+44 345 094 0945
www.waterstons.com

Article

Mar 2026

The rise of shadow cloud and shadow AI: growing data exposure risks from unmanaged AI tools

In recent months, organisations across industries have seen a sharp increase in employees using unmanaged AI tools and unsanctioned cloud services to support day-to-day tasks. This trend, often driven by productivity pressures and a desire for rapid results, is inadvertently creating significant security, compliance, and intellectual property risks.

From uploading sensitive documents to public GenAI tools, to using unauthorised cloud applications for code review or file conversion, organisations are now facing an expanded threat surface where corporate data can be exposed without detection, logging, or control.

Shadow Cloud and GenAI: an emerging enterprise-wide risk

What's happening?

As AI-enabled tools become more accessible, staff are increasingly bringing them into their workflow without organisational approval. Examples observed across multiple client environments include:

- Uploading internal code snippets to personal AI assistants for debugging or optimisation
- Submitting business reports, metrics, or client data to public AI platforms for rewriting or summarisation
- Using unknown cloud applications for PDF-to-DOCX or image conversions
- Using browser-based AI plugins with unrestricted access to corporate content.

While this saves time, it bypasses organisational governance, security monitoring, data classification, and regulatory controls.

Why this matters

Unvetted AI and cloud services pose several material risks:

1. Data exposure and loss of intellectual property

Public AI tools may retain or learn from uploaded content. Once submitted, organisations often lose control of where data is stored, how long it persists, or how it may be used in future.

2. Loss of visibility and monitoring

Security teams cannot protect what they cannot see. Unmanaged AI usage creates Shadow IT and Shadow AI services that operate outside the organisation's control, preventing effective risk assessment or response.

3. Compliance, contractual, and regulatory breaches

Uploading personal data, client information, or restricted documents to public AI tools may violate GDPR, contractual obligations, or sector-specific regulations.

4. Supply chain and third-party risk

Unauthorised use of consumer-grade AI tools introduces unknown third-party dependencies, limited SLAs, unclear security commitments, and limited recourse in the event of a breach.

A shift in attacker tactics

Threat actors increasingly target exposed data in cloud applications, misconfigured AI integrations, or poorly understood API connections. When employees use unsanctioned tools, organisations lose the ability to:

- Identify anomalies
- Detect suspicious data movement
- Enforce DLP policies
- Validate identity or access controls.

This creates blind spots that attackers can exploit with ease.

The growing need for AI and cloud governance

Mitigating Shadow Cloud and Shadow AI requires organisations to move beyond reactive controls and establish a clear governance framework combining visibility, technical guardrails, and staff enablement.

Tools such as Netskope and other CASB/SASE platforms now play a critical role in providing:

- Full visibility of cloud and AI usage
- Risk scoring for applications
- Granular policy enforcement
- Real-time data loss prevention
- Controls for GenAI access and safe use.

The objective is not to block innovation, but to enable safe, governed access that protects the organisation while supporting productivity.

Organisations should:

- **Establish visibility into cloud and AI usage.** Implement cloud security platforms (CASB/SSE/SASE) to identify which AI and cloud applications employees are using, what data is being transferred, and from where.
- **Implement policy-based access controls for AI applications.** Define approved AI tools, restrict high-risk services, and create tiered access based on data sensitivity.
- **Deploy enterprise-grade data loss prevention (DLP) controls.** Prevent sensitive data including source code, financial information, and client data from being uploaded to unmanaged services.
- **Develop and communicate a formal AI use policy.** Provide clear guidance to employees on which tools are allowed, what data can be shared, and how to use AI safely and responsibly.
- **Introduce secure, sanctioned AI alternatives.** Offer approved GenAI tools integrated into existing security governance, reducing the incentive to use personal or public services.
- **Strengthen user awareness and training.** Educate staff on the risks of data exposure, privacy concerns, and the importance of using sanctioned solutions.
- **Regularly review third-party AI services.** Assess security posture, data handling practices, retention policies, and compliance alignment before enabling access.
- **Monitor and audit AI-related data flows.** Continuously review logs and alerts to detect unusual interactions, large data transfers, or atypical user behaviour.