HOSPITAL & LTC

### Trusted creds, untrusted acts



**An admin token deleted backup snapshots. Our SIEM [Security Information and Event Management] logged it but treated it as a routine cleanup because the token was from a trusted service account.**

SVP/VP Compliance, Australia

GOV AGENCY

### Built for people, not agents



**When an internal AI agent started pulling customer data across five tools and emailing summaries, the governance gap was clear.**

CIO, Netherlands

AUTOMOTIVE

# Where existing tools and processes failed

# Five moves for defensible security posture

Organizations with defensible posture didn't get there by adding review steps. They moved the controls into the systems that do the work so governance runs at the speed the agents run.

That choice shows up in everything the study measured downstream. Agents are inventoried automatically rather than recorded after the fact. Enterprisewide accountability sits with a named individual. Evidence is captured as work happens rather than assembled under pressure. Posture can be demonstrated on demand because nothing has to be reconstructed.

And the discipline holds across enterprise IT, operational technology, and physical security environments.

1

Build a continuous inventory and map agent access

2

Embed security before design

3

Unify visibility across agents, identities, and posture

4

Capture continuous evidence

5

Assign an accountable leader across the enterprise

## MOVE 1

# Build a continuous inventory and map agent access

Register every agent the moment it goes live, with its reach attached.

## Make the record a byproduct of deployment

- 1 Register agents at deployment. An inventory built after the fact is already out of date.
- 2 Record what each agent can reach: the data, systems, and permissions it holds today.
- 3 Apply the same standards, regardless of where the agent originates. Vendor and marketplace agents need an owner and a scope too.
- 4 Register each agent as a CMDB item in AI Control Tower, and agentlessly discover OT and IoT assets.

## MOVE 2

# Embed security before design

Put the security requirements in the project brief, before there's an architecture to review.

## Move the conversation upstream of the architecture

- 1 Set the requirements while it is still an idea, not once the architecture is built.
- 2 Give security a seat in that first conversation and authority over what agents reach.
- 3 In OT and physical, push it into procurement. Agents arrive embedded in the equipment.
- 4 Write policy as code and hold deployment until the check passes.

## MOVE 3

# Unify visibility across agents, identities, and posture

Run agents, identities, and posture on one platform, so the answer is current when the question arrives.

## One platform, one data model, one answer

- 1 Visibility means the answer is current the moment someone asks.
- 2 Use one data model for agents, identities, and posture.
- 3 Carry that view past IT, into OT and physical security.
- 4 Give agents the context they need to act with precision across any data or system.

## MOVE 4

# Capture continuous evidence

Capture the approval, the scope, and the action together, so the evidence is ready before anyone asks.

## Evidence is recorded, not assembled

- 1 Log approval, scope, and action at the moment they happen.
- 2 Sort out retention now. Traces may get trimmed at thirty days; auditors ask about years.
- 3 Design for the later question: what was this agent allowed to do, and who approved it?
- 4 Let evidence fall out of the work, and monitor controls continuously.

## MOVE 5

# Assign an accountable leader across the enterprise

Give a leader enterprisewide accountability, while each function stays responsible for the agents it runs.

## Shared responsibility still needs a leader

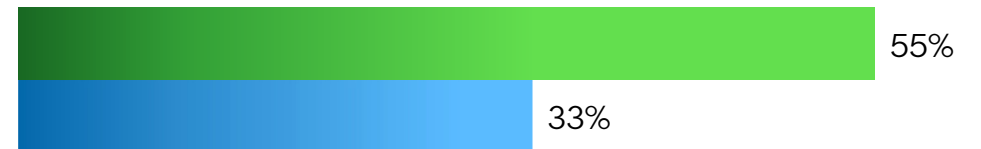
- 1 While agentic security is everyone's job, overall governance should have a dedicated, accountable leader.
- 2 Give that leader real scope: the framework, the gates, the response plan, and the evidence.
- 3 Functions still own the agents they run. Split it by environment and the seams become the exposure.
- 4 One named owner and a governed lifecycle per agent in AI Control Tower.

# Defensible security posture delivers greater results

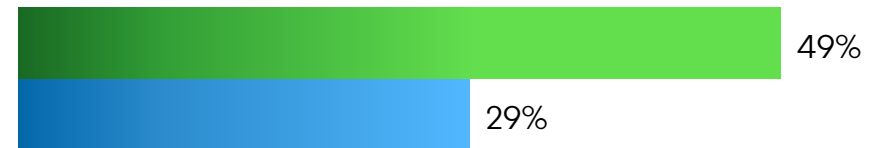
Automated real-time anomaly detection



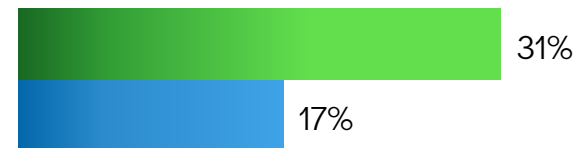
Contain incidents in under 24 hours



Mandatory automated deployment gates



Real-time visibility into 90%+ of agents



● Defensible security posture

● All others

# Secure, then scale

Our research points to a simple truth: agentic AI creates real value when people can trust it. That trust grows when governance is built directly into the systems where agents operate. Deployment isn't the hard part anymore. It's about governing what you've already deployed and proving its compliance at the moment someone asks.

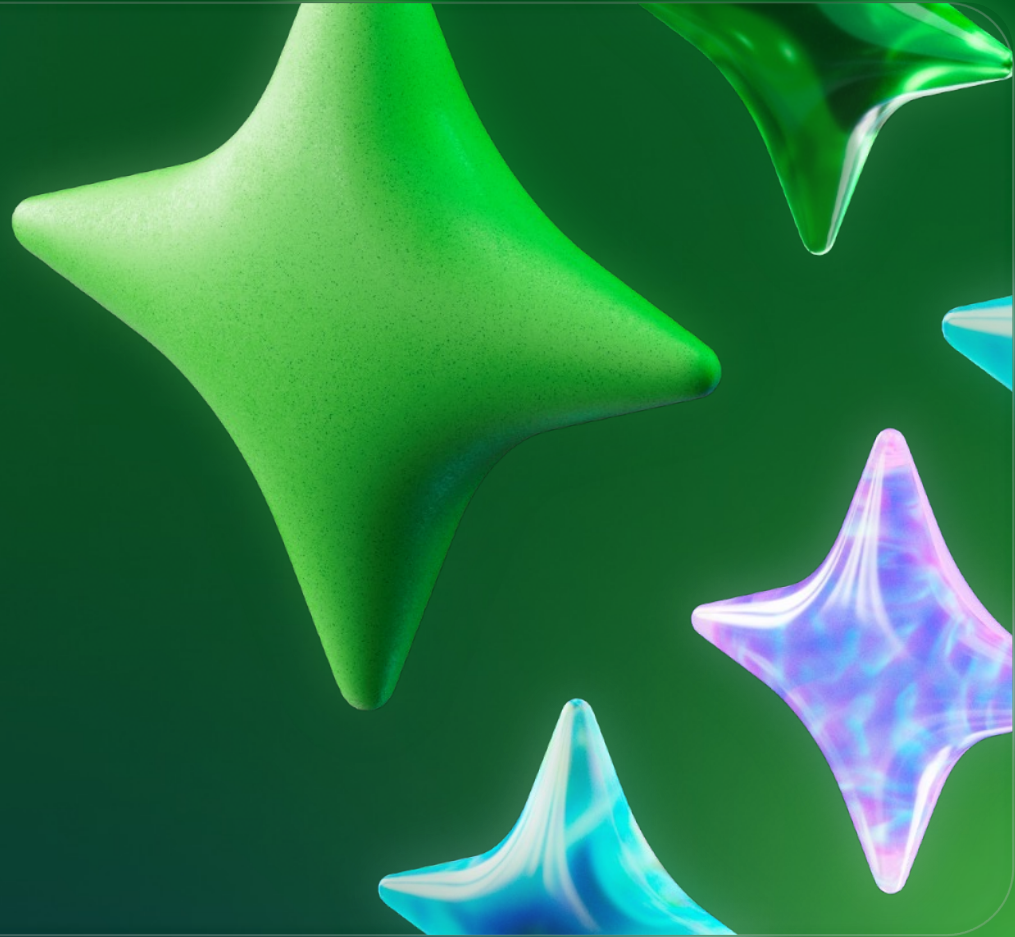
With the right controls in place from the start, every new agent carries the same guardrails, and security teams get the visibility, ownership, and evidence they need to move as quickly as the business needs them to. Incidents can be resolved faster. The proof is easier to find. And confidence becomes something teams earn every day, not something they simply hope for.

The organizations that treat governance as an afterthought will spend the next wave of AI adoption trying to catch up to systems that are already moving ahead. But the leaders who build it in from the beginning—with ongoing inventory, clear ownership, connected visibility, and evidence captured as work happens—will define what it means to run an AI workforce responsibly, confidently, and at scale.

**That's how leaders will shape the agentic era with confidence, clarity, and impact.**



# Appendix



# Authors and contributors

## Authors



**Ben de Bont**  
CISO  
ServiceNow



**Nadir Izrael**  
Global VP of Cybersecurity  
and Risk Products  
ServiceNow



**Rahul Prakash**  
VP and GM, Identity Security  
ServiceNow

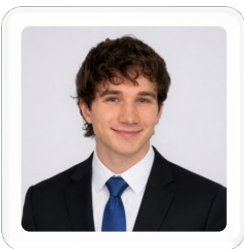


**David James**  
Director, Product and  
Solutions Marketing  
ServiceNow

## Research leaders



**René Stranghoner**  
Head of Thought  
Leadership Research  
ServiceNow



**Evan Volness**  
Research Analyst,  
Thought Leadership Research  
ServiceNow

## Research partners

Phronesis Partners is a global research, analytics, thought leadership, and advisory firm with deep expertise in technology, AI, and automation. From evaluating how AI is reshaping enterprise demand to helping firms refine their market positioning in fast-evolving categories, it enables clients to translate rapid technological change into tangible business outcomes.

Science Says is a research advisory firm dedicated to translating the latest scientific research in AI, management, marketing, and business into practical insights.

## Acknowledgements

A special thanks to Jessica Buckley, head of brand content; Marissa Amendolia Finn, director of brand content experience; Annalyn Kurtz, director of thought leadership editorial; Emma Kieckhafer, director of social media; Rama Sawhney, integrated marketing director, security and risk; Jessica Denney, senior content strategist, security and risk; and Ellen James, senior marketing operations, security and risk

Thank you to all the ServiceNow colleagues who helped bring this research to life, especially Evan Ramzipoor, Ryan Breen, Kim Nelson-Ingram, Angela Chen, Sheryl Domingue, Zoe Gaylard, Phillip del Moral, and Jingsi Chen.

# Survey demographics

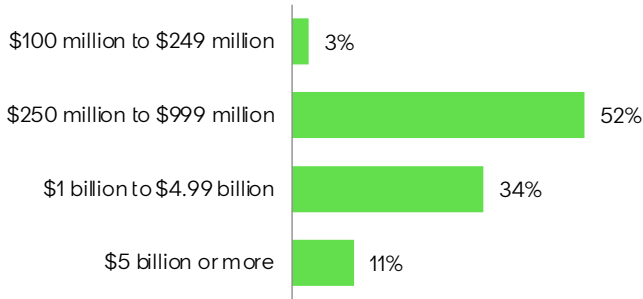
## Regions and countries

|                 |              |
|-----------------|--------------|
| <b>Americas</b> | <b>1,300</b> |
| Brazil          | 150          |
| Canada          | 200          |
| Mexico          | 150          |
| U.S.            | 800          |
| <b>APAC</b>     | <b>1,201</b> |
| Australia       | 300          |
| India           | 500          |
| Japan           | 200          |
| Singapore       | 201          |
| <b>EMEA</b>     | <b>1,265</b> |
| Belgium         | 75           |
| France          | 150          |
| Germany         | 225          |
| Netherlands     | 175          |
| Nordic region   | 90           |
| Saudi Arabia    | 125          |
| UAE             | 125          |
| UK              | 300          |

## Industry

|                |     |
|----------------|-----|
| Banking        | 655 |
| Government     | 336 |
| Healthcare     | 450 |
| Insurance      | 450 |
| Life sciences  | 395 |
| Manufacturing  | 585 |
| Retail         | 470 |
| Tech and telco | 425 |

## Revenue



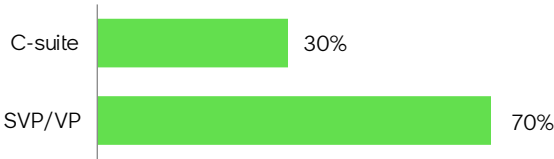
## Participating organizations

All participating organizations have AI agents or autonomous AI tools in a production environment.

## Respondent qualification

Respondents were required to be at the VP level or higher within their organization and either be the primary decision-maker for security or AI governance strategy or be directly involved in and influence security or AI governance strategy.

## Role



# Methodology

## The agentic security scale

The scale is built from five behavioral pillars: attack surface, security by design, visibility, accountability, and audit readiness. Each pillar is scored from responses to diagnostic survey questions that measure observable behaviors and steps organizations have taken to build agentic security, and posture is defined in four categories:

- **Limited:** Security governance exists, but it was never designed with AI agents in mind. Agents go live without an agent-specific inventory, without clear ownership, and without any evidence trail built for them. The controls are there. They just were not made for this.
- **Emerging:** The organization sees the gap and has started to respond, but the response has not yet hardened into structure. Existing security policies get stretched over agentic deployments unchanged, and accountability stays shared or unspoken across the organization.
- **Advancing:** A defined framework is in place, and the structural choices behind it were made on purpose. Coverage is not complete, and some evidence still has to be pulled together after the fact. The foundation holds. What remains is closing the gaps.
- **Defensible:** Governance is built into how the organization operates. Agents are inventoried automatically, accountability sits with a named individual, evidence is captured as it happens, and posture can be shown on demand with nothing to reconstruct.

## Scoring methodology

Every organization earns its place on the scale through measured behavior. Five dimensions determine placement, each scored 1 to 4, and dimensions are weighted:

### Attack surface – 25%

How is a new AI agent discovered by security tools at deployment?  
Automatic registration = highest, no process = lowest

### Security by design – 25%

At what stage does security governance begin in the deployment process?  
Before design = highest, no involvement = lowest

### Visibility – 20%

How is a complete view of agent activity obtained?  
Single interface = highest, not possible = lowest

### Accountability – 15%

Who is accountable for agentic AI security?  
Named individual = highest, undefined = lowest

### Audit readiness – 15%

How fast can a complete evidence package be produced?  
Immediate/on demand = highest, not possible = lowest

The weighting is based on proactive and reactive measures. Proactive dimensions—attack surface and security by design—carry more weight than the reactive ones because reducing exposure before an agent goes live does more for posture than catching problems after.

- Limited: < 2.5
- Emerging: 2.5 to < 3.1
- Advancing: 3.1 to < 3.5
- Defensible: ≥ 3.5

The cutoffs sit above the whole numbers by design. Each tier reflects dominant behavior across all five dimensions.



**ServiceNow** (NYSE: NOW) is the AI control tower for business reinvention. The ServiceNow AI Platform integrates with any cloud, any model, and any data source to orchestrate how work flows across the enterprise. By unifying legacy systems, departmental tools, cloud applications, and AI agents, ServiceNow provides a single pane of glass that connects intelligence to execution across every corner of business. With more than 100 billion workflows running on the platform each year, ServiceNow helps organizations turn fragmented operations into coordinated, autonomous workflows that deliver measurable results.

Learn how ServiceNow puts AI to work for people at [servicenow.com](https://servicenow.com).