



Strengthening Security Operations with Responsible AI

Ontinue uses and develops agentic artificial intelligence (as well as other types of AI, machine learning, and automation) (collectively, “**AI Technology**”) to deliver managed Security Operations with the speed and quality required to alleviate burden on in-house security teams defending their organizations from today’s threat landscape. This Ontinue Responsible AI Policy applies to Ontinue’s use and development of AI Technology provided within Ontinue’s Services. This policy supplements Ontinue’s Multi-Services Agreement, available at www.ontinue.com/msa (the “**Agreement**”). Capitalized terms in this Policy shall have the same meaning as the capitalized terms in the Agreement.

AI Functions Improve Security Incident Analysis

Ontinue applies AI capabilities as part of its Services to analyze security incidents and distinguish benign events from genuine threats. Ontinue uses AI Technology to develop frameworks, data pipelines, and prompt logic. AI Technology operates entirely within the Ontinue tenant. Customer Data is only used to enhance the accuracy of incident analysis in the ION SecOps Platform and is never used to train third party AI models or to improve general third party AI capabilities.

Strong Controls Protect Customer Data

Ontinue enforces strict technical and organizational safeguards to prevent unauthorized access or misuse of Customer Data. Conditional access policies, remote working controls, and regular security audits ensure that only compliant, secure devices can access Customer Data. These controls maintain a high level of protection across all operational environments.

Additionally, Ontinue ensures that third party AI Technology does not store Customer Data. All processing occurs entirely within the Ontinue tenant, minimizing exposure to external systems or third parties. As Customer Data is not stored by third party AI Technology, upon termination or expiration of a Customer’s agreement to receive the Services, all Customer Data is handled in accordance with Ontinue’s data retention policies.

AI Systems Provide Full Auditability

Ontinue designs its AI systems to be transparent and auditable, so that every AI assisted decision can be traced, reviewed, and audited. The Ontinue ION SecOps Platform displays the tools, checks, and parameters used during analysis and provides natural-language explanations of reasoning steps, including references to supporting evidence. This ensures traceability and accountability for every AI-assisted conclusion.

Feedback Mechanisms Continuously Improve AI Accuracy

Ontinue Cyber Defenders can report AI Technology errors or inaccuracies directly within their operational workflows. Outputs from AI Technology are continuously monitored for drift, quality issues, and erroneous behavior. This is achieved through extensive audit logging, automated alerting, and analytical dashboards at the ION SecOps Platform level, using state of the art frameworks. The Ontinue AI engineering team reviews feedback from the Cyber Defenders and customers, and regularly incorporates it into continuous improvement processes, ensuring that the analysis supported by AI Technology remains accurate and reliable.

AI Monitoring Detects Issues Early

Ontinue uses a sophisticated evaluation framework to detect deviations, bias, or security issues in outputs of AI Technology. Every incident escalated to the Cyber Defense Center is also reviewed by a human Cyber Defender, ensuring consistent human oversight and reducing the risk of undetected anomalies.

AI Systems Align To Regulatory and Industry Standards

Ontinue aligns its AI practices with the EU AI Act and ISO 42001, ensuring strong governance, transparency, data protection, and continuous risk management. This compliance framework ensures responsible, secure, and well-regulated AI capabilities for all customers.

AI Systems Operate in Secure Azure Regions

Ontinue operates its systems using AI Technology in Europe. In exceptional scenarios such as disaster recovery, operations may temporarily shift to another GDPR-compliant region. Regardless of where Ontinue's tenant infrastructure is located, Ontinue develops and/or maintains the AI Technology within the Ontinue tenant.

Interfaces and APIs Are Protected Against Unauthorized Access

Ontinue protects all interfaces and APIs through secured access mechanisms and compliant devices. Regular audits and certifications reinforce the security of these integration points and ensure that only authorized systems can interact with Ontinue's AI Technology.

AI Components Undergo Regular Security Assessments

Ontinue conducts regular security audits of its AI Technology. **Ontinue maintains certifications such as ISO 27001, ISO 27018, and SOC 1 Type II,** ensuring that security standards are consistently upheld across Ontinue's entire ecosystem.