

Special Edition
Private Cloud Outlook 2026

The New Security Mandate for Enterprise AI



Contents

Introduction	3
AI-Driven Threats Are Outpacing Traditional Operations	4
The impact on IT priorities	5
The three-year security horizon	7
The geopolitical dimension	8
Current Governance Models Are Lagging	9
Private Cloud Is the High-Confidence Answer to Security Challenges	10
Growing trust in private cloud	11
Recommendations for IT Leaders	12
Take the Next Step: Align Infrastructure to the Threat	13

Introduction

Enterprise AI is no longer experimental. It's in production, at scale, and it's rewriting the rules of enterprise security.

Our recently published [Private Cloud Outlook 2026](#) report, based on research from 1,800 global IT decision-makers across eight countries, explores the impacts of AI on enterprise IT. As IT organizations move AI workloads into production, they're gravitating toward private cloud for better cost predictability, governance, and performance. They are also facing new security challenges that traditional tools and techniques weren't built to handle.

Building on the Private Cloud Outlook 2026 findings as well as our first special report, [From Modernization to AI Readiness: The New Platform Imperative](#), this report examines how organizations are managing security today, where confidence is highest and lowest, and what the next three years will demand.

Three findings stand out:

01

AI-driven threats are outpacing traditional operations.

The volume, speed, and complexity of threats are overwhelming most security teams.

02

Current governance models are lagging.

Many IT teams lack centralized security governance and the consistent, automated enforcement that production-scale AI needs.

03

Private cloud is the high-confidence answer.

IT leaders report significantly higher trust in private cloud for recovery, compliance, and sovereignty, choosing it two-to-one over public cloud for their most critical applications.

AI-Driven Threats Are Outpacing Traditional Operations

Before diving into the research findings, let’s consider the external context. The threat landscape has changed structurally in recent months with the emergence of frontier AI models that can discover and exploit vulnerabilities in a matter of hours. Responding after a breach is no longer sufficient — the speed of AI-driven threats requires a shift to proactive security for private cloud workloads. The data in this report was collected just before the industry began responding to these new risks. Even so, the findings remain highly relevant to understanding today’s security landscape and enterprise IT readiness.

Recent media analysis depicts how quickly threats are evolving:

	World Economic Forum (April 20, 2026): Experts warn that the risk of frontier AI is a fundamental resilience issue for global stability. See World Economic Forum’s analysis .
	ISACA (April 17, 2026): Security analysts point out that the “time to exploit new vulnerabilities has been reduced from days or weeks to mere hours.” Read more in ISACA’s Industry News .
	Reuters (April 13, 2026): Regulators and security researchers raise alarm bells about advanced models that “could expose legacy banking systems to unprecedented cyber risk.” See the coverage by Reuters .
	SecurityWeek (April 7, 2026): Frontier AI models have already identified thousands of zero-day critical vulnerabilities, including a 27-year-old flaw in OpenBSD. Read the SecurityWeek article .

These articles share a common theme: The same capabilities that make AI powerful for enterprises make it advantageous for attackers.

The impact on IT priorities

Even before AI took center stage, security was already the biggest pressure in cloud management. As noted in the Private Cloud Outlook 2026 report:

Security dictates where workloads live. Thirty-two percent of IT leaders name security and compliance as the single most important factor when deciding where to place mission-critical workloads—ranking it above cost, performance, and speed.

Security is driving companies back to private infrastructure. Fifty-one percent of organizations that have repatriated (or are considering repatriating) workloads from the public cloud cite security or compliance concerns. This is the number-one driver behind repatriation, up from 27% in 2025.

Security is the biggest public cloud hurdle. Security risks are cited as a top-three public cloud challenge by 29% of respondents, making it the number-one challenge globally. Compliance follows closely at 27%.



AI raises the stakes further. Data protection and privacy is now the number-one new IT requirement created by AI, cited by 37% of leaders. Security controls and risk management follow at 36%, and data sovereignty and location constraints at 29%. These top requirements are about governance—not infrastructure capacity or cost. The hardest part of scaling production AI is protecting the data and meeting the compliance obligations that come with it.

Compliance is a big concern: 61% of IT leaders are very or extremely concerned about meeting regulatory compliance and data residency rules for AI workloads.

TOP

AI Requirements

37% of enterprises say **data protection and privacy** is the **biggest new IT requirement created by AI**

Q: Where is AI creating biggest new requirements for IT; n=1800

61%

are very or extremely **concerned about meeting regulatory compliance and data residency requirements** for AI-based workloads

Q: How concerned is the organization about the following aspects of generative/agent AI: Infrastructure costs, AI hardware lock in, meeting residency requirements and data residency requirements; n=1800



The three-year security horizon

Compliance anxiety is already showing up in forward planning. Looking ahead, 69% of enterprises are very or extremely concerned about meeting data privacy regulations when storing data in the public cloud. Meanwhile, 67% worry about maintaining business continuity during a public cloud outage, and 63% are concerned about keeping up with evolving compliance requirements in the public cloud.

Two of the top-three security requirements pertain to data governance and sovereignty. Only one (ransomware protection, cited by 37%) represents a traditional perimeter security requirements. That is a meaningful change to what “security” means in practice.

TOP SECURITY REQUIREMENTS OVER THE NEXT 3 YEARS

#1

Data privacy requirements (GDPR, personal data protection)

#2

Securing emerging workloads and technologies (AI)

#3

Protecting against cyberattacks including ransomware

Q: Which security-related requirements will have the greatest impact on IT in next 3 years; n=1800

CURRENT CONCERNS ABOUT STORING DATA IN PUBLIC CLOUD — VERY/EXTREMELY CONCERNED

69%

Ensuring compliance with data privacy regulations

66% in 2025

67%

Ability to maintain business continuity during an outage

New in 2026

63%

Keeping up to date with evolving requirements

61% in 2025

Q: Concerned with allowing aspects of storing data in the public cloud; n=1800



The geopolitical dimension

Geopolitics has become an infrastructure problem. Four out of five IT leaders say geopolitical and regulatory factors are actively shaping their IT strategy right now.

These pressures carry real operational and financial consequences. Nearly half of enterprises (49%) report increased compliance and audit requirements, meaning they are spending more on compliance overhead than they did a year ago. On top of that, 41% are experiencing rising infrastructure costs and complexity as a direct result of these geopolitical shifts.

For many, the impact requires architectural changes. Thirty-seven percent of organizations need to

change where their data is stored or processed. Another 30% say political factors are actively forcing them to repatriate workloads back from the public cloud or halt their planned cloud migrations altogether.

Jurisdictional demands also impact internal teams and operations. Thirty-six percent of leaders note that achieving sovereignty requires building entirely new skills within their IT teams, while 31% are rewriting their disaster recovery and business continuity plans just to comply with local laws.

Trying to address these sovereign deployment requirements reactively is a recipe for disruption and massive migration bills down the road. The organizations staying ahead of this are the ones building sovereignty directly into their infrastructure operating model today.

Enterprises that address sovereign deployment requirements reactively will face more disruptive and more expensive migrations later. The organizations getting ahead of this are building sovereignty into the infrastructure operating model now.



Current Governance Models Are Lagging

Building sovereignty directly into infrastructure requires achieving automated, consistent enforcement at scale. Most organizations aren't there yet.

We see this gap clearly in how security policies are enforced. **Nearly two-thirds of enterprise organizations—64%—have not reached full security enforcement automation. In fact, only 36% of organizations have reached the highest level of maturity,** where security is centrally governed and enforced. The remaining 64% are managing security in fragments:

- Thirty-six percent define policies centrally but apply them locally, which naturally leads to inconsistent protection.
- Sixteen percent have common standards but variable execution.
- Twelve percent still operate in disconnected silos.

Without consistent, automated policy enforcement across workloads, organizations also lack the internal controls needed to prevent threats from propagating laterally within the private cloud environment.

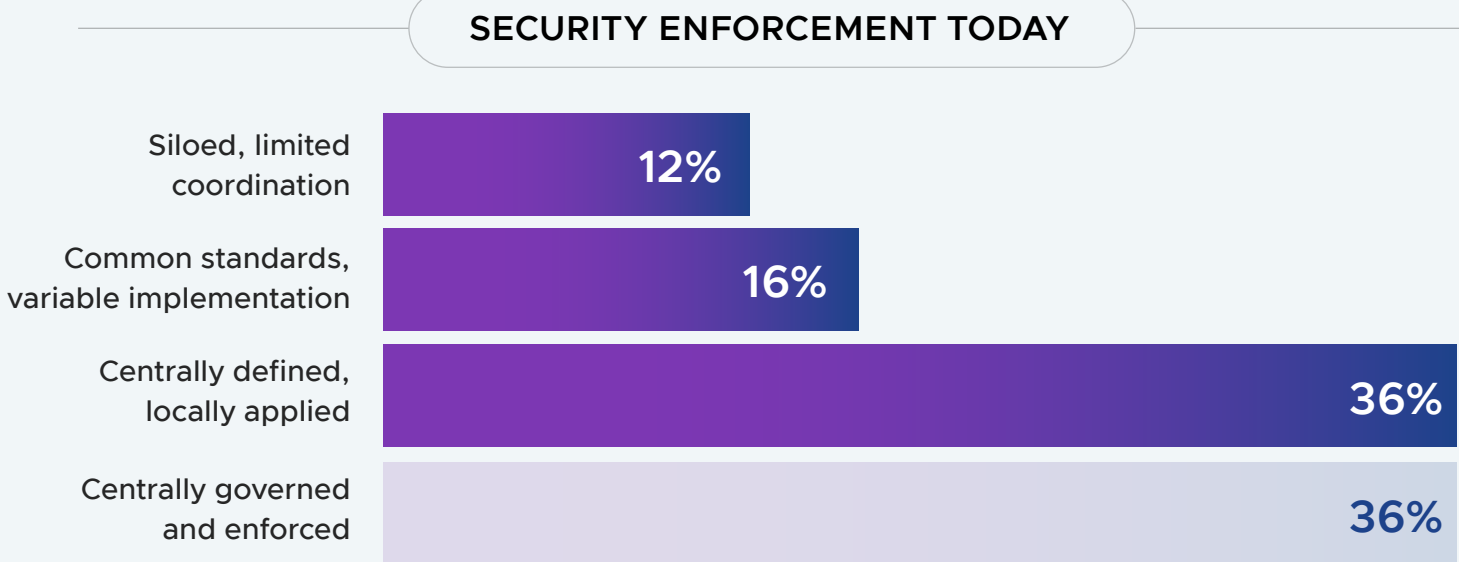
Compliance governance tells a similar story; **56% of enterprises lack centrally managed compliance that is audit-ready.**

- Twenty-eight percent have documented compliance policies that are inconsistently enforced.
- Nineteen percent have standardized but largely manual compliance processes.
- Nine percent of organizations have individual teams react to issues as they pop up.

Relying on manual or localized governance in a world where threats move at machine speed poses an operational liability. Attackers using AI can identify, exploit, and propagate a breach faster than a human-led security process can detect it. A governance model built for yesterday's threat velocity won't hold at today's pace.



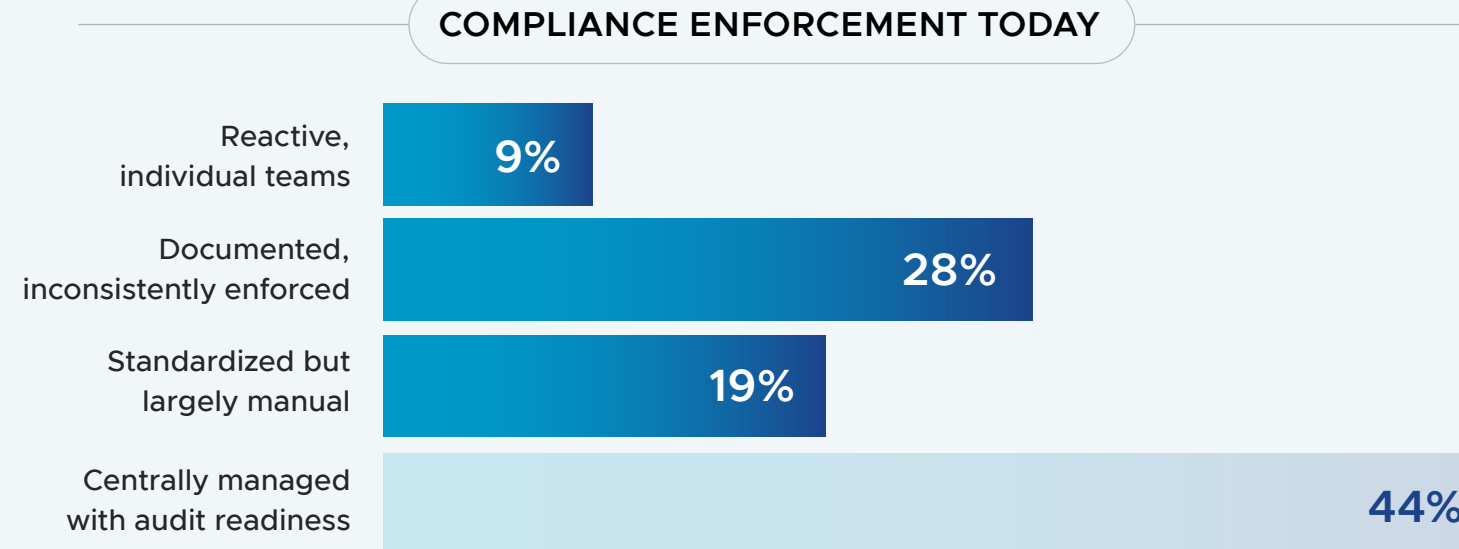
64% of organizations have not reached full security enforcement automation



Q: How security is managed across your organization's cloud environments today; n=1800



56% of enterprises lack centrally managed compliance with audit readiness



Q: How compliance requirements are managed across your organization's cloud environments; n=1800

As AI workloads scale and threat velocity increases, organizations are accepting structural exposure.



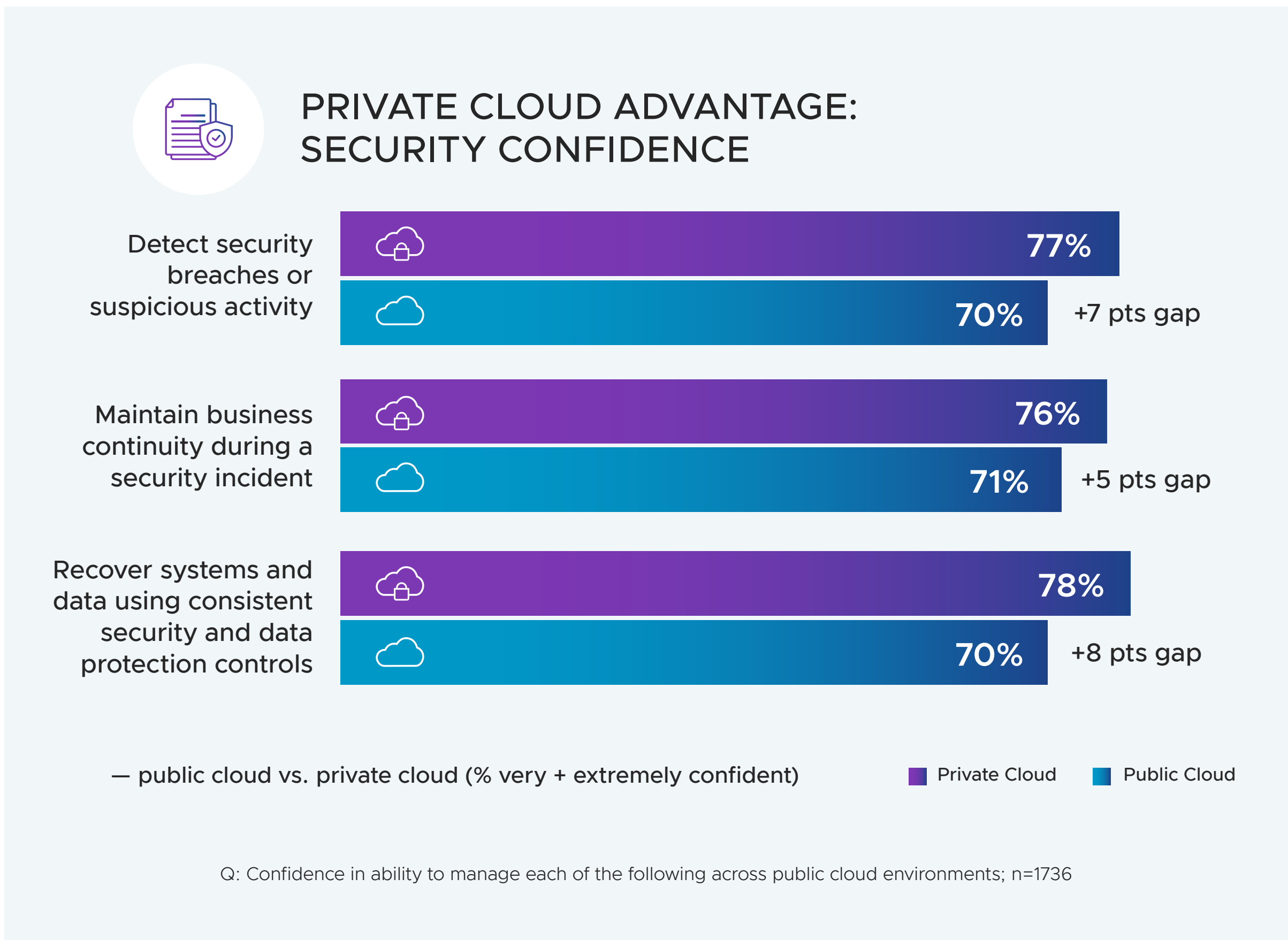
Private Cloud Is the High-Confidence Answer to Security Challenges

When you look at the gap between the rising threat level and lagging governance models, the next step for enterprise security is clear. Organizations need an environment where they have total control over their data and security policies.

When we asked 1,800 IT leaders how confident they are in specific security capabilities across their public and private cloud environments, private cloud won on every single dimension.

- **Breach detection:** 77% of leaders are very or extremely confident in their private cloud capabilities, compared to 70% in public cloud.
- **Business continuity during a security incident:** 76% are highly confident in their private cloud’s ability to keep the business running, compared to 71% in public cloud.
- **System recovery with consistent security and data protection controls:** 78% of leaders are highly confident in their private cloud, compared to 70% in public cloud.

That eight-point gap in system recovery is a crucial number. In a ransomware attack or a major breach, your recovery speed and consistency determine whether the business survives. Private cloud confidence leads by its widest margin precisely on that capability.



Confidence in your security environment is a business continuity question. As attack velocity increases, the gap between a high-confidence and a lower-confidence environment widens. Organizations running critical or AI-sensitive workloads in a lower-confidence environment are accepting avoidable risks.

Growing trust in private cloud

Enterprises show a striking level of confidence in this architecture: 93% trust their private cloud for security and compliance. In fact, when asked to name the single greatest advantage of private cloud over public cloud, security and compliance came out on top globally at 25% and ranked ahead of cost predictability, performance, and even full infrastructure control (22%).

That level of trust has a direct impact on how workloads get placed. More than half of enterprises (51%) prefer private cloud for workloads with strict security or compliance needs, versus just 27% who favor public cloud—a two-to-one preference. Security and compliance also dominate platform buying decisions: 83% of leaders rate it as highly important when evaluating private cloud platforms, with 45% calling it extremely important. No other selection factor comes close.

Today, 54% of enterprises report that data sovereignty and residency requirements are already actively shaping their IT decisions. The demand is here now.

Ultimately, a secure architecture is just a starting point. High confidence in private cloud infrastructure only translates to actual security when your operational model matches your platform’s capabilities. Achieving this alignment depends on specific, coordinated actions across three key leadership roles.

WHY PRIVATE CLOUD WINS ON SECURITY

#1

Advantage of Private Cloud: Security and Compliance

Enterprises name security and compliance capabilities as private cloud’s **single greatest advantage** over public cloud

Q: Single greatest advantage of private cloud compared to public cloud; n=1800



Q: How much do you agree with each of the following statements about private cloud; n=1800

Recommendations for IT Leaders

We have looked at the mounting external pressures, the internal governance gap, and why private cloud is the high-confidence choice for enterprise security. Now, the question is how to translate these insights into a practical plan.

Securing an AI-driven enterprise cannot be a siloed effort. It requires coordinated action across three leadership roles: CIOs, Infrastructure VPs, and Platform Engineering Leaders.

For CIOs:

Align your security governance model to AI threat velocity.



Ensure your teams can enable proactive security and are ready for the security operations changes that will be impacted by Frontier AI. Only 36% of enterprises have reached fully automated security enforcement. If your organization is not in that group, closing this gap must be a top priority with a defined timeline. Audit where your high-risk workloads are currently running. If sensitive data or AI models live in environments where your teams have lower security confidence, that's a placement decision that needs to be revisited.

For Infrastructure VPs:

Automate enforcement before AI workloads overwhelm manual processes.



It's time to move from "centrally defined" security to "centrally enforced" security. Right now, 36% of enterprises have centrally defined standards but still rely on local teams to manually apply them. At the speed of AI-driven threats, that lag between policy and enforcement is where breaches happen. Build and test detection, continuity, and recovery capabilities across every environment where critical workloads run. The system-recovery confidence gap between private and public cloud is an operational exposure you can address today.

For Platform Engineering Leaders:

Shift security down into the platform.



More than a third of enterprises (36%) cite security controls and risk management as a top new IT requirement for AI. Instead of expecting every application developer to be a security expert, your team should build security directly into the platform itself. Shift-down security helps catch the vulnerabilities that shift-left security often misses. Security is embedded into the platform and runtime layers themselves. By using automated guardrails, pre-approved service catalogs, and consistent policy templates, you can extend robust protection to every app team automatically.

Take the Next Step: Align Infrastructure to the Threat

VMware Cloud Foundation delivers automated, policy-based guardrails for security and compliance, unified security management across VMs, containers, and AI workloads, and sovereign deployment capabilities for environments with strict data-residency requirements.

If you haven't yet reviewed your upgrade readiness, schedule time with your Broadcom account team. Infrastructure decisions made in the next twelve months will define your security posture for the next three years.

The data shows where leading enterprises are already moving. The question is whether your organization is moving with them.



