ARCTIQ + SentinelOne

Secure AI Adoption with Prompt Security

AI adoption is accelerating to boost productivity and developer empowerment. However, rapid deployment often outpaces security, exposing organizations to sensitive data leaks, Shadow AI, and emerging threats like prompt injection.

Arctiq partners with SentinelOne to bridge this gap. By leveraging Prompt Security, we provide the visibility, governance, and real-time protection needed to safely operationalize AI across the enterprise.

Introducing the Shadow AI Assessment

Arctiq offers a free 14-day assessment powered by Prompt Security from SentinelOne to identify unsanctioned tools and sensitive data risks. This evaluation provides the visibility needed to enable safe, governed AI adoption without disrupting employee workflows.

Accelerated Discovery:
A two-week timeline to uncover unsanctioned or abusive AI usage.

Frictionless Setup:
30-minute configuration with silent deployment via browser extension.

Monitor-Only Detection:
Identify sensitive data leakage and unapproved tools in real time.

Strategic Readout:
A 45-minute formal review of usage patterns, identified risks, and a roadmap for AI governance.

ARCTIQ

The Arctiq + SentinelOne Solution

Following the Shadow AI Assessment, Arctiq helps organizations implement governance and security controls for AI using Prompt Security from SentinelOne.

Real-Time AI Visibility
Discover sanctioned GenAI tools and unsanctioned Shadow AI usage across the organization. Monitor prompts, responses, and shared data to give security teams clear visibility into how AI is used across employees, developers, and business units.

Policy-Based AI Controls
Apply guardrails that protect sensitive information while enabling productivity. Capabilities such as data redaction, tokenization, and prompt filtering help prevent confidential information from being shared with public AI tools.

AI Attack and Runtime Protection
Inspect AI interactions in real time to detect and stop prompt injection attempts, jailbreak attacks, malicious output manipulation, and prompt leaks, helping reduce exposure to emerging AI threats.

Model-Agnostic AI Security
Secure AI environments across major LLM providers including OpenAI, Anthropic, Google models, and self-hosted or on-premise deployments. This allows organizations to maintain consistent governance as their AI ecosystem grows.

MCP Gateway Security
Protect AI applications and integrations by intercepting prompts, responses, and calls between AI systems and Model Context Protocol servers. Dynamic risk scoring enables organizations to allow, block, filter, or redact interactions while maintaining productivity.

Why Arctiq

Arctiq provides expertise across the full data and AI lifecycle, helping organizations move from experimentation to secure, production-ready AI environments.

Our capabilities include:

- AI adoption strategy and governance frameworks
- Data engineering and AI enablement
- Shadow AI discovery and risk assessment
- AI runtime security implementation
- Integration with existing security operations platforms

By combining strategic advisory with Prompt Security from SentinelOne, Arctiq helps organizations adopt AI securely while enabling innovation and operational efficiency.

Ready to secure AI across your organization?

▶ Contact us to begin your Shadow AI Assessment.

Book a Consultation